A loss of confidentiality is the unauthorized disclosure of information. Integrity—“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…”

Thus the option 1) Black-box test is correct. Explanation: Fran is conducting a Black-box test. In Black-box testing, the tester does not have access to the internal workings, source code, or details of the application being tested.

The consistency, accuracy and trustworthiness of data must be maintained over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure it can't be altered by unauthorized people -- for example, in data breaches.

Activists are either individuals or members of a larger group of outsider attackers who are motivated by social or political causes.

By carefully scoping the penetration test and defining clear objectives and rules of engagement, organizations can conduct effective and efficient security assessments while minimizing risks and maximizing the value of the testing process.

By focusing on all aspects of the CIA model—confidentiality, integrity, and availability—the government agency can establish a comprehensive security framework to protect classified information from unauthorized access, ensure its accuracy and reliability, and maintain its availability for authorized use.

Modification or destruction of data is an example of an integrity breach.

The military organization should focus on confidentiality to ensure the security of its communications.

This is an example of phishing, which is a form of social engineering where attackers attempt to deceive individuals into revealing sensitive information such as passwords by impersonating a trusted entity.

The next step in the process should be conducting a follow-up penetration test to verify the effectiveness of the remediation. This helps ensure that the vulnerabilities have been properly addressed and that the security measures implemented are adequate to protect the system. Therefore, the correct answer is:

Conducting a follow-up penetration test to verify the effectiveness of the remediation.

vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software running on them.

Expert-Verified Answer. Final answer: Someone who finds a flaw in a system and reports that flaw to the vendor of the system is called a B. White Hat Hacker.

The principle being followed in this scenario is "Separation of Privilege." This principle ensures that critical tasks require the collaboration of multiple individuals, reducing the risk of unauthorized access or misuse. Therefore, the correct answer is:

Separation of privilege

The correct answer is "Least privilege." This principle ensures that individuals are granted access only to the resources and information necessary for the performance of their job roles or functions, minimizing the potential damage from accidental or intentional misuse.

The correct answer is: "Confidentiality, integrity, and availability." These three goals of information security, often referred to as the CIA triad, form

the foundation for designing and implementing effective security measures to protect data and systems.

The correct answer is: "reverse social engineering." Reverse social engineering involves manipulating victims by exploiting their trust, empathy, and other social engineering tactics to achieve malicious goals.

Reconnaissance, scanning, infiltration and escalation, exfiltration, access extension, assault, and obfuscation are considered _____.

The correct answer is: "hacking steps." These steps outline various stages of a typical hacking or cyberattack process.

Someone who legally breaks into a system to assess security deficiencies is a _____. Black hat hacker Script Kiddy Penetration tester Hacktivist

The correct answer is: "Penetration tester."

Black hat hacker is someone who engages in hacking activities for malicious purposes or personal gain. Unlike ethical hackers or penetration testers, black hat hackers exploit security vulnerabilities in systems or networks for illegal activities such as stealing sensitive information, spreading malware, causing damage, or gaining unauthorized access to systems. Their actions are typically motivated by financial gain, political motives, or simply to cause harm.

Script Kiddy-

A "script kiddie" (sometimes spelled "script kiddie" or abbreviated as "skid") is a term used to describe an individual who lacks advanced coding skills or technical knowledge but still attempts to engage in hacking activities by using pre-written scripts or tools developed by others. These individuals typically rely on automated tools or scripts to exploit vulnerabilities in computer systems or networks without

fully understanding how the tools work or the underlying mechanisms behind the attacks.

Script kiddies are often viewed as amateur hackers who lack the expertise and creativity of more skilled hackers (referred to as "hackers" or "crackers"). Their activities may range from simple website defacements to launching low-level distributed denial-of-service (DDoS) attacks, but they are generally considered less sophisticated and less capable than experienced hackers.

Penetration tester –

Someone who legally breaks into a system to assess security deficiencies is commonly referred to as a "penetration tester" or "ethical hacker." They conduct controlled attacks on systems to identify vulnerabilities and weaknesses that could be exploited by malicious actors, with the ultimate goal of improving the overall security posture of the system or organization.

Hacktivist –

A "hacktivist" is a portmanteau of "hacker" and "activist." It refers to individuals or groups who use their hacking skills to promote a particular social or political agenda. Hacktivism typically involves the use of hacking techniques to gain unauthorized access to computer systems or networks for the purpose of making a political statement, raising awareness about social issues, or protesting against perceived injustices.

Hacktivist activities may include website defacements, distributed denial-of-service (DDoS) attacks, data breaches, or leaking sensitive information to the public. While

some hacktivist actions may be relatively benign, others may involve illegal activities and pose significant risks to the targeted organizations or individuals.

Notable hacktivist groups include Anonymous, LulzSec, and WikiLeaks, among others. Their motivations vary, ranging from advocating for internet freedom and transparency to challenging government policies or corporate practices.

The activity that hackers conduct to map inside defenses in an organization is "Reconnaissance."

Acme Widgets recently experienced an attack in which the attacker broke into a file server and stole product plans. Which of the following is a goal of information security that was violated? Integrity Availability Accountability Confidentiality

ChatGPT

The goal of information security that was violated in this scenario is **Confidentiality**.

_____ is the process to find out what is on a target system. Enumeration Scanning Phishing Mapping

ChatGPT

ChatGPT

The process to find out what is on a target system is called **Enumeration**.

A hospital is responsible for storing and managing patient medical records. What aspect of the CIA model should the hospital focus on to ensure the accuracy of the records? All of the above Integrity Confidentiality Availability

ChatGPT

ChatGPT

The hospital should focus on **Integrity** to ensure the accuracy of the records.

The government agency should focus on **Confidentiality** to ensure the security of the classified information.

The activity related to gaining access or infiltration and escalation in an organization is indeed **"Infiltration."**

UDP does not check if the connection is secure.

User Datagram Protocol (UDP)?

UDP is a connectionless protocol

☐

UDP has a small header size of 8 bytes

☐

UDP does not guarantee packet delivery in order

The responsibility of the (A) record in the Domain Name System (DNS) is:

"Address associated with the host."
The primary role of the Domain Name System (DNS) as an application-layer protocol in network communication is:

"To map domain names to IP addresses."

The layer in the OSI model that is responsible for addressing and routing is the "Network" layer.

The following layers in the TCP/IP model? Transport Layer Session Layer Application Layer Network Layer

---

Transport Layer Application Layer Network Layer

The TCP protocol uses the three-way handshake to establish a connection between network devices. Which of the following messages is the first message in the handshake? SYN " (Synchronize)

One of the responsibilities of the Data Link Layer is framing all packets from the network layer.

1. **Design reviews**: Expert assessment of system design to spot potential vulnerabilities.
2. **Built security test cases**: Creating tests focusing on security to find vulnerabilities.
3. **Final security review**: Thorough evaluation before deployment to ensure all security needs are met.
4. **Threat modelling**: Identifying threats, vulnerabilities, and countermeasures to mitigate risks.

1. **DOM-based XSS**: Malicious script injected into the Document Object Model of a webpage by client-side script.
2. **Persistent XSS**: Malicious script stored in a web app's database and executed when retrieved by other users.
3. **Dynamic XSS**: Malicious script dynamically generated and executed on the client-side in response to user interactions.
4. **Reflected XSS**: Malicious script included in a request to a server, reflected back in the server's response, and executed by the victim's browser.

1. **Compile time defences**: Measures implemented during code compilation to prevent vulnerabilities.
2. **Run-time**: Actions taken during program execution to enhance security.
3. **Input validation**: Process of verifying and sanitizing user inputs to prevent vulnerabilities.
4. **Encryption of memory access**: Securing memory access through encryption methods.

1. **Detection**: Identifying security threats or vulnerabilities.
2. **Defensive coding**: Writing code with security considerations to prevent vulnerabilities.
3. **Compile-time**: Security measures applied during code compilation.
4. **Run-Time prevention**: Security actions taken during program execution to prevent attacks.

5. **Detection**: Involves identifying and recognizing potential security threats or vulnerabilities in software systems. This can include techniques such as signature-based detection, anomaly detection, and code analysis to spot potential security issues.
6. **Defensive coding**: This refers to writing code in a manner that anticipates and mitigates potential security vulnerabilities. It involves practices such as input validation, output encoding, and proper error handling to prevent exploitation by attackers.
7. **Compile-time**: These are security measures that are implemented during the compilation phase of software development. They aim to harden the codebase against potential security threats by using techniques such as static code analysis, code reviews, and compiler settings that enforce security-related rules.
8. **Run-Time prevention**: These are security mechanisms that are active during the execution of the software. They aim to detect and prevent security breaches as the program runs. Examples include runtime checks for buffer overflows, memory corruption, and unauthorized access attempts.

If a program writes more information into the computer's memory than the memory was designed to hold, it is a **Buffer Overflow** Attack.

A key recommendation from NIST to reduce software vulnerabilities is **Building more resilient architectures**.

The reason Buffer overflow vulnerabilities are often missed is that input tests are small and rarely trigger the overflow. Typically, during testing, inputs provided to the program may not be large enough to exceed the buffer's capacity, thereby failing to trigger the overflow condition. This can

result in the vulnerability going undetected until exploited under real-world conditions.

---

1. **Small input tests:** Limited test scenarios may overlook potential buffer overflow issues due to insufficiently large inputs.
2. **Unknown input size:** Lack of knowledge about maximum input sizes can lead to inadequate buffer allocation.
3. **Lack of safe coding:** Failure to implement bounds checking and input validation increases the risk of buffer overflow vulnerabilities.
4. **Incomplete buffer size checks:** Merely confirming buffer sizes without robust validation can still leave programs vulnerable to overflow.

Which of the following is a type of SQL injection win in which additional queries are added after legitimate requests to malicious inject SQL statements?

Answer: Piggybacked queries

Sure, here's an explanation of each type of SQL injection attack:

1. **Inferential Attack**: In this type of attack, the attacker doesn't directly interact with the database but rather observes the behavior of the application to infer the structure and content of the database.

2. **Tautology**: This attack injects code into conditional statements in a way that they always evaluate to true, bypassing any authentication or authorization checks.

3. **End of Line Comment**: After injecting code into a field, legitimate code that follows can be nullified by appending an end-of-line comment, allowing the injected code to execute independently.

4. **Piggybacked Queries**: In this type of attack, the attacker adds additional queries beyond the intended query, piggybacking the attack on top of a legitimate request, allowing them to execute arbitrary SQL statements.

---

1. **Inferential Attack**: Observes application behavior to deduce database structure and content.
2. **Tautology**: Injects code into conditional statements to always evaluate as true.
3. **End of Line Comment**: Nullifies legitimate code by appending an end-of-line comment after injection.
4. **Piggybacked Queries**: Adds extra queries alongside legitimate ones to execute arbitrary SQL statements.

1. **Design reviews**: Evaluating software design documents for security vulnerabilities early in development.
2. **Final security review**: Comprehensive assessment of implemented security controls before deployment.
3. **Built security test cases**: Specific tests to evaluate security controls during the testing phase.
4. **Threat modelling**: Structured approach to identify and prioritize security threats in a system.

The type of attack where the attacker redirects the victim to another place using a script embedded in the URL is called a "Redirect XSS (Cross-Site Scripting) Attack."

XSS: Injection of malicious scripts into web pages.

XML injection: Exploiting vulnerabilities in XML parsing.

Database dumping: Unauthorized extraction of database contents.

SQL injection: Injecting malicious SQL code into web application inputs.

In the context of a buffer overflow attack, a buffer refers to a region of memory allocated to store data temporarily. When the amount of data written to this buffer exceeds its capacity, it can overflow into adjacent

memory locations, potentially overwriting critical program data or even executing arbitrary code. This overflow can be exploited by attackers to manipulate program behavior and gain unauthorized access or cause a system to crash.

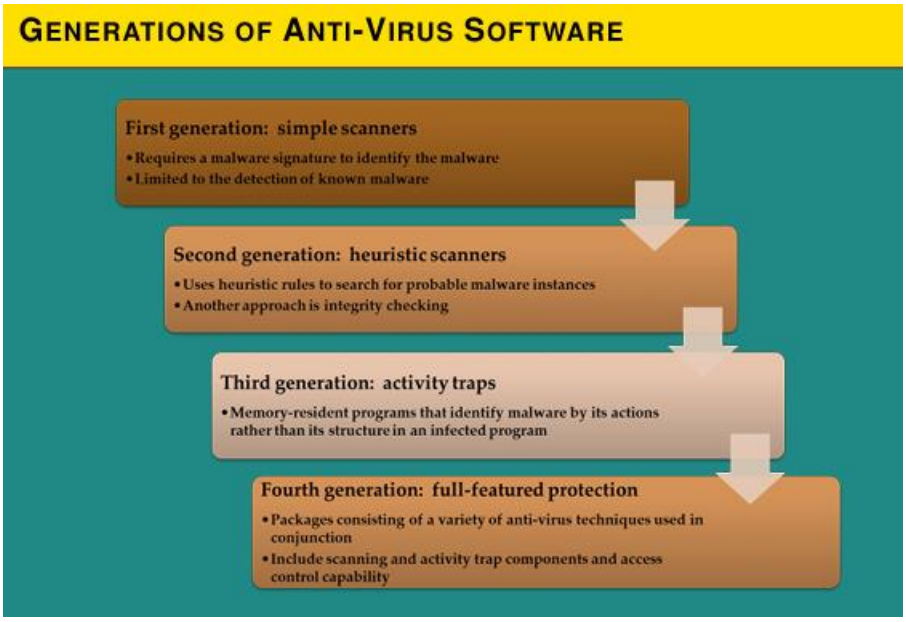
Server variables: Attackers can forge the values that are placed in HTTP and network headers and exploit this vulnerability by placing data directly into the headers.

- **SQL statements**: Injecting SQL commands into user inputs to manipulate database operations.
- **Server outputs**: Manipulating server-generated data to execute unintended actions.
- **User input avenue**: Injecting SQL commands through application user interfaces.
- **Server variables**: Forging values in server-side variables like HTTP headers to exploit vulnerabilities.
    - In a **SQL injection** attack, the attacker sends unauthorized commands directly to a database.

---

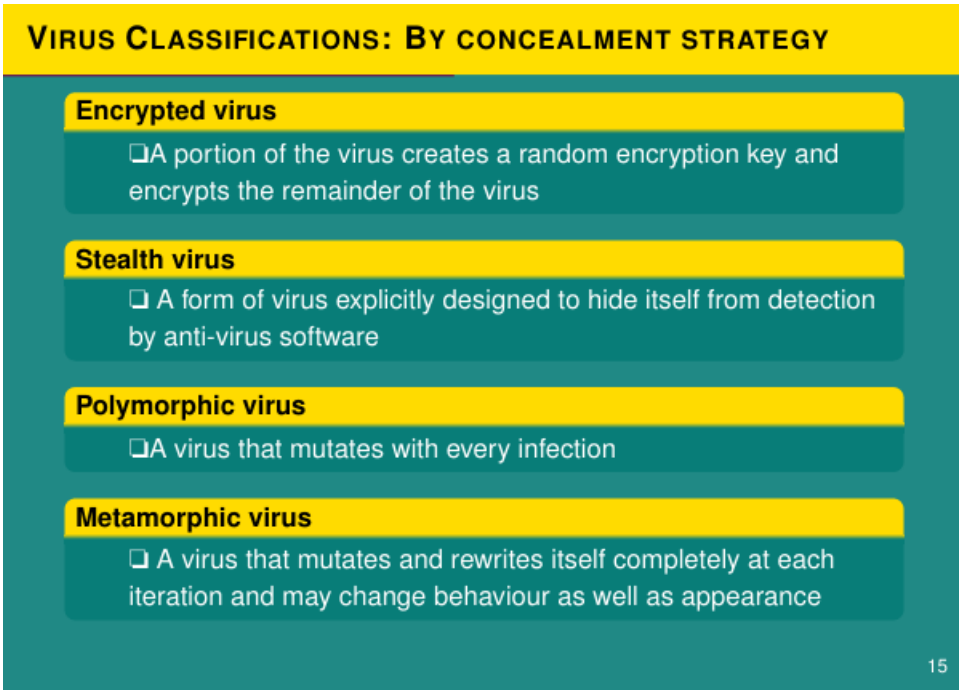
1. **Rootkits**: Malware that hides itself on a system by modifying existing programs.
2. **Macro**: Malware embedded in document macros, activated when the document is opened.
3. **Clickjacking**: Deceptive technique to trick users into clicking on hidden elements on a webpage.
4. **Worms**: Self-replicating malware that spreads across networks, exploiting vulnerabilities.

