UNIT 03 Network Forensics

3.1 Network Forensic:

The word “forensics” means the use of science and technology to investigate and establish facts in criminal or civil courts of law. Forensics is the procedure of applying scientific knowledge for the purpose of analyzing the evidence and presenting them in court.

Network forensics is a subcategory of digital forensics that essentially deals with the examination of the network and its traffic going across a network that is suspected to be involved in malicious activities, and its investigation for example a network that is spreading malware for stealing credentials or for the purpose analyzing the cyber-attacks. As the internet grew cybercrimes also grew along with it and so did the significance of network forensics, with the development and acceptance of network-based services such as the World Wide Web, e-mails, and others.

With the help of network forensics, the entire data can be retrieved including messages, file transfers, e-mails, and, web browsing history, and reconstructed to expose the original transaction. It is also possible that the payload in the uppermost layer packet might wind up on the disc, but the envelopes used for delivering it are only captured in network traffic. Hence, the network protocol data that enclose each dialog is often very valuable.

For identifying the attacks investigators must understand the network protocols and applications such as web protocols, Email protocols, Network protocols, file transfer protocols, etc.

Investigators use network forensics to examine network traffic data gathered from the networks that are involved or suspected of being involved in cyber-crime or any type of cyber-attack. After that, the experts will look for data that points in the direction of any file manipulation, human communication, etc. With the help of network forensics, generally, investigators and cybercrime experts can track down all the communications and establish timelines based on network events logs logged by the NCS.

Processes Involved in Network Forensics:

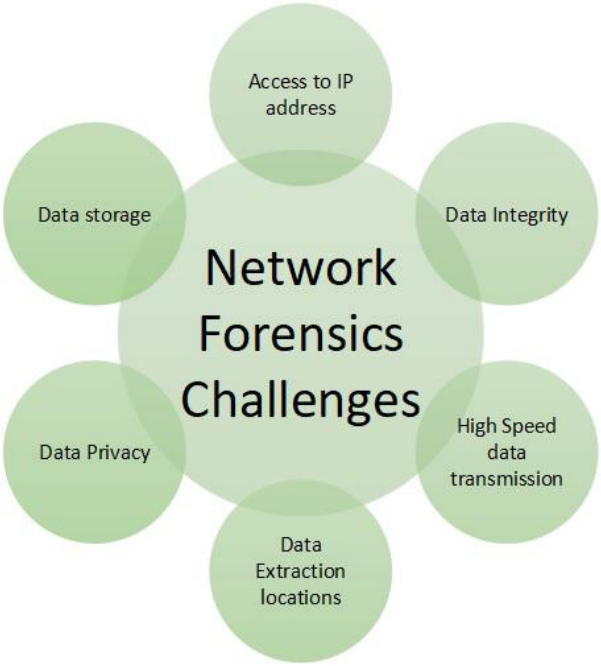
Some processes involved in network forensics are given below:

- **Identification:** In this process, investigators identify and evaluate the incident based on the network pointers.
- **Safeguarding:** In this process, the investigators preserve and secure the data so that the tempering can be prevented.
- **Accumulation:** In this step, a detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
- **Observation:** In this process, all the visible data is tracked along with the metadata.

- **Investigation:** In this process, a final conclusion is drawn from the collected shreds of evidence.
- **Documentation:** In this process, all the shreds of evidence, reports, conclusions are documented and presented in court.

Challenges in Network Forensics:

- The biggest challenge is to manage the data generated during the process.
- Intrinsic anonymity of the IP.
- Address Spoofing.



Advantages:

- Network forensics helps in identifying security threats and vulnerabilities.
- It analyzes and monitors network performance demands.
- Network forensics helps in reducing downtime.
- Network resources can be used in a better way by reporting and better planning.
- It helps in a detailed network search for any trace of evidence left on the network.

Disadvantage:

- The only disadvantage of network forensics is that It is difficult to implement.

