



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.passapply.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

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

- A. Phishing
- B. Vishing
- C. Spoofing
- D. DDoS

Correct Answer: A

<https://en.wikipedia.org/wiki/Phishing> Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data. An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

QUESTION 2

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

- A. WPA2 Personal
- B. WPA3-Personal
- C. WPA2-Enterprise
- D. WPA3-Enterprise

Correct Answer: D

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data: ?Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)?Key derivation and confirmation: 384bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)?Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve?Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)The 192-bit security mode offered by WPA3- Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform



baseline of security within a WPA3 network.

QUESTION 3

While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: `nmap -Pn -p- -si kiosk.adobe.com www.riaa.com`. `kiosk.adobe.com` is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?

- A. Conduct stealth scan
- B. Conduct ICMP scan
- C. Conduct IDLE scan
- D. Conduct silent scan

Correct Answer: C

Once a suitable zombie has been found, performing a scan is easy. Simply specify the zombie hostname to the -si option and Nmap does the rest. Example 5.19 shows an example of Ereet scanning the Recording Industry Association of America by bouncing an idle scan off an Adobe machine named Kiosk.

Example 5.19. An idle scan against the RIAA

```
# nmap -Pn -p- -sl kiosk.adobe.com www.riaa.com
```

```
Starting Nmap ( http://nmap.org ) Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental  
Nmap scan report for 208.225.90.120 (The 65522 ports scanned but not shown below are in state: closed) Port State  
Service 21/tcp open ftp 25/tcp open smtp 80/tcp open http 111/tcp open sunrpc 135/tcp open loc-srv 443/tcp open https  
1027/tcp open IIS 1030/tcp open iad1 2306/tcp open unknown 5631/tcp open pcanywheredata 7937/tcp open unknown  
7938/tcp open unknown 36890/tcp open unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 2594.47 seconds
```

<https://nmap.org/book/idlescan.html>

QUESTION 4

Internet Protocol Security IPsec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

- A. Protect the payload and the headers
- B. Encrypt
- C. Work at the Data Link Layer
- D. Authenticate

Correct Answer: D

**QUESTION 5**

Trempe 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 Trempe's requirements?

- A. Gateway-based IDS
- B. Network-based IDS
- C. Host-based IDS
- D. Open source-based

Correct Answer: C

[312-50V12 Practice Test](#)

[312-50V12 Study Guide](#)

[312-50V12 Braindumps](#)