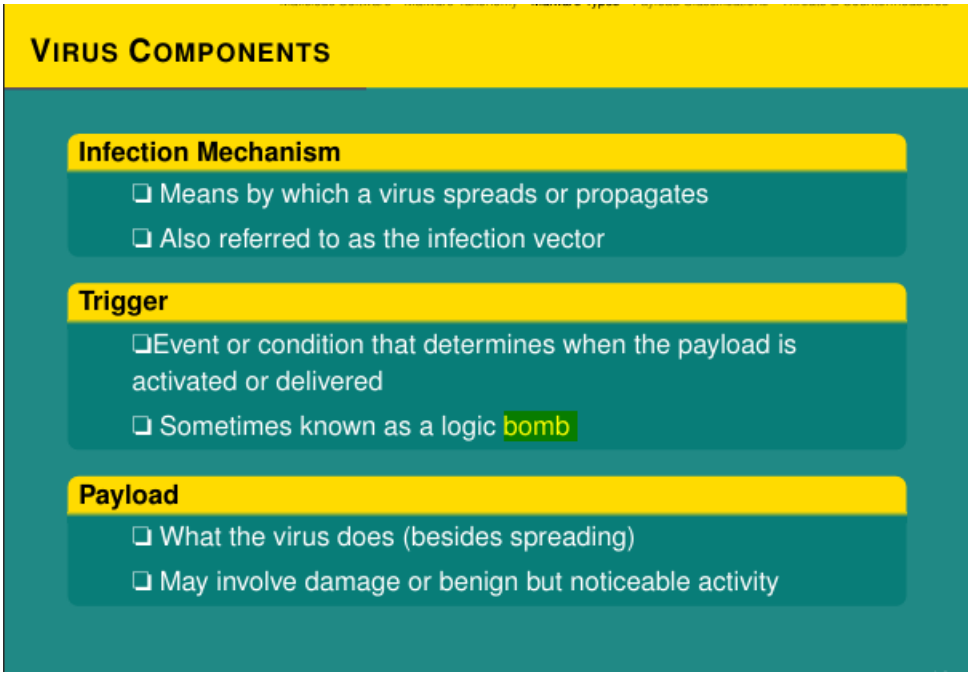
GENERATIONS OF ANTI-VIRUS SOFTWARE



MALICIOUS CODE AND ACTIVITY

- Any program that carries out actions that you (user/System) did not intend to do is considered to be a Malicious software (malware)
- Malicious code attacks one or more of the three information security properties:
  - **Confidentiality**: Malware can disclose your organisation's private information
  - **Integrity**: Malware can modify database records, either immediately or over a period of time
  - **Availability**: Malware can erase or overwrite files or inflict considerable damage to storage media





- Payload: Encrypting files, stealing data, or displaying messages on the infected system.

- Trigger (Logic bomb): A specific event or condition that activates the payload, such as a particular date or time.

- Propagation mechanism: Sending copies of itself through email attachments, network shares, or USB drives.

- Infection mechanism: Injecting malicious code into executable files, modifying system settings, or exploiting vulnerabilities in software.

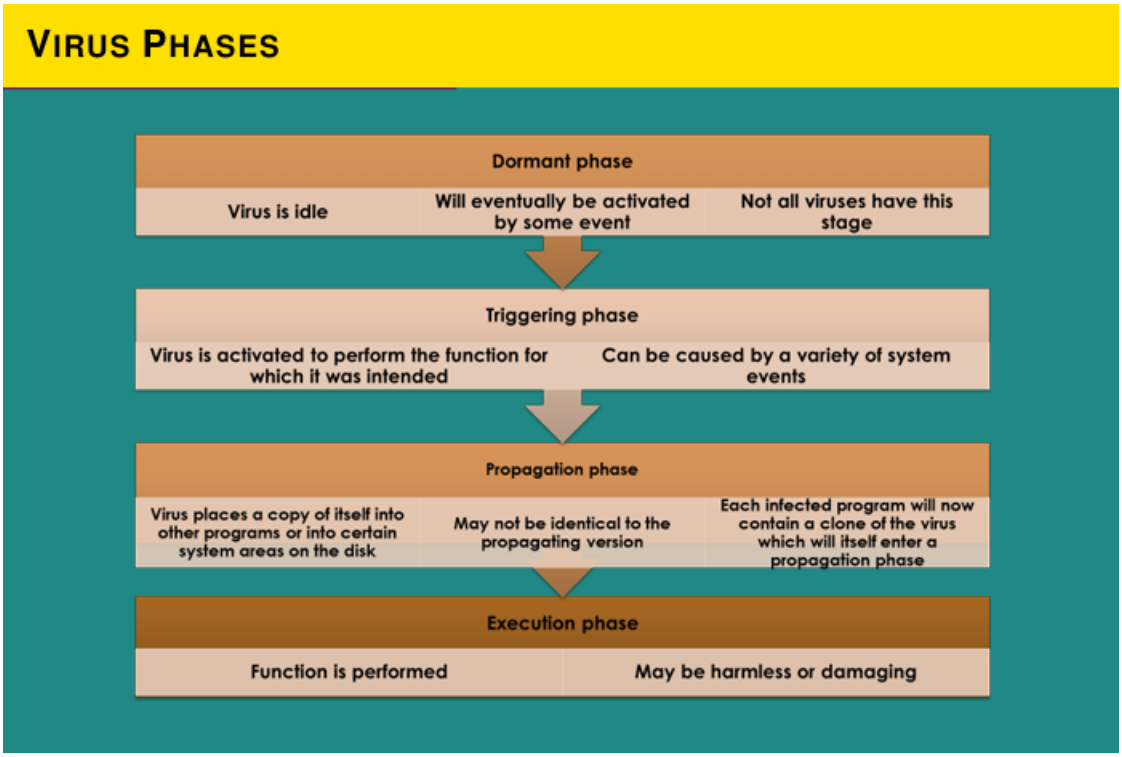
The payload of a virus defines **what happens after it reaches the target**. It encompasses the actions or effects that the virus executes on the infected system, such as causing system corruption, stealing information, creating backdoors for remote access, or engaging in other malicious activities.

Coordinated: Malware that contributes to larger-scale attacks, often working collectively with other infected devices to achieve specific goals, like launching DDoS attacks.

Auto-spreading: Malware that independently spreads to vulnerable systems, exploiting security weaknesses without manual intervention. Examples include worms.

Dynamic: Malware with changing behaviors or characteristics, making detection difficult. It adapts over time to evade security measures.

Static: Malware with fixed behaviors and characteristics. It doesn't change once deployed, performing predefined actions or payloads.

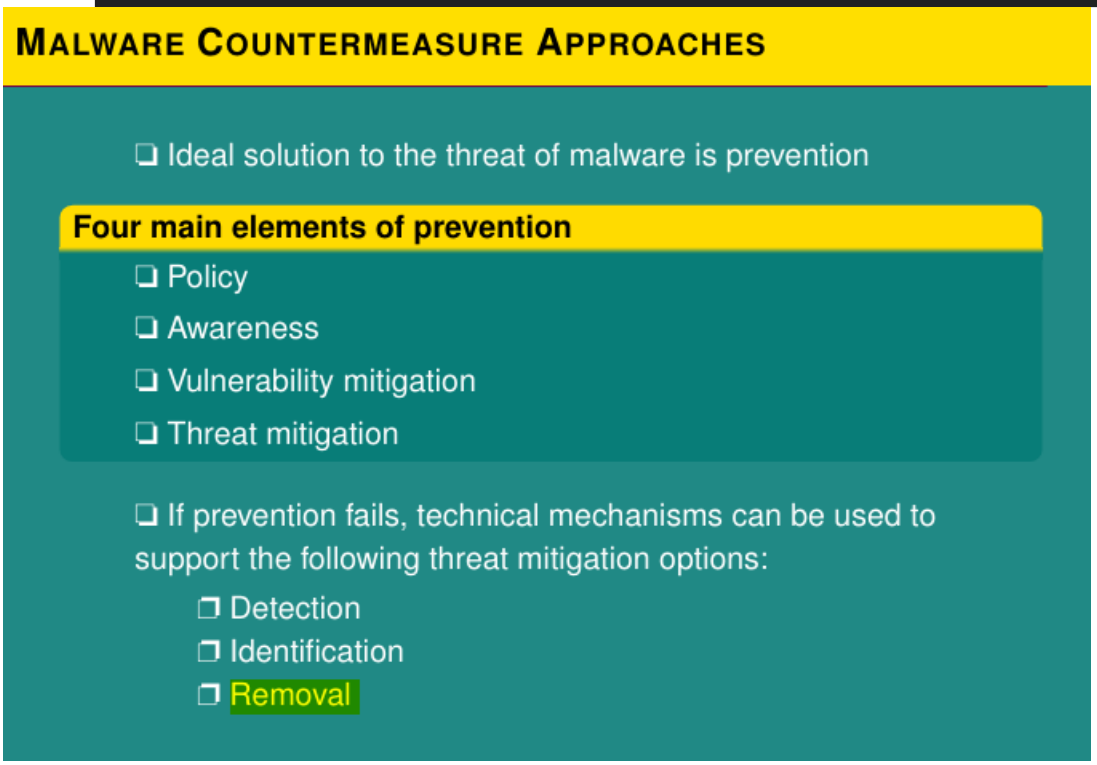


1. Metamorphic: Worm that completely changes its code and behavior with each iteration.
2. Polymorphic: Malware that alters its appearance while retaining its core functions.
3. Multipartite: Malware that spreads through multiple methods, combining virus and worm characteristics.
4. Zero-Day: Exploits unknown vulnerabilities in software or systems before they are patched.

- **Coordinated**: Malware involved in large-scale attacks.
- **Persistent**: Malware that remains on a system for a long time.
- **Act alone**: Independent malware.
- **Transient**: Malware in temporary memory, not persistent.

- **Keyloggers**: Record keystrokes, capturing sensitive information.
- **System corruption**: Damages physical equipment, like the Stuxnet worm targeting industrial systems.

- **Stealthing rootkit**: Hides malware by modifying the OS, granting covert access.
- **Phishing**: Deceives users into revealing sensitive data through impersonation.



Keyloggers: Capture keystrokes for data theft.

Stealthing rootkit: Conceals malware presence for covert access.

System corruption: Damages physical equipment, like the Stuxnet worm.

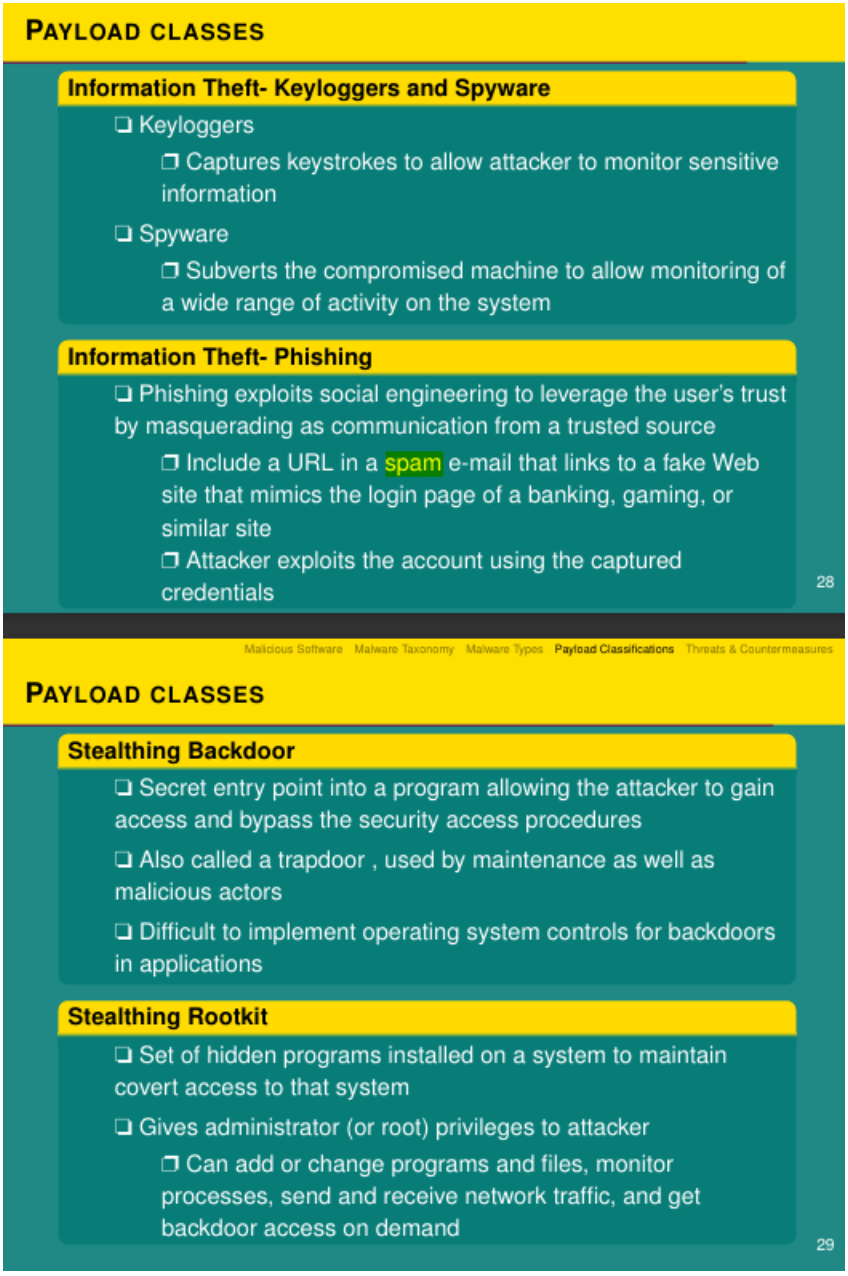
Attack agents bot: Controls other computers for coordinated attacks.

Phishing: Cyber attackers trick individuals into revealing sensitive information via emails or messages.

Stealthing Rootkit: Malware that installs hidden programs to maintain unauthorized access.

Keyloggers: Malware that records keystrokes to steal sensitive information.

System Corruption: Malware causing physical or software damage.

