Project Report
Cryptography
110673
Instructor : Dr. Maaz Bin Ahmed

Members:-
Safiullah Rehmani(12413)
Rameez Hussain (8290)

Table of Contents

Threat .....
Threat mode in networked devices .....
Threat mode in isolated devices .....
Threat actors in isolated devices .....
Insider .....
Man in middle.....
Adversary.....
Insider categories .....
Planted .....
Loyal.....
Use case of planted insider .....
Damage canvas.....

THREAT

The probability of a threat's harmful act or even its existence is caused by flaws in computer systems' hardware and software security, which make it easier for threat actors to cross lines and carry out unlawful operations inside of computer systems. unwanted effects on the system or application.
Examples of Threats Viruses on computers
A computer virus is a piece of software designed to alter a computer's functionality without the user's knowledge or consent and is likely the most well-known danger to computer security. The virus multiplies and operates on its own, typically causing computer damage.

Spyware dangers
Any application that tracks your online actions or instals software without your permission for the aim of making money or getting personal information is considered spyware, a major danger to your computer's security. We've gathered a significant amount of information to assist you in avoiding spyware dangers and remaining secure online.

Predators and hackers
Malware and other dangers to computer security are made by people, not machines. Programmers who engage in cyber terrorism by hacking into computer systems to steal, change, or destroy information are known as hackers and predators. These online predators have access to your data, may lock you out, and can steal your identity. As you might have suspected, one of the best methods to defend yourself against this type of hackers is by using online security solutions with identity theft protection.

Phishing
Through phoney emails or instant chats, phishers pretend to be a reliable individual or company in an effort to get private or sensitive information. Attacks by phishers are

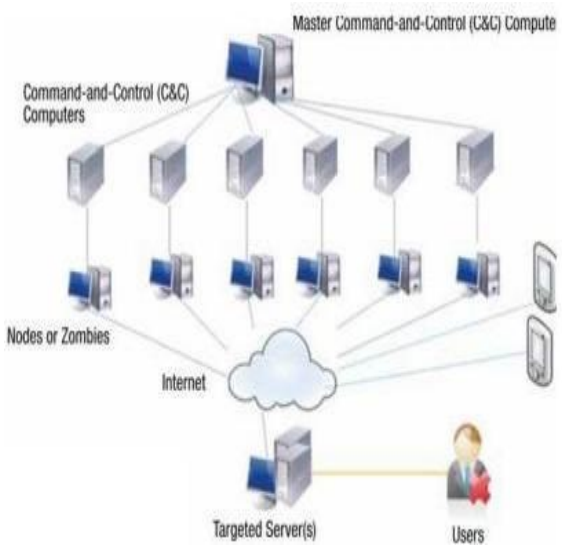
Phishers impersonate a trusted person or business and attempt to steal sensitive financial or personal information through fraudulent emails or instant messages. Phishing attacks are some of the most successful methods for cybercriminals looking to prevent data leaks.

The networked devices' threat mode

Any user must first be authenticated, often using a username and password. An access policy, such as which services users may access, is then enforced by a firewall after verification. This component may not search for potentially hazardous information, such as computer worms or network-borne Trojan horses, despite being successful at preventing unauthorised access. It can be found with the use of antivirus software or an intrusion prevention system (IPS). and stop such viruses from functioning. An anomaly-based intrusion detection system may also keep track of network activity like cable traffic and log it for auditing and high-level analysis in the future. To ensure privacy, communication between two hosts utilising a network can be encrypted. Security dangers drastically rise as massive open networks are developed. 20 or more years. To have safe access to these hazards, it is essential to take preventative action in advance. In addition to closing off the network from the outside world, there are various techniques to counteract these network dangers.

1. Multiple Attacks

In a distributed attack, an enemy must introduce code, such as a Trojan horse or backdoor software.
"Trusted" software that will thereafter be made available to a large number of other businesses and those firms' customers Attacks that target hardware or software during the production or distribution processes are known as distribution attacks.
These attacks inject malicious code to get unauthorised access to information or build a backdoor into the product.
These attacks inject malicious code to get unauthorised access to information or build a backdoor into the product.