3.2 Types of Network Configuration

1. **LAN-Local Area Network**
2. **WAN-Wide Area Network**
3. **MAN-Metropolitan Area Network**

3.3 Network Components

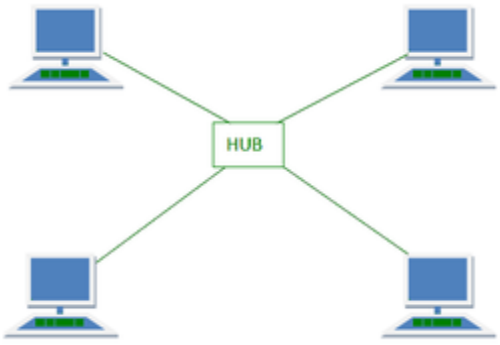
computer network is a system that connects multiple independent computers in such a way that they can share information and resources. Some of the Physical Components of the Computer Network are mentioned below:

1. NIC(Network Interface Card)
2. HUB
3. Router
4. Modem
5. Switch
6. Nodes
7. Media

1. NIC(Network Interface Card): NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model. There are two types of NIC:

- **Wired NIC:** Cables and Connectors use Wired NIC to transfer data.
- **Wireless NIC:** These connect to a wireless network such as Wifi, Bluetooth, etc.

2. HUB: A HUB is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one.



3. Router: A Router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make

decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

4. Modem: A Modem is a short form of Modulator/Demodulator. The Modem is a hardware component/device which can connect computers and other devices such as routers and switches to the internet. Modems convert or modulate the analog signals coming from telephone wire into a digital form that is in form of 0s and 1s.

5. Switch: A Switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

6. Nodes: Node is a term used to refer to any computing devices such as computers that send and receive network packets across the network. Two Types of nodes are :

- **End Nodes:** These type of nodes is going to be the starting point or the end point of communication. E.g., computers, security cameras, network printers, etc.
- **Intermediary Nodes:** These nodes are going to be in between starting point or end point of the end nodes. E.g., Switches, Bridges, Routers, cell towers, etc.

7. Media: Also known as Link which is going to carry data from one side to another side. This link can be Wired Medium (Guided Medium) and Wireless Medium (Unguided Medium). It is of two types:

1. Wired Media
2. Wireless Media

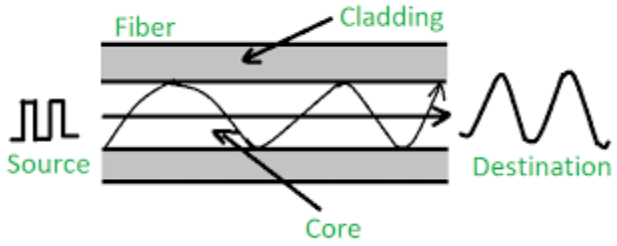
Examples of Wired media are as follows:

Ethernet: Ethernet is the most widely used LAN technology, which is defined under IEEE standards 802.3. There are two types of Ethernet:

1. Ethernet straight-through cable (used for two different devices).

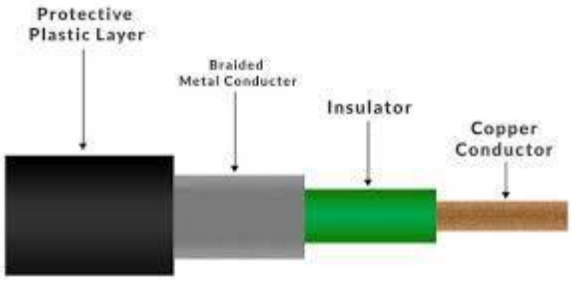
2. Ethernet crossover cable (used for two same devices).

Fibre Optic Cable: In this data is transferred in the form of light waves.



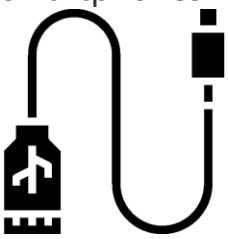
Optic Fibre Cable

Coaxial Cable: Mainly used for audio and video communications.



Coaxial Cable

USB Cable: USB Stands for Universal Serial Bus. Mainly used to connect PC and smartphones.



USB Cable

Examples of Wireless media are as follows:

- Infrared (E.g. short-range communication – TV remote control).
- Radio (E.g. Bluetooth, Wi-Fi).
- Microwaves (E.g. Cellular system).
- Satellite (E.g. Long range communications – GPS).