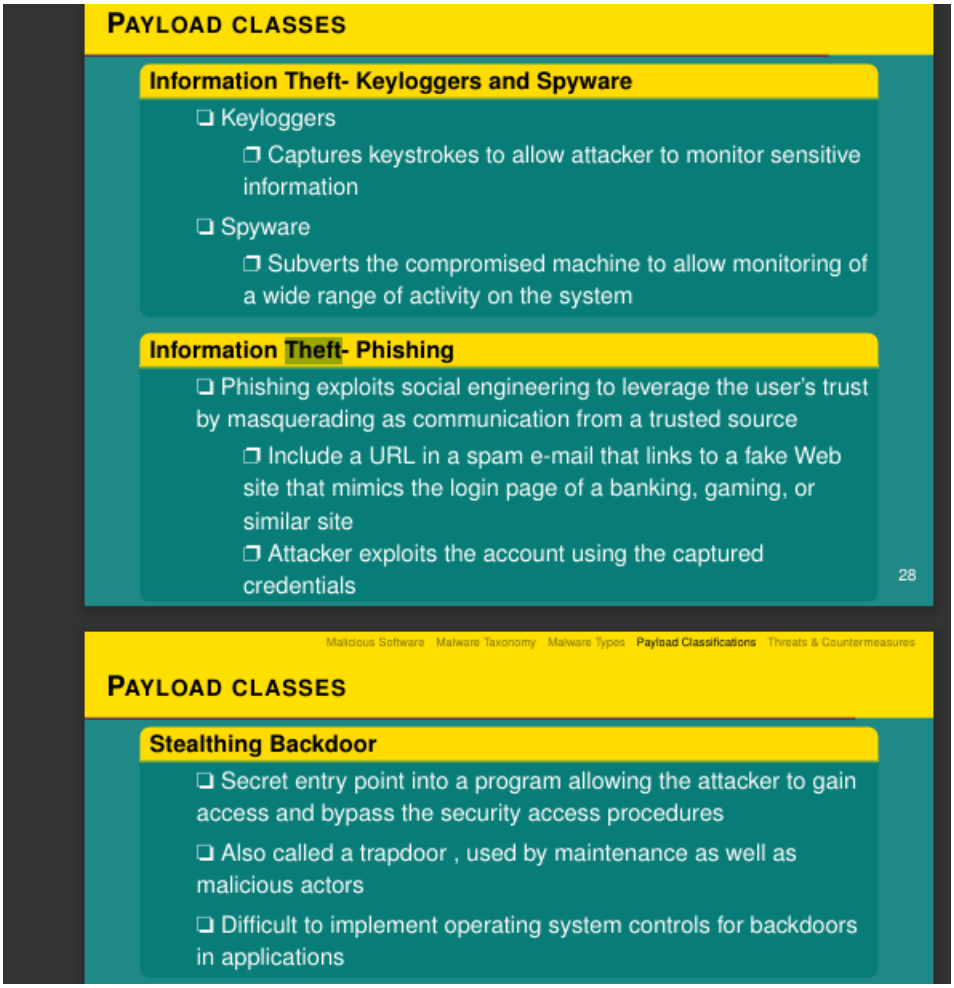


Phishing: Deceptive emails or messages used to steal sensitive information.

System corruption: Damages physical equipment or infrastructure to disrupt operations.

Stealthing rootkit: Installs hidden programs for covert access to execute unauthorized commands.

Keyloggers: Capture keystrokes to monitor and steal sensitive information.



- Where it install itself
  - This dimension generally applies to only persistent malware (Ones that requires installation)
  - Malware are categorised based on which layer of the system stack the malware is installed and run on
  - this could the firmware, the boot sector, the operating system level, the driver, the api, or user application
- How it is triggered
  - **Auto-spreading malware** runs and then looks for other vulnerable machines on the Internet, compromises these machines and installs itself on them;
  - **User-activated malware** is run on a computer only because a user accidentally downloads and executes it, e.g., by clicking on an attachment or URL in a received email.

LWARE CLASSIFICATION APPROACH

- Static or dynamically updated
  - Malware that are supported by an infrastructure and can still communicate with such infrastructure are dynamically updated with new version regularly.
  - Static malware or one time malware has no infrastructure to support it and are standalone software with no network connection to an external infrastructure
- Act alone or coordinated attack
  - **Act alone malware** are isolated malware that runs on their own. They do not participate in a larger scale attack. Such malware usually have a specific target.
  - **Coordinated malware** are attacks that contribute to a larger scale attack as on their own they will not cause much damage. For example, collectively several devices infected by such malware can cause networks or systems to crash (DDoS).

ACTIVE CONTENT VIRUS

- ❑ Active content
  - ❒ Refers to dynamic objects that do something when the user opens a webpage (ActiveX, Java, JavaScript, VBScript, macros, browser plugins, PDF files, and other scripting languages)
  - ❒ Has potential weaknesses that malware can exploit
- ❑ Active content threats are considered mobile code because these programs run on a wide variety of computer platforms
- ❑ Users download bits of mobile code, which gain access to the hard disk and do things like fill up desktop with infected file icons

21

WORM TECHNOLOGY

1. **Multiplatform**: Worms are not Operating System specific.
2. **Multi-exploit**: Worms penetrate systems using a variety of methods
3. **Ultrafast spreading**: Exploit various techniques to optimize the rate of spread of the worm
4. **Polymorphic**: To evade detection, skip past filters, and foil real-time analysis, worms adopt the virus polymorphic technique.
5. **Metamorphic**: In addition to changing their appearance, metamorphic worms have a collection of behaviour patterns that are unleashed at different stages of propagation.
6. **Zero-day exploit** : To achieve maximum surprise and distribution, a worm should exploit an unknown vulnerability that is only discovered by the general network community when the worm is launched.

23

Malicious codes commonly target confidentiality, integrity, and availability.

A stealth virus is a virus type designed to hide itself from detection by antivirus software.

Stealth Virus: Hides itself from antivirus detection by concealing its presence and actions on infected systems.

Multipartite Virus: Infects various file types and uses multiple methods to spread, making detection and removal more difficult.

Metamorphic Virus: Changes its code structure with each infection, making it hard for antivirus software to detect.

Polymorphic Virus: Alters its code while maintaining the same overall structure, making detection challenging.

The protocol that offers several functions to encrypt emails, depending on user capabilities, is S/MIME (Secure/Multipurpose Internet Mail Extension).

Sure:

1. PGP (Pretty Good Privacy): Standard for email encryption and digital signatures. Uses a Public-Private Key method, often used for secure document sharing via email.

2. S/MIME (Secure/Multipurpose Internet Mail Extension): Enhances email security by providing encryption and digital signatures. Offers various encryption methods depending on user capabilities.

3. TLS (Transport Layer Security): Ensures secure communication over a network, commonly used in email systems, web browsing, and other applications.

4. IPsec (Internet Protocol Security): Provides security at the IP layer, enabling encryption and authentication for data transmitted over networks, including LANs, WANs, and the Internet.

Allows client-server to authenticate, negotiate encryption algorithms, establish cryptographic keys, and establish a secure communication channel.

Following services IPSec provide?

Data Origin Authentication
Access Control
Confidentiality

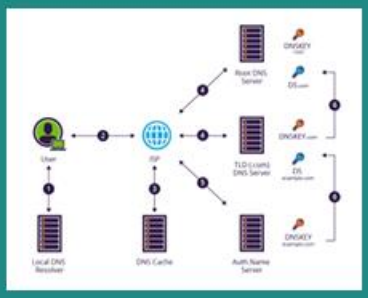
Preventative controls aim to stop security breaches,

while supportive controls provide foundational technical capabilities. Recovery controls respond to breaches by restoring lost resources, and detection controls identify security incidents.

DNS THREATS PREVENTION

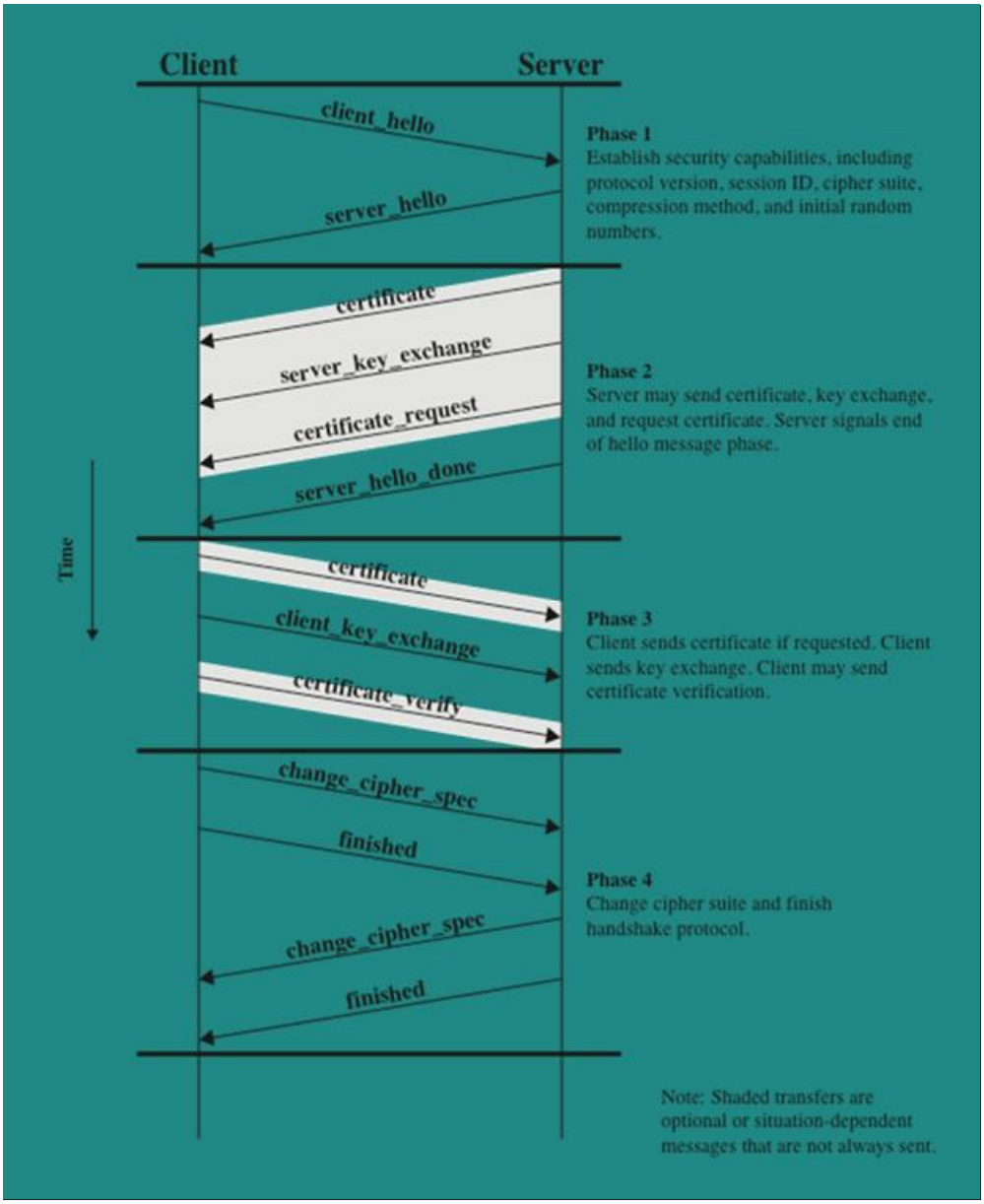
- To prevent DNS Hijacking and DNS Pharming, DNS Security (DNSSEC) is deployed to ensure:
  - Authenticity of DNS answer origin
  - Integrity of reply
  - Authenticity of denial of existence
  - Accomplishes this by signing DNS replies at each step of the way
  - Uses public-key cryptography to sign responses

- DNSSEC adds considerable load to dns servers with packet sizes considerably larger than 512 byte size of UDP packets



DNSSEC Signing

8



1. **Management Controls**:
    - Focus on security policies, planning, and standards influencing operational and technical controls.
    - Address issues needing management attention.
2. **Operational Controls**:
    - Ensure correct implementation of security policies and standards.
    - Correct operational deficiencies, primarily through people-centric mechanisms.

3. **Technical Controls**:
    - Implement hardware and software security capabilities.
    - Range from basic to complex measures securing data, information, and IT systems.
4. **Supportive Controls**:
    - Foundational IT security capabilities.
    - Interrelated with and support the implementation of other security controls.

()

- **End-to-End Encryption**: Secures communication by preventing third-party access.
- **Email Encryption**: Hides email content to protect sensitive information.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions)**: Standard for email encryption and signing.
- **Email Authentication**: Verifies sender identity to prevent phishing and spam.

Encapsulation header: Provides information for processing the encapsulated data, typically used in tunneling protocols.

Authentication payload: Contains cryptographic material for verifying the authenticity of the packet.

Authentication header: Provides authentication and integrity-checking for the entire packet, including the IP header and payload.

Encapsulation security payload: Contains the encrypted data and optional integrity check value, used to ensure confidentiality and integrity of the payload.
Sure:

- **Signed and enveloped data**: Signs and encrypts the email message for both integrity and confidentiality.

- **Clear Signed data**: Digitally signs the email message without encrypting its contents.

- **Enveloped data**: Encrypts the email message to protect its confidentiality.

- **Signed data**: Digitally signs the email message without encrypting its contents.

The SSH protocol authenticates the client-side user to the server and creates a **Tunnel** between the client and the server.

- Three-way handshake: A process in networking where three messages are exchanged to establish a TCP connection between a client and a server.
- Logical channel: A communication path or connection between two devices in a network that allows them to exchange data.
- Tunnel: A virtual private network (VPN) technology that creates a secure, encrypted connection over an existing network infrastructure.

- Transport: The layer in the OSI model responsible for end-to-end communication between devices and hosts on a network.

- **Enveloped data**: Data that is encrypted using the recipient's public key, ensuring only the intended recipient can decrypt and access it.
- **Signed and enveloped data**: Data that is both encrypted using the recipient's public key and signed using the sender's private key, providing confidentiality and integrity.
- **Signed data**: Data that is digitally signed using the sender's private key to ensure its integrity and authenticity but remains unencrypted.
- **Clear Signed data**: Data that is digitally signed using the sender's private key but remains unencrypted, allowing its contents to be viewed by anyone.

UDP does not perform any security checks or ensure the security of the connection. It is a connectionless protocol designed for simplicity and efficiency, but it does not provide any mechanisms for ensuring the security or integrity of the data being transmitted.

A typical networking packet contains a header, some payload, and a trailer.

The Transport Layer is responsible for maintaining end-to-end communications between hosts across the network.

The primary function of the Dynamic Host Configuration Protocol (DHCP) is to dynamically distribute IP addressing and configuration information to clients.

1. **Source MAC spoofing**: Falsifying the MAC address of a device to impersonate another on a network.

2. **Destination ARP spoofing**: Sending fake ARP messages to associate an attacker's MAC address with a different IP address, redirecting traffic.
3. **Destination address spoofing**: Forging the destination address of packets to deceive the recipient into processing them.
4. **Source address spoofing**: Altering the source address of packets to disguise the true origin, often used in malicious activities.

The following are considered an IP vulnerability

☑

No integrity checking

☑ ☐

Unencrypted Transmission

☑

No Source Authentication

Denial of service (DoS) and distributed denial of service (DDoS) attacks have the same effect. However, a DDoS attack _____.

☑

is launched from large numbers of hosts that have been compromised

---

FTP (File Transfer Protocol) is designed to send and receive files, but all transmissions are sent in the clear.

SMTP: Sends emails between servers.
FTP: Transfers files between client and server.
Telnet: Interactive text communication protocol.
POP: Retrieves email from a server to a client.

Blind IP Spoofing is:

"IP spoofing without knowing the ACK sequence pattern."

A common method used by attackers to perform session hijacking is "Network sniffing."

---

1. **Brute force attacks:** Automated guessing of passwords.
2. **Network sniffing:** Intercepting and analyzing data on a network.
3. **Cross-site scripting (XSS):** Injecting malicious scripts into web pages.
4. **SQL injection:** Exploiting web app vulnerabilities to manipulate databases.

A type of denial of service (DoS) attack is a SYN flood.

---

1. **SYN flood**: Floods a system with SYN requests to overwhelm it.
2. **Session hijack**: Unauthorized takeover of an active session.
3. **Spyware**: Malicious software gathering user information without consent.
4. **Eavesdropping**: Unauthorized interception of private communication.

AC

You

For an attacker to hijack a TCP session, they need to_____ does an attacker need to do to "enter" a TCP session? Determine the correct sequence number the server is expecting from the client Spoof the client's IP address All of the above Inject data into the session before the client sends its next packet

---

1. Man-in-the-middle attack: Intercepting and possibly altering communications between two parties.
2. Typo squatting: Registering a domain name similar to a popular website with the intent of capturing traffic.