1. Insider attack

An insider attack involves someone from the inside, such as an authorized employee, attacking a network insider
attacks may or may not be malicious. An insider attack is a malicious attack committed on a network or computer
system by a person with authorized access to the system. Initiates who make attacks (initiate attacks) have different
an advantage over external attackers because they have and may know the credentials to access the system
network architecture and system policies and procedures. In addition, there may be less security against. Because many organizations focus on protecting against external attacks and cannot focus on insiders
attackers.

2. Close in Attack

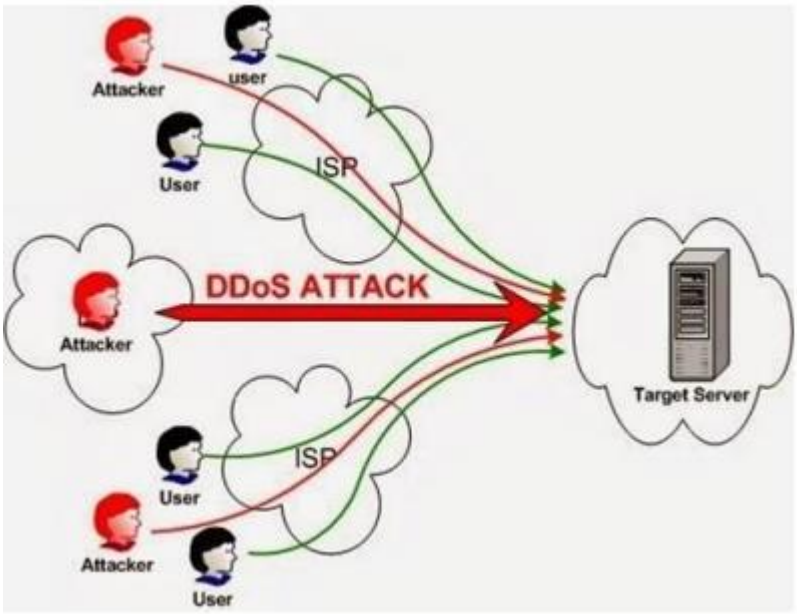
A close in attack involves someone trying to get physically close to network data, components, and systems to learn more about network Melee attacks consist of regular individuals coming into close physical proximity networks, systems or devices to collect and modify or deny access to information. Close physical proximity is achieved through hidden network access, open access, or both. In other words, to Melee attack and attackers are physically enclosed to the target system and benefit from physical enclosure get useful information like password and security code etc. One popular form of close attack is social engineering in social engineering attacks where the attacker compromises

network or system through a social interaction with a person, through an email message or telephone. It can be different tricks used by an individual to disclose company security information. Information that the victim discloses hackers would most likely be used in a subsequent attack to gain unauthorized access to the system or network.

3. Denial of Service Attack

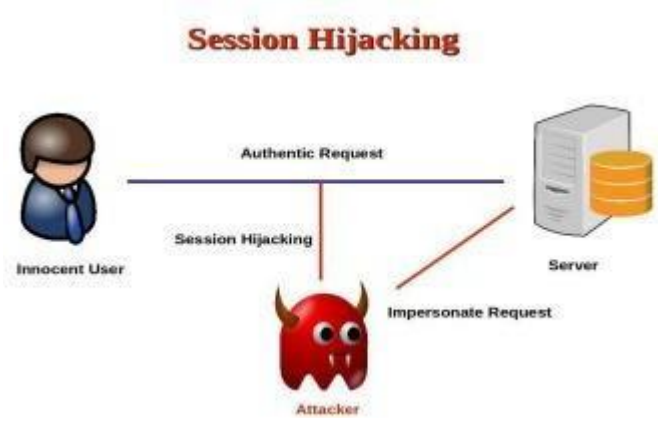
Denial of service (DOS) attack, a type of network attack designed to bring a network to its knees
it overwhelms it with unnecessary traffic. In a computer network, a denial-of-service attack is an attempt to make a machine or
network resource unavailable to intended users, such as temporarily or indefinitely interrupting or suspending services
host connected to the Internet. A DOS Attack can be initiated in many ways:

1) transmission failure
2) traffic redirection
3) DNS attack
4) Connection flooding.