3.4 Attacks on network components

1. Password-Based Attacks

Password-based access control is the common denominator of most network and operating system **security policies**. You can, therefore, determine who you are, that is, your user name and your password, your computer and your network access rights. Old systems do not always secure identity information because authentication information is transmitted through the network. This could give an eavesdropper legitimate user access to the network. The intruder has the same privileges as an actual client if he enters a legitimate user account. Therefore, the intruder may also build later access accounts if the client has administrator-leaved privileges.

2. Man-in-the-Middle Attack

As its name suggests, when someone in the center is constantly tracking, capturing and monitors your contact, someone between you and the person with whom you interact. The attacker can, for instance, restart the data exchange. Computers can not determine how they share information on a low level of the network layer While computers are communicating. Man-in – the- middle attacks are just like those who take up your identity to read your text. The other person might assume you are because the intruder may deliberately respond so that you sustain the exchange and obtain more information. His attack can do the same damage as an app layer attack mentioned below in this section.

3. Close-in Attack

A Close-in Attack involves someone who attempts to physically enter the elements, data or structures of a network to find out more about a close-in attack consists of ordinary persons entering near physical proximity to networks, systems or facilities to alter or collect information or to reject access. Near physical proximity is achieved by sudden network entry, open access, or both. A popular form of close attack is social engineering in a social engineering attack. Through social interaction, an email message or a telephone, the attacker exploits the network and device.

4. Identity Spoofing

The IP address of a device is used to classify a legitimate business by most networks and operating systems. An intruder can also create IP packets from valid addresses in the corporate intranet using specific programs. An attacker can. The hacker may alter, remove, or erase your data after accessing the network using a valid IP address. As defined in the following sections, the attacker may also perform other Types of Attacks.

5. Compromised-Key Attack

One key is a secret code or number required for the processing of secure information. While it is possible to obtain a key for an attacker to be a complicated and resource-intensive process. After an attacker gets a password, it is considered a corrupted key. An attacker uses the affected key to gain access to secure communication without the attack being detected by the sender or recipient. The attacker may decrypt or alter the information by using the affected key to generate additional keys to give the attacker access to any other secure communications.

6. Application-Layer Attack

An application-layer attack targets database servers, triggering a failure on a server's operating system or applications deliberately. It helps the intruder to bypass standard access controls. This situation is used by the intruder, who gets control of your application, device or network and can do any of the following:

- Read your data or add, operating system, delete or change them.
- Introduce a virus system to copy viruses in your network using your computers and software applications.
- Introduce a sniffer to evaluate and collect information that can crash or corrupt the network and systems in the end.

7. Passive Attack

A Passive Attack tracks unencrypted traffic and scans for code or confidential information for other attack forms. Passive threats include traffic analyzes, insecure contact surveillance, weakly encrypted traffic decryption, and encryption information collecting, for example, passwords. Passive network monitoring allows opponents to see future measures. Passive attacks lead, with no user consent or knowledge, to the disclosure of information or data files to an attacker.

8. Active Attack

The Attacker attempts to hack or crack into secure systems in an aggressive attack. It can take place through stealth, worms, viruses or Trojan horses. Aggressive attacks include attempts to circumvent or break safety software, malicious codes, and theft or alteration. Such attacks have been installed on a network backbone, take advantage of the information in transit, join an enclave electronically or target a remote authorized user while attempting to link to an enclave. Active attacks lead to data files, DoS and alteration. Software is exposed and disseminated.

9. DoS

A **DoS** Attack renders legitimate users unable to use a network, server or other resources. In one of the three groups.

1. **Bandwidth Flooding:** The Attacker sends a dilution of packets to the target host — so many packets that the access path to the target is blocked, and legit packets can not enter the server.
2. **Vulnerability Attack:** This means sending a set of well-constructed messages on the targeted host to a vulnerable program or operating system. If a compromised program or operating system is sent the correct sequence of packages, the service can stop, or the host can crash.
3. **Connection Flooding:** Many TCP connections on the target host are formed half-open or completely open. With these fake connections, the host can be so enmeshed that it can no longer accept valid connections.