3. URL hijacking: Redirecting traffic intended for one URL to a different destination.
4. Session hijacking: Covertly taking over a valid session to gain unauthorized access.

Sure, here are the definitions:

1. Man-in-the-middle attack: A type of cyberattack where the attacker intercepts and possibly alters communications between two parties who believe they are communicating directly with each other.

2. Typo squatting: A form of cybersquatting where someone registers a domain name similar to a popular or commonly visited website but with a slight variation, often a common misspelling, with the intent of capturing traffic intended for the legitimate site.

3. URL hijacking: A type of cyberattack where an attacker takes control of a Uniform Resource Locator (URL) and redirects traffic intended for the original URL to a different destination, usually a malicious website.

4. Session hijacking: A cyberattack where an attacker covertly takes over a valid session between a user and a host system, allowing the attacker to impersonate the user and gain unauthorized access to the system or information.

Sure!

SMTP: Simple Mail Transfer Protocol - A protocol used for sending and receiving email over the Internet.

DNS: Domain Name System - A hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

HTTP: Hypertext Transfer Protocol - An application protocol for distributed, collaborative, hypermedia information systems.

VoIP: Voice over Internet Protocol - A technology that allows users to make voice calls using a broadband Internet connection instead of a regular phone line.

Session hijacking refers to the unauthorized seizure of an ongoing communication session between two parties, often with the intent to gain unauthorized access to information or resources.

A web attack is a malicious attempt to disrupt or compromise the security, availability, or integrity of a website or web application. This can involve exploiting vulnerabilities in web servers, applications, or user interactions to gain unauthorized access, steal data, or cause other forms of harm.

Denial of service (DoS) is a cyber attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

The type of attack likely taking place in this scenario is **Session hijacking**. In session hijacking, an attacker takes control of a user's session after the user has successfully authenticated. By manipulating HTTP headers, the attacker can hijack the user's session and impersonate them, gaining unauthorized access to the user's account and possibly sensitive information.

- **XML injection**: Exploiting vulnerabilities in XML parsers or processors to inject malicious code or data into XML documents, potentially leading to security breaches.
- **Cross-site scripting (XSS)**: A type of security vulnerability that enables attackers to inject malicious scripts into web pages viewed by other users, allowing them to steal information or perform actions on behalf of the user.

- **Session hijacking**: Unauthorized seizure of an active session between a user and a web application, allowing an attacker to impersonate the user and gain unauthorized access.

- **SQL injection**: Exploiting vulnerabilities in web applications' SQL database queries to execute arbitrary SQL code, potentially enabling attackers to access, modify, or delete sensitive data.

---

1. **IP fragmentation**:
    - IP fragmentation is the process of breaking down large IP packets into smaller fragments to fit within the maximum transmission unit (MTU) size of a network. This fragmentation occurs when a packet is too large to traverse a network path without being divided into smaller pieces. Fragments are reassembled by the receiving host.
2. **Smurf**:
    - Smurf is a type of distributed denial-of-service (DDoS) attack that involves sending large amounts of ICMP echo request (ping) traffic to a network's broadcast address using a spoofed source IP address. This causes all hosts on the network to respond to the ping requests, overwhelming the victim's network with responses and causing it to become inaccessible.
3. **SYN flooding**:
    - SYN flooding is a type of denial-of-service (DoS) attack that exploits the three-way handshake process of the TCP protocol. In this attack, the attacker sends a large number of SYN (synchronize) requests to a target server but does not respond to the SYN-ACK (synchronize-acknowledgment) packets sent by the server, leaving the server's connection resources tied up and unable to establish legitimate connections.
4. **Ping flooding**:
    - Ping flooding, also known as ICMP flooding, is a type of denial-of-service (DoS) attack that involves sending a large volume of ICMP echo request (ping) packets to a target server or network. The goal of the attack is to overwhelm the target's network bandwidth or

processing capacity, causing it to become slow or unresponsive to legitimate requests.

An attacker can confirm that a port is listening by using a FIN Scan when:

- **The port does not respond.**

In a FIN Scan, the attacker sends a FIN (finish) packet to the target port. If the port is not listening, there will be no response. If the port is listening, the port should respond with an error response, indicating that the port is closed.

The type of scan considered the most reliable but can potentially reveal information about the attacker is the **Connect scan**.

A Connect scan fully connects to the target IP address and port in a complete TCP handshake. While reliable, this scan can potentially reveal information about the attacker because it establishes a full connection with the target, leaving more traces in the target's logs compared to other types of scans like SYN scans.

---

1. **SYN Scan**: This type of scan is also known as a half-open scan. It involves sending SYN requests to the target to gather information about open ports without completing the TCP handshake. When an open port is identified, the TCP handshake is reset before it can be completed. SYN scans are stealthier than full Connect scans but can potentially be detected by intrusion detection systems.
2. **Connect Scan**: A Connect scan fully connects to the target IP address and port in a complete TCP handshake. This method is reliable but can potentially reveal information about the attacker because it establishes a full connection with the target, leaving more traces in the target's logs compared to other types of scans like SYN scans.
3. **Ping Scan**: Also known as an ICMP echo request, a ping scan sends a single ICMP echo request from the source to the destination device. A response from an active device returns an ICMP echo reply, unless the IP address is not available on the network or the ICMP protocol is filtered. Ping scans are often used to check if a host is reachable.

4. **FIN Scan**: A FIN scan sends a FIN (finish) packet to the target. If the port is not listening, no response is received. If the port is listening, an error response is received. FIN scans are used to determine if ports are open or closed, and they exploit a subtle aspect of TCP behavior. However, some systems may not respond to FIN packets, making this scan less reliable in certain situations.

---

1. **SMTP (Simple Mail Transfer Protocol):** SMTP is a communication protocol used for transmitting email messages over the internet. It works between mail servers to send and receive emails. SMTP is a text-based protocol that operates on TCP port 25.
2. **Telnet:** Telnet is a network protocol used to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. It allows a user to remotely access and manage devices or systems over a network.
3. **POP (Post Office Protocol):** POP is a protocol used by email clients to retrieve email messages from a mail server. It allows users to download messages from the server to their local device for reading and storage. POP operates on TCP port 110.
4. **FTP (File Transfer Protocol):** FTP is a standard network protocol used to transfer files between a client and a server on a computer network. It provides a way for users to upload, download, and manage files on remote servers. FTP operates on TCP ports 20 and 21 for data transfer and control, respectively.

The protocol commonly used in the transfer of email but does not include protection against sniffing is **SMTP** (Simple Mail Transfer Protocol).

Session hijacking is:

A type of attack that involves intercepting and taking over an established session between a client and server.

In this attack, the attacker exploits vulnerabilities in the session management mechanism to gain unauthorized access to a legitimate user's

session. By doing so, the attacker can impersonate the user, access sensitive information, or perform malicious actions on behalf of the user without their knowledge.

The benefit of using asymmetric encryption among the options provided is:

"It provides many cybersecurity goals."

Asymmetric encryption, also known as public-key encryption, offers several advantages, including:

- Confidentiality: Public keys can encrypt messages, but only the corresponding private key can decrypt them, ensuring confidentiality.
- Authentication: Public keys can verify the sender's identity, as only the owner of the private key can produce a valid signature.
- Non-repudiation: Signatures generated with private keys can prove the sender's identity, preventing them from denying their actions.
- Key distribution: Asymmetric encryption eliminates the need for secure key exchange since public keys can be freely distributed.

Therefore, the correct option is that asymmetric encryption provides many cybersecurity goals.

In a symmetric cryptographic system, each pair of users needs a unique key. Since there are 50 users, each user needs a key to communicate securely with every other user.

The formula to calculate the number of pairs in a group of n users is:

$$\text{Number of pairs} = \frac{n \times (n-1)}{2}$$

Substituting $n = 50$ into the formula:

$$\text{Number of pairs} = \frac{50 \times (50-1)}{2} = \frac{50 \times 49}{2} = \frac{2450}{2} = 1225$$

So, the system has a total of 1225 pairs of keys. Therefore, the correct answer is 1225.

When developing a cryptographic algorithm to ensure that the message received is identical to the message originally sent, the goal is to provide **Integrity**. Integrity ensures that data is not altered without authorization, allowing recipients to verify that the received message has not been tampered with during transmission.

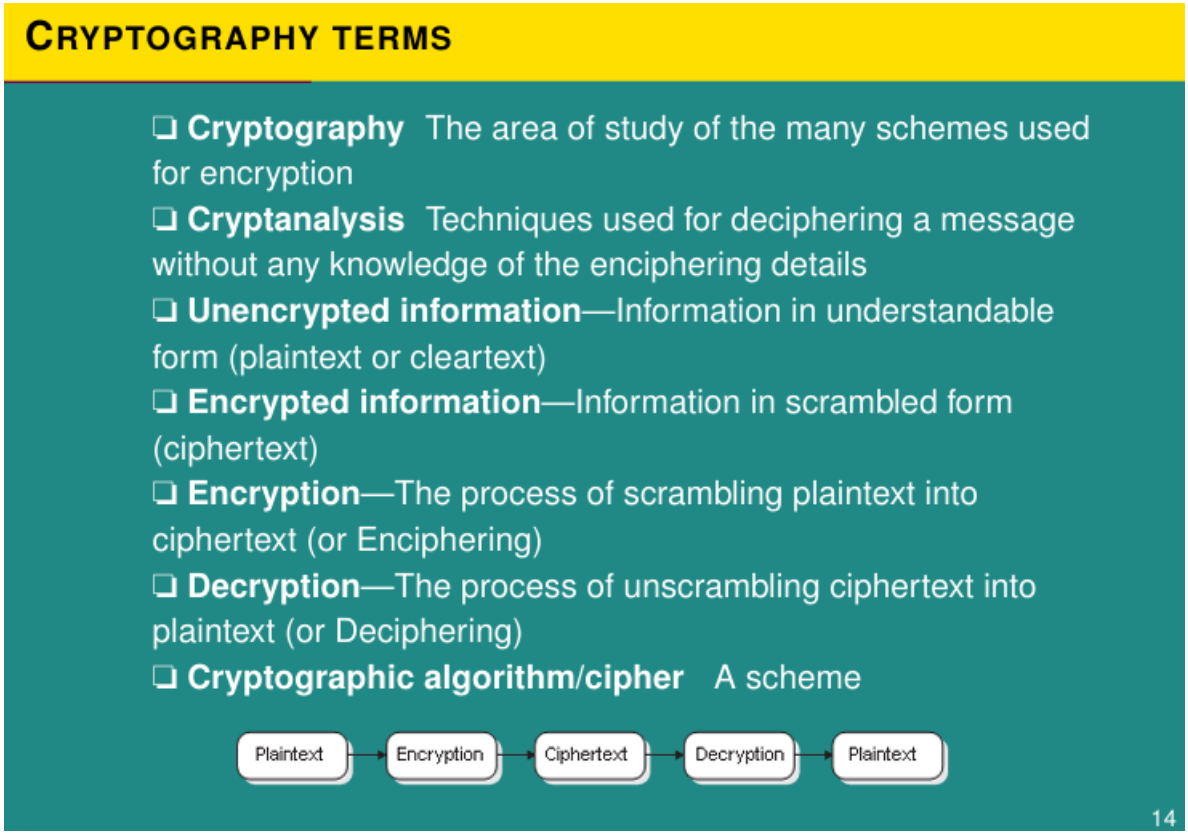
1. **Confidentiality**: Confidentiality in cryptography refers to the protection of data from unauthorized access or disclosure. It ensures that only authorized parties can access sensitive information.
2. **Integrity**: Integrity in cryptography refers to the assurance that data has not been altered or tampered with during transmission. It ensures that the data remains unchanged and trustworthy.
3. **Non-Repudiation**: Non-repudiation in cryptography refers to the ability to prove the origin of a message and prevent the sender from denying that they sent it. It provides assurance that the sender cannot later deny their involvement in the communication.
4. **Authentication**: Authentication in cryptography refers to the process of verifying the identity of a user or entity. It ensures that the parties involved in a communication are who they claim to be, preventing unauthorized access and impersonation.

1. **Ciphertext**: Encrypted text resulting from the encryption process, which transforms plaintext into an unreadable format using cryptographic algorithms and keys.
2. **Algorithm**: A step-by-step procedure or formula for solving a problem or accomplishing a task, often used in the context of computing to refer to a set of instructions for performing a specific task.

3. **Plain text**: The original, unencrypted text or data before any encryption or cryptographic processing has been applied.
4. **Key**: A piece of information used in conjunction with an algorithm (such as encryption or decryption) to transform plaintext into ciphertext or vice versa. Keys can be used to encrypt or decrypt data and are crucial for the security of cryptographic systems.

To decrypt the ciphertext "FDQW ZDLW IRU VXPPHU" encrypted using the Caesar cipher with a rotation value of 3, we simply need to shift each letter in the ciphertext three positions to the left in the alphabet.

So, the plaintext message is "CAUSE BACK FOR TESTING".



Sure, here are the definitions for each term:

1. **Cipher text**: This refers to the encrypted form of a message, which is produced using an encryption algorithm and a key. Cipher text appears as random or scrambled data, making it unintelligible without decryption.

2. **Algorithm**: An algorithm is a step-by-step procedure or set of rules used for solving a problem or accomplishing a task. In cryptography, algorithms are mathematical functions used to encrypt and decrypt data.

3. **Plain text**: Plain text is the original, unencrypted form of a message. It's the readable text before any encryption or encoding has been applied.

---

5. **Key**: In cryptography, a key is a piece of information (typically a string of bits) used to control the transformation of plain text into cipher text during encryption, and vice versa during decryption. The security of encrypted data often relies on the secrecy and complexity of the key.

Sure, here are the definitions:

1. **Secret key**: A key used in symmetric encryption, known only to the sender and receiver, used for both encryption and decryption of messages.

2. **Ciphertext**: The encrypted message produced as output after encryption. It appears as gibberish and is unreadable without decryption.

3. **Cryptanalysis**: The study and practice of analyzing information systems to study their hidden aspects in order to gain understanding or to recover the plaintext or key used for encryption.

5. **Plaintext**: The original, readable message before encryption or after decryption. It is the input to an encryption algorithm or the output of a decryption algorithm.

following statements are correct?

- [x] A Hash function computes the checksum to prevent forgery
- [x] A hash function is a one-way function
- [x] A Hash function detects if any tampering occurred during transmission

1. **MAC (Message Authentication Code):** A MAC is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. It is generated using a secret key and a message, and it ensures that the message has not been tampered with.
2. **HMAC (Hash-based Message Authentication Code):** HMAC is a specific type of MAC that involves a cryptographic hash function in combination with a secret key. It provides a way to verify both the integrity and authenticity of a message.
3. **SHA (Secure Hash Algorithm):** SHA is a family of cryptographic hash functions designed by the National Security Agency (NSA). It generates a fixed-size hash value from input data of arbitrary size. SHA functions are widely used in various security applications and protocols.

These terms are fundamental in cryptography and are often used in ensuring the security of communication and data integrity.

Symmetric encryption is the type of encryption that uses a single key for both encryption and decryption. So, the correct option is:

"A type of encryption that uses a single key for both encryption and decryption"

If a company with 50 users is using an asymmetric cryptographic system, it typically means that each user has a key pair consisting of a public key and a private key. So, for 50 users, there would be 50 pairs of keys. Therefore, the correct answer is:

100

1. **Access Control**: Access control is the process of protecting a resource so that it is used only by those allowed to. It involves mitigations put into place to protect a resource from threats, such as preventing unauthorized use.
2. **Logical Access Control**: Logical access control involves deciding which users can gain access to a system, monitoring their actions within that system, and influencing or restraining their behavior.
3. **Access Control Principles**: These are fundamental guidelines or rules that govern the implementation and operation of access control systems. They include principles such as need-to-know, least privilege, and separation of duties.
4. **Access Control Models**: Access control models are frameworks that dictate how subjects (users or processes) can access objects (resources or data). Examples include discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC).
5. **Authentication, Authorization & Accountability (AAA)**: AAA refers to the three core components of access control. Authentication verifies the identity of users, authorization determines what actions they are allowed to

perform, and accountability ensures that actions can be traced back to individuals.

