Eccouncil

(ECSS)

EC-Council Certified Security Specialist v9.0

Total: **50 Questions**

Link:

MYEXAM.FR

Question: 1

A security strategy in which several protection layers are placed throughout an information system helps to prevent direct attacks against an information system and data because a break in one layer only leads the attacker to the next layer. What is this security strategy called?

A. Network Security Zoning
B. Defense in Depth
C. Multi-aspect Model
D. Threat Modeling

Answer: B

Question: 2

Which of the following attack allows attackers to bypass client-ID security mechanisms and gain access privileges, and then inject malicious scripts into specific web pages?

A. Cross-Site Scripting (XSS)
B. Buffer Overflow
C. Denial-of-Service
D. Parameter/Form Tampering

Answer: A

Question: 3

The security of the network can be increased in a number of ways, for instance, by installing a special kind of web server and through packet filtering. What type of server is implemented as an intermediary server between a client and a server to act as a shield and protect and hide the computer from the outside network?

A. Application Server
B. Telnet Server
C. Web Server
D. Proxy Server

Answer: D

Question: 4

An algorithm which is a part of the U.S. government's long-term project to develop a set of standards for publicly available cryptography as authorized by the Computer Security Act of 1987 accepts a message of 264 bits in length and a 160-bit message output digest is produced to complicate text searching. Which of the following algorithms is a family of two similar hash functions, with different block sizes, and uses 32-bit words and 64-bit words?

A. SHA-2
B. SHA-0
C. SHA-1
D. SHA-3

Answer: C

Question: 5

Kelly is taking backups of the organization's data. Currently, he is taking backups of only those files which are created or modified after the last backup. What type of backup is Kelly using?

A. Differential Backup
B. Full Backup
C. Normal Backup
D. Incremental Backup

Answer: D

Question: 6

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide for the confidentiality of data on wireless networks at a level equivalent to that of the wired LANs. In a wireless LAN, the network can be accessed without physically connecting to the LAN. On what layer of the OSI model, WEP utilizes an encryption mechanism for minimizing unauthorized access on the WLAN?

A. Physical layer
B. Data link layer
C. Network layer
D. Application layer

Answer: B

Question: 7

A DoS attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. At the data link layer, DoS attacks can be done easily. DoS attacks at the application and transport layers are primarily the same, but the interaction between the network, data-link, and physical layers which increase the risk of a DoS attack on a wireless network is different. An attacker can create a device that will saturate the 802.11 frequency bands with noise. If the attacker can create enough RF noise to reduce the signal-to-noise ratio to an unusable level, then the devices within the range of the noise will be effectively taken offline to block the communication. What type of DoS attack is being discussed here?

A. Network DoS Attack
B. Application DoS Attack
C. Physical DoS Attack
D. Data-link DoS Attack

Answer: C

Question: 8

Which of the following is an intentional act of sending multiple copies of the identical content to the same recipient?

A. Mail Storm
B. Spamming
C. Mail Bombing
D. Phishing

Answer: C

Question: 9

Timothy works as a network administrator in a multinational organization. He decides to implement a dedicated network for sharing storage resources. He uses a _____ as it separates the storage units from the servers and the user network.

A. NAS
B. SAS
C. SAN
D. SCSA

Answer: C

Question: 10

Firewall protection is provided by different types of firewalls. One of the firewall types works at the session layer of the OSI model, or the TCP layer of TCP/IP, and monitors TCP handshaking between packets to determine whether a requested session is legitimate. This level hides information about the private networks they protect, but they do not filter individual packets. Identify the type of firewall described above.

A. Application-Level Firewall
B. Stateful Multilayer Inspection Firewall
C. Packet Filtering Firewall
D. Circuit-Level Gateway Firewall

