# Quiz by Ethical Hacking Master Hamdani Arif

## Number 1

Which of the following web server components facilities storage on another machine or disk if the original disk becomes full, in addition to providing object-level security?

1. Web server
2. Server root
3. Document root
4. Virtual document tree

The answer is **Virtual Document Tree,** A virtual document tree is a feature provided by web server software that allows administrators to define multiple document roots or directories that can be located on different machines or disks. When the primary disk becomes full, the virtual document tree can automatically redirect requests for files or resources to an alternate storage location specified within the tree.

Each multiple-choice answer explanations

1. Web server: A web server is a software that handles incoming requests and serves web pages to clients. It manages the processing of HTTP requests, handles file retrieval, and delivers content to the requesting client. However, a web server typically does not have built-in capabilities for storage on another machine or disk if the original disk becomes full, nor does it directly provide object-level security.
2. Server root: The server root refers to the top-level directory on a web server where all the files and resources are stored. It is the main directory from which the web server serves content. While the server root plays a crucial role in determining the file structure and access points, it does not inherently provide the specific capabilities mentioned in the question.
3. Document root: The document root, also known as the web root, is the directory on a web server where the files for a specific website are stored. It is the base directory from which web documents and resources are served. Similar to the server root, the document root is responsible for determining the file structure of a website, but it does not inherently provide the mentioned capabilities.
4. Virtual document tree: The virtual document tree, or virtual directory structure, is a feature provided by the web server software. It allows administrators to define multiple document roots or directories that can be located on different machines or disks. This feature enables the web server to distribute file storage across multiple locations and automatically redirect requests if the primary disk becomes full. Additionally, the virtual document tree can enforce object-level security, allowing administrators to apply specific access controls and permissions to different directories within the tree.

## **Number 2**

James is a professional hacker, he decided to target an organization network. He identified a vulnerable protocol that saves on port 23. Which allowed him to communicate with a remote host through a command line interface which of the following protocols allowed James to interact with a remote host?

1. SNMP
2. Telnet
3. HTTP
4. FTP

Answer

The answer **Telnet** is that telnet is a network protocol that provides a command interface for remotely accessing and managing devices (“….on port 23. Which allowed him to communicate with a remote host through a command line interface….”)

Explanation of a-d answer to this multiple choice

1. SNMP (Simple Network Management Protocol): SNMP is a protocol used for network management and monitoring. It is not typically used for interacting with a remote host through a command line interface. SNMP is more focused on retrieving and manipulating information about network devices and systems, such as routers, switches, and servers.
2. Telnet: Telnet is a protocol that allows remote access to devices or computers over a network. It provides a command-line interface that enables users to execute commands and manage the remote host. However, Telnet is considered insecure because it transmits data, including usernames and passwords, in plain text, making it susceptible to interception and unauthorized access.
3. HTTP (Hypertext Transfer Protocol): HTTP is the protocol used for transmitting data over the internet. It is primarily used for communication between web browsers and web servers, enabling the retrieval and display of web pages. While HTTP can involve command-like interactions (e.g., submitting form data), it is not typically used for direct command-line access to a remote host.
4. FTP (File Transfer Protocol): FTP is a protocol used for transferring files over a network. It is commonly used to upload and download files between a client and a server. Like HTTP, FTP is not designed for command-line interaction with a remote host.

## Number 3

A third-party security auditor receives a mail from one of the client organizations seeking advice on securing corporate data. They suggest a cloud deployment model that provides complete control over corporate data and can be managed within the organization. Which of the following deployment model has the auditor suggested to the organization?

1. Public Cloud
2. Multi-Cloud
3. Private Cloud
4. Community Cloud

the answer is “**Private Cloud**”, The Private Cloud deployment model offers complete control over corporate data and allows the organization to manage the cloud infrastructure internally. In a Private Cloud, the cloud infrastructure is dedicated to a single organization, providing exclusive use and control over the resources, data, and applications hosted within the cloud environment. It is typically managed and operated by the organization's own IT department or a trusted third party.

**Each multiple-choice answer explanations**

A. Public Cloud: The Public Cloud deployment model refers to a cloud infrastructure that is shared among multiple organizations or users. In this model, the cloud provider owns and manages the infrastructure, and the organization accesses cloud services and resources over the internet. With a Public Cloud, the organization does not have complete control over corporate data or the underlying infrastructure.

