CySA+ Final Review part 2

53. Netstat -aon

Question #53 *Topic 1*

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command netstat -aon from the command line and receives the following output:

LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

A. Line 1

B. Line 2

C. Line 3

D. Line 4

E. Line 5

F. Line 6

Correct Answer: *D*

55. Enforce unique session IDs

Question #55 *Topic 1*

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.
Which of the following will remediate this software vulnerability?

A. Enforce unique session IDs for the application.

B. Deploy a WAF in front of the web application.

C. Check for and enforce the proper domain for the redirect.

D. Use a parameterized query to check the credentials.

E. Implement email filtering with anti-phishing protection.

Correct Answer: *A*

Preventing Unvalidated Redirects and Forwards

Safe use of redirects and forwards can be done in a number of ways:

- Simply avoid using redirects and forwards.
- If used, do not allow the URL as user input for the destination.
- Where possible, have the user provide short name, ID or token which is mapped server-side to a full target URL.
  - This provides the highest degree of protection against the attack tampering with the URL.
  - Be careful that this doesn't introduce an enumeration vulnerability where a user could cycle through IDs to find all possible redirect targets
- If user input can't be avoided, ensure that the supplied **value** is valid, appropriate for the application, and is **authorized** for the user.
- Sanitize input by creating a list of trusted URLs (lists of hosts or a regex).
  - This should be based on an allow-list approach, rather than a block list.
- Force all redirects to first go through a page notifying users that they are going off of your site, with the destination clearly displayed, and have them click a link to confirm.

https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

56. NDA

Question #56 *Topic 1*

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities.
Which of the following would be BEST to implement to alleviate the CISO's concern?

A. DLP

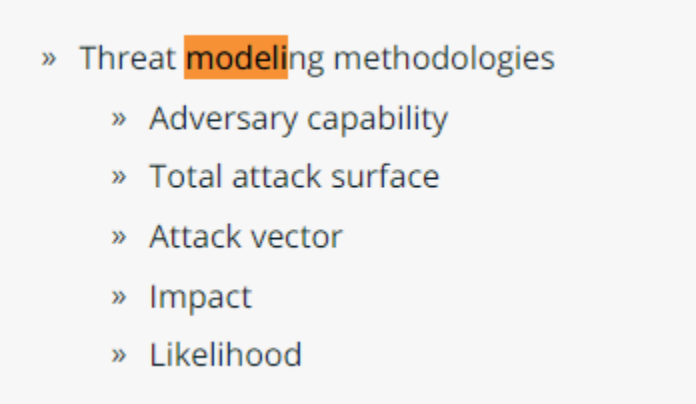
B. Encryption

C. Test data

D. NDA

Correct Answer: *A*
Reference:
https://quizlet.com/242556910/flashcards

57. Threat modeling methodologies



Question #57 *Topic 1*

A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.
Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

A. Attack vectors
B. Adversary capability
C. Diamond Model of Intrusion Analysis
D. Kill chain
E. Total attack surface

Correct Answer: *B*
Reference:
https://www.secureworks.com/blog/advanced-persistent-threats-apt-b

58. False negative?

Question #58 *Topic 1*

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

```
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct
version 3.5.71. It may no longer be supported.
The engine version is out of date. The oldest supported version
from the vendor is 4.2.11.
```

The analyst uses the vendor's website to confirm the oldest supported version is correct.
Which of the following BEST describes the situation?

A. This is a false positive, and the scanning plugin needs to be updated by the vendor.

B. This is a true negative, and the new computers have the correct version of the software.

C. This is a true positive, and the new computers were imaged with an old version of the software.

D. This is a false negative, and the new computers need to be updated by the desktop team.

Correct Answer: *D*

Explanation

The type of error that occurred is a false negative. The vulnerability scan indicated no vulnerabilities existed when, in fact, one was present.

A true negative is when a vulnerability scan reports no issues and no issues exist. A true positive is when a vulnerability scan reports a vulnerability that does exist. A false positive is when a vulnerability scan reports a vulnerability that does not exist.

Security analysts should analyze reports from a vulnerability scan. This involves reviewing and interpreting scan results. As a result, security analysts need to identify false positives, identify exceptions, and prioritize response actions.

60. Insecure APIs

Question #60 *Topic 1*

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser.
The product manager suggests using a PaaS provider to host the application.
Which of the following is a security concern when using a PaaS solution?

A. The use of infrastructure-as-code capabilities leads to an increased attack surface.

B. Patching the underlying application server becomes the responsibility of the client.

C. The application is unable to use encryption at the database level.

D. Insecure application programming interfaces can lead to data compromise.

Correct Answer: *B*

Q61

Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:

```
POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body>
<GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.or
g/2001/XMLSchema-instance"></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22

POST /services/v1_0/Public/Members.svc/soap <<a:Password>Password123
</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/>
<a:Username>somebody@companyname.com</a:Username></request></Login>
</s:Body></s:Envelope> 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89

POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body>
<GetIPLocation+xmlns="http://tempuri.org/"> <a:IPAddress>516.7.446.605
</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation>
</s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22

POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body>
<IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+x
mlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken>
<a:ImpersonateUserId>0</a:ImpersonateUserId><a:LocationId>161222
</a:LocationId> <a:NetworkId>4</a:NetworkId><a:ProviderId>''1=1
</a:ProviderId><a:UserId>13026046</a:UserId></a:Authentication>
</request></IsLoggedIn></s:Body></s:Envelope> 192.168.5.66 - -
api.somesite.com 200 0 1378 1209 48 192.168.4.89
```

Which of the following MOST likely explains how the clients' accounts were compromised?

