Are the countermeasures that you need to put in place to avoid, mitigate, or counteract security risks due to threats or attacks.

- CONTROL

It has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

- OFFICIAL INFORMATION

It is a threat which can exploit smooth vulnerability which has been known in the past as well.

- ZERO DAY

It provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment

- GROUP POLICY

It could be a set of rules connected by the proprietor, maker or director of a network, site, or service

- ACCEPTABLE USER POLICY

It ought to report what sort of mindfulness program is in put and how is it communicated on a normal premise.

- ACCEPTABLE USER POLICY

What does confidentiality of data imply to

- Rules which restrict access only to those who need to know

An administrator notices that former temporary employees' accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

- Implement an account expiration date for permanent employees.

During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

- Ssl 1.0

It is an authentication method that identifies and recognizes people based on voice recognition or physical traits such as a fingerprint, face recognition, iris recognition, and retina scan.

- Biometric

Electronic records that are not archival. Click here for tips on identifying and deleting electronic records that have met retention.

- Delete

It requires understanding how people experience change and what they need to change successfully.

- **INDIVIDUAL Change management**

It is the discipline that guides how we prepare, equip and support individuals to successfully adopt change in order to drive organizational success and outcomes.

- Change management

It ought to state clearly the prerequisites forced on clients for passwords

- passwords

It distinguishes all the ways that the system can be remotely accessed and what is in put to guarantee that get to be from as it were authorized people

- Remote access

It could be a level of quality or fulfillment

- standard

It regularly contains an interface to a Web location that the spimmer is attempting to market.

- spim

It is a type of malware from cryptology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

- Ransomware

These attacks start with commonly used, weak passwords like Password123 and move on from there.

- Dictionary attack

It does this by monitoring a user's input and keeping a log of all keys that are pressed.

- Keylogger

All the following are Environmental Threats except

- Assessment

It can be difficult to detect because the network transmissions will appear to be operating normally.

- Eavesdropping attacks

What does confidentiality of information allude to?

- Rules which restrict access only to those who need to know

Observe and check the progress or quality of (something) over a period

- **MONITORING**

A security administrator wants to ensure that the message the administrator sends out to their Chief Financial Officer (CFO) does not get changed in route. Which of the following is the administrator MOST concerned with?

- DATA INTEGRITY

It is protection of available information or information resources.

- INFO SECURITY

These are attacks designed to compromise network security by either eavesdropping on or intercepting and manipulating network traffic.

- NETWORK-BASED ATTACKES

A return to a normal state of health, mind, or strength.

- RECOVERY

It only denies a permission until the user or group can perform the permission

- IMPLICIT DENY

Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

- **STENOGRAPHY**

It is the practice of converting a password to a longer and more random key for cryptographic purposes such as encryption.

- KEY STRETCHING

Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

- ROLE BASED ACCESS CONTROL

It may be an explanation that uncovers a few or all of the ways a party assembles, employments, discloses, and oversees a client or client's information

- PRIVACY POLICY

It is almost utilization and what substance sifting is in put.

- **INTERNET**

It provides guidelines regarding wireless access points and the management by ITS of 802.11X and related wireless standards access.

- WIRELESS STANDARD POLICY

It gives rules with respect to remote access points and the administration by ITS of 802.11X and related remote guidelines get to

- WIRELESS STANDARD POLICY

It ought to clearly recognize how the arrangement will be implemented and how security breaches and/or wrongdoing will be dealt with.

- ENFORCEMENT
-

These are a critical segment of a pentest in which preparation can make a major impact on the success of a pentest.

- PASSWORD ATTACK

It is the act of masking a communication from an obscure source as being from a known, trusted source

- SPOOFING

It means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things.

- SOFTWARE ATTACKS

A security administrator examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90). Which of the following attack types has occurred?

- BUFFER OVERFLOW

It is relatively straightforward using an open source tool called Reaver

- WPS ATTACK

It could be a program that collects chunks of information that are likely to be account names and their related passwords so that an aggressor can utilize those qualifications to posture as the individual they were stolen from.