B. Multi-Cloud: The Multi-Cloud deployment model involves using multiple cloud service providers to host different aspects of an organization's infrastructure. It enables organizations to distribute their workloads across multiple cloud environments. While Multi-Cloud can offer flexibility and redundancy, it does not inherently provide complete control over corporate data within the organization itself.

C. Private Cloud: The Private Cloud deployment model is characterized by dedicated cloud infrastructure exclusively used by a single organization. It provides complete control over corporate data and allows the organization to manage the cloud infrastructure internally. In a Private Cloud, the organization has control over security measures, data privacy, and compliance. This model aligns with the auditor's suggestion of complete control and management within the organization.

D. Community Cloud: The Community Cloud deployment model involves sharing a cloud infrastructure among organizations with similar interests, such as regulatory requirements or security concerns. It allows organizations to collaborate and share resources while maintaining some level of control and customization. However, it may not provide the same level of complete control over corporate data as the Private Cloud model.

## Number 4

In which of the following levels of the OSI model an attacker gains control over the HTTP user of the session by obtaining the session id and create new unauthorized session by using the stolen data?

1. Transport Level
2. Presentation Level
3. Network Level
4. Application Level

The answer is **Application Level,** as we already know the OSI seven layer has seven layers, The layers are as follows:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

The Application layer is responsible for providing network services directly to the end user and includes protocols such as HTTP (Hypertext Transfer Protocol) used for web browsing. By obtaining the session ID, the attacker can impersonate the user and create a new unauthorized session, effectively gaining control over the user's HTTP session. This attack typically involves session hijacking or session theft, where the attacker steals or manipulates the session ID to gain unauthorized access.

**Another multiple-choice answer explanation:**

A. Transport Level: The Transport layer of the OSI model is responsible for reliable end-to-end delivery of data between hosts. It includes protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). However, obtaining the session ID and creating an unauthorized session typically occurs at a higher layer in the OSI model.

B. Presentation Level: The Presentation layer of the OSI model is responsible for data formatting, encryption, and translation between different data formats. It ensures that data is properly formatted for the application layer to interpret. While encryption may play a role in protecting the session ID, the actual unauthorized session creation would typically occur at a higher layer.

C. Network Level: The Network layer of the OSI model is responsible for addressing, routing, and forwarding data packets across different networks. It includes protocols such as IP (Internet Protocol). However, obtaining the session ID and creating an unauthorized session typically occurs at a higher layer.

D. Application Level: The Application layer of the OSI model is the highest layer and is responsible for providing network services directly to the end-user. It includes protocols such as HTTP (Hypertext Transfer Protocol) used for web browsing. In the context of the given scenario, where an attacker gains control over the HTTP user session by obtaining the session ID and creating an unauthorized session, it occurs at the Application layer. By stealing the session ID, the attacker can impersonate the user and establish a new session with unauthorized access.

Another layer explanation

1. Physical Layer: The Physical layer is the lowest layer of the OSI model. It deals with the physical transmission of data bits over a communication channel. It specifies the electrical, mechanical, and procedural aspects of the physical connection between devices. It includes characteristics such as voltage levels, data encoding, cables, connectors, and signaling methods. The Physical layer ensures that data is reliably transmitted between devices.
2. Data Link Layer: The Data Link layer is responsible for the reliable transfer of data between two directly connected nodes over a physical layer network. It provides error detection and correction mechanisms, and flow control, and defines protocols for addressing and accessing the media. The Data Link layer is divided into two sublayers: the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer.

* The LLC sublayer is responsible for multiplexing protocols, error control, and managing data frames.
* The MAC sublayer handles media access control and defines protocols for sharing a common communication medium between multiple devices.

The Data Link layer establishes and maintains a link between adjacent nodes and ensures error-free transmission over the physical layer.

1. Session Layer: The Session layer is responsible for establishing, managing, and terminating sessions or connections between applications. It provides the mechanisms for organizing and synchronizing communication sessions between devices. The Session layer facilitates dialogue control, allowing applications to initiate, maintain, and close communication sessions.

## Number 5

A professional hacker hired by an agency to disrupt the business services of their rival company, he employed a special type of malware that consume a server’s main memory and network bandwidth when identify the type of malware he has used in the above scenario.

