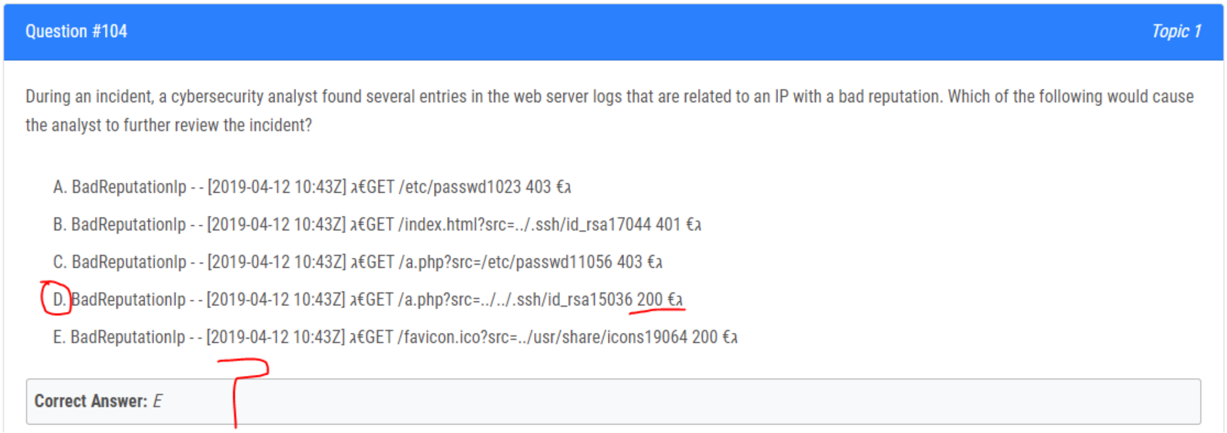
CySA+ Final Review part 4

104. BadReputationIP



Question #104 *Topic 1*

During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation. Which of the following would cause the analyst to further review the incident?

A. BadReputationIp - - [2019-04-12 10:43Z] ג€GET /etc/passwd1023 403 €ג

B. BadReputationIp - - [2019-04-12 10:43Z] ג€GET /index.html?src=../.ssh/id_rsa17044 401 €ג

C. BadReputationIp - - [2019-04-12 10:43Z] ג€GET /a.php?src=/etc/passwd11056 403 €ג

[✓ D.] BadReputationIp - - [2019-04-12 10:43Z] ג€GET /a.php?src=../../.ssh/id_rsa15036 200 €ג

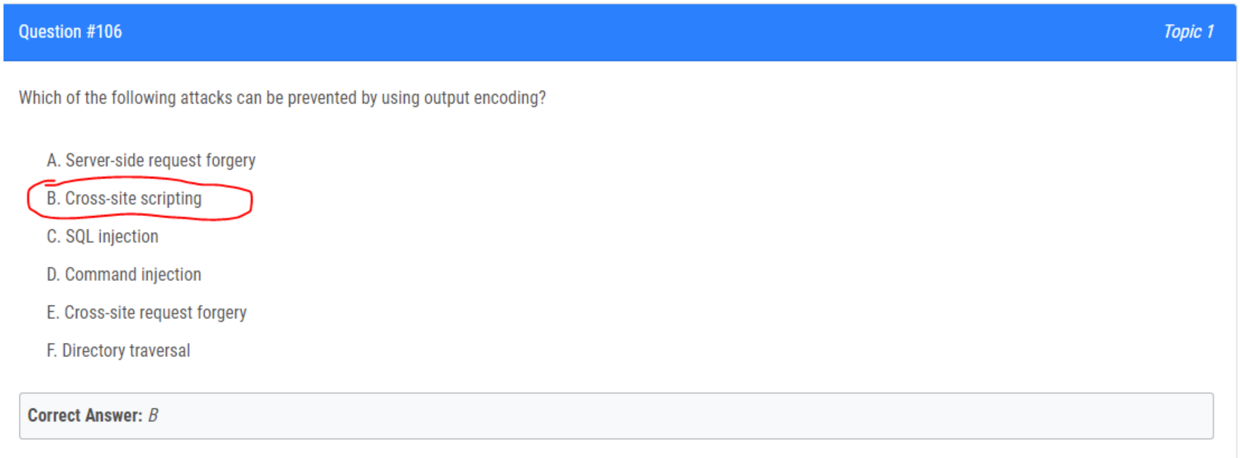
E. BadReputationIp - - [2019-04-12 10:43Z] ג€GET /favicon.ico?src=../usr/share/icons19064 200 €ג

Correct Answer: *E*

?