- PASSWORD STEALER

It is the prevention of unauthorized users from accessing your wireless network and stealing the data using your Wi-Fi network.

- WIRELESS SECURITY

Which of the following is best practice to put at the end of an ACL?

- IMPLICIT DENY

Facts and statistics collected together for reference or analysis.

- DATA

What does integrity of data refer to?

- The level of assurance which can be given as to how accurate and trustworthy data is

What does integrity of information allude to

- **The level of assurance which can be given as to how accurate and trustworthy data is**

The process of putting a decision or plan into effect also known as execution.

- IMPLEMENTATION

It is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

- THREAT

A security technique that regulates who or what can view or use resources in a computing environment

- ACCESS CONTROL

A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts. Joe will need network access to all directories, folders and files within the accounting department.
Which of the following configurations will meet the requirements?

- Create an account with role-based access control for accounting.

Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

- blowfish

Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

- **BLOWFISH**

Paper and electronic records to the University Archives if they have permanent legal, fiscal, administrative, or historical value.

- TRANSFER

It is a living document that provides guidelines for your organization's social media use.

- **SOCIAL MEDIA POLICY**

It ought to recognize the parts and duties of clients getting to assets on the organization's network

- User Access to Computer Resources

It is the conceptual show that characterizes the structure, behavior, and more sees of a system

- SYSTEM ARCHITECTURE

Which of the following might a security administrator actualize to relieve the hazard of tailgating for a huge organization?

- Train employees on risks associated with social engineering attacks and enforce policies.

It is a growing problem for individual computer users as well as large corporations and organizations.

- **DATA THEFT**

It is the act of stealing information stored on computers, servers, or other devices from an unknowing victim with the intent to compromise privacy or obtain confidential information.

- DATA THEFT

An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

- Shoulder surfing

It is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder

- Shoulder surfing

All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate?

- Shoulder surfing

It is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

- Logic bomb

Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

- **Logic Bomb**

It Use a program to generate likely passwords or even random character sets.

- Brute force

Sara, a hacker, is completing a website form to request a free coupon. The site has a field that limits the request to 3 or fewer coupons. While submitting the form, Sara runs an application on her machine to intercept the HTTP POST command and change the field from 3 coupons to 30. Which of the following was used to perform this attack?

- Xml injection

An attacker attempted to compromise a web form by inserting the following input into the username field: admin)(|(password=*))
Which of the following types of attacks was attempted?

- LDAP injection

After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings?

- **War chalking**

The practice of marking open wireless access points is called which of the following?

- War chalking

It is also called access point mapping

- War driving

Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users?

- EVIL TWIN

A network analyst received several reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks?

- REPLAY

It happens when a cybercriminal listens stealthily on a secure network communication, intervention it, and after that falsely delays or resends it to mislead the collector into doing what the programmer needs

- Replay attack

The delay or repeat of the data transmission is carried out by the sender or by the malicious entity, who intercepts the data and retransmits it.

- WIRELESS REPLAY ATTACK

What is not needed to be protected?

- Intruder

A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

- AVAILABILITY

Franz is working on her college applications online, when the admissions site crashes. She is incapable to turn in her application on time.

- **AVAILABILITY**

It is the third core security principle, and it is defined as a characteristic of a resource being accessible to a user, application, or computer system when required.

- **AVAILABILITY**

A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

- Availability

Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

- Longer MTBF of hardware due to lower operating temperatures??
- Higher data integrity due to more efficient SSD cooling
- Increased availability of network services due to higher throughput

What isn't objective of security?

- VULNERABILITY

It is the quality or state of being uncovered to the plausibility of being assaulted or hurt, either physically or candidly.

- RISK

A shortcoming which can be misused by a risk actor, such as an aggressor, to perform unauthorized activities inside a computer system.

- VULNERABILITY

A weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.

- VULNERABILITY

JP gets his phone bill within the mail. The charge was assumed to be for $80, but the mail individual spilled water on the charge, spreading the ink. The charge presently inquires for $8.