1. Rootkit
2. Armored Virus
3. Spyware
4. Worm

The answer is a **worm,** because Worm is a self-replicating type of malware that spreads across networks and systems by exploiting vulnerabilities. It does not require human intervention to spread and can propagate itself from one host to another, often using network services or communication protocols. Once a Worm infects a system, it can consume system resources, including main memory and network bandwidth, as it continues to spread and replicate. The primary characteristic of a Worm is its ability to self-propagate and spread rapidly, causing disruptions to the targeted network or system. In the scenario described, the hacker employed a Worm to disrupt the business services of their rival company by consuming the server's main memory and network bandwidth.

**Another multiple-choice answer explanation:**

1. Rootkit: A Rootkit is a type of malicious software designed to gain unauthorized access and control over a system while hiding its presence from detection. It allows the attacker to maintain persistent access and control over the compromised system. However, a Rootkit is not specifically known for consuming a server's main memory and network bandwidth.
2. Armored Virus: An Armored Virus is a type of computer virus that has been specifically designed to make its detection and removal more difficult. It typically uses various techniques to obfuscate its code and make it harder for antivirus software to detect and analyze it. However, an Armored Virus is not typically associated with consuming a server's main memory and network bandwidth.
3. Spyware: Spyware is a type of malware that is designed to gather information about a user or organization without their knowledge or consent. It can monitor activities, collect personal information, and transmit it to a remote attacker. While Spyware can have negative impacts on system performance, it is not typically known for consuming a server's main memory and network bandwidth to the extent described in the scenario.
4. Worm: A Worm is a self-replicating type of malware that spreads across networks and systems. It does not require human intervention to spread and can consume system resources as it continues to replicate and spread. Worms are known for their ability to consume a server's main memory and network bandwidth, causing disruptions to the targeted network or system. In the given scenario, where the hacker employed a special type of malware to consume server resources, a Worm is the most likely option.

## Number 6

A professional hacker is attempting to break into a target network through an application server. In this process, she identified a logic flaw in the target web application that provided visibility into the source code. She exploited this vulnerability to launch further attacks on target web applications. Which of the web application vulnerabilities was identified by he in above scenario?

1. Insecure Deserialization
2. Command Injection
3. Broken Authentication
4. Security Misconfiguration

Answer

The answer is **Broken Authentication**. Broken Authentication is a vulnerability that occurs when there are flaws in the authentication and session management mechanisms of a web application. It can enable attackers to bypass authentication controls, gain unauthorized access, and impersonate other users. the hacker identified a logic flaw in the web application that provided visibility into the source code. This suggests that there is a weakness in the authentication or session management process, allowing the hacker to view the application's source code and potentially discover additional vulnerabilities or exploit them further.

A. Insecure Deserialization: Insecure deserialization is a vulnerability that occurs when an application improperly handles serialized objects, which can lead to various security issues. Attackers may exploit this vulnerability to execute arbitrary code, tamper with serialized data, or perform other malicious actions. In the scenario described, the hacker did not exploit a vulnerability related to deserialization but rather identified a logic flaw in the web application.

B. Command Injection: Command injection is a vulnerability that arises when an application allows an attacker to execute arbitrary commands on the underlying operating system. It typically occurs when user-supplied input is improperly validated or sanitized and is directly used in constructing system commands. Although command injection can be a severe vulnerability, it does not match the description provided in the scenario.

C. Broken Authentication: Broken Authentication refers to vulnerabilities in the authentication and session management mechanisms of a web application. It can enable attackers to bypass authentication controls, gain unauthorized access, or impersonate other users. In the given scenario, the hacker identified a logic flaw in the web application that provided visibility into the source code, suggesting a weakness in authentication or session management.

D. Security Misconfiguration: Security misconfiguration occurs when a web application is not securely configured, leaving it vulnerable to attacks. This can include improper file permissions, default credentials, exposed sensitive information, and other configuration weaknesses. While security misconfiguration can be a significant vulnerability, it does not align with the specific scenario described.

## Number 7

A professional hacker configured her wireless router in an organization’s premises and advertised it with a spoofed SSID. She lured victims to connect to the router by sending the fake SSID. She stared sniffing all the traffic from the victim that is passing thought his wireless router. Which on the following types of attack.