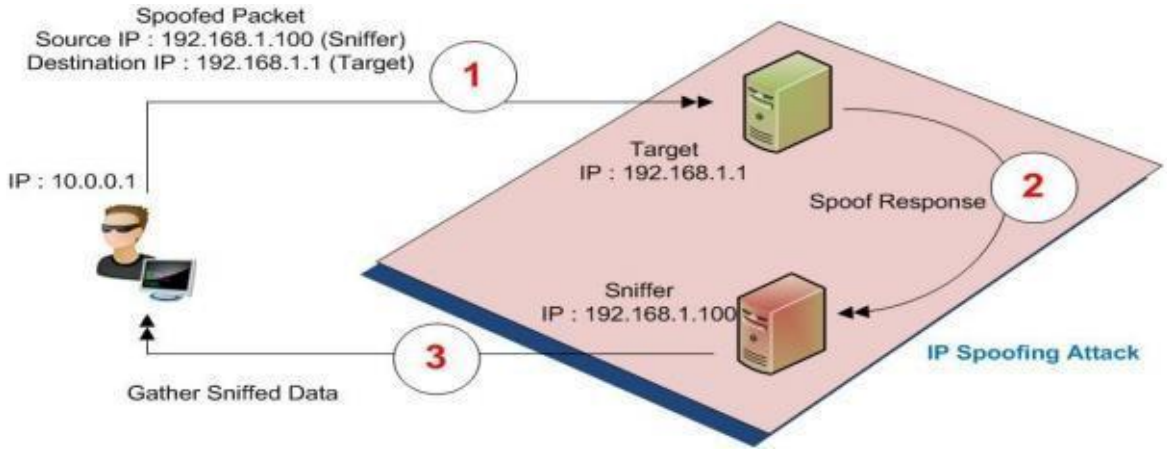
4. Hijack Attack

In a hijack attack, a hacker takes over a session (Hijack session) between an innocent user and an individual server and
disconnects the other individual from communication. The innocent user still believes he is talking to
the original party and may accidentally send some private information to the hacker.



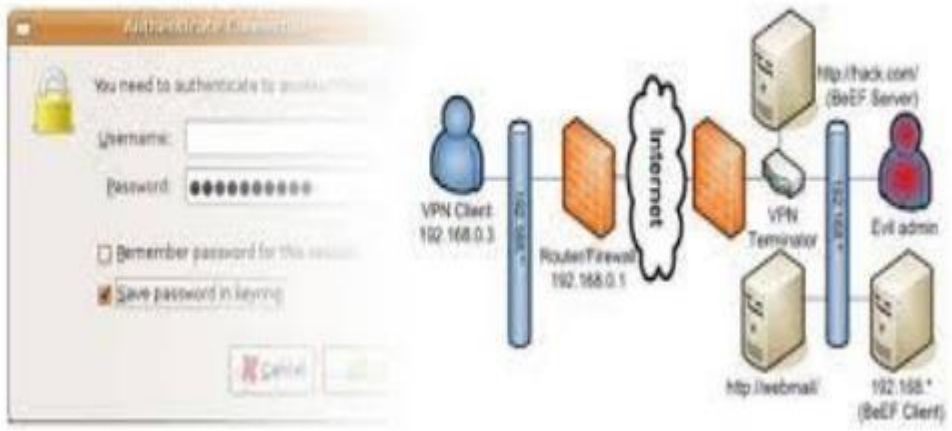
5. Spoof Attack

In a spoof attack, the hacker modifies/changes the source IP address of the (sanded) packets so that
They seem to come from someone else and the receiver thought the packets came from the real source address. This
may be an attempt to bypass your firewall rules.