- **INTEGRITY**

It is the state of being whole and unified.

- **INTEGRITY**

It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control?

- INTEGRITY

PJ is buying books from an online retail location, and she finds that she can alter the cost of a book from $19.99 to $1.99. Which portion of the CIA set of three has been broken?

- INTEGRITY

Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

- Integrity

Alice is buying books from an online retail site, and she finds that she can change the price of a book from £19.99 to £1.99. Which part of the CIA triad has been broken?

- Integrity

Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concept is Sara using?

- **INTEGRITY**

It is the assurance that someone cannot deny the validity of something.

- **NON-REPUDIATION**

Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability?

- NON-REPUDIATION

It is the affirmation that somebody cannot deny the legitimacy of something.

- NON-REPUDIATION

It is defined as the act of determining who someone or what something is.

- **IDENTIFICATION**

It is the process of verifying the identity of a person or device.

- **AUTHENTICATION**

A user ID and password together provide which of the following?

- AUTHENTICATION

It is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features.

- Authorization

It is one way to enable security during the process of message transmission when the message is intended for a recipient only.

- **HASHING**

Which of the following concepts describes the use of a one-way transformation in order to validate the integrity of a program?

- HASHING

It uses a single key to encrypt and decrypt data.

- **Symmetric encryption**

It also known as public key cryptography

- Asymmetric encryption

In cybersecurity, what does CIA stand for?

- Confidentiality, Integrity, Availability

It is to set upon in a powerful, rough, antagonistic, or forceful way, with or without a weapon

- **ATTACK**

It is to set upon in a forceful, violent, hostile, or aggressive way, with or without a weapon

- ATTACK

It is an illegal act of entering, seizing, or taking possession of another's property.

- INTRUSION

What is not goal of security?

- **Intrusion**

Which of the following BEST describes using a smart card and typing in a PIN to gain access to a system?

- **Multifactor authentication**

A policy requires employees to take time away from their job.

- Mandatory vacations

A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

- Enforce mandatory vacations

Which of the following access controls enforces permissions based on data labeling at specific levels?

- Mandatory access control

-

It involves first identifying the groups and people who will need to change as the result of the project, and in what ways they will need to change.

- Organizational change management

It includes to begin with recognizing the bunches and individuals who will have to be compelled to alter as the result of the project, and in what ways they will ought to change.

- **Organizational change management**

It gives the IT department a method to review the changes before they are implemented.

- CHANGE MANAGEMENT

It is the action or process of classifying something according to shared qualities or characteristics.

- **CLASSIFICATION**

Confidential records such as research data, student folders, personnel records, and financial records that have account numbers listed

- SHRED

Expired credit cards, visas, passports, and IDs.

- SHRED

It is the continued possession, use, or control of documentation

- RETENTION

Every paper or electronic record has a specific amount of time that it needs to be kept.

- **RETENTION**

Is the act or process of throwing away or getting rid of documentation

- **DISPOSAL**

It may be a common rule, guideline, or piece of counsel.

- GUIDELINES

It is a built up or official way of doing something.

- PROCEDURES

It gives centralized administration and setup of operating systems, applications, and users' settings in an Active Directory environment.

- GROUP POLICY

It could be an individual who picks up unauthorized get to to computer records or systems in arrange to encourage social or political closes.

- HACKTIVIST

It may be an amusing or pernicious misdirection.

- HOAX

It is often a chain message telling recipients to forward the mail to all their contacts.

- HOAX

It is frequently a chain message telling beneficiaries to forward the mail to all their contacts.

- Hoax

A human resources employee receives an email from a family member stating there is a new virus going around. In order to remove the virus, a user must delete the Boot.ini file from the system immediately. This is an example of which of the following?

- **Hoax**
-

Isn't restricted to looking through the junk for self-evident treasures like get to codes or passwords composed down on sticky notes.

- DUMSPER DIVING

It particularly targets senior administration that hold control in companies, such as the CEO, CFO, or other administrators

- **WHALING**

Which of the following attacks targets high level executives to gain company information?