6. **Policy Definition Phase**: In this phase, access control policies are established, defining who has access to what systems or resources. It is closely tied to the authorization phase.
7. **Policy Enforcement Phase**: In this phase, access requests are either granted or rejected based on the authorizations defined in the policy definition phase. It involves identification, authentication, and accountability mechanisms.
8. **Physical Access Control**: Physical access control involves controlling access to physical resources, such as buildings, rooms, or equipment, typically using mechanisms like keycards or biometric scanners.
9. **Subject**: In the context of access control, a subject is an entity (usually a user or a process) that requests access to an object.
10. **Object**: An object, in access control, refers to the resource or data that is being protected and accessed by subjects.
11. **Security Kernel**: The security kernel is the central component of a computer system that enforces access control policies. It intercepts access requests, consults access control rules, and logs access activities.
12. **Biometrics**: Biometrics refers to the use of unique physical or behavioral characteristics, such as fingerprints or voice patterns, to verify a person's identity.
13. **Tokens**: Tokens are physical or digital devices used for authentication, such as smart cards or hardware tokens.
14. **Passwords**: Passwords are secret character strings used to authenticate users.
15. **Single Sign-On (SSO)**: Single sign-on is a mechanism that allows users to access multiple systems or applications with a single set of credentials.
16. **Kerberos**: Kerberos is a network authentication protocol that uses symmetric-key cryptography to provide secure authentication between clients and servers.

17. **RADIUS**: RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol used for remote user authentication and authorization.
18. **TACACS+**: TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol that provides authentication, authorization, and accounting services, often used in network devices.
19. **DIAMETER**: Diameter is a protocol that extends the functionality of RADIUS for authentication, authorization, and accounting in IP-based networks.
20. **Attribute-based Access Control (ABAC)**: ABAC is an access control model that determines permissions based on attributes associated with the user, the resource, and the current context.
21. **Discretionary Access Control (DAC)**: DAC is an access control model where access rights are determined by the owner of the resource.
22. **Mandatory Access Control (MAC)**: MAC is an access control model where access rights are determined by security labels and security clearances.
23. **Rule-based Access Control (RBAC)**: RBAC is an access control model where access rights are determined by a set of rules or policies.
24. **Non-Discretionary Access Control**: Non-Discretionary Access Control is a type of access control where access rules are managed by security administrators rather than resource owners.

Access is granted based on security clearances.

In a mandatory access control (MAC) system, access is determined by comparing security labels associated with subjects (users) and objects (resources). These security labels represent security clearances, which indicate the sensitivity or classification level of the resource. Users are granted access based on their security clearances, ensuring that only those with appropriate authorization can access sensitive financial transactions. The access decision is not based on factors such as job function, role, or

owner's permission, but rather on the security clearance level assigned to the user and the resource.

1. **Access Control**: The process of protecting resources to ensure they are used only by authorized entities and to prevent unauthorized use.
2. **Logical Access Control**: Controls access to computer systems, networks, and data based on user credentials and authentication methods.
3. **Access Control Principles**: Fundamental guidelines for managing access to resources, including identification, authentication, authorization, and accountability.
4. **Access Control Models**: Frameworks that dictate how subjects access objects and enforce access control rules and objectives. Examples include Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC).
5. **Authentication, Authorization & Accountability (AAA)**: A security framework comprising three components:
    - **Authentication**: Verifying the identity of users or entities attempting to access resources.
    - **Authorization**: Granting or denying access to resources based on the permissions assigned to authenticated users.
    - **Accountability**: Tracking and logging user activities to ensure that actions can be traced back to specific individuals or entities for auditing and accountability purposes.

1. **Theoretical access control**: This term doesn't have a commonly accepted definition in the context of access control. It might refer to theoretical models or concepts related to access control, but it's not a standard term.
2. **Physical access control**: Physical access control refers to the measures taken to restrict access to physical locations, such as buildings, rooms, or data centers. This can include methods like keycards, biometric scanners, or security guards.

3. **Security kernel**: A security kernel is the central component of an operating system responsible for enforcing security policies and access controls. It controls access to system resources based on predefined rules and policies.
4. **Logical access control**: Logical access control involves controlling access to computer systems and data based on user credentials and permissions. This typically includes methods such as username/password authentication, access control lists (ACLs), and role-based access control (RBAC).

1. **Tree**: In the context of file organization in Windows, a tree represents the hierarchical structure of directories or folders, with each directory branching out into subdirectories or files.
2. **Structure**: In the context of access control or file organization, structure refers to the way data or resources are organized or arranged, often implying a systematic layout or framework.
3. **DAG**: DAG stands for Directed Acyclic Graph. In file organization, it's a type of data structure that represents relationships between files or directories in a network or file system, where each edge represents a link between files or directories.
4. **Files & Folders**: In computing, files contain data or information stored under a specific name, while folders (also known as directories) provide a way to organize files in a hierarchical structure.

Sure, here are the definitions:

1. **Dynamic Biometric**: This refers to biometric authentication methods that involve the measurement and analysis of unique biological traits or behavioral characteristics of individuals, such as keystroke dynamics, voice patterns, or signature motions, to verify their identity.

2. **Synchronous Token**: A synchronous token is a type of authentication token that calculates a number at both the authentication server and the

token itself. This number is then compared to verify the identity of the user. Synchronous tokens often use time-based or event-based synchronization.

3. **Asynchronous Token**: An asynchronous token is another type of authentication token that does not involve complex calculations. Instead, it relies on the user physically possessing the token as proof of identity. USB tokens and smart cards are examples of asynchronous tokens.

5. **Static Biometric**: This refers to biometric authentication methods that involve the measurement of static physical characteristics of individuals, such as fingerprints, iris patterns, facial features, or hand geometry, to verify their identity. These characteristics do not change over time and are used for authentication purposes.

Sure! Here are shortened definitions for each:

1. **RADIUS**: Centralized protocol for remote user authentication, authorization, and accounting.

2. **TACACS+**: Advanced protocol for centralized AAA services with TCP transport.

3. **TACACS**: Older version of TACACS+, providing similar AAA functions.

5. **Diameter**: Protocol overcoming limitations of RADIUS, offering enhanced security and support for diverse networks.

The following security principles are principle that any access control models is built on?

- [ ] Seperation of privilege
- [ ] least privilege
- [ ] Need to know

1. **ABAC (Attribute-Based Access Control)**: ABAC is an access control model where access rights are determined by evaluating attributes associated with the user, the resource being accessed, and the current environmental conditions.
2. **RBAC (Role-Based Access Control)**: RBAC is an access control model where access rights are granted based on the roles that users have within the system. Users are assigned roles, and access permissions are associated with these roles.
3. **DAC (Discretionary Access Control)**: DAC is an access control model where the owner of a resource has full control over who can access that resource and what actions they can perform on it. Access is based on the discretion of the resource owner.
4. **MAC (Mandatory Access Control)**: MAC is an access control model where access rights are determined by the system and are based on security labels assigned to subjects and objects. Access is granted or denied based on the security clearance level of the subject and the sensitivity level of the object.

- **Single sign-on (SSO)**: A mechanism where users have one password for all systems and applications they need to access, simplifying the authentication process.
- **Asynchronous token**: An authentication method where a physical token, such as a USB token or smart card, is used for authentication without the need for calculations at the device.

- **Synchronous token**: An authentication method where a token, such as a time-based or event-based token, generates a number that both the authentication server and the device can calculate and verify.
- **Biometrics**: An authentication method that uses physical or behavioral characteristics unique to an individual, such as fingerprints, facial recognition, or voice patterns, for authentication.

Certainly! Here are the definitions:

1. **Access Control**: The process of protecting a resource so that it is used only by those allowed to, often involving mitigations to prevent unauthorized use.

2. **Logical Access Control**: The process of deciding which users can access a system, monitoring their activities, and influencing their behavior on that system.

3. **Access Control Principles**: Core concepts governing how access to resources is managed, including identification, authentication, authorization, and accountability (AAA).

4. **Access Control Models**: Frameworks dictating how subjects access objects, typically based on security operation principles such as need to know, least privilege, and separation of privileges.

5. **Authentication, Authorization & Accountability (AAA)**: Three essential components in access control systems, where authentication verifies user identities, authorization determines access rights, and accountability tracks actions for audit purposes.

6. **Policy Definition Phase**: The stage where access policies are established, defining who has access to what systems or resources.

7. **Policy Enforcement Phase**: The stage where access requests are granted or rejected based on the authorizations defined in the policy definition phase.

8. **Physical Access Control**: Controls access to physical resources, often using methods like keycards or biometrics.

9. **Security Kernel**: The central point of access control in computer systems, enforcing access control policies and logging access requests.

10. **Logical Access Control Solutions**: Technologies and methods used to control logical access, such as biometrics, tokens, passwords, and single sign-on.

11. **Authentication Types**: Various methods of verifying user identities, including authentication by knowledge, ownership, characteristics, and location.

12. **Discretionary Access Control (DAC)**: Access control where the owner decides who can access resources.

13. **Mandatory Access Control (MAC)**: Access control based on comparing security labels with security clearances.

14. **Role-Based Access Control (RBAC)**: Access control based on user roles within a system.

15. **Attribute-Based Access Control (ABAC)**: Access control based on user and resource attributes, allowing for flexible authorization rules.

16. **AAA Protocols**: Protocols used for authentication, authorization, and accounting, such as RADIUS, TACACS+, and DIAMETER.

17. **Single Sign-On (SSO)**: Authentication mechanism where users have one password for multiple systems.

18. **Kerberos**: Authentication protocol using symmetric-key cryptography to provide authentication for client/server applications.

19. **Federated Identities**: System where users can log in with credentials from a trusted service, avoiding the need for multiple accounts.

20. **Access Control Matrix**: A representation showing the access rights of subjects for objects in a system.

21. **Open Policy**: Access policy where access is granted by default unless explicitly restricted.

22. **Closed Policy**: Access policy where access is restricted by default, requiring explicit permissions for access.

23. **Closed with Negative Authorization**: Access policy where access is restricted by default, and certain entities are explicitly denied access.

24. **Open with Negative Authorization**: Access policy where access is granted by default, but certain entities are explicitly denied access.

1. **Access Control Models**: Frameworks that dictate how subjects access objects and enforce rules and objectives. Examples include Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC).
2. **Centralized AAA**: Authentication, Authorization, and Accounting (AAA) systems where these functions are managed by centralized servers. Examples include RADIUS, TACACS+, and DIAMETER.
3. **Decentralized AAA**: Authentication, Authorization, and Accounting (AAA) systems where access control is managed closer to the users, often at the local level.
4. **Access Control Types**: Methods and mechanisms used to control access to resources. Examples include Physical Access Control, Logical Access Control, and Attribute-Based Access Control.

Sure, here are the definitions:

1. **Diameter**: A protocol that builds upon the functionality of RADIUS, providing authentication, authorization, and accounting (AAA) functionality. It uses TCP as its transport protocol and offers more capabilities than RADIUS.

2. **RADIUS (Remote Authentication Dial-In User Service)**: A client/server protocol and software that enables remote access users to communicate with a central server to authorize their access to the requested system or service. It provides centralized access control for network devices.

3. **Federated Identities**: A single sign-on mechanism where users can log in with their credentials from one service to access multiple services without the need to create new user accounts for each service. Examples include using credentials from Facebook or Google to access other services.

5. **Kerberos**: A network authentication protocol that uses tickets to provide secure authentication for client/server applications. It authenticates users and services on a network to ensure secure communication.

1. **Firewall Systems**: A security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.

2. **Intrusion Detection Systems (IDS)**: A security tool that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.
3. **Intrusion Prevention Systems (IPS)**: A security technology that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.
4. **Honeypots**: A security mechanism set up to detect, deflect, or counteract attempts at unauthorized use of information systems. It consists of data (often trap data) that appears to be a legitimate part of the site or network but is actually isolated and monitored and that seems to contain information or a resource of value to attackers.
5. **Packet Filtering Firewall**: A type of firewall that filters network packets based on predefined rules such as source and destination addresses, ports, and protocols.
6. **Stateful Filtering Firewall**: A type of firewall that monitors the state of active connections and makes decisions based on the context of the traffic.
7. **Application Proxy Firewall**: A type of firewall that acts as an intermediary for requests from clients seeking resources from other servers. It inspects traffic at the application layer and can provide additional security features.
8. **Circuit-Level Gateway**: A type of firewall that works at the session layer of the OSI model and sets up two separate TCP connections: one between the client and itself, and another between itself and the server.
9. **Host-Based Firewall (Personal Firewall)**: A firewall that is installed and operates on individual hosts (computers) to control traffic to and from that host.
10. **Intrusion Detection**: The process of monitoring events occurring in a computer system or network and analyzing them for signs of possible incidents, violations, or imminent threats to security policies.
11. **Anomaly Detection**: A method of intrusion detection that involves establishing a baseline of normal behavior and identifying deviations from this baseline that may indicate suspicious or malicious activity.
12. **Signature/Heuristic Detection**: A method of intrusion detection that involves comparing observed events or patterns against a database of

known attack signatures or heuristic rules to identify known malicious behavior.

13. **Host-Based Intrusion Detection System (HIDS)**: An intrusion detection system that monitors and analyzes the internals of a computing system rather than just the network packets.
14. **Network-Based Intrusion Detection System (NIDS)**: An intrusion detection system that monitors network traffic for suspicious activities or policy violations.
15. **Host-Based Intrusion Prevention System (HIPS)**: An intrusion prevention system that monitors and controls activity at the host level, typically on individual computers or servers.
16. **Network-Based Intrusion Prevention System (NIPS)**: An intrusion prevention system that monitors and controls activity at the network level, typically at key points within the network infrastructure.
17. **Honeynets**: A network of honeypots designed to detect and monitor unauthorized access attempts and capture information about the methods and tools used by attackers.
18. **Low Interaction Honeypot**: A honeypot that emulates only the services and protocols required to attract and monitor potential attackers, offering limited interaction with them.
19. **High Interaction Honeypot**: A honeypot that emulates a complete computing environment, providing a realistic target for attackers and allowing extensive interaction with them.
20. **Hybrid Interaction Honeypot**: A honeypot that combines features of both low and high interaction honeypots, offering a balance between realism and resource consumption.

1. **Intrusion Detection System (IDS)**: A hardware or software device that analyzes received traffic to identify possible security intrusions. IDSs gather and analyze information from various areas within a computer or a network to identify potential security breaches.
2. **Intrusion Prevention System (IPS)**: An extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity.

IPSs can be host-based, network-based, or distributed/hybrid and use various techniques such as signature-based detection, anomaly detection, and protocol analysis to identify and mitigate threats.

3. **Firewall**: A security system, either hardware or software-based, that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls establish a barrier between a trusted internal network and an untrusted external network (like the internet) to prevent unauthorized access and protect against malicious activities.
4. **Anti-Virus**: Software designed to detect, prevent, and remove malicious software (malware) from a computer or network. Antivirus programs scan files and monitor the system's behavior to identify and eliminate viruses, worms, Trojans, and other types of malware.

