# 312-50V11 Q&As

Certified Ethical Hacker v11 Exam

## Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

**https://www.leads4pass.com/312-50v11.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted. What is the defensive technique employed by Bob in the above scenario?

A. Output encoding

B. Enforce least privileges

C. Whitelist validation

D. Blacklist validation

Correct Answer: C

**QUESTION 2**

When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication "open" but sets the SSID to a 32-character string of random letters and numbers.

What is an accurate assessment of this scenario from a security perspective?

A. Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.

B. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging "security through obscurity".

C. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.

D. Javik\\'s router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.

Correct Answer: C

**QUESTION 3**

An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.

What is the best example of a scareware attack?

A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"

B. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account."

C. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."

D. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."

Correct Answer: D

**QUESTION 4**

Robin, a professional hacker, targeted an organization\\'s network to sniff all the traffic. During this process.

Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.

What is the attack performed by Robin in the above scenario?

A. ARP spoofing attack

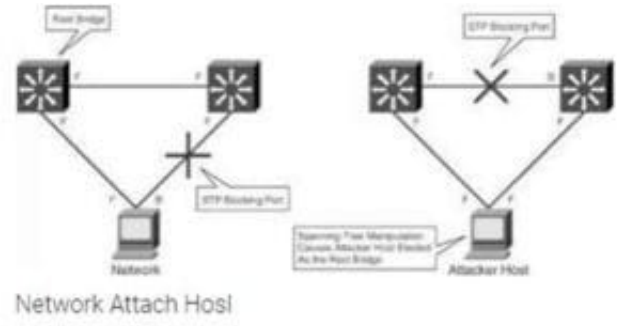
B. VLAN hopping attack

C. DNS poisoning attack

D. STP attack

Correct Answer: D

STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm. STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/ TCA) using bridge protocol data units (BPDU). An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker\\'s system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.




switch

**QUESTION 5**

What is the most common method to exploit the "Bash Bug" or "Shellshock" vulnerability?

A. SYN Flood

B. SSH

C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server

D. Manipulate format strings in text fields

Correct Answer: C

**QUESTION 6**

Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem

B. getuid

C. keylogrecorder

D. autoroute

Correct Answer: A

**QUESTION 7**

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

A. Code injections

B. Improper use of CORS

C. No ABAC validation

D. Business logic flaws

Correct Answer: B

**QUESTION 8**

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [inurl:]

B. [related:]

C. [info:]

D. [site:]

Correct Answer: B

**QUESTION 9**

In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy

B. A legitimate communication path within a computer system or network for transfer of data

C. It is a kernel operation that hides boot processes and services to mask detection

D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Correct Answer: A

**QUESTION 10**

is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

A. DNSSEC

B. Resource records

C. Resource transfer

D. Zone transfer

Correct Answer: A

**QUESTION 11**

What is a "Collision attack" in cryptography?

A. Collision attacks try to get the public key

B. Collision attacks try to break the hash into three parts to get the plaintext value

C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

D. Collision attacks try to find two inputs producing the same hash

Correct Answer: D

**QUESTION 12**

Which file is a rich target to discover the structure of a website during web-server footprinting?

A. Document root

B. Robots.txt

C. domain.txt

D. index.html

Correct Answer: C

File TXT records are a type of Domain Name System (DNS) record that contains text information for sources outside of your domain. You add these records to your domain settings. You can use TXT records for various purposes. Google uses them to verify domain ownership and to ensure email security. You verify your domain through your domain host (typically where you purchased your domain name). Your domain host maintains settings called DNS records that direct internet traffic to your domain name. For details, see Identify your domain host. Google gives you a TXT verification record to add to your domain host\\'s DNS records. When Google sees the record exists, your domain ownership is confirmed. The verification record does not affect your website or email.

**QUESTION 13**

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications.

He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby

used this virtual tower to interrupt the data transmission between the user and real tower, attempting to

hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual

tower and redirected the victim to a malicious website.

What is the attack performed by Bobby in the above scenario?

A. Wardriving

B. KRACK attack

C. jamming signal attack

D. aLTEr attack

Correct Answer: D

**QUESTION 14**

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

A. Use multiple antivirus softwares

B. Pay a ransom

C. Keep some generation of off-line backup

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

Correct Answer: C

**QUESTION 15**

At what stage of the cyber kill chain theory model does data exfiltration occur?

A. Actions on objectives

B. Weaponization

C. installation

D. Command and control

Correct Answer: A

The longer an adversary has this level of access, the greater the impact. Defenders must detect this stage as quickly as possible and deploy tools which can enable them to gather forensic evidence. One example would come with network packet captures, for damage assessment. Only now, after progressing through the primary six phases, can intruders take actions to realize their original objectives. Typically, the target of knowledge exfiltration involves collecting, encrypting and extracting information from the victim(s) environment; violations of knowledge integrity or availability are potential objectives also . Alternatively, and most ordinarily , the intruder may only desire access to the initial victim box to be used as a hop point to compromise additional systems and move laterally inside the network. Once this stage is identified within an environment, the implementation of prepared reaction plans must be initiated. At a minimum, the plan should include a comprehensive communication plan, detailed evidence must be elevated to the very best ranking official or board , the deployment of end-point security tools to dam data loss and preparation for briefing a CIRT Team. Having these resources well established beforehand may be a "MUST" in today\\'s quickly evolving landscape of cybersecurity threats