- **WHALING**

All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate?

- WHALING

It can be current or previous representatives, temporary workers or trade accomplices that picks up get to an organization arrange, system or information and discharge this data without authorization by the organization.

- **MALICIOUS INSIDERS**

It is also known as piggybacking

- **TAILGATING**

At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe?

- TAILGAITING

It is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

- **CYBERTERRORISM**

A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would BEST serve this purpose?

- **ANTI-SPYWARE**

It may be a program that can duplicate itself and infect a computer without the user’s consent or information. Early viruses were usually a few forms of executable code that was hidden within the boot sector of a disk or as an executable file.

- VIRUS

Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

- Theft of the physical database server

It is a self-replicating program that copies itself to other computers over the network without the need for any user intervention.

- **WORM**

It does not corrupt or modify files on a target computer.

- **WORMS**

It is an executable program that appears as a desirable or useful program.

- TROJAN HORSE

These are considered one of the most serious types of malware since they may be used to gain unauthorized access to remote systems and perform malicious operations.

- ROOTKITS

It is a type of malware that constantly changes its identifiable features in order to evade **detection.**

- **Polymorphic Malware**

It will continue to spread and infect devices even if its signature changes to avoid detection

- **Polymorphic Malware**

Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of?

- BACKDOOR

These are carried out by either hacking a node in the network or introducing a fabricated node in the network.

- **SINKHOLE ATTACK**

A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place?

- **BLUEJACKING**

It is a hacking method that allows an individual to send anonymous messages to Bluetooth-enabled devices within a certain radius.

- **BLUEJACKING**

Which of the following describes how an attacker can send unwanted advertisements to a mobile device?

- BLUEJACKING

It is also known as bluehacking.

- **Bluejacking**

It is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs

- BLUESNARFING

It allows hackers to remotely access Bluetooth device data, such as a user's calendar, contact list, emails and text messages.

- BLUESNARFING

It is a device hack performed when a wireless, Bluetooth-enabled device is in discoverable mode.

- BLUESNARFING

It is an attack on the protocol used to determine a device's hardware address (MAC address) on the network when the IP address is known.

- ARP POISING

It is an assault that traps a client into clicking a webpage component which is undetectable or masked as another component.

- Clickjacking

It could be a pernicious strategy of deceiving a client into clicking on something distinctive from what the client sees

- CLICKJACKING

It is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element.

- Clickjacking

It is the use of messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same website.

- SPAMMING

It is the action of sending promotions by e-mail to individuals who don't need to get them

- SPAMMING

It is the utilize of informing systems to send a spontaneous message

- SPAM

A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the following can the

security Administrator implement to mitigate the risk of an online password attack against users with weak passwords?

- Decrease the account lockout time

It ensures protection to a Wi-Fi network from unauthorized access.

- WIRELESS SECURITY

-

It is assurance of accessible data or data assets.

- Information Security

It is the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

- Information Security

-

Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

- Steganography

It can limit access to sensitive environments to normal business hours when. oversight and monitoring can be performed to prevent fraud, abuse, or intrusion.

- Time of day restrictions

It limits when users can access specific systems based on the time of day or week.

- Time of day restrictions

Which of the following security concepts can prevent a user from logging on from home during the weekends?

- **Time of day restrictions**

Which of the following security concepts can avoid a client from logging on from home amid the ends of the week?

- Time of day restrictions

A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during nonworking days. Which of the following should the technician implement to meet managements request?

- Time of day restrictions

It can limit access to sensitive environments to normal business hours when. oversight and monitoring can be performed to prevent fraud, abuse, or intrusion.

- Time of day restrictions
-

It establishes secure connections between hosts.

- Key exchange

It is an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers.

- Session Keys

A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client-side certificate. Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory. How many authentication factors are in use by the VPN system?

- 3

It is a principle that prevents any single person or entity from being able to have full access or complete all the functions of a critical or sensitive process.

- Separation of duties

It ought to incorporate a well-defined security vision for the organization.