- **Intrusion Detection System (IDS):** A hardware or software device that analyzes received traffic to identify possible security intrusions. IDSs can detect unauthorized access, misuse, and anomalies in network or system activity.
- **Intrusion Prevention System (IPS):** An extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity. IPSs can actively respond to security threats by blocking or filtering malicious traffic.
- **Firewall:** A security device or software application that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the internet.
- **Anti-Virus:** Software designed to detect, prevent, and remove malicious software, including viruses, worms, and other types of malware, from computers and networks. Anti-virus programs scan files and processes for known patterns or signatures of malicious code.

Certainly!

1. **Circuit-level gateway firewall**: A type of firewall that operates at the session layer of the OSI model and works by monitoring TCP handshakes between packets to determine whether to allow or deny traffic. It does not inspect the contents of the packets, making it less secure but faster in terms of processing.

2. **Packet filtering firewall**: A firewall that examines packets of data as they pass through the network and makes decisions to allow or deny their transmission based on pre-defined rules such as source and destination IP addresses, port numbers, and protocols. It operates at the network layer (Layer 3) of the OSI model.

3. **Content filtering firewall**: A type of firewall that inspects the actual contents of data packets to filter or block traffic based on keywords, file types, URLs, or other content-related criteria. It is often used to enforce acceptable use policies, prevent malware downloads, and restrict access to certain websites or services.

5. **Application-level gateway firewall**: Also known as a proxy firewall, it operates at the application layer (Layer 7) of the OSI model and acts as an intermediary between client applications and the internet. It inspects incoming and outgoing traffic at the application level, providing deep packet inspection and granular control over application-specific protocols. This type of firewall offers enhanced security but may introduce latency due to additional processing.

1. **Modification**: Unauthorized alteration of system files, settings, or configurations, typically done by malware to compromise system integrity or security.
2. **Trojan**: A type of malicious software that disguises itself as legitimate software to deceive users into installing it. Once installed, trojans can perform various harmful actions, such as stealing sensitive information, damaging files, or giving attackers unauthorized access to the system.
3. **Privilege escalation**: The unauthorized act of gaining higher levels of access or privileges on a system or network than originally intended by the system administrator or owner. Attackers exploit vulnerabilities to elevate their privileges, allowing them to perform actions they would not normally be able to do.
4. **Buffer overflow**: A software vulnerability that occurs when a program writes more data to a buffer, or temporary storage area, than it was allocated to hold. This can lead to the overwriting of adjacent memory locations, potentially causing the program to crash or allowing attackers to execute arbitrary code and take control of the system.

1. **User Identity:** Refers to the identification of individuals or entities accessing a system or network. User identity is typically established through authentication mechanisms such as usernames, passwords, biometrics, or security tokens. Access control systems use user identity to determine permissions and restrictions for accessing resources.
2. **Network Activity:** Describes the interactions and communications occurring within a network infrastructure. Network activity includes data transmission, device connections, data routing, and any other operations involving networked devices. Monitoring network activity is essential for detecting anomalies, intrusions, or malicious behavior.
3. **IP Addresses:** Unique numerical labels assigned to devices connected to a network that use the Internet Protocol (IP) for communication. IP addresses serve as identifiers for both source and destination devices in data

transmission. IPv4 addresses are 32-bit numerical values, while IPv6 addresses are 128-bit hexadecimal values.

4. **Application Protocols:** Sets of rules and conventions governing the exchange of data between software applications over a network. Application protocols define the format, syntax, semantics, and synchronization of data exchanged between applications. Examples of application protocols include HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and DNS (Domain Name System).

Certainly, here are the definitions for each type of firewall:

1. **Host-based firewall**: A host-based firewall is a software application or component installed on an individual computer or device to monitor and control incoming and outgoing network traffic based on predetermined security rules. It operates at the operating system level and provides protection specific to the host where it is installed.

2. **Application-level gateway firewall**: Also known as a proxy firewall or application proxy, this type of firewall operates at the application layer (Layer 7) of the OSI model. It mediates communication between internal and external networks by examining and filtering messages at the application level. It offers granular control over specific applications and protocols, often providing advanced features like content filtering and caching.

3. **Circuit-level gateway firewall**: A circuit-level gateway operates at the session layer (Layer 5) of the OSI model and works by monitoring and validating TCP handshakes between internal and external networks. Rather than inspecting the contents of packets, it establishes and manages

connections based on predefined access control policies. It provides basic security by verifying session information but lacks the deep packet inspection capabilities of other firewall types.

4. **Packet filtering firewall**: Packet filtering firewalls operate at the network layer (Layer 3) or transport layer (Layer 4) of the OSI model and examine packets of data as they pass through the firewall. They filter packets based on predefined rules, such as source and destination IP addresses, ports, and protocols. Packet filtering firewalls are efficient and can provide basic security, but they offer limited visibility into the contents of packets and may not detect more sophisticated attacks.

For the scenario described, the best choice would be an **Application-level gateway firewall**. Here's why:

1. **Application-level gateway firewall**: This type of firewall operates at the application layer (Layer 7) of the OSI model, allowing it to inspect and filter traffic based on specific applications and protocols. It can enforce policies to prevent employees from accessing certain external applications by examining the content of packets and making decisions based on the application-level data. This granular control over applications makes it suitable for restricting access to specific external services while still allowing legitimate network traffic to pass through.

While the other firewall types mentioned also have their advantages, such as Packet filtering firewall for basic traffic filtering and Circuit-level gateway firewall for session-level control, they may not offer the same level of application-specific control and filtering capabilities as an Application-level gateway firewall. Additionally, a stateless inspection firewall, also known as

a packet filtering firewall, lacks the ability to inspect the contents of packets beyond basic header information, making it less suitable for enforcing application-specific policies.

classification of firewall.

Here's a brief explanation of the other types:

1. **Stateful filtering firewall**: This type of firewall monitors the state of active connections and makes decisions based on the context of the traffic, such as whether it is part of an established connection or a new connection attempt.
2. **Packet filtering firewall**: Packet filtering firewall examines packets of data as they pass through the firewall and makes decisions to allow or deny them based on predefined rules, typically considering attributes like source and destination IP addresses, port numbers, and protocols.
3. **Application proxy firewall**: Also known as an application-level gateway firewall, this type operates at the application layer of the OSI model and can inspect and filter traffic based on specific applications and protocols. It provides more granular control over network traffic compared to packet filtering firewalls by analyzing the content of packets at the application layer.

Certainly, here are definitions for each of the terms:

1. **Sandbox-based**: A sandbox-based intrusion prevention system (IPS) operates by executing potentially malicious code in an isolated environment, known as a sandbox, to observe its behavior without risking harm to the production network. This method allows the system to analyze

the behavior of suspicious files or programs in a controlled environment to determine if they pose a threat.

2. **Anomaly-based**: An anomaly-based intrusion prevention system (IPS) establishes a baseline of normal network behavior by monitoring and analyzing network traffic over a period of time. It then compares current activity against this baseline to identify deviations that may indicate potential security threats. Anomaly-based IPS can detect unknown or previously unseen attacks by flagging unusual patterns or behaviors that deviate from the norm.

3. **Protocol Analysis**: Protocol analysis refers to the examination and interpretation of network protocol data to detect abnormalities or violations. In the context of intrusion prevention systems (IPS), protocol analysis involves scrutinizing network traffic at the protocol level to identify suspicious or unauthorized activities. This may include identifying non-compliant behavior, malformed packets, or deviations from standard protocol specifications.

4. **Heuristic-based**: Heuristic-based intrusion prevention systems (IPS) use rules, algorithms, or statistical methods to identify potential security threats based on known patterns or characteristics of attacks. Unlike signature-based systems that rely on specific signatures or patterns of known threats, heuristic-based IPS can detect previously unseen attacks by recognizing general attributes or behaviors associated with malicious activity. This approach allows heuristic-based IPS to provide protection against emerging or zero-day threats.

Sure, here are the definitions for each term:

1. **Internet networks**: Refers to the interconnected global network of computers and other devices that communicate using the Internet Protocol (IP). It encompasses a vast array of networks, including public, private, academic, business, and government networks.

2. **External networks**: In the context of an organization, external networks refer to networks that are outside the organization's internal infrastructure. These networks may include connections to the internet, connections to partner organizations, or connections to remote offices.

3. **Perimeter**: In the context of network security, the perimeter refers to the boundary or edge of a network where it interfaces with external networks such as the internet. It is the first line of defense against unauthorized access and cyber threats.

4. **Public information**: Public information refers to data or content that is freely available and accessible to anyone without restrictions. It may include information published on websites, in public databases, or through other public channels.

1. **Internet networks:** Refers to the interconnected networks that use the Internet Protocol Suite (TCP/IP) to communicate with each other globally.
2. **External networks:** Networks that exist outside of an organization's internal network infrastructure. These can include the internet, partner networks, or other networks not controlled by the organization.
3. **Perimeter:** In the context of network security, the perimeter refers to the boundary between an organization's internal network and external

networks, typically where security measures such as firewalls are implemented to control access.
4. **Public information:** Information that is accessible to or intended for the general public. This can include information published on websites, social media, or other publicly available sources.

Certainly! Here are the definitions for the terms provided:

1. **Compromised**: In the context of network security, "compromised" refers to a state where a system, device, or network has been successfully breached or infiltrated by unauthorized entities. Once compromised, the integrity, confidentiality, or availability of the system may be compromised, and unauthorized activities, such as data theft, malware installation, or unauthorized access, may occur.

2. **Protected**: "Protected" indicates a state in which systems, networks, or resources are safeguarded against potential threats, vulnerabilities, or risks. It implies the implementation of security measures, such as firewalls, intrusion detection systems, encryption, access controls, and security policies, to prevent unauthorized access, exploitation, or damage. Protected systems are actively defended against potential attacks and vulnerabilities.

3. **Safe**: "Safe" denotes a condition in which systems, environments, or operations are free from harm, danger, or risk. It implies that adequate security measures have been implemented to mitigate or eliminate potential threats and vulnerabilities effectively. Safe systems ensure the integrity, confidentiality, and availability of data and resources, minimizing the likelihood of unauthorized access, data breaches, or disruptions.

4. **Working**: "Working" simply refers to the operational state of a system, device, or network, indicating that it is functioning correctly and performing its intended tasks or functions as expected. It implies that the system is operational, responsive, and capable of carrying out its designated operations or activities without any significant issues or malfunctions.

Sure, here are the definitions for the terms provided:

1. **Sandbox-based IPS**: A sandbox-based IPS relies on a sandbox environment to analyze and execute suspicious files or code in a controlled and isolated environment. It observes the behavior of these files or code and determines if they pose a threat based on their actions within the sandbox. Sandboxing helps in detecting and preventing zero-day attacks and other previously unknown threats by analyzing their behavior rather than relying on predefined signatures or patterns.

2. **Heuristic-based IPS**: Heuristic-based IPS uses rules and algorithms to identify potentially malicious behavior based on general characteristics or patterns rather than specific signatures. It looks for deviations from normal behavior and flags activities that appear suspicious or anomalous. While heuristic-based detection can detect previously unknown threats, it may also generate false positives if legitimate activities resemble suspicious behavior.

4. **Anomaly-based IPS**: Anomaly-based IPS establishes a baseline of normal network behavior by analyzing historical data or observing current network traffic patterns. It then identifies deviations or anomalies from this baseline, which may indicate potential security

threats or attacks. Anomaly-based detection is effective against new and evolving threats but may require fine-tuning to reduce false positives.

5. The Heuristic-based IPS is considered less effective than the Anomaly-based IPS.
7.

4. **Protocol Analysis IPS**: Protocol analysis IPS examines network protocols to detect abnormalities or violations in the communication patterns between network entities. It analyzes the headers and payloads of network packets to ensure compliance with protocol specifications and detect any unauthorized or suspicious activities. Protocol analysis IPS can identify protocol-level attacks and unauthorized protocol usage.

In the context of the given statement, since heuristic-based IPS relies on general rules and patterns, it may be considered less effective than anomaly-based IPS, which can detect deviations from normal behavior more accurately by establishing a baseline of expected network activity.

The "Perimeter-based" intrusion prevention system is not typically considered a distinct type of intrusion prevention system.

- Network-based IPS: Monitors network traffic at selected points on a network and attempts to block or prevent detected malicious activity. It operates at the network level, inspecting packets as they pass through the network.

- Hybrid-based IPS: A hybrid IPS combines features of both network-based and host-based IPS solutions. It can provide comprehensive protection by monitoring both network traffic and activity on individual hosts.
- Host-Based IPS: Installed on individual hosts or devices, a host-based IPS monitors the activity and behavior of applications and processes running on that host. It can detect and prevent attacks targeting the host itself.
- Perimeter-based IPS: This term is less commonly used compared to the others listed. However, a perimeter-based IPS typically refers to an IPS deployed at the network perimeter, where it can monitor traffic entering or exiting the network. It focuses on protecting the network boundary from external threats.

CRYPTANALYSIS METHODS

❏ **Brute Force Attack**: This method involves trying every possible key until the correct one is found. It is often time-consuming and requires signifcant computational power, especially against systems with long and complex keys.

❏ **Dictionary Attack**: This method involves the attacker using a list of common words, phrases, and previously leaked passwords to attempt to guess a password.

❏ **Frequency Analysis**: This technique is particularly effective against simple substitution ciphers. It involves analysing the frequency of characters or groups of characters in the ciphertext and comparing them to the expected frequencies in the language of the plaintext.

❏ **Known Plaintext Attack**: If the attacker has access to both the plaintext and its corresponding ciphertext, they might be able to deduce the key or identify a weakness in the encryption algorithm.

❏ **Differential Cryptanalysis**: This method involves analysing the differences in the input that lead to differences in the output. It’s often used against block ciphers to fnd a correlation that can help in deducing the key.

❑ **Rainbow Table Attack**: This method is used against hash functions and involves using precomputed tables of hash values to fnd plaintexts that produce certain hash values.

❑ **Quantum Computing:** Though still in its infancy, quantum computing poses a potential future threat to traditional cryptographic algorithms, as it could theoretically break many of the current encryption methods.

HASH AND DIGITAL SIGNATURE

❑ Digital signatures combine public key cryptography and hashing.

❑ Digital signatures (certifcates) are stored in a public Key Infrastructure domain

❑ Creating a digital signature of existing data requires two main steps:

1 The message or information to be sent is passed through a hashing algorithm that creates a hash to verify the integrity of the message.

2 The hash is passed through the encryption process using the sender’s private key as the key in the encryption process.

❑ The sender then sends the signature along with the original unencrypted message to a recipient who can reverse the process.

Data Encryption Standard (DES) and 3DES

- Data Encryption Standard (DES)
  - Developed by IBM and adopted by NIST in 1977
  - 64-bit blocks and 56-bit keys
  - Small key space makes exhaustive search attack feasible since late 90s
  - Is a symmetric encryption Algorithm
- Triple DES (3DES)
  - Nested application of DES with three different keys K_A, K_B, and K_C
  - Effective key length is 168 bits, making exhaustive search attacks unfeasible
  - $C \quad EK_C(DK_B(E_KA(P)))$; $P \quad DK_A(E_KB(D_KC(C)))$
    - Note the Encrypt and Decrypt combination
  - Equivalent to DES when KA=KB=KC (backward compatible)

KEY DISTRIBUTION TECHNIQUES

- **Paper distribution**
  - It requires no technology to use.
  - However, it does require a person to do something to install the key.
- **Digital distribution**
  - can be in the form of CDs or email but must be protected during transmission.
  - For electronic distribution, a higher-level key, must protect the keys in transit and storage.
  - The Internet Security relies on this form of Keys distribution called public key infrastructure (PKI).
- **Hardware distribution**
  - Keys Distributed via **hardware** such as a smart card, or a plug-in module.
  - The advantage is that no copies exist outside of these components.

