# Eccouncil

## 312-50V12 Exam

**Certified Ethical Hacker Exam**

# Version: 5.1

Topic 1, Exam Pool A

## Question: 1

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

A. Application

B. Transport

C. Session

D. Presentation

**Answer: D**

Explanation:

https://en.wikipedia.org/wiki/Presentation_layer

In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as

the data translator for the network. It is sometimes called the syntax layer. The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.

Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

## Question: 2

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

A. The WAP does not recognize the client's MAC address

B. The client cannot see the SSID of the wireless network

C. Client is configured for the wrong channel

D. The wireless client is not configured to use DHCP

## Answer: A

Explanation:

https://en.wikipedia.org/wiki/MAC_filtering

MAC filtering is a security method based on access control. Each address is assigned a 48-bit address, which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address. We can configure the filter to allow connection only to those devices included in the white list. White lists provide greater security than blacklists because the router grants access only to selected devices.

It is used on enterprise wireless networks having multiple access points to prevent clients from

communicating with each other. The access point can be configured only to allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to a network.

The router allows configuring a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network. The router has several functions designed to improve the network's security, but not all are useful. Media access control may seem advantageous, but there are certain flaws.

On a wireless network, the device with the proper credentials such as SSID and password can authenticate with the router and join the network, which gets an IP address and access to the internet and any shared resources.

MAC address filtering adds an extra layer of security that checks the device's MAC address against a list of agreed addresses. If the client's address matches one on the router's list, access is granted; otherwise, it doesn't join the network.

## Question: 3

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

A. Social engineering

B. Piggybacking

C. Tailgating

D. Eavesdropping

|                                              | **Answer: A** |
| --- | --- |

Explanation:

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

Incorrect answers:

Tailgating and Piggybacking are the same thing

Tailgating, sometimes referred to as piggybacking, is a physical security breach in which an unauthorized person follows an authorized individual to enter a secured premise.

Tailgating provides a simple social engineering-based way around many security mechanisms one would think of as secure. Even retina scanners don't help if an employee holds the door for an unknown person behind them out of misguided courtesy.

People who might tailgate include disgruntled former employees, thieves, vandals, mischief-makers, and issues with employees or the company. Any of these can disrupt business, cause damage, create unexpected costs, and lead to further safety issues.

Eavesdropping https://en.wikipedia.org/wiki/Eavesdropping

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information. Since the beginning of the digital age, the term has also come to hold great significance in the world of cybersecurity.

The question does not specify at what level and how this attack is used. An attacker can eavesdrop on a conversation or use special software and obtain information on the network. There are many options, but this is not important because the correct answer is clearly not related to information interception.

**Question: 4**

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Traceroute

B. Hping

C. TCP ping

D. Broadcast ping

**Answer: B**

Explanation:

https://tools.kali.org/information-gathering/hping3

http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf

## Question: 5

Which is the first step followed by Vulnerability Scanners for scanning a network?

A. OS Detection

B. Firewall detection

C. TCP/UDP Port scanning

D. Checking if the remote host is alive

**Answer: D**

Explanation:

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

1. Locating nodes: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.

2. Performing service and OS discovery on them: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services and the operating system on the target systems.

3. Testing those services and OS for known vulnerabilities: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

**Thank You for trying 312-50V12 PDF Demo**

To try our 312-50V12 practice exam software visit link below

https://www.certshero.com/312-50V12.html

# Start Your 312-50V12 Preparation

Use Coupon "20OFF" for extra 20% discount on the purchase of Practice Test Software. Test your 312-50V12 preparation with actual exam questions.