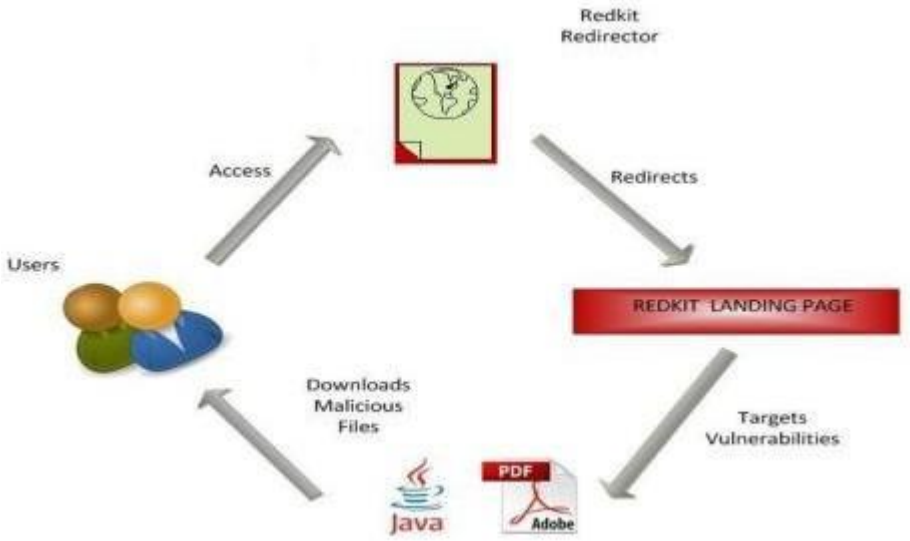
6. Password Attack

An attacker is trying to crack passwords stored in a network account database or a password-protected file. They exist
three main types of password attacks: dictionary attack, brute force attack and hybrid attack. Dictionary attack
it uses a wordlist file, which is a list of potential passwords. A brute force attack is when the attacker tries everything possible
combined characters.



7. Exploit attack

The meaning of exploit is "to use something to your own advantage", an Exploit is a piece of software and a sequence
some command or piece of data. In this type of attack, the attacker knows about the real security problem inside
operating system or piece of software and uses this knowledge by exploiting a vulnerability to occur
to computer hardware and software or something electronic that is usually computerized. Some things are often
it includes, for example, gaining control of a computer system and allowing privilege escalation and associated denial of service Attack



.

8. Buffer overflow

A buffer overflow is the same as a stack overflow, a buffer overflow attack escalates when an attacker sends more data to
application than expected. A buffer overflow attack usually results in an attacker gaining administrative access
system in a command line or shell..

Threat mode in isolated devices

The emergence of isolated devices has brought enormous possibilities and likely uses cases that affect our life from various aspects. It comes with ups and downs
and dark sides. IoT is becoming more and more popular and attractive attackers. Security issues in the IoT environment arise from the sloppy programming design of IoT devices and heterogeneous interconnected complex protocols. Several attacks targeting connected devices have been reported in the media and include popular brands such as Philips. It has
it has also been reported that even a single bug can affect a wide range of products from WiFi cameras, camera recorders and cloud storage devices from of the same supplier. A single defect affected multiple devices from manufacturers reuse the vulnerable code in different device models. Latest news about two hackers remotely controlling the air conditioner, radio, windshield wipers
and even the Jeep Accelerator presents a security gap in the IoT systems installed in the jeep. That kind of failure can be life-threatening for a jeep driver There have been reports of a leaked WikiLeaks document which states that some Samsung TV models are also vulnerable.
These vulnerable TVs secretly record audio when the TV screen is off and send it to the Central Intelligence Agency (CIA) server while the TV is on and its Internet connection is restored. In 2014, it was also revealed
that more than 100,000 consumer gadgets including home network routers, Televisions and refrigerators were the target of a large-scale attack 750,000 malicious emails to individuals and businesses.
The stakes for vulnerable devices on the network are quite high. PUSH
there is a strong need to identify and audit vulnerable devices before granting they have access to our home network. Securing a home network is difficult reach from many threats such as denial of service, backdoor and remote administrative programs, malware, etc. With the enormous potential of IoT comes security and privacy concerns. Some IoT devices
which are deployed in the users' network are vulnerable and can be exploited attackers. Since IoT devices can connect to the Internet,