PURPOSE OF PUBLIC KEY INFRASTRUCTURE (PKI)

- Provides a mechanism through which two parties can establish a trusted relationship even if the parties have no prior knowledge of one another
- PKI brings trust, integrity, and security to electronic transactions
- PKI framework used to manage, create, store, and distribute keys and digital certificates

- Digital signatures combine public key cryptography and hashing.
- Digital signatures (certificates) are stored in a public Key Infrastructure domain
- Creating a digital signature of existing data requires two main steps:
  1. The message or information to be sent is passed through a hashing algorithm that creates a hash to verify the integrity of the message.
  2. The hash is passed through the encryption process using the sender's private key as the key in the encryption process.
- The sender then sends the signature along with the original unencrypted message to a recipient who can reverse the process.

HASH AND DIGITAL SIGNATURE (CONT.)

- When the receiver receives the message with the signature, that receiver will first validate the identity of the sender and then retrieve the public key to decrypt the signature.
- Once the signature is decrypted, the resulting cleartext is actually the message hash from the sender.
- Then, the receiver will run the same hashing algorithm to generate a local hash of the received message.
- Then, the hashes, both the original and the one newly created, should match.
  - If they do not, the message has been altered because the sender calculated the hash.
  - If the hash values do match, the message has been proven to come from the stated sender and has not been altered.

DIGITAL CERTIFICATES

- To ensure compatibility between CAs, digital certificates are commonly built and formatted using the X.509 certificate standard.
  - X.509 certificate is used to bind the identity of owner of a public key containing information such as the public key, the hostname, the issuer, etc..

ADVANCED ENCRYPTION STANDARD (AES)

- Advanced Encryption Standard (AES)
  - Selected by NIST in 2001 through open international competition and public discussion
  - 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
  - Exhaustive search attack not currently possible
  - AES-256 is the symmetric encryption algorithm of choice

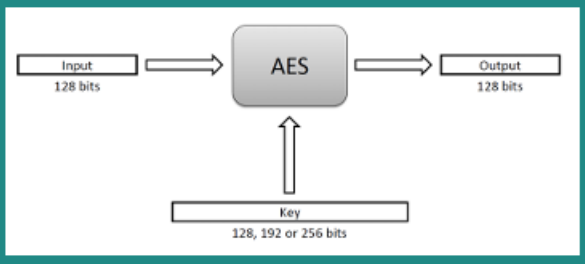


Figure 1: The Advanced Encryption Standard (AES)

ASYMMETRIC CIPHERS: RSA

- RSA (Rivest–Shamir–Adleman) is a Public key Cryptosystem that uses Block Cipher.

have a look at this example online RSA Visual

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

RIVEST CIPHER 4 (RC4)

- Designed in 1987 by Ron Rivest for RSA Security
- Trade secret until 1994
- Is a Symmetric encryption algorithm with up to 2,048 bits keys
- Simple algorithm and remarkable speed

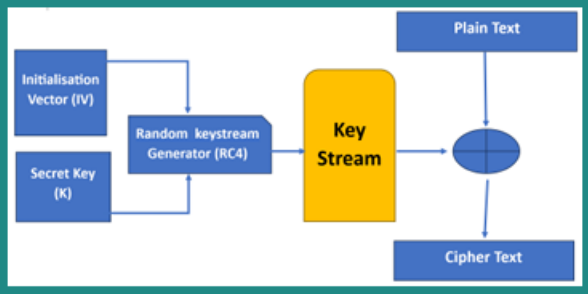
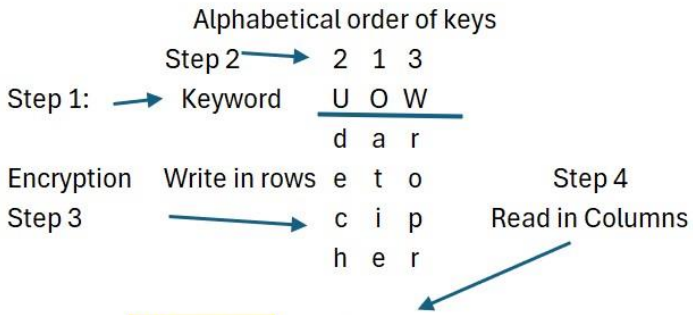


Figure 5: Rivest Cipher 4 (RC4)

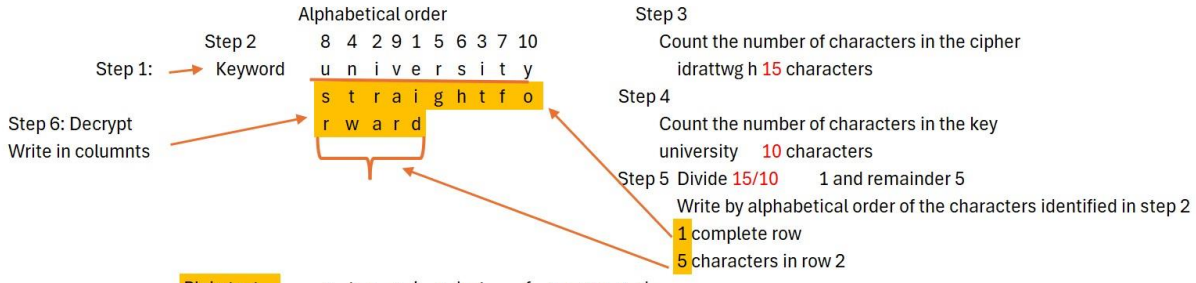
Answers based on Last year ICT

The encryption of the following message "dare to cipher" using the keyword "UOW and the transposition method will result in the cipher text _____



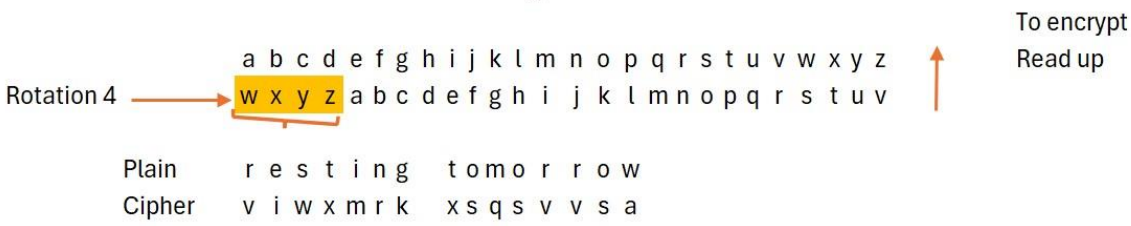
Correct answer: atie de chropr

The decryption of the cipher message "idrattwg hfsraro" using the keyword "university" and the transposition method will result in the plain text_____

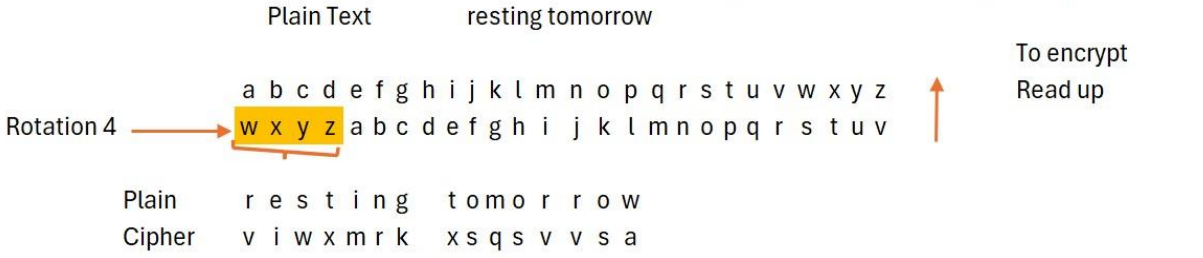


Correct answer: straight forward

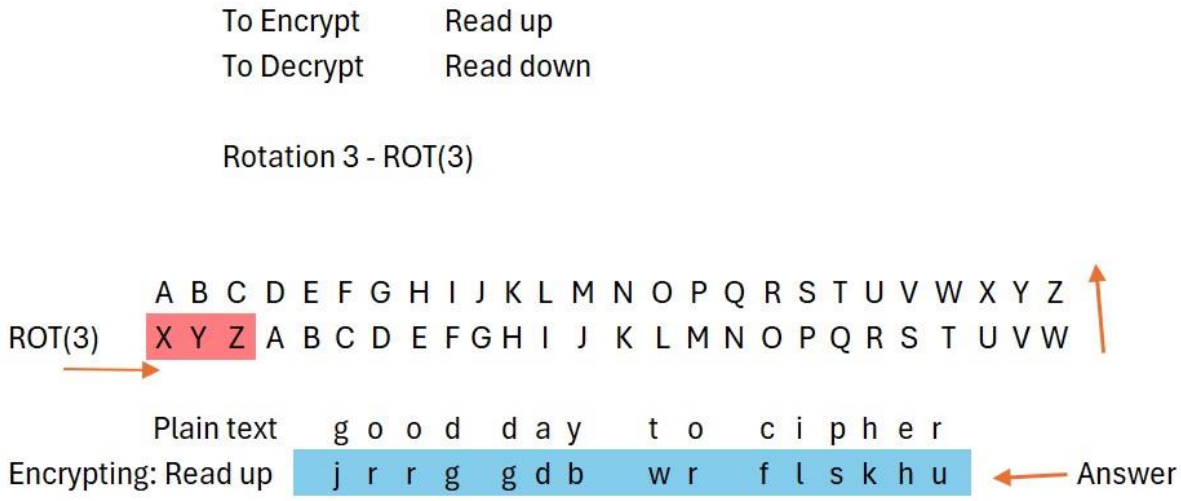
The encryption of the message " resting tomorrow" using the substitution method with a rotate value of 4 will result in the cipher text [viwxmrk xsqsvvsa]



The encryption of the message " resting tomorrow" using the substitution method with a rotate value of 4 will result in the cipher text [viwxmrk xsqsvvsa]



The encryption of the message " good day to cipher" using the substitution method with a rotate value of 3 will result in the cipher text



The three pillars of security in the CIA (Confidentiality, Integrity, and Availability) triangle are:

1. Confidentiality: Ensuring that information is accessible only to those authorised to access it.
2. Integrity: Ensuring that information is accurate, reliable, and has not been tampered with.
3. Availability: Ensuring that information and resources are available when authorised users need them.

Authentication is a related concept but not one of the three pillars specifically defined in the CIA triangle. Authentication refers to the process of verifying the identity of a user or system.

Critical web application security flaws include five flaws related to insecure software code,

All of the options provided—unvalidated input, injection flaws, and buffer overflow—are considered critical web application security flaws related to insecure software code. These vulnerabilities can be exploited by attackers to compromise the security and integrity of web applications.

Authentication is the access control component that verifies the identity of a user, ensuring that they are who they claim to be. It typically involves the user providing credentials such as a username and password, biometric data, security tokens, or other authentication factors. Once the user's identity is successfully verified, they are granted access to the system or resources based on their authorisation level.

Packet filtering firewalls operate at the network layer, while application firewalls operate at the application layer. Packet filtering firewalls operate at the network layer of the OSI model, where they filter traffic based on information contained within the packet headers, such as source/destination IP addresses, port numbers, and protocol types. They make decisions on whether to allow or block traffic purely based on this network-level information.
Application firewalls, on the other hand, operate at the application layer of the OSI model. They are designed to inspect and filter traffic based on the content of the data payload, as well as the context of the application-level protocols being used (e.g., HTTP, FTP). Application firewalls have the ability to understand and analyze the application-specific protocols, allowing them to enforce security policies based on the actual content of the traffic.

Tunnel mode encrypts the entire packet, while transport mode encrypts only the payload.

Integrity refers to the assurance that data has not been altered or tampered with and remains intact and unchanged from its original form. It ensures that information has retained its accuracy and consistency over time. In digital security, integrity is often achieved through cryptographic mechanisms such as hashing and digital signatures, which allow the verification of data integrity.

Creating predictable sequence numbers can actually make it easier for attackers to predict and hijack sessions. Randomization or non-predictable sequence number generation is typically preferred to enhance security and make session hijacking more difficult for attackers.

Since the steps given include escalation of privilege, covering tracks, and planting backdoors, then it is Hacking steps. An ethical hacker will not plant backdoors. They will be only doing this to identify weaknesses.

Decryption is the process of converting ciphertext (encrypted text) back into plaintext (original, readable text) using a cryptographic key or algorithm. It is the inverse operation of encryption, where ciphertext is produced from plaintext using an encryption algorithm and a key. Decryption requires the proper key or information to reverse the encryption process and reveal the original message.

Denial of Service (DoS) attacks involve disrupting or impairing the availability of a service, system, or network to legitimate users. These attacks can occur through various means, including the consumption of bandwidth (flood attacks), consumption of resources (such as CPU or memory exhaustion attacks), and exploitation of programming defects (such as vulnerabilities in software or protocols).

During phase three of the TLS handshake process, if the server requests a certificate from the client (depending on the server's configuration), the client sends its certificate (if available). Additionally, the client sends the key exchange information, and optionally, the client may also send certificate

verification. This phase allows the client to provide the necessary authentication and key exchange information to the server to establish a secure connection.

DIAMETER is a network protocol that provides client/server authentication, authorization, and accounting (AAA) services in a distributed network environment. It allows users to access network services securely regardless of their location and provides features such as roaming and protection against replay attacks.

IPSec operates at the network layer (IP layer) of the OSI model, not the IP layer itself. While IPSec provides numerous benefits such as providing strong security for all traffic crossing the perimeter, minimising overhead for traffic within a company or workgroup, and being transparent to applications, it does not directly relate to the ease of allocating IP addresses for connections. IP addressing and allocation are separate concepts from the functionality provided by IPSec. Therefore, "IPSec is in the IP layer so it is easy to allocate an IP address for each connection" option is not considered a benefit of IPSec.

A firewall is a basic security device that acts as a barrier between a network and the outside world or between systems within a network. It filters traffic based on predefined rules and policies, allowing or blocking traffic based on factors such as source/destination IP addresses, port numbers, protocols, and packet contents. Firewalls are commonly used to protect networks and systems from unauthorised access, malicious attacks, and other security threats.

Passwords are generally considered the weakest authentication mechanism among the options provided. They are vulnerable to various attacks such as brute force attacks, dictionary attacks, and password guessing. Users often choose weak passwords or reuse passwords across multiple accounts, further increasing the risk of unauthorized access. Compared to passphrases, one-time passwords, and token devices, passwords typically offer lower security due to their susceptibility to being compromised.

The principle of "Separation of Privilege" refers to the concept of dividing tasks or permissions among multiple entities to prevent a single entity from having complete control or access to critical functions.

The payload in a virus is the component that determines what actions the virus will perform once it has infected a system. This can include various malicious activities such as deleting files, stealing data, spreading further infections, or causing other forms of damage to the infected system. The payload is what makes the virus dangerous and harmful to the target system.

In an XSS (Cross-Site Scripting) reflection vulnerability, the attacker injects malicious script content, such as JavaScript, into data that is supplied to a website. This data could be provided through user input fields, URLs, or other forms of input. When the website processes the supplied data and includes it in the dynamically generated web page content, the malicious script is executed in the context of the user's browser. This can lead to various attacks, such as stealing cookies, session hijacking, or performing actions on behalf of the user without their consent.

Handling potential failures properly and safely in a program is essential to minimise the risk of program crashes or errors. By implementing proper error-handling mechanisms, such as exception handling, input validation, and defensive programming techniques, developers can anticipate and address potential failures before they lead to program instability or unexpected behaviour. This not

only improves the reliability and stability of the program but also enhances the user experience by reducing the likelihood of encountering errors or crashes during program execution.

Passive sniffing is a type of network sniffing where an attacker monitors network traffic without actively sending packets onto the network. This method allows the attacker to eavesdrop on communication between devices on the network without directly interacting with them. Passive sniffing is often used on internal networks to capture sensitive information such as passwords, usernames, and other data transmitted between systems.

A buffer overflow attack occurs when a program writes more data into a buffer (a temporary storage area in memory) than it was designed to hold. This can lead to data overflow into adjacent memory locations, potentially allowing an attacker to execute arbitrary code or manipulate the program's behaviour. Buffer overflow attacks are a common type of security vulnerability and can be exploited to gain unauthorized access to systems or execute malicious code.