1. AP MAC Spoofing Attack
2. AD-Hoc connection attack
3. Rogue AP attack
4. Key Reinstallation attack

The answer is **Rogue AP (Access Point) Attack,** A Rogue AP attack involves the unauthorized setup of an access point within an organization's premises, typically with the intention of intercepting network traffic and compromising the security of connected devices. In this case, the hacker configured a wireless router with a spoofed SSID (fake network name) to deceive victims into connecting to it. By luring victims to connect to the rogue access point, the hacker gains control over the network traffic passing through that wireless router. This allows them to sniff (capture) and potentially analyze sensitive information transmitted between the victim's device and other devices on the network.

The answer of another answer is

A. AP MAC Spoofing Attack: This attack involves spoofing or impersonating the MAC address (unique identifier) of an authorized access point to gain unauthorized access to a network. While related to access point impersonation, it does not specifically address the scenario where the hacker sets up their own rogue access point.

B. Ad-Hoc Connection Attack: An ad-hoc connection is a direct peer-to-peer wireless connection between devices without the need for an access point. This type of attack would involve manipulating or exploiting vulnerabilities in ad-hoc connections, but it does not align with the scenario described.

D. Key Reinstallation Attack: A Key Reinstallation Attack, also known as a KRACK attack, is a vulnerability that targets the WPA2 protocol used for securing Wi-Fi connections. It allows an attacker to reinstall a previously used encryption key, potentially leading to the decryption of sensitive information. While wireless security protocols can be targeted in rogue access point attacks, the specific focus in this scenario is on the creation of a rogue access point.

## Number 8

In which of the following phases to the cyber kill chain methodologies does the adversary create a tailored malicious payload based on the vulnerabilities identified?

1. Exploitation
2. Weaponization
3. Command and control
4. Installation

The answer is **Weaponization,** as we know there are 7 steps of the cyber kill chain methodology as follows:

1. Reconnaissance: The attacker gathers information about the target system or organization.
2. **Weaponization: In this stage, the attacker creates or modifies a malicious payload, such as a piece of malware, that can exploit specific vulnerabilities identified during the reconnaissance phase. The payload is tailored to the target's vulnerabilities and objectives.**
3. Delivery: The attacker delivers the weaponized payload to the target system, often through various means such as email attachments, malicious websites, or compromised software.
4. Exploitation: In this stage, the attacker exploits the vulnerabilities present in the target system using the weaponized payload. This allows them to gain unauthorized access or control over the system.
5. Installation: The attacker establishes a foothold in the compromised system and installs additional tools or malware to maintain persistence and further their objectives.
6. Command and Control: The attacker establishes communication channels and maintains control over the compromised system, enabling them to issue commands, exfiltrate data, or perform other malicious activities.
7. Actions on Objectives: This is the final stage where the attacker achieves their ultimate goals, such as stealing data, disrupting services, or causing other harm to the target organization.

## Number 9

Which of the following cloud-based attacks involves an adversary interrupting the soap message, and sending it to the server as a legitimate user that results in intrusion into the cloud and execution of malicious code?

1. Cloud hopper attack
2. Wrapping attack
3. Cloud cryptojacking
4. Side-channel attacks

the attack involving the interception of SOAP messages and intrusion into the cloud is known as a **Wrapping attack.** A Wrapping attack, also known as a SOAP/XML Wrapping attack, is a type of attack that targets web services using the SOAP (Simple Object Access Protocol) protocol. In this attack, the adversary intercepts the SOAP message exchanged between a client and a server, modifies it, and then forwards it to the server as a legitimate user. By doing so, the attacker can bypass security measures and gain unauthorized access to the cloud environment, potentially executing malicious code or performing other malicious activities.