A. The clients' authentication tokens were impersonated and replayed.

B. The clients' usernames and passwords were transmitted in cleartext.

C. An XSS scripting attack was carried out on the server.

D. A SQL injection attack was carried out on the server.

Correct Answer: *A*

Q62

Question #62 *Topic 1*

A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.
Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.

B. Remove the servers reported to have high and medium vulnerabilities.

C. Tag the computers with critical findings as a business risk acceptance.

D. Manually patch the computers on the network, as recommended on the CVE website.

E. Harden the hosts on the network, as recommended by the NIST framework.

F. Resolve the monthly job issues and test them before applying them to the production network.

Correct Answer: *AB*

63. Deidentification

Question #63 *Topic 1*

A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.
Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

A. Deidentification

B. Encoding

C. Encryption

D. Watermarking

Correct Answer: *C*

8. C. This is an example of data masking, removing enough digits from sensitive information to render it non-sensitive. Tokenization would replace the existing number with an unrelated number. Purging would remove the data completely. The data is not deidentified because the customer's name appears on the receipt.

Data Minimization

If we can't completely remove data from a dataset, we can often transform it into a format where the original sensitive information is deidentified. The *deidentification* process removes the ability to link data back to an individual, reducing its sensitivity.

An alternative to deidentifying data is transforming it into a format where the original information can't be retrieved. This is a process called *data obfuscation* and we have several tools at our disposal to assist with it:

- *Hashing* uses a hash function to transform a value in our dataset to a corresponding hash value. If we apply a strong hash function to a data element, we may replace the value in our file with the hashed value.
- *Tokenization* replaces sensitive values with a unique identifier using a lookup table. For example, we might replace a widely known value, such as a student ID, with a randomly generated 10-digit number. We'd then maintain a lookup table that allows us to convert those back to student IDs if we need to determine someone's identity. Of course, if you use this approach, you need to keep the lookup table secure!
- *Masking* partially redacts sensitive information by replacing some or all of sensitive fields with blank characters. For example, we might replace all but the last four digits of a credit card number with X's or *'s to render the card number unreadable.

Q64 Containment

Question #64

A network attack that is exploiting a vulnerability in the SNMP is detected.
Which of the following should the cybersecurity analyst do FIRST?

A. Apply the required patches to remediate the vulnerability.

B. Escalate the incident to senior management for guidance.

C. Disable all privileged user accounts on the network.

D. Temporarily block the attacking IP address.

Correct Answer: *A*
Reference:
https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-protocol-version-detection.html

Obi_Wan_Jacoby Highly Voted 1 year, 4 months ago
I also am going with D. The reason is that D seems to be part of the "Containment" phase of the Incident Response Process, whereas Answer A is for sure part of the "Eradication/Recovery" phase (Recovery) as patching systems is mentioned at the end of that phase.
upvoted 25 times

Q65. One VPC

Question #65 *Topic 1*

An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented.
Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?

A. Create three separate cloud accounts for each environment. Configure account peering and security rules to allow access to and from each environment.

B. Create one cloud account with one VPC for all environments. Purchase a virtual firewall and create granular security rules.

C. Create one cloud account and three separate VPCs for each environment. Create security rules to allow access to and from each environment.

D. Create three separate cloud accounts for each environment and a single core account for network services. Route all traffic through the core account.

Correct Answer: *C*

Q67

Question #67 *Topic 1*

A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.
Which of the following commands would MOST likely indicate if the email is malicious?

A. sha256sum ~/Desktop/file.pdf

B. file ~/Desktop/file.pdf

C. strings ~/Desktop/file.pdf | grep "<script"

D. cat < ~/Desktop/file.pdf | grep -i .exe

Correct Answer: *A*

Q68. Air Gap

Question #68 *Topic 1*

A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet.
Which of the following solutions would meet this requirement?

A. Establish a hosted SSO.

B. Implement a CASB.

C. Virtualize the server.

D. Air gap the server.

Correct Answer: *A*

When a system is physically isolated, we say that there is an air gap between it and the other systems. Air gaps are not totally secure, however. As was proved by the Stuxnet attack, corrupted USB drives can be used to "jump" the air gap.

A sheep dip computer is a system that has been isolated from the other systems and is used for analyzing suspect files and messages for malware. It may be isolated using an air gap, but is not the air gap itself.

A virtual LAN is a logical Layer 2 segmentation technique used on switches. It does not create an air gap, because systems are still physically connected.

A demilitarized zone (DMZ) is a section of the network separated from the internal network logically where resources are place that can be accessed from the Internet. A DMZ does not create an air gap since systems are still physically connected.

60. Simulation

SIMULATION -

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

λ€¢ TLS 1.2 is the only version of TLS running.

λ€¢ Apache 2.4.18 or greater should be used.

λ€¢ Only default ports should be used.

INSTRUCTIONS -

Using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Part 1

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Part 1

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8675/ssh open   ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Part 2

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Correct Answer: *Part 1 Answer:*
Check on the following:

AppServ1 is only using TLS.1.2 -

AppServ4 is only using TLS.1.2 -
AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater
Part 2 answer:
Recommendation:
Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

70 Stealth Command

When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

A. nmap â€"sA â€"O <system> -noping

B. nmap â€"sT â€"O <system> -P0

C. nmap â€"sS â€"O <system> -P0

D. nmap â€"sQ â€"O <system> -P0

Correct Answer: *C*

Reference:

https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

Stealth scan

Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.

```
> nmap -sS scanme.nmap.org
```

You can use the '**-sS**' command to perform a stealth scan. Remember, stealth scanning is slower and not as aggressive as the other types of scanning, so you might have to wait a while to get a response.

71. Detection phase

Question #71 *Topic 1*

A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.

B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.

C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.

D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Correct Answer: *D*

References

CySA+ Objectives