- Security policies

It addresses any data that's secured against ridiculous divulgence.

- Sensitive data

It has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

- Official document

Records that are not confidential and do not contain personal/financial identifying information.

- Recycle

It ought to clearly recognize how the arrangement will be implemented and how security breaches and/or wrongdoing will be dealt with.

- enforcement

It talks about what in the event that any Network Security Intrusion Detection or Prevention Framework is utilized and how it is executed.

- Intrusion Detection

It is the teach that guides how we plan, prepare and back people to effectively embrace alter in arrange to drive organizational victory and results.

- change management

It incorporates how to handle connections, through sifting, individual utilize of the mail framework, dialect confinements, and authentic necessities

- E-Mail

It is the act of disguising a communication from an unknown source as being from a known, trusted source.

- Spoofing

He uses the same tools and techniques as a hacker but does so in order to disrupt services and bring attention to a political or social cause.

- Script kiddie

It is generally assumed that most of them are juveniles who lack the ability to write sophisticated programs or exploits on their own and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities.

- **SCRIPT KIDDIE**

It is the process by which a URL is wrongly removed from the search engine index and replaced by another URL.

- URL hijacking

It can lead to a tremendous drop in guests of websites.

- Url hijacking

It is type of phishing attacks that try to lure victims via voice calls.

- Vishing

It is the false hone of making phone calls or clearing out voice messages implying to be from legitimate companies in arrange to initiate people to uncover individual data, such as bank subtle elements and credit card numbers.

- Vishing

It may be a strategy utilized to pick up get to to information, frameworks, or systems, basically through deception

- Social Engineering

This technique typically relies on the trusting nature of the person being attacked.

- Social Engineering

It is the term used for a broad range of malicious activities accomplished through human interactions.

- Social Engineering Attacks

It is the false hone of sending emails implying to be from legitimate companies in arrange to actuate people to uncover individual data, such as passwords and credit card numbers.

- Phishing

It is somebody without the right verification takes after a confirmed worker into a limited zone.

- Tailgating

It copies (something) whereas overstating its characteristic highlights for comedian impact

- Spoofing

It happens both exterior and interior companies and decreasing the hazard of insider information burglary at the corporate level is anything but simple

- Malicious insiders

The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection. Which of the following has happened on the workstation?

- Zero-day attack

-

A type of virus that has been designed to thwart attempts by analysts from examining its code by using various methods to make tracing, disassembling and reverse engineering more difficult

- Armored virus

It may also protect itself from antivirus programs, making it more difficult to trace.

- armored virus

It is a program that can copy itself and infect a computer without the user's consent or knowledge. Early viruses were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file

- **Viruses**

It is a software program designed to provide a user with administrator access to a computer without being detected.

- ROOTKITS

It is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel or, less commonly, libraries or applications.

- rootkits

It is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel or, less commonly, libraries or applications.

- Rootkits

It can also install additional software, which can redirect your web browser to other sites or change your home page.

- Spyware

A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

- SPYWARE

It gathers your personal information and relays it to advertisers, data firms, or external users.

- Spyware

These were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file

- Viruses

Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks?

- Brute force

Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?

- Zero-day

-

It may be a Trojan that's planned to accumulate data from a system.
- Password stealer

It takes advantage of the specific capacity limits that apply to any network resources – such as the infrastructure that enables a company’s website.
- Denial-of-service attack

It is also known as black hole DNS
- Sinkhole Attacks

It may be a sort of assault where the aggressor breaks into the communication between the endpoints of a arrange association.
- **MAN IN THE MIDDLE**

It attacks are often facilitated by social engineering attacks which lure the user to a fake site.
- MAN IN THE MIDDLE

It is an assault where the assailant subtly transfers and conceivably modifies the communications between two parties who accept that they are specifically communicating with each other.
- Man-in-the-Middle Attacks

It can be difficult to detect because the network transmissions will appear to be operating normally.
- Man-in-the-Middle Attacks

It 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.
- Denial-of-service attack