HTTP status codes:
403 - Forbidden.
401 - Access denied.
200 - OK. The client request has succeeded.

106. Output encoding for XSS



Question #106 *Topic 1*

Which of the following attacks can be prevented by using output encoding?

A. Server-side request forgery

[✓ B. Cross-site scripting]

C. SQL injection

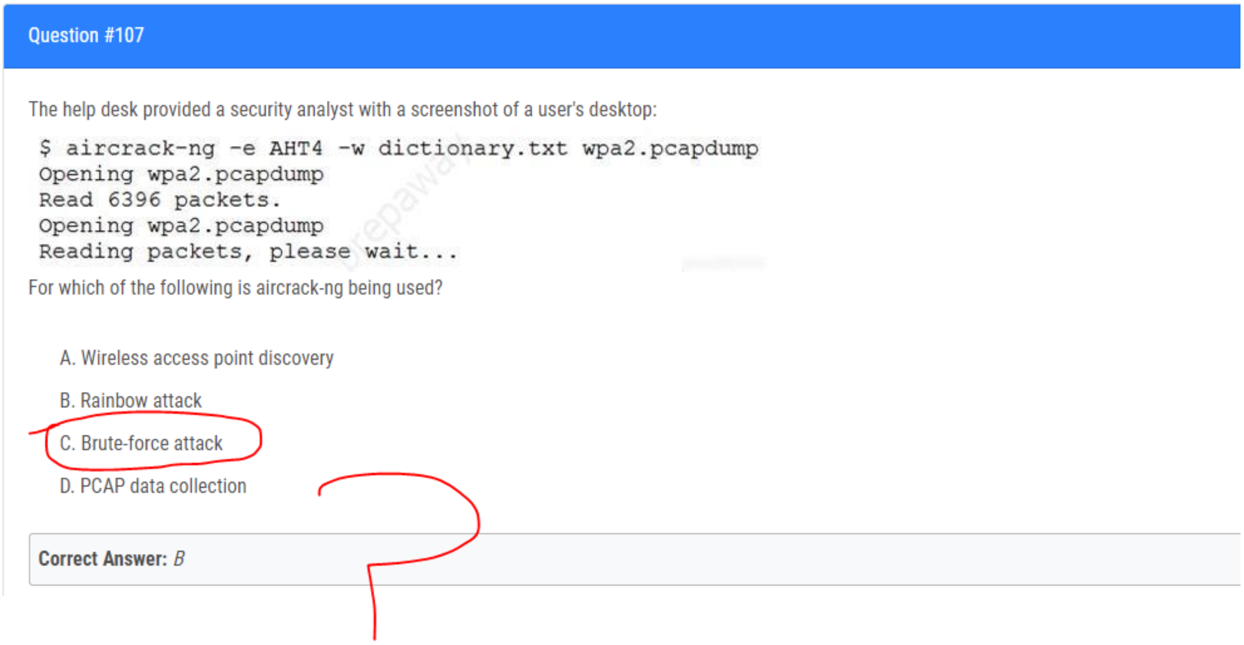
D. Command injection

E. Cross-site request forgery

F. Directory traversal

Correct Answer: *B*

107. Aircrack-ng



Question #107

The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?

A. Wireless access point discovery

B. Rainbow attack

[✓ C. Brute-force attack]

D. PCAP data collection

?

Correct Answer: *B*

Wireless Assessment Tools

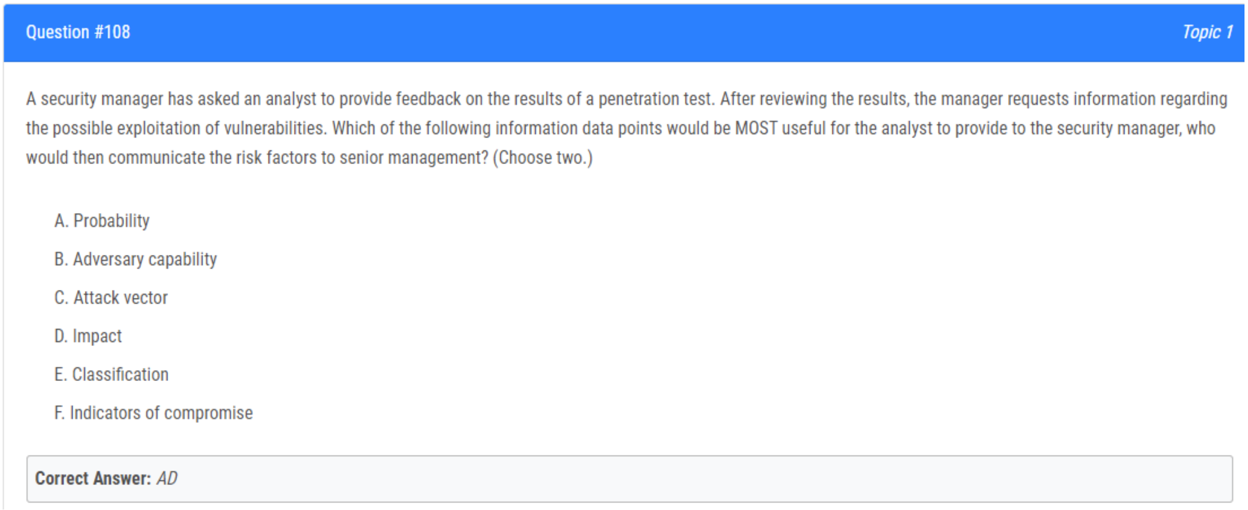
If you are tasked with performing a vulnerability assessment of a wireless network, there are three tools covered on the CySA+ exam that you might find useful. As you prepare for the exam, you should know the names and purposes of each of these tools:

