Vendor: Cisco

Exam Code:210-250

Exam Name: Cisco Cybersecurity Fundamentals

Version: Demo

QUESTION 1

What type of spoofing attack uses fake source IP addresses that are different than their real IP addresses?

A. MAC spoofing

B. IP spoofing

C. application spoofing

D. name spoofing

Correct Answer: B

QUESTION 2

Which term describes the act of a user, without authority or permission, obtaining rights on a system, beyond what were assigned?

A. authentication tunneling

B. administrative abuse

C. rights exploitation

D. privilege escalation

Correct Answer: D

QUESTION 3

Which of the following statements is not true about a daemon process?

A. A daemon is a process that runs in the background.

B. A daemon\\'s parent process is typically the init process.

C. Daemons are controlled by the active user.

D. Not all daemons are automatically started.

Correct Answer: C

QUESTION 4

Which security technology would be best for detecting a pivot attack?

A. Virtual private network (VPN)

B. Host-based antivirus

C. NetFlow solution looking for anomalies within the network

D. Application layer firewalls

Correct Answer: C

QUESTION 5

Which term represents the chronological record of how evidence was collected, analyzed, preserved, and transferred?

A. chain of evidence

B. evidence chronology

C. chain of custody

D. record of safekeeping

Correct Answer: C

QUESTION 6

Which one of the following attacks results when attackers place themselves in line between two devices that are communicating, with the intent of performing reconnaissance or manipulating the data as it moves between the devices?

A. Man-in-the-path

B. Man-in-the-middle

C. Routing protocol attacks

D. Routing injection attacks

Correct Answer: B

QUESTION 7

What two protocols are used to retrieve email? (Choose two.)

A. IMAP

B. POP

C. LDAP

D. MTA

Correct Answer: AB

QUESTION 8

What are the two best ways to protect a device from a rootkit attack? (Choose two.)

A. Do nothing, because rootkits are not common and are difficult to develop.

B. Keep current with software updates and security patches from the vendor.

C. Maintain a strong password policy.

D. Utilize anti-malware, anti-virus, and next generation firewall and IPS services within the network.

Correct Answer: BD

QUESTION 9

In addition to helping secure and control web traffic, web content security systems also provide which three security options? (Choose three.)

A. network access controls (NAC)

B. advanced malware protection (AMP)

C. remote VPN access controls

D. insightful reporting

E. secure mobility

Correct Answer: BDE

QUESTION 10

After a large influx of network traffic to externally facing devices, you begin investigating what appears to be a denial of service attack. When you review packet capture data, you notice that the traffic is a single SYN packet to each port. Which kind of attack is this?

A. SYN flood

B. port scanning

C. traffic fragmentation

D. host profiling

Correct Answer: A

QUESTION 11

What are two controls that the Cisco WSA can use to validate web requests? (Choose two.)

A. basic URL filtering that leverages pre-defined, category-based web usage controls

B. AMP for isolating reputable exploits and malware samples to its local disk for further investigation

C. a reputation database that is used to analyze web requests as part of a security control procedure

D. IPS-based signatures that are loaded in the Cisco WSA to prevent intrusions and alert system administrators

E. a reputation database within the Cisco WSA that uses Snort-like rule sets to combat RootKit intrusions

Correct Answer: AC

QUESTION 12

If a web server accepts input from the user and passes it to a bash shell, to which attack method if it vulnerable?

A. input validation

B. hash collision

C. command injection

D. integer overflow

Correct Answer: C