Vulnerable IoT devices are attractive for attackers to target in a variety of ways attacks on other devices on the network and network penetration. One solution to deal with such vulnerable devices is to patch them
updated security solution. However, most device manufacturers do not
produce a patch in a timely manner due to the associated support overhead. It is it was also seen that production and support for the device was discontinued after short time of its launch.

Ordinary access points provided by Smart Office Home Office (SOHO)
routers that are widely used in home networks lack security measures such as such as wireless client isolation, guest network allocation, updated encryption modules etc. Naive users do not have enough knowledge about the need
to update the router's firmware. For the common user, there is a firmware update a daunting task as it requires a number of manual tasks. Thus, old routers contain a high risk of exploitation due to the lack of a proper security mechanism and repairs.

Whenever a device connects to an AP, it is authenticated by the wireless authentication mechanism implemented on the router. After successful authentication an IoT device with an AP has an IP connection granted to the IoT device. IP connectivity leases are provided by the DHCP server. In this kind of scenario, security the AP provided is a critical factor for network protection. If the AP is not protected by a security feature that limits the ability of vulnerable people device, an attacker can use this vulnerable device to attack other devices in the net.

For example, any compromised surveillance camera in the explained home setup can upload live feed to some remote server
an attacker can have a 24/7 live view of the home. This kind of situation violates total home security which completely defeats the purpose of having a camera in the home. So device identification before granting access
network is very important. With proper device identification
and defining its security boundaries can be the security of the entire network maintained..

Threat actors for isolated devices

A threat actor, also known as a malicious actor, is any person or organization that intentionally causes harm in the digital realm. They exploit weaknesses in computers, networks, and systems to conduct disruptive attacks on individuals or organizations.

Most people are familiar with the term "cybercriminal". It resembles the thieves behind a ransomware attack or dark images of personal information exposed on the dark web. The term "threat actor" includes cybercriminals, but is much broader. Idealists such as hacktivists and terrorists, insiders and even internet trolls are all seen as threat actors.

I. Insider

An insider threat is a risk to an organization's security coming from someone associated with the organization, such as an employee, former employee, supplier, consultant, board member, or vendor.

These threats can be malicious or random Initiates can deal damage in several ways:
Theft, leakage or destruction of data Selling company secrets
Breakdown of systems, networks or other IT resources Misplacement of company equipment
Sending an email attachment to the wrong person Fall victim to fraudsters
Misconfiguration of network or database settings

There are many different types of insider threats that pose security risks:

Non-responders:
A small percentage of people do not respond to security awareness training. While they may not intend to be careless, they are among the most at-risk members because their behavior follows consistent patterns. For example, individuals with a strong history of phishing are likely to be attacked again.

Inadvertent Insiders:
Negligence is the most common and most expensive form of insider threat. This group generally exhibits secure behavior and conforms to information security policies, but causes security incidents due to isolated errors. For example, a
common insider threat is the storage of intellectual property on unsecured personal devices.

Collusion:
Insider collaboration with malicious external threats is a rare but significant threat due to the increasing frequency with which cybercriminals attempt to recruit employees through the dark web. A Community Emergency Response Team (CERT) study found that collusion between insiders and outsiders accounted for 16.75% of security incidents caused by insiders.