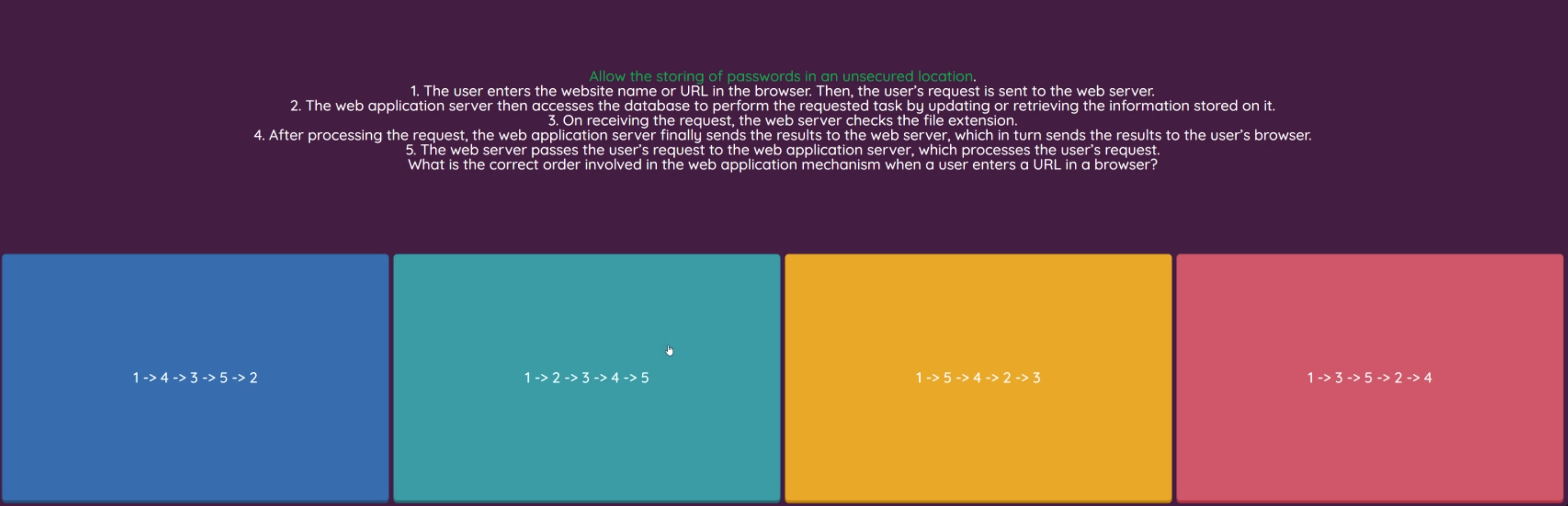
**A. Cloud hopper attack: The Cloud Hopper attack,** also known as APT10, is a cyber-espionage campaign that targets managed IT service providers (MSPs) to gain unauthorized access to their client’s networks. It involves compromising MSPs and then using their access to infiltrate and monitor the networks of their clients. It does not specifically involve interrupting SOAP messages or the execution of malicious code.

**B. Wrapping attack: A Wrapping attack,** also known as a SOAP/XML Wrapping attack, targets web services that use the SOAP (Simple Object Access Protocol) protocol. In this attack, the adversary intercepts the SOAP message exchanged between a client and a server, modifies it, and sends it to the server as a legitimate user. By doing so, the attacker can bypass security measures and gain unauthorized access to the cloud environment, potentially executing malicious code or performing other malicious activities. This aligns with the description provided in the scenario.

**C. Cloud cryptojacking: Cloud cryptojacking,** refers to the unauthorized use of cloud computing resources for cryptocurrency mining. In this attack, an attacker compromises cloud instances or applications to mine cryptocurrencies without the knowledge or permission of the cloud owner. Cloud cryptojacking does not specifically involve interrupting SOAP messages or the execution of malicious code.

**D. Side-channel attacks: Side-channel** attacks are a class of attacks that exploit information leaked through unintended side channels such as power consumption, electromagnetic radiation, or timing variations. These attacks target the implementation or physical characteristics of a system rather than directly interrupting SOAP messages in cloud-based attacks.

## Number 10



The answer is 1-2-3-4-5

Explanation

the web application mechanism involves the user's browser sending a request to the web server, which passes it to the web application server for processing. The web application server performs the necessary operations, and the results are returned to the web server, which sends them back to the user's browser for display or further interaction.

## Number 11

Which of the following communication standard is also known as WiMax and is designed to provide multiple physical layer (PHY) and MAC options ?

