312-50V12 Q&As

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?

A. The use of security agents in clients\\' computers

B. The use of DNSSEC

C. The use of double-factor authentication

D. Client awareness

Correct Answer: B

QUESTION 2

Joseph was the Web site administrator for the Mason Insurance in New York, who\\'s main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker\\'s message \\'\\'Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance\\'s internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
YOu @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

A. ARP spoofing

B. SQL injection

C. DNS poisoning

D. Routing table injection

Correct Answer: C

QUESTION 3

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. What is the technique followed by Peter to send files securely through a remote connection?

A. DMZ

B. SMB signing

C. VPN

D. Switch network

Correct Answer: C

QUESTION 4

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.

What will you call these issues?

A. False positives

B. True negatives

C. True positives

D. False negatives

Correct Answer: A

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don\\'t have

a vulnerability when, in fact, you do.

A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL

Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack

surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest.

By doing so, there is a good chance that real web application vulnerabilities will be left undetected.

When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL

Injection

vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected.

This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

QUESTION 5

Jim\\'s company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim\\'s company keeps the backup tapes in a safe in the office. Jim\\'s company is audited each year, and the results from this year\\'s audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and transport them in a lock box.

B. Degauss the backup tapes and transport them in a lock box.

C. Hash the backup tapes and transport them in a lock box.

D. Encrypt the backup tapes and use a courier to transport them.

Correct Answer: A