- *Aircrack-ng* is a suite of tools designed for wireless network testing. The tools in this suite can capture packets from wireless networks, conduct packet injection attacks, and crack preshared keys used on WEP, WPA, and WPA2 networks.
- *Reaver* is a specialized tool used to find WPA and WPA2 passphrases specifically on networks that support the Wi-Fi Protected Setup (WPS) feature.
- *Hashcat* is a general-purpose password cracking tool that may also be used on wireless networks.

This chapter covers the following topics related to Objective 1.4 (Given a scenario, analyze the output from common vulnerability assessment tools) of the CompTIA Cybersecurity Analyst (CySA+) CS0-002 certification exam:

- **Web application scanner**: Covers the OWASP Zed Attack Proxy (ZAP), Burp Suite, Nikto, and Arachni scanners.
- **Infrastructure vulnerability scanner**: Covers the Nessus, OpenVAS, and Qualys scanners.
- **Software assessment tools and techniques**: Explains static analysis, dynamic analysis, reverse engineering, and fuzzing.
- **Enumeration**: Describes Nmap, hping, active vs. passive enumeration, and Responder.
- **Wireless assessment tools**: Covers Aircrack-ng, Reaver, and oclHashcat.
- **Cloud infrastructure assessment tools**: Covers ScoutSuite, Prowler, and Pacu.

108. Probability and Impact



Question #108 *Topic 1*

A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to senior management? (Choose two.)

A. Probability

B. Adversary capability

C. Attack vector

D. Impact

E. Classification

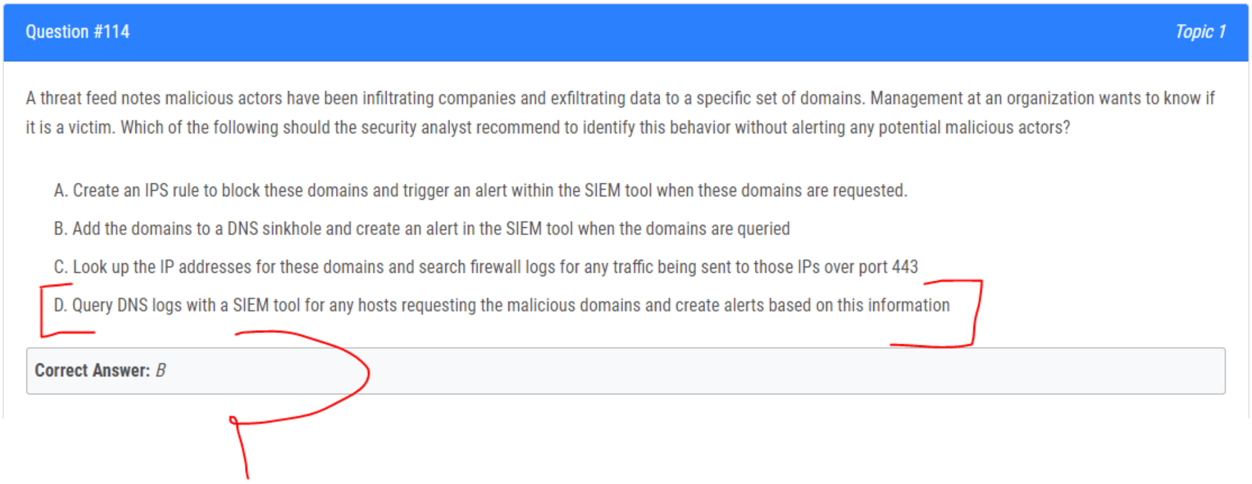
F. Indicators of compromise

Correct Answer: *AD*

Prescriptive Frameworks

Some frameworks are designed to provide organizations with a list of activities that comprise a prescription for handling certain security issues common to all. The frameworks described in this section are prescriptive.