1. 802.11n
2. 802.11g
3. 802.16
4. 802.15.1

The answer is **IEEE 802.16**

1. 802.11n: This is a Wi-Fi standard that supports higher data rates and improved network performance compared to earlier Wi-Fi standards. It operates in the 2.4 GHz and 5 GHz frequency bands and uses multiple-input multiple-output (MIMO) technology to enhance wireless communication. However, 802.11nD is not known as WiMax and does not provide multiple physical layer (PHY) and MAC options like 802.16.
2. 802.11g: This is another Wi-Fi standard that operates in the 2.4 GHz frequency band and provides data rates up to 54 Mbps. While it offers improved speeds compared to the older 802.11b standard, it is not referred to as WiMax and does not offer multiple PHY and MAC options like 802.16.
3. 802.16: This communication standard is also known as WiMax (Worldwide Interoperability for Microwave Access). It is specifically designed to provide wireless broadband access over long distances. It supports multiple PHY and MAC options, allowing flexibility in adapting to different deployment scenarios and network configurations. WiMax is typically used for last-mile connectivity, extending broadband access to areas where wired infrastructure is not readily available.
4. 802.15.1: This is the Bluetooth standard, which is designed for short-range wireless communication between devices. It operates in the 2.4 GHz frequency band and provides data rates up to 3 Mbps. While Bluetooth has its own set of features and applications, it is not referred to as WiMax and does not offer multiple PHY and MAC options like 802.16.

## Number 12

A network administrator, was instructed to enhance wireless security and implement a centralized authentication mechanism for clients. To achieve this, he implemented a wireless encryption technology that uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards Kerberos and certificates. Which of the following technology has smith implemented in the above scenario

1. WPA2-Enterprise
2. WPA3-Personal
3. WPA3-Enterprise
4. WPA2-Personal

The answer for this case is **WPA2-Enterprise** because WPA2-Enterprise is a wireless encryption technology that provides a higher level of security by using a centralized authentication mechanism. It supports Extensible Authentication Protocol (EAP) and RADIUS for client authentication. It allows for multiple authentication methods, such as token cards, Kerberos, and certificates, which align with the mentioned scenario of using multiple authentication methods.

**Another multiple-choice answer explanation:**

1. WPA2-Enterprise
2. WPA3-Personal: WPA3-Personal is a Wi-Fi security standard that provides enhanced security for personal networks. However, it does not involve centralized authentication mechanisms or support multiple authentication methods, so it is not the correct choice for this scenario.
3. WPA3-Enterprise: WPA3-Enterprise is a Wi-Fi security standard that provides enhanced security for enterprise networks. While it does support centralized authentication mechanisms, it does not specifically mention the use of multiple authentication methods, which are mentioned in the given scenario. Therefore, it is not the correct choice.
4. WPA2-Personal: WPA2-Personal is a Wi-Fi security standard that provides security for personal networks. It uses a pre-shared key (PSK) for authentication and does not involve centralized authentication mechanisms or support multiple authentication methods. Hence, it is not the correct choice for the scenario described.

## Number 13

Cybersol Inc., an mnc, decide to employ cloud services for their development. They consulted a cloud provider and requested development tools, configuration management, and deployment platforms for developing custom applications, identify the types of cloud services by cybersol inc. in the above scenario.

1. Security as a service (SECaas)
2. Identify as a service (IDaaS)
3. Platform as a services (PaaS)
4. Infrastructure as a service (iaas)

the answer is Platform as a Service (PaaS) because Platform as a Service (PaaS) is a cloud service model that provides developers with a platform to build, deploy, and manage applications. It includes development tools, configuration management capabilities, and deployment platforms to support the entire application development lifecycle.

The other options mentioned are:

1. Security as a Service (SECaas): This cloud service model focuses on providing security-related services such as antivirus, firewall, intrusion detection, and vulnerability scanning. While security is essential, it is not directly related to the development tools, configuration management, and deployment platforms requested by Cybersol Inc.
2. Identity as a Service (IDaaS): This cloud service model offers identity and access management solutions, including user authentication, authorization, and single sign-on capabilities. It is not directly related to the development tools and platforms requested by Cybersol Inc.
3. Platform as a services (PaaS)
4. Infrastructure as a Service (IaaS): This cloud service model provides virtualized computing resources such as virtual machines, storage, and networks. It does not directly cater to the development tools, configuration management, and deployment platforms requested in the scenario.

## Number 14

A security professional has recently joined the company and he has been trained in various security practices to be followed to protect passwords from being compromised. While implementing the security practices, she notices that the system is susceptible to password-cracking attacks.

1. Set the password change policy to 30 days
2. Do not use password that can be found in a dictionary
3. Do not use cleartext protocols with weak encryption
4. Allow the storing of password in an unsecured location

The Answer is D

my grandmother if she knows English, she will be also answered D :D

## Number 15

A professional hacker managed to penetrate the target company network and tamper with software by adding a malicious script in the production that holds persistence on the network. Which of the following phases of hacking is he is currently in

1. Clearing tracks
2. Maintaining access
3. Gaining access
4. Scanning

The answer is **maintaining access,** because this phase typically occurs after the hacker has successfully gained initial access to the target network. In this case, the hacker has already penetrated the company network and tampered with the software by adding a malicious script that holds persistence on the network. By doing so, they have ensured continued access and control over the compromised system, thereby maintaining their access for further exploitation or malicious activities.