Persistent Malicious Insiders:
This type of insider threat most often attempts to exfiltrate data or perform other malicious actions such as installing malware for financial gain. A Gartner study on criminal insider threats found that 62 percent of malicious insiders are people looking for supplemental income.
Disgruntled Employees: Disgruntled employees may intentionally sabotage security tools, data security controls, or commit intellectual property theft. These types of employees can be identified through behavioral analysis because they can follow specific patterns of behavior. For example, they can start looking at sources of sensitive data when they file a notice or have been fired before access is removed.

Moles:
An impostor who is technically an outsider but has managed to gain access from the inside. It is someone outside the organization who impersonates an employee or partner.

II. Man in middle

A man-in-the-middle attack is a type of eavesdropping attack where attackers interrupt an existing conversation or data transfer. After inserting themselves into the "middle" of the transfer, attackers impersonate both legitimate participants.
This allows an attacker to capture information and data from either party while sending malicious links or other information to both legitimate participants in a way that may not be detected until it is too late.

You can think of this type of attack as similar to a game of telephone where one person's words are passed from participant to participant until they change before reaching the final person. In a man-in-the-middle attack, a middle participant manipulates a conversation unknown to either of the two legitimate participants, acting to obtain confidential information and otherwise cause harm.

Man-in-the-middle attacks:

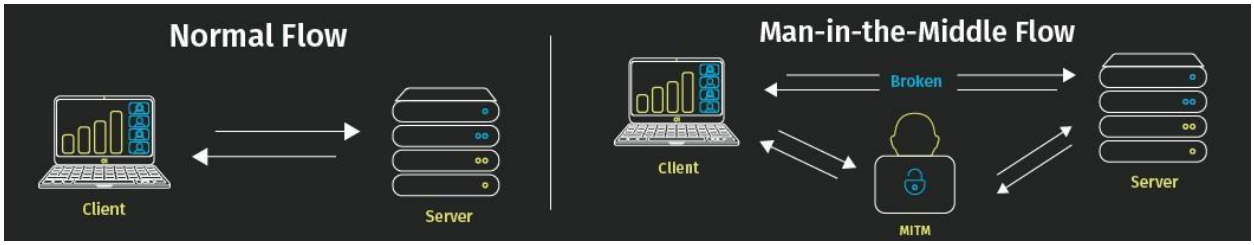
They are a type of session hijacking
Engage attackers who insert themselves as relays or proxies into an ongoing, legitimate conversation or data transfer
Take advantage of the real-time nature of conversations and data transfers to avoid detection
Allow attackers to capture confidential data
Allow attackers to insert malicious data and links in a manner indistinguishable from legitimate data

Examples of MITM Attacks

Scenario 1: Intercepting Data

1. The attacker installs a packet sniffer to analyze network traffic for insecure communications.
2. When a user logs in to a site, the attacker retrieves their user information and redirects them to a fake site that mimics the real one.
3. The attacker's fake site gathers data from the user, which the attacker can then use on the real site to access the target's information.

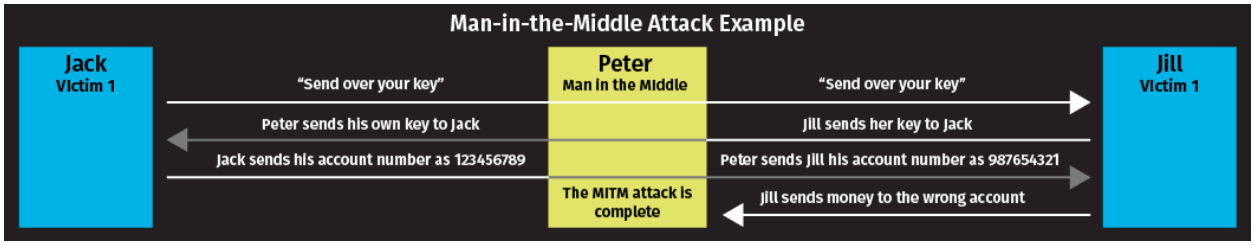
In this scenario, an attacker intercepts a data transfer between a client and server. By tricking the client into believing it is still communicating with the server and the server into believing it is still receiving information from the client, the attacker is able to intercept data from both as well as inject their own false information into any future transfers.