114. Query DNS logs



Question #114 *Topic 1*

A threat feed notes malicious actors have been infiltrating companies and exfiltrating data to a specific set of domains. Management at an organization wants to know if it is a victim. Which of the following should the security analyst recommend to identify this behavior without alerting any potential malicious actors?

A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested.

B. Add the domains to a DNS sinkhole and create an alert in the SIEM tool when the domains are queried

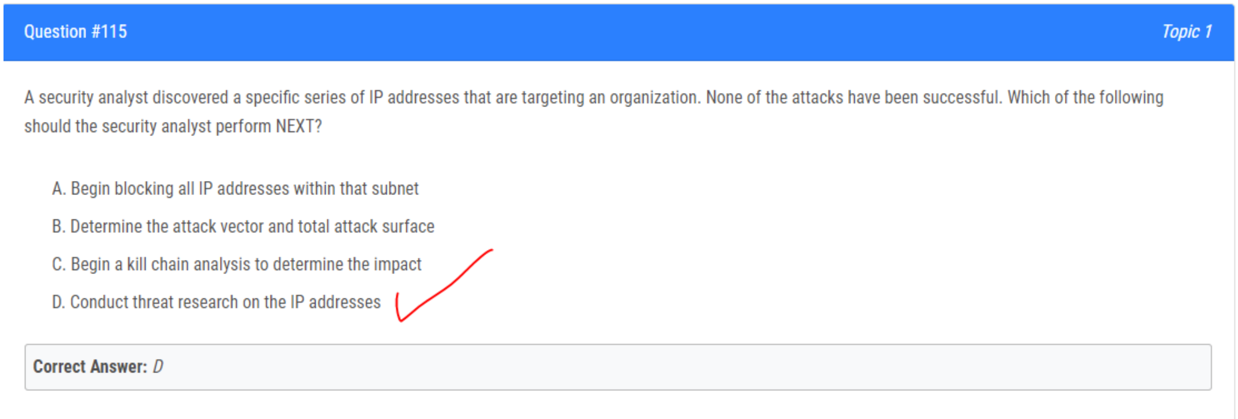
C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443

[✓ D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information]

Correct Answer: *B*

D

115. Threat Research



Question #115 *Topic 1*

A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

A. Begin blocking all IP addresses within that subnet

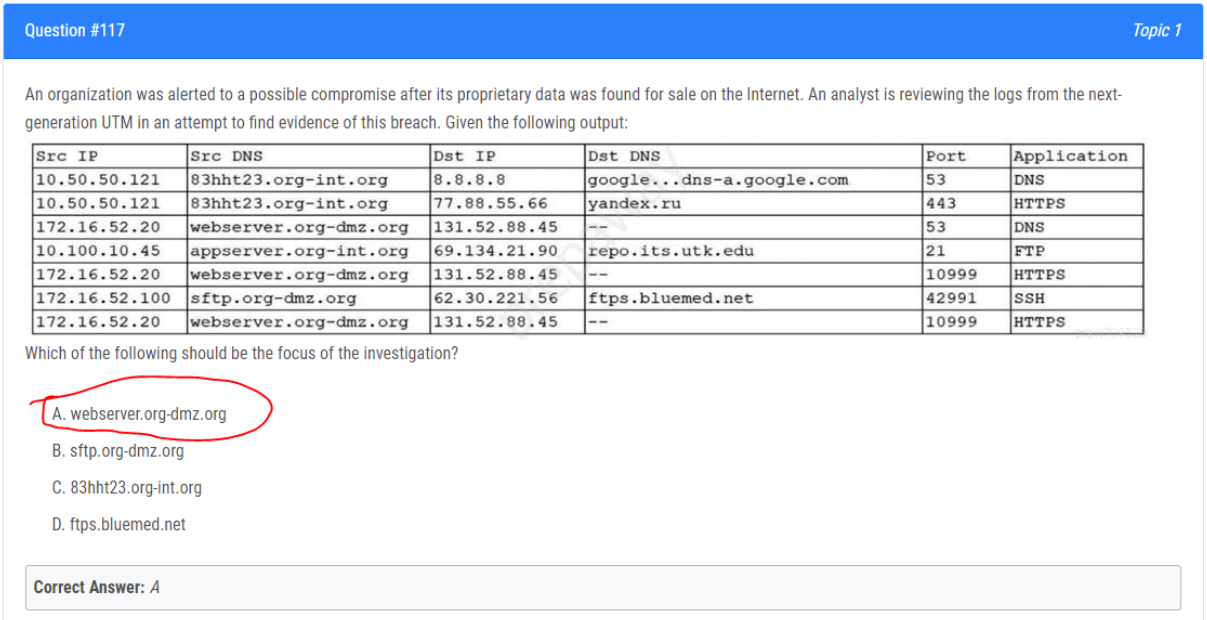
B. Determine the attack vector and total attack surface