Non-repudiation refers to the ability to have definite proof that a message originated from a specific party and that the sender cannot later deny having sent the message. It provides assurance that the sender cannot deny the authenticity or integrity of the message, thereby ensuring accountability for the actions taken. Non-repudiation mechanisms typically involve the use of digital signatures or other cryptographic techniques to create irrefutable evidence of the origin and integrity of electronic communications.

A dictionary password attack is a cryptanalysis attack that involves using a long list of commonly used words, phrases, or combinations that have been pre-defined and can be quickly accessed (like a dictionary) to attempt to break a password. This method is effective against passwords that are simple words, names, or phrases commonly found in dictionaries. The attacker tries each word or phrase from the dictionary list to gain unauthorised access to a system or account.

Enumeration is the process of gathering information about a target system, such as usernames, network shares, services running on the system, and more. It is an essential step in the process of network penetration testing and vulnerability assessment.

Anomaly detection is generally more effective at identifying new or previously unknown attacks compared to signature/heuristic detection. This is because anomaly detection focuses on identifying deviations from normal behaviour, allowing it to detect abnormal or unusual activities that may indicate potential security threats, even if they are not specifically known or predefined. Therefore, anomaly detection is particularly useful for detecting previously unknown or zero-day attacks.

To achieve confidentiality and non-repudiation in communication between Alice and Bob, Alice needs to use her private key for signing (to provide non-repudiation) and Bob's public key for encryption (to ensure confidentiality).

Mandatory Access Control (MAC) is a security model where access to resources is determined by security labels assigned to both subjects (users or processes) and objects (resources or data). These security labels are typically assigned by a system administrator or security policy and cannot be changed by users. MAC enforces access control based on predefined rules and policies, regardless of the user's discretion or the resource owner's preferences.

Least privilege refers to providing users, processes, or systems with only the minimum level of access or permissions required to perform their tasks or functions. This means that individuals or

entities should only have access to the resources or information necessary for their specific role or job function and no more.

A worm is a type of malware program specifically designed to replicate itself and spread to other computers or systems without needing to attach to or infect other files. Worms typically exploit vulnerabilities in network protocols or operating systems to propagate and can spread rapidly across networks, causing widespread damage and disruption. Unlike viruses, worms do not require a host program to propagate, making them self-contained entities capable of independent replication and transmission.

Mandatory Access Control (MAC) is a security model where access to resources is determined by security labels assigned to both subjects (users or processes) and objects (resources or data). In governmental organizations and environments with sensitive data, MAC is often preferred because it provides a high level of control over access permissions. MAC enforces access control based on predefined rules and policies, regardless of the user's discretion or the resource owner's preferences. This ensures that sensitive data is protected according to strict guidelines and regulations.

In Tunnel mode of IPSec, the entire original IP packet, including the original IP header, is encrypted and encapsulated within a new IP packet. This provides protection for the entire packet, including the original header, payload, and any additional headers added by IPSec.
Transport mode, only encrypts the payload of the original IP packet, leaving the original IP header intact.

In a block cipher, the plaintext is divided into fixed-length blocks, and each block is encrypted separately. The output of the first encryption process (known as the ciphertext) can then be used as input for the encryption of the next block. This process continues until all blocks have been encrypted. Block ciphers are widely used in modern cryptography and are often used in combination with other techniques, such as mode of operation to provide secure encryption.

The triggering phase is the phase in which a virus becomes activated. During this phase, certain conditions or events, known as triggers, cause the virus to execute its malicious payload, initiating its harmful activities on the infected system.

Transport Layer Security (TLS) is a cryptographic protocol that provides secure communication over a network by encrypting the data exchanged between two parties. It ensures the confidentiality, integrity, and authenticity of the transmitted data. TLS is commonly used to secure communication over the Internet, such as web browsing (HTTPS), email transmission (SMTPS, POP3S, IMAPS), and other applications requiring secure network communication.

A digital signature is a cryptographic technique used to provide authentication, integrity, and non-repudiation for digital messages or documents. It involves applying a mathematical algorithm to a message or document along with a private key to produce a unique digital signature. The recipient can then use the sender's public key to verify the digital signature, ensuring that the message has not been altered since it was signed and that it indeed originated from the claimed sender. Therefore, a digital signature allows the recipient to verify both the source and integrity of the data.

A sniffer, also known as a network sniffer or packet sniffer, is a tool or device designed to capture and analyse network traffic as it moves across the network. Sniffers can monitor and intercept data packets flowing through a network segment, allowing administrators to inspect network activity for troubleshooting, security analysis, or performance monitoring purposes.

Static biometrics refers to biometric characteristics that do not change over time or with use. Recognition by fingerprint, retina, and face are examples of static biometrics because these characteristics remain relatively constant for an individual and can be used for identification or authentication purposes.

Static biometrics refers to biometric characteristics that do not change over time or with use. Recognition by fingerprint, retina, and face are examples of static biometrics because these characteristics remain relatively constant for an individual and can be used for identification or authentication purposes.

The handshake protocol is considered the most complex part of the TLS (Transport Layer Security) protocol suite. It is responsible for negotiating the security parameters between the client and server, establishing a secure connection, and authenticating both parties. The handshake involves multiple steps, including cryptographic key exchange, cipher suite negotiation, and verification of the server's identity through digital certificates. This process ensures the confidentiality, integrity, and authenticity of the communication session, making it a critical component of the TLS protocol.

The answer "Anomaly detection relies on signature-based scanning, while signature/heuristic detection relies on behaviour-based" accurately describes the main difference between anomaly detection and signature/heuristic detection. Anomaly detection involves analysing behaviour over time, while signature/heuristic detection uses a set of known malicious patterns or attack rules.

Hashing algorithms are primarily used for data integrity verification, where they produce a unique hash value (digest) for a given input data. This hash value can then be compared against a previously generated hash value to verify if the data has been altered or tampered with. They also can provide trust in the form of non-repudiation. On the other hand public key infrastructure provides trust in the form of confidentiality and Authentication. The question is focused on the goals of Integrity and Trust.

During the propagation phase of a virus, the virus replicates and places a copy of itself into other programs or system areas. In this phase, the virus spreads to other files, programs, or system areas, creating copies of itself to infect additional systems or spread within the current system. This propagation process allows the virus to expand its reach and increase its potential impact.

Active session hijacking is a type of attack where the attacker intercepts and takes over an established session between two parties by actively injecting themselves into the communication. Unlike passive session hijacking, where the attacker merely eavesdrops on the session, in active session hijacking, the attacker actively participates in the communication to manipulate or control the session. This allows the attacker to interact with the remaining party as if they were the legitimate party that has been disconnected.

A multipartite virus is a type of computer virus that has the ability to infect multiple types of files and spread across various parts of a system. It can infect both executable files and boot sectors. However, a multipartite virus can not only infect multiple files but they infect files in different ways making it potentially more damaging and difficult to remove compared to viruses that infect only one type of file in one way.

All the options listed describe valid types of buffer overflow attacks:
Buffer overflow in the stack occurs when the attacker overflows a buffer located on the stack, typically by inputting more data than the buffer can hold, leading to overwriting adjacent memory addresses, including function return addresses.

Buffer overflow in the heap happens when the attacker overflows a buffer allocated on the heap, often by dynamically allocating memory and then writing more data than the allocated buffer size, leading to overwriting adjacent memory blocks.
Buffer overflow using global or static variables in the program happens as global or static variables are stored in a fixed memory location, and overflowing them can lead to similar consequences as stack or heap-based buffer overflows, depending on how they are accessed and used within the program.

Mock Test

Sure, here are the shortened definitions for each term:

1. **In-Band**: Attacker sends malicious query and retrieves results in the same channel.

2. **Internal**: No specific SQL Injection type; may refer to attacks originating from within an organization's network.

3. **Inferential**: Attacker infers success/failure of injected query from application behavior.

4. **Out-of-Band**: Attacker triggers external communication to retrieve data, bypassing direct channel.

The type of encryption that uses the same key to both encrypt and decrypt information is called "Symmetric encryption." In symmetric encryption, the same key is used for both encryption and decryption processes. This means that both the sender and the recipient of the encrypted data share the

same secret key, which is used to transform plaintext into ciphertext and vice versa. This contrasts with asymmetric encryption, where separate keys are used for encryption and decryption.

The security principle which states that individuals will be given only the level of access that is appropriate for their specific job role or function is called **least privilege**.

- **Least Privilege**: This principle ensures that individuals are granted only the minimum level of access or permissions necessary to perform their job duties, reducing the risk of unauthorized access or misuse of resources.

- **Job Rotation**: Job rotation involves periodically rotating employees between different job roles or functions within an organization. While it can have security benefits by mitigating the risk of fraud or collusion, it's not directly related to granting appropriate access levels.

- **Separation of Duties**: Separation of duties (SoD) divides tasks and responsibilities among multiple individuals to prevent a single person from having complete control over critical processes. This principle helps reduce the risk of errors, fraud, or unauthorized activities.

- **Implicit Deny**: Implicit deny is a concept used in access control lists (ACLs) where if a user's access request does not match any specific permission or rule explicitly defined in the ACL, access is automatically denied. It serves as a default rule when no other permissions are granted.

The security principle that Sarah needs to employ if she needs a security system that checks every user's access against the access control mechanism is **Complete Mediation**.

- **Complete Mediation**: This principle dictates that every access to every object must be checked against the access control mechanism to ensure that unauthorized access is not granted. This means that the security system should validate access permissions for each user request, leaving no gaps where unauthorized access could occur.

The other principles listed are:

- **Fail-safe Default**: This principle states that access should be denied by default in case of uncertainty or ambiguity in access control decisions.

- **Economy of Mechanism**: This principle suggests that security mechanisms should be as simple and straightforward as possible to reduce the likelihood of errors and vulnerabilities.

- **Separation of Privilege**: This principle, also known as Separation of Duty, involves dividing tasks and responsibilities among multiple individuals to prevent any single person from having complete control over critical processes. It's not directly related to the continuous checking of access against access control mechanisms.

DNSSEC focuses on ensuring the authenticity and integrity of DNS data, including providing mechanisms to validate the authenticity of DNS responses and detecting modifications to DNS data.

The function that consists of two phases of encryptions, one with a symmetric encryption key and one with a public key, is **Enveloped data**.

Given the principles listed and the scenario of high employee turnover, the access control model most appropriate would be **Role-based access control (RBAC)**.

Here's why:

1. **Least privilege**: RBAC aligns well with the principle of least privilege. It assigns access rights based on the roles that users have within the system, ensuring that users are granted only the privileges they need to perform their work tasks and job functions.

2. **Separation of privileges**: RBAC also facilitates separation of privileges by defining different roles with specific sets of permissions. Sensitive functions can be split into tasks performed by users in different roles, thereby enhancing security.

3. **Need to know**: While RBAC does not directly address the need-to-know principle, it indirectly supports it by granting access based on roles, which are typically associated with specific job functions and tasks. Users are given access only to the resources and data required for their roles.

RBAC provides a structured approach to access control, allowing organizations to efficiently manage access rights, especially in

environments with high employee turnover where roles and responsibilities may change frequently.

Role Based Access Control follows the same principle of least privilege. It gives users in a company only the access they need based on their roles or job functions. This is very important in a company with high employee turnover. It won't be accessible if administrators allow users to assign full control of their data and give them the freedom to give or deny access to their files (DAC). MAC is used in environments where access is given based on security labels and security clearance. It is the most secure but the most complex to manage and will be very difficult for administrators to implement it and manage it. File access control Implements ACL and is not an access control model. It also implements DAC.

In Discretionary Access Control (DAC), access to resources is determined by the resource owner, who has discretion over who can access the resource. This model allows the resource owner to grant or revoke access permissions based on their discretion. In a company with high employee turnover, DAC provides flexibility for resource owners (e.g., managers, supervisors) to quickly adjust access permissions as employees join or leave the organization.

Mandatory Access Control (MAC) and Role-Based Access Control (RBAC) typically involve more rigid access control policies that may not be as easily adaptable to frequent changes in personnel. File Access Control (FAC) is not a widely recognized access control model.

The scanning method that the hacker should avoid due to being considered too noisy and potentially getting flagged as malicious is the **CONNECT scan**.

Ping scans involve sending ICMP echo requests (ping) to determine if a host is alive. While ping scans are quick and can provide information on which hosts are active on a network, they can also generate significant network traffic and may trigger intrusion detection systems (IDS) or firewalls, potentially alerting network administrators to the presence of an attacker.

In contrast, the other scanning methods mentioned (Connect scan, Fin scan, Syn scan) are generally considered less noisy and are commonly used by attackers during information gathering assessments. Among them, Syn scans (also known as Stealth scans) are particularly popular because they are stealthier and less likely to be detected compared to Ping scans.

A connect scan is considered the most noisy as it will complete the handshake, and therefore, if the request is malicious, it will be detected. On the other hand, a ping scan will simply look at which ports are open using an ICPM echo reply message.
SYN scan and FIN scan are also noisy, but since the hacker is only attempting to identify if the port exists or not and they are not flooding the network with those requests, it will most likely go undetected if done with care. A syn scan will simply ask the server for a connection on a specific port; once it receives a response (hence, knowing the port is open), it will stop responding. The FIN scan will simply send a FIN message to a port even if a connection does not exist. When the port responds that there is no connection, the hacker will know that the port exists and is open.

Based on the symptoms described, the attack that is likely happening here is **MAC flooding**.

MAC flooding is a type of attack where the attacker floods the switch with fake MAC addresses, thereby filling up the switch's MAC address table (CAM table). Once the table is full, the switch enters a fail-open mode, where it behaves like a hub and floods incoming traffic to all ports, instead of selectively forwarding traffic based on MAC addresses. This behavior can lead to network congestion and a denial of service for legitimate devices trying to connect to the switch.

In this scenario, the central switch failing to accept new device connections despite available ports suggests that it might be overwhelmed with fake MAC addresses, possibly due to a MAC flooding attack.

The cryptanalysis technique the hacker is using in this scenario is a **Rainbow Table Attack**.

A Rainbow Table Attack is a type of precomputed attack used to crack password hashes. In this technique, a large table of precomputed hash values (known as a "rainbow table") is generated beforehand. These tables contain hash values for commonly used passwords and their corresponding plaintexts. When a hacker obtains a hashed password, they compare it against the entries in the rainbow table to find a match, effectively reversing the hash function and revealing the plaintext password.

In the scenario described, the hacker has obtained the hashed value of the password from the Active Directory Server and is attempting to decipher it using a large precomputed table of hash values, which aligns with the method of a Rainbow Table Attack.

The option that refers to an intrusion detection system (IDS) programmed to identify known attacks occurring in an information system or network by comparing sniffed traffic or other activity with that stored in a database is:

Signature analysis

Ping of death DoS/DDoS attack exploits some operating systems' inability to handle the large packet size that is allowed (65,536 bytes). A ping of death is conducted using crafted large-sized ICMP packets and more often leads to the Operating system crashing. This should be confused with the ICMP flood where the network is flooded with a very large amount of ICMP packets (normal size) that a device or a network can network and become unavailable.

Good work- ESP protects the confidentiality of data by encrypting the payload of all IP packets. Malicious actors will still be able to conduct message replay or a man-in-middle attack (by authentication); however, the data is in an encrypted form, and as long as the keys are protected, they won't be useful for the hacker.. ESP does not protect DoS

Phase 1, client hello server hello
Phase 2, Server send keys and certificates
Phase 3 Client send certificates (if needed) and keys
Phase 4- choose cipher suite and complete the handshake

Injection is the correct answer.

SQL queries should be executed in the back end as they are. A malicious actor modifies those queries from the web application, and the server executes unintended SQL commands.