Scenario 2: Gain access to resources

An attacker creates a fake chat service that mimics that of a well-known bank. Using the knowledge gained from the data captured in the first scenario, the attacker impersonates the bank and initiates a chat with the target.The attacker then starts a chat on a real banking site, pretends to be the target, and provides the necessary information to gain access to the target's account.

In this scenario, an attacker intercepts the conversation and forwards parts of the discussion to both legitimate participants.



III. Adversary

An entity that is not authorized to access or modify information, or who works to defeat any protections afforded the information.

In its most simplistic definition, a cyber adversary is someone or a group that intends to perform malicious actions against other cyber resources. However, there is a lot of nuances in defining adversaries, which the simple definition doesn't cover.

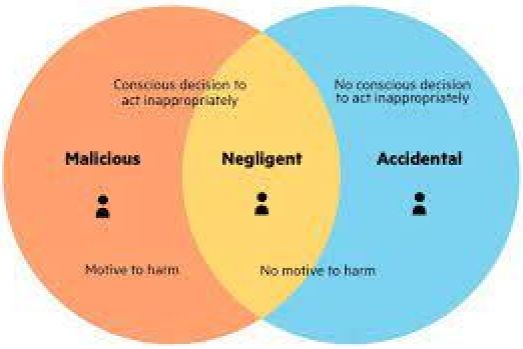
INSIDER CATEGORIES:

Insider:

an insider is any person from an organization who has an a authorized access to the resources of organization.

Insider Threats:

Insider threats are threats that come from within an organization .It can be caused by a current or even former employee who has access to the network resources,devices and other sites that holds data.



Insider categories:

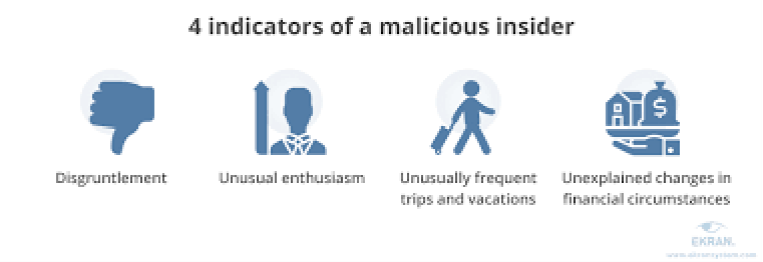
1) Negligent insider:

Negligent insider are those who ignore any safety precautions when using buseiness computers.

For example,an employee may have ignored any warnings about phishing emails still choosing to open up without knowing what kind of trouble they are goin tgo cause.

2) Malicious insider:

Bad actors such as current or former employees,third parties or partners uses their privileged access to steal intellectual property or company data for fraud ,revenge Or blackmail.



3) Accidental insider:

Some unintentially put your network under fire,
A simple example of this would be an employee downloading a file from internet,thinking it is safe ,while in reality it is a threat to your network.

4) Problematic insider:

some intentionally carry out malicious activities.
they can be anyone, from unhappy employees seeking revenge to employees looking to make extra money by sharing confidential information

Consequences of such threats:
There are a whole list of consequences your business can face :

- ranging from data loss to a damaged reputation.

- Attacks leads to a loss in reputation or finances.

- Drop in sale due to loss of trust from customers to legal costs.

How can insider Threats be detected:
Here is the list of direct indicators in case of insider threats attacks:

- Data Exfiltration.
- Unauthorized use fo external systems
- Abnormal network activities such as crawling ,downloading of internal portals
- Sharing data with outsiders

Indirect indicators in case of insider threats attacks:

- Workspace access outside job hours.
- Attempts to access priviliges areas
- Complaints of unethical or hostile behaviours.
- Violations of corporate policies.