C. Begin a kill chain analysis to determine the impact

[✓ D. Conduct threat research on the IP addresses]

Correct Answer: *D*

117. UTM Logs



Question #117 *Topic 1*

An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Src IP	Src DNS	Dst IP	Dst DNS	Port	Application
10.50.50.121	83hht23.org-int.org	8.8.8.8	google...dns-a.google.com	53	DNS
10.50.50.121	83hht23.org-int.org	77.88.55.66	yandex.ru	443	HTTPS
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	53	DNS
10.100.10.45	appserver.org-int.org	69.134.21.90	repo.its.utk.edu	21	FTP
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS
172.16.52.100	sftp.org-dmz.org	62.30.221.56	ftps.bluemed.net	42991	SSH
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS

Which of the following should be the focus of the investigation?

[✓ A. webserver.org-dmz.org]

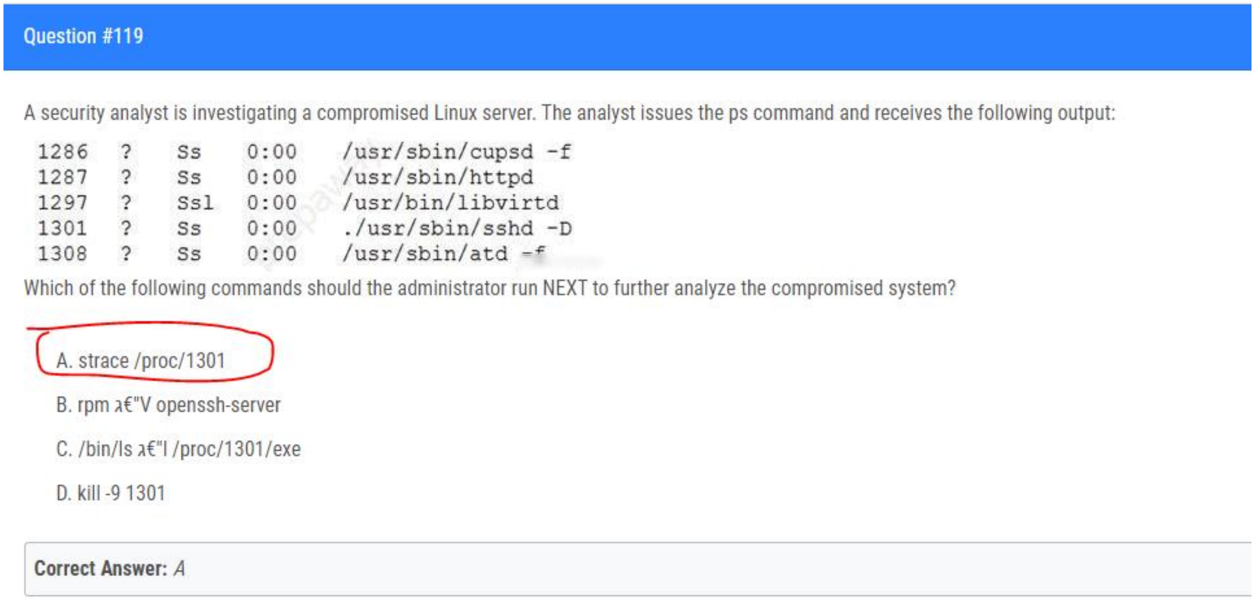
B. sftp.org-dmz.org

C. 83hht23.org-int.org

D. ftps.bluemed.net

Correct Answer: *A*

119. Strace linux command



Question #119

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:

```
1286  ?  Ss   0:00  /usr/sbin/cupsd -f
1287  ?  Ss   0:00  /usr/sbin/httpd
1297  ?  Ssl  0:00  /usr/bin/libvirtd
1301  ?  Ss   0:00  ./usr/sbin/sshd -D
1308  ?  Ss   0:00  /usr/sbin/atd -f
```

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

[✓ A. strace /proc/1301]

B. rpm ג€"V openssh-server

C. /bin/ls ג€"l /proc/1301/exe

D. kill -9 1301

Correct Answer: *A*

References

[Chapter 4 Analyzing Assessment Output | CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide, 2nd Edition (oreilly.com)]