Answer: D

Question: 11

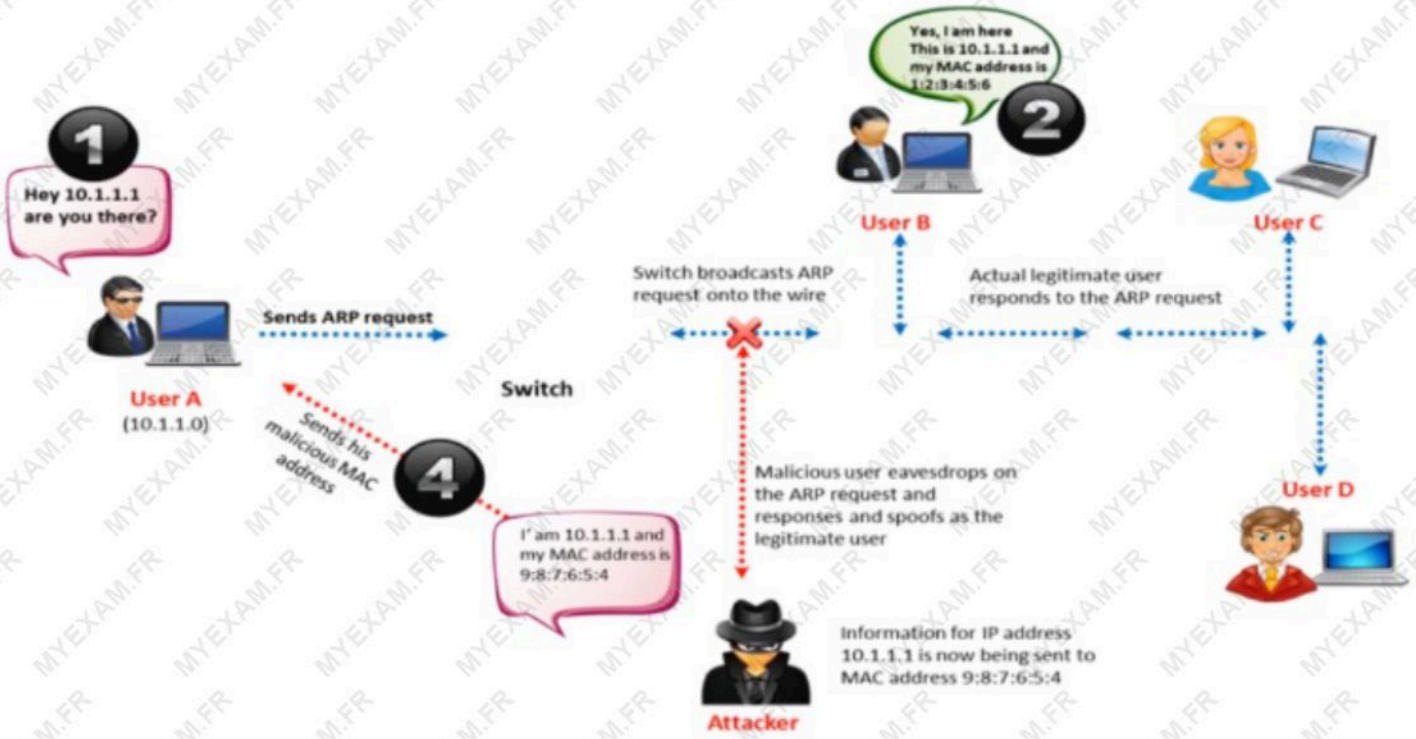
Which of the following contains extra material that is referred to in the report?

A. Appendices
B. Summary
C. Acknowledgements
D. References

Answer: A

Question: 12

ARP is Address Resolution Protocol which is used to map network layer IP addresses to data link layer MAC addresses.



Using the diagram above, choose the appropriate option that justifies ARP spoofing:

A. When a request is made for a MAC address, the user's machine replies with a fake MAC address.

B. The computer sends the data to the attacker's system rather than the original destination due to forged ARP replies.

C. The host analyzes all the requests on the network and blocks the MAC address request.

D. When an attacker requests the MAC address the Switch blocks the entire request.

Answer: B

Question: 13

Which of the following is a Linux journaling file system?

A. FAT

B. HFS

C. Ext3

D. BFS

Answer: C

Question: 14

Each firm, such as a law firm or a computer forensics firm dealing with report writing has its own established report format. An investigative report format has basically four sections. Which section of investigative report format is dedicated to the background and summary?

A. Section 1

B. Section 3

C. Section 4

D. Section 2

Answer: D

Question: 15

VPN technology is structured on the basis of tunneling. It requires the setting up and upholding of a logical network connection. The packets built in a particular VPN protocol design are put in a nutshell inside another base or carrier protocol. They are then transmitted between the VPN client and the server and deencapsulated finally on the receiving side. Which of the following statements best describes the function of voluntary tunneling?

A. Managing of connection setup is carried out by the VPN client

B. Authenticates clients and relates them with certain VPN servers using logic built into the broker's device

C. Details of the VPN server's connectivity from the VPN clients are concealed

D. VPN connection is managed between the client and a VPN server

Answer: A