The other explanation about another option in this multiple-choice answer:

1. Clearing tracks: This phase typically occurs after an attacker has completed their activities and wants to remove any evidence of their presence in the compromised system or network. They would try to erase logs, delete traces of their activities, and cover their tracks to avoid detection. However, in the given scenario, the hacker is actively maintaining access and has not yet reached the point of covering their tracks.
2. Maintaining access
3. Gaining access: This phase refers to the initial stage of hacking, where the attacker tries to find vulnerabilities, exploit them, and gain unauthorized access to the target system or network. In the given scenario, the hacker has already penetrated the company network and tampered with the software, so they have progressed beyond the gaining access phase.
4. Scanning: Scanning is a phase where the attacker scans the target network or system for potential vulnerabilities or weaknesses. It is an information gathering stage where they try to identify open ports, services, or any security loopholes that can be exploited. In the given scenario, the hacker has already managed to penetrate the network and tamper with the software, indicating that they have completed the scanning phase.

## Number 16

In which of the following phases of session hijacking does an attacker change the sequence number of acknowledgment number (SEQ/ACK) of the server to halt data transmission to a legitimate user

1. Session ID prediction
2. Packet Injection
3. Session Desynchronization
4. Command Injection

The answer is **Session Desynchronization,** is because this phase the attacker changes the sequence number or acknowledgment number (SEQ/ACK) of the server to halt data transmission to a legitimate user, in this attack, the attacker manipulates the sequence and acknowledgment numbers to disrupt the established TCP session between the client and server.

1. Session ID prediction: Session ID prediction is a technique where an attacker tries to guess or predict the session ID used by a server to identify a specific user session. By successfully predicting the session ID, the attacker can impersonate the legitimate user and gain unauthorized access. However, it does not involve changing sequence or acknowledgment numbers, so it is not the correct option for the given scenario.
2. Packet Injection: Packet injection is a technique where an attacker injects malicious packets into a network to disrupt communication or manipulate data. It can be used for various purposes, such as injecting malware, modifying data, or even launching denial-of-service attacks. While packet injection can cause disruption to data transmission, it does not specifically involve changing sequence or acknowledgment numbers, so it is not the correct option for the given scenario.
3. Session Desynchronization
4. Command Injection: Command injection is a type of attack where an attacker injects malicious commands into a vulnerable system or application, which are then executed with the privileges of the targeted system or application. This attack is typically used to gain unauthorized access, execute arbitrary commands, or perform other malicious activities. Command injection does not involve changing sequence or acknowledgment numbers, so it is not the correct option for the given scenario.

## Number 17

which of the following trojans can an attacker use for the auto-deletion of files, folders, and registry entries as well as local network drives to cause the operating system to fail

1. Defacement Trojan
2. Destructive Trojan
3. E-Banking Trojan
4. Backdoor Trojan

The answer is **Destructive Trojan,** Destructive Trojans are specifically designed to cause harm and damage to the targeted system. They can delete or corrupt files, folders, registry entries, and even spread to connected network drives, ultimately leading to system failure or instability. The primary goal of a Destructive Trojan is to disrupt normal system operation and potentially render the system inoperable or unusable.

1. Defacement Trojan: This type of trojan is used to change the appearance of a website or web page, like defacing it with unauthorized modifications. It is not primarily focused on deleting files or causing the operating system to fail. Defacement Trojans alter the visual presentation of a website rather than causing direct harm to the operating system.
2. Destructive Trojan
3. E-Banking Trojan: E-Banking Trojans target online banking systems and aim to steal sensitive information like login credentials and credit card details. While they can cause financial harm, they are not focused on file deletion or causing the operating system to fail.
4. Backdoor Trojan: Backdoor Trojans create secret entry points in a compromised system, allowing unauthorized access and control. While they can cause damage, their main purpose is to provide ongoing access rather than specifically focusing on file deletion or causing the operating system to fail.

## Number 18

A network administrator in a company, manages network connectivity to 200 employees in six different rooms. Every employee has their own laptop to connect to the internet through a wireless network, but the company has only one broadband connection. Which of the following types of wireless networks allows he to provide internet access every laptop and bring all the devices to a single network?

