DUMPSARENA

Certified Ethical Hacker v10 Exam

ECCouncil 312-50v10

Version Demo

Total Demo Questions: 15

Total Premium Questions: 322

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

A. DynDNS

B. DNS Scheme

C. DNSSEC

D. Split DNS

ANSWER: D

QUESTION NO: 2

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occuring during non-business hours. After further examination of all login activities, it is notices that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realized the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux serves to synchronize the time has stopped working?

A. NTP

B. TimeKeeper

C. OSPF

D. PPP

ANSWER: A

QUESTION NO: 3

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password

B. Encrypt the data on the hard drive.

C. Use a strong logon password to the operating system.

D. Back up everything on the laptop and store the backup in a safe place.

ANSWER: B

QUESTION NO: 4

What is attempting an injection attack on a web server based on responses to True/False questions called?

A. DMS-specific SQLi

B. Compound SQLi

C. Blind SQLi

D. Classic SQLi

ANSWER: C

QUESTION NO: 5

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Application Layer

B. Data tier

C. Presentation tier

D. Logic tier

ANSWER: D

QUESTION NO: 6

When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least twice a year or after any significant upgrade or modification

B. At least once a year and after any significant upgrade or modification

C. At least once every two years and after any significant upgrade or modification

D. At least once every three years or after any significant upgrade or modification

ANSWER: B

QUESTION NO: 7

Which of the following will perform an Xmas scan using NMAP?

A. nmap -sA 192.168.1.254

B. nmap -sP 192.168.1.254

C. nmap -sX 192.168.1.254

D. nmap -sV 192.168.1.254

ANSWER: C

QUESTION NO: 8

You are monitoring the network of your organizations. You notice that:

1. There are huge outbound connections from your Internal Network to External IPs

2. On further investigation, you see that the external IPs are blacklisted

3. Some connections are accepted, and some are dropped

4. You find that it is a CnC communication

Which of the following solution will you suggest?

A. Block the Blacklist IP's @ Firewall

B. Update the Latest Signatures on your IDS/IPS

C. Clean the Malware which are trying to Communicate with the External Blacklist IP's

D. Both B and C

ANSWER: D

QUESTION NO: 9

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

A. SQL injection attack

B. Cross-Site Scripting (XSS)

C. LDAP Injection attack

D. Cross-Site Request Forgery (CSRF)

ANSWER: B

QUESTION NO: 10

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

A. Linux

B. Unix

C. OS X

D. Windows

ANSWER: D

QUESTION NO: 11

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain. If the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

A. list domain=abccorp.local type=zone

B. ls –d accorp.local

C. list server=192.168.10.2 type=all

D. lserver 192.168.10.2 –t all

ANSWER: B

QUESTION NO: 12

Bob, your senior colleague, has sent you a mail regarding aa deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bob denies that he had ever sent a mail.

What do you want to “know” to prove yourself that it was Bob who had send a mail?

A. Confidentiality

B. Integrity

C. Non-Repudiation

D. Authentication

ANSWER: C

QUESTION NO: 13

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

A. Multi-cast mode

B. Promiscuous mode

C. WEM

D. Port forwarding

ANSWER: B

QUESTION NO: 14

Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: -Verifies success or failure of an attack – Monitors system activities – Detects attacks that a network-based IDS fails to detect. – Near real-time detection and response – Does not require additional hardware – Lower entry cost. Which type of IDS is best suited for Tremp's requirements?

A. Network-based IDS

B. Open source-based IDS

C. Host-based IDS

D. Gateway-based IDS

ANSWER: C

QUESTION NO: 15

What would you enter, if you wanted to perform a stealth scan using Nmap?

A. nmap -sU

B. nmap -sS

C. nmap -sM

D. nmap -sT

ANSWER: B