Vendor: CertNexus

Exam Code:CFR-310

Exam Name: CyberSec First Responder

Version: Demo

QUESTION 1

An administrator believes that a system on VLAN 12 is Address Resolution Protocol (ARP) poisoning clients on the network. The administrator attaches a system to VLAN 12 and uses Wireshark to capture traffic. After reviewing the capture file, the administrator finds no evidence of ARP poisoning. Which of the following actions should the administrator take next?

A. Clear the ARP cache on their system.

B. Enable port mirroring on the switch.

C. Filter Wireshark to only show ARP traffic.

D. Configure the network adapter to promiscuous mode.

Correct Answer: D

Reference: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_arp_poisoning.htm

---

QUESTION 2

According to Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, an organization must retain logs for what length of time?

A. 3 months

B. 6 months

C. 1 year

D. 5 years

Correct Answer: C

Reference: https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

---

QUESTION 3

Which of the following is a method of reconnaissance in which a ping is sent to a target with the expectation of receiving a response?

A. Active scanning

B. Passive scanning

C. Network enumeration

D. Application enumeration

Correct Answer: C

QUESTION 4

In which of the following attack phases would an attacker use Shodan?

A. Scanning

B. Reconnaissance

C. Gaining access

D. Persistence

Correct Answer: A

Reference: https://books.google.com.pk/books?id=3bzPDwAAQBAJandpg=PA41andlpg=PA41anddq=attack+phases+would+an+attacker+use+Shodanandsource=blandots=phUbfR8BOYandsig=ACfU3U1sg5J67s_sL_Ixpr3OiqdCIraKUwandhl=enandsa=Xandved=2ahUKEwjazaKCssXpAhUC4YUKHcJ5CVwQ6AEwAXoECBMQAQ#v=onepageandq=attack%20phases%20would%20an%20attacker %20use%20Shodanandf=false

---

QUESTION 5

Which of the following are well-known methods that are used to protect evidence during the forensics process? (Choose three.)

A. Evidence bags

B. Lock box

C. Caution tape

D. Security envelope

E. Secure rooms

F. Faraday boxes

Correct Answer: ACD

QUESTION 6

Which of the following types of attackers would be MOST likely to use multiple zero-day exploits executed against high-value, well-defended targets for the purposes of espionage and sabotage?

A. Cybercriminals

B. Hacktivists

C. State-sponsored hackers

D. Cyberterrorist

Correct Answer: C

QUESTION 7

During an incident, the following actions have been taken:

-Executing the malware in a sandbox environment

-Reverse engineering the malware

-Conducting a behavior analysis

Based on the steps presented, which of the following incident handling processes has been taken?

A. Containment

B. Eradication

C. Recovery

D. Identification

Correct Answer: A

The "Containment, eradication and recovery" phase is the period in which incident response team tries to contain the incident and, if necessary, recover from it (restore any affected resources, data and/or processes).

Reference: https://blog.rapid7.com/2017/01/11/introduction-to-incident-response-life-cycle-of-nist-sp-80061/

QUESTION 8

As part of an organization\\'s regular maintenance activities, a security engineer visits the Internet Storm Center advisory page to obtain the latest list of blacklisted host/network addresses. The security engineer does this to perform which of the following activities?

A. Update the latest proxy access list

B. Monitor the organization\\'s network for suspicious traffic

C. Monitor the organization\\'s sensitive databases

D. Update access control list (ACL) rules for network devices

Correct Answer: D

QUESTION 9

A network administrator has determined that network performance has degraded due to excessive use of social media and Internet streaming services. Which of the following would be effective for limiting access to these types of services, without completely restricting access to a site?

A. Whitelisting

B. Web content filtering

C. Network segmentation

D. Blacklisting

Correct Answer: B

Reference: https://umbrella.cisco.com/solutions/web-content-filtering

---

QUESTION 10

Network infrastructure has been scanned and the identified issues have been remediated. What is the next step in the vulnerability assessment process?

A. Generating reports

B. Establishing scope

C. Conducting an audit

D. Assessing exposures

Correct Answer: C

Reference: https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPGSM01.pdf

---

QUESTION 11

Which common source of vulnerability should be addressed to BEST mitigate against URL redirection attacks?

A. Application

B. Users

C. Network infrastructure

D. Configuration files

Correct Answer: A

Reference: https://blog.qualys.com/securitylabs/2016/01/07/open-redirection-a-simple-vulnerabilitythreatens-your-web-applications

---

QUESTION 12

An unauthorized network scan may be detected by parsing network sniffer data for:

A. IP traffic from a single IP address to multiple IP addresses.

B. IP traffic from a single IP address to a single IP address.

C. IP traffic from multiple IP addresses to a single IP address.

D. IP traffic from multiple IP addresses to other networks.

Correct Answer: C