1. 3G/4G hotspot
2. Lan-to-Lan wireless network
3. Extension to wired network
4. Multiple wireless access points

The answer is to provide internet access to every laptop and bring all the devices to a single network, the network administrator can use multiple wireless access points (WAPs). Each WAP can be strategically placed in different rooms to ensure adequate coverage and connectivity throughout the office space.

By setting up multiple WAPs, the network administrator can extend the wireless network's coverage and allow all laptops to connect to the same network. This configuration allows seamless roaming between access points, ensuring that employees can move freely between rooms without losing their internet connection.

1. 3G/4G hotspot, typically provides internet access to a limited number of devices and is more suitable for mobile connectivity rather than serving a large number of employees in an office setting.
2. LAN-to-LAN wireless network, is used to connect multiple local area networks (LANs) over a wireless link. It wouldn't be the best choice for providing internet access to laptops in different rooms within a single LAN.
3. extension to a wired network, refers to extending the reach of a wired network using wired connections. While this can be a valid solution, given that the laptops are connected wirelessly, it doesn't directly address the requirement of bringing all the devices to a single wireless network.
4. Multiple wireless access points

## Number 19

An organization has implemented BYOD policy that allows employees to bring their personal devices for business operations. One day, during lunchtime, Joseph, an employee, transferred project details to his collogue using freely available Wi-Fi. An attacker connected to the same Wi-Fi network sniffed the communication and gained access to the shared data. Which of the following BYOD risk was demonstrated in the above scenario?

1. Disgruntled employees
2. Infrastructure issues
3. Sharing confidential data on unsecured networks
4. Improperly disposing of devices

The answer is sharing confidential data on unsecured networks

**Little noted about BYOD (Bring Your Own Device):**

BYOD policies introduce various security risks, and one of the major concerns is the use of unsecured networks. When employees connect their personal devices to public or unsecured Wi-Fi networks, it increases the risk of data interception and unauthorized access by malicious actors.

## Number 20

In which of the following testing approaches does a penetration tester perform security standards, frame, laws and acts?

1. Adversarial goal-based assessment
2. Objective-oriented penetration testing approach
3. Red-team-oriented penetration testing approach
4. Compliance-oriented penetration testing approach

In a compliance-oriented penetration testing approach, the penetration tester focuses on assessing an organization's compliance with security standards, frameworks, laws, and acts. The goal is to determine if the organization's systems, processes, and controls meet the required compliance requirements.

This approach involves evaluating whether the organization is adhering to industry-specific standards, regulatory frameworks, and legal obligations. The penetration tester would assess the organization's systems, identify any vulnerabilities or weaknesses that could potentially violate compliance requirements, and provide recommendations for remediation.

1. adversarial goal-based assessment, refers to a penetration testing approach where the tester acts as an adversary with specific goals in mind. It focuses on simulating real-world attacks to identify vulnerabilities and weaknesses.
2. objective-oriented penetration testing approach, is not a recognized term in the field of penetration testing. It does not specifically refer to a well-known approach or methodology.
3. red-team-oriented penetration testing approach, involves simulating an attack by a malicious actor or an external threat to test an organization's defenses and incident response capabilities.

# Music I Listen to While Write This Document

Ascoltare. *Chilling around a campfire by the side of the lake / A short chill acoustic playlist*. https://youtu.be/7419Z1vm344?list=TLPQMTgwNjIwMjOPzWo8l1sMmg

CNS, Faith. *Angels Like You - Miley Cyrus*. https://youtu.be/2lqmrV7u8Xw?list=TLPQMTgwNjIwMjN5snO8HRax4Q

GUSTIXA. *Full Album Terbaru & Fasetya | New Song 2022 | Lo-Fi Remix*. https://youtu.be/qvswtm2pEkE?list=TLPQMTgwNjIwMjN5snO8HRax4Q

Meadow. *A Hollow Coves Playlist | we are all lost trying to be someone.* https://youtu.be/DPBIuzlcx6U

Yoasobi. *アイドル Idol*. https://youtu.be/ZRtdQ81jPUQ?list=TLPQMTgwNjIwMjN5snO8HRax4Q

Mari Samuelsen. Vivaldi - "Summer" from Four Seasons

https://youtu.be/g65oWFMSoK0