Vendor:EC-COUNCIL

Exam Code:312-38

Exam Name: Certified Network Defender (CND)

Version: Demo

QUESTION 1

An IDS or IDPS can be deployed in two modes. Which deployment mode allows the IDS to both detect and stop malicious traffic?

A. passive mode

B. inline mode

C. promiscuous mode

D. firewall mode

Correct Answer: B

QUESTION 2

Which of the following is a session layer protocol?

A. RPC

B. SLP

C. RDP

D. ICMP

Correct Answer: A

QUESTION 3

Which type of firewall consists of three interfaces and allows further subdivision of the systems based on specific security objectives of the organization?

A. Screened subnet

B. Bastion host

C. Unscreened subnet

D. Multi-homed firewall

Correct Answer: D

QUESTION 4

You work for a professional computer hacking forensic investigator DataEnet Inc. To explore the e-mail information about an employee of the company. The suspect an employee to use the online e-mail systems such as Hotmail or Yahoo. Which of the following folders on the local computer you are going to check to accomplish the task? Each

correct answer represents a complete solution. Choose all that apply.

A. cookies folder

B. Temporary Internet Folder

C. download folder

D. History Folder

Correct Answer: ABD

QUESTION 5

Management asked Adam to implement a system allowing employees to use the same credentials to access multiple applications. Adam should implement the _____ authentication technique to satisfy the request.

A. Single-sign-on

B. Smart card authentication

C. Two-factor authentication

D. Biometric

Correct Answer: A

QUESTION 6

The bank where you work has 600 windows computers and 400 Red Hat computers which primarily serve as bank teller consoles. You have created a plan and deployed all the patches to the Windows computers and you are now working on updating the Red Hat computers. What command should you run on the network to update the Red Hat computers, download the security package, force the package installation, and update all currently installed packages?

A. You should run the up2data -u command.

B. You should run the up2date --d -f -u command.

C. You should run the WSUS --d -f -u command.

D. You should type the sysupdate --d command.

Correct Answer: B

QUESTION 7

Syslog and SNMP are the two main _____ protocols through which log records are transferred.

A. Pull-based

B. Push-based

C. Host-based

D. Network-based

Correct Answer: B

QUESTION 8

John works Incident Director of Tech World Inc. His job is to set up a wireless network in his organization. For this purpose, he needs to decide on appropriate equipment and policies need to set up a network. Which of the following stages of the incident handling process to help him accomplish the task?

A. Preparation

B. None

C. Recovery

D. the eradication of

E. containment

Correct Answer: A

QUESTION 9

Identify the correct statements regarding a DMZ zone:

A. It is a file integrity monitoring mechanism

B. It is a Neutral zone between a trusted network and an untrusted network

C. It serves as a proxy

D. It includes sensitive internal servers such as database servers

Correct Answer: B

QUESTION 10

Which of the following is a distributed application architecture that partitions tasks or workloads between service providers and service requesters? Each correct answer represents a complete solution. Choose all that apply.

A. Client-server computing

B. Peer-to-peer (P2P) computing

C. Client-server networking

D. Peer-to-peer networking

Correct Answer: AC

Client-server networking is also known as client-server computing. It is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and

servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client does not share any of its resources,

but requests a server\\'s content or service function. Clients therefore initiate

communication sessions with servers which await (listen to) incoming requests.

Answer options D and B are incorrect. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the

application. They are said to form a peer-to-peer network of nodes. Peer-to-peer networking (also known simply as peer networking) differs from client-server networking, where certain devices have the responsibility to provide or "serve" data,

and other devices consume or otherwise act as "clients" of those servers.

QUESTION 11

If Myron, head of network defense at Cyberdyne, wants to change the default password policy settings on the company\\'s Linux systems, which directory should he access?

A. /etc/logrotate.conf

B. /etc/hosts.allow

C. /etc/crontab

D. /etc/login.defs

Correct Answer: D

QUESTION 12

Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company\\'s network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs respond with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?

A. The type of scan she is using is called a NULL scan.

B. Cindy is attempting to find live hosts on her company\\'s network by using a XMAS scan.

C. Cindy is using a half-open scan to find live hosts on her network.

D. She is utilizing a RST scan to find live hosts that are listening on her network.

Correct Answer: C