DUMPSBOSS.COM

Certified Ethical Hacker v10 Exam

ECCouncil 312-50v10

Version Demo

Total Demo Questions: 15

Total Premium Questions: 340

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

Initiating an attack against targeted business and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits. What type of attack is outlined in the scenario?

A. Heartbeat Attack

B. Spear Phishing Attack

C. Shellshock Attack

D. Watering Hole Attack

ANSWER: D

QUESTION NO: 2

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP

B. 128 bit and CRC

C. 128 bit and CCMP

D. 128 bi and TKIP

ANSWER: C

QUESTION NO: 3

Which of the following tools can be used for passive OS fingerprinting?

A. tcpdump

B. nmap

C. ping

D. tracert

ANSWER: A

QUESTION NO: 4

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating

C. Piggybacking

D. Announced

ANSWER: B

QUESTION NO: 5

If an attacker uses the command SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'; which type of SQL injection attack is the attacker performing?

A. End of Line Comment

B. UNION SQL Injection

C. Illegal/Logically Incorrect Query

D. Tautology

ANSWER: A

QUESTION NO: 6

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. The amount of time and resources that are necessary to maintain a biometric system

B. How long it takes to setup individual user accounts

C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information

D. The amount of time it takes to convert biometric data into a template on a smart card

ANSWER: C

QUESTION NO: 7

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company's SQL database.

B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.

C. Attempts by attackers to access password stored on the user's computer without the user's knowledge.

D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

ANSWER: B

QUESTION NO: 8

What is the minimum number of network connections in a multihomed firewall?

A. 3

B. 2

C. 5

D. 4

ANSWER: B

QUESTION NO: 9

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations. Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA. In this context, what can you say?

A. Bob can be right since DMZ does not make sense when combined with stateless firewalls

B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one

C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations

D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

ANSWER: C

QUESTION NO: 10

Which of the following is the best countermeasure to encrypting ransomwares?

A. Use multiple antivirus softwares

B. Keep some generation of off-line backup

C. Analyze the ransomware to get decryption key of encrypted data

D. Pay a ransom

ANSWER: B

QUESTION NO: 11

How can rainbow tables be defeated?

A. Password salting

B. Use of non-dictionary words

C. All uppercase character passwords

D. Lockout accounts under brute force password cracking attempts

ANSWER: A

QUESTION NO: 12

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

A. False negative

B. True negative

C. True positive

D. False positive

ANSWER: D

QUESTION NO: 13

In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Keyed Hashing

B. Key Stretching

C. Salting

D. Double Hashing

ANSWER: C

QUESTION NO: 14

Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Network security policy

B. Information protection policy

C. Access control policy

D. Remote access policy

ANSWER: D

QUESTION NO: 15

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