10. Packet Sniffer

A passive receiver that records a copy of each flying packet is a packet sniffer. By every passive receiver near the wireless transmitter, it can get a copy of each transmitted packet. Such packages can contain some sensitive information such as social security numbers, passwords, personal messages, and business secrets. Cryptography includes some of the best defences from packet sniffing.

11. Malware

Malware is specifically intended for interrupting, damaging or obtaining licensed computer system access. Some of the malware today replicates itself: Once the host becomes infected, it is looking for connections to other hosts via the internet from that host and seeks entry in even more **hosts** from the newly infected host. Self-replicating malware can propagate exponentially rapidly in this way.

12. Insider Attack

Insider Attacks involve someone from inside of the company or system, such as an insecure worker who may be malicious or not malicious by targeting the network for insider attacks. Intentional malicious insiders eavesdrop, steal data or erase it, fraudulently use it or deny access to other users who have been licensed. There are no traditional malicious attacks due to lack of consideration, awareness or intentional security circumvention, for example, executing a mission.

3.5 Network attack Evidences-Firewall, backdoor

A backdoor attack is a way to access a computer system or encrypted data that bypasses the system's customary security mechanisms. A developer may create a backdoor so that an application, operating system (OS) or data can be accessed for troubleshooting or other purposes. Attackers make use of backdoors that software developers install, and they also install backdoors themselves as part of a computer exploit. A backdoor attack occurs when threat actors create or use a backdoor to gain remote access to a system. These attacks let attackers gain control of system resources, perform network reconnaissance and install different types of malware. In some cases, attackers design a worm or virus to take advantage of an existing backdoor created by the original developers or from an earlier attack.

To illustrate how backdoors undermine security systems, consider a bank vault that is protected with several layers of security. It has armed guards at the front door, sophisticated locking mechanisms and biometric access controls that make it impossible to access without proper authorization. However, a backdoor that bypasses these measures, such as a large ventilation shaft, makes the vault vulnerable to attack.

The malicious actions threat actors perform once they access a system include the following:

- stealing sensitive information;
- performing fraudulent transactions;
- installing spyware, keyloggers and Trojan horses;
- using rootkits;
- launching denial of service (DoS) attacks;
- hijacking servers; and
- defacing websites.

The consequences of a backdoor attack vary. In some cases, they can be immediate and severe and result in a data breach that harms customers and the business. In other cases, the effect shows up later, as the attacker uses the backdoor first for reconnaissance and returns later to execute a series of direct attacks.

Backdoor attacks can be large-scale operations, targeting government or enterprise IT infrastructure. However, smaller attacks are used to target individuals and personal computing implementations.

Advanced persistent threats are sophisticated cyber attacks that might use a backdoor to attack a system on multiple fronts. With these sorts of attacks, the backdoor could remain in the system for a long time.

What is a backdoor attack?

A backdoor attack occurs when threat actors create or use a backdoor to gain remote access to a system. These attacks let attackers gain control of system resources, perform network reconnaissance and install different types of malware. In some cases, attackers design a worm or virus to take advantage of an existing backdoor created by the original developers or from an earlier attack.

To illustrate how backdoors undermine security systems, consider a bank vault that is protected with several layers of security. It has armed guards at the front door, sophisticated locking mechanisms and biometric access controls that make it impossible to access without proper authorization. However, a backdoor that bypasses these measures, such as a large ventilation shaft, makes the vault vulnerable to attack.

The malicious actions threat actors perform once they access a system include the following:

- stealing sensitive information;
- performing fraudulent transactions;
- installing spyware, keyloggers and Trojan horses;
- using rootkits;

- launching denial of service (DoS) attacks;
- hijacking servers; and
- defacing websites.

The consequences of a backdoor attack vary. In some cases, they can be immediate and severe and result in a data breach that harms customers and the business. In other cases, the effect shows up later, as the attacker uses the backdoor first for reconnaissance and returns later to execute a series of direct attacks.

Backdoor attacks can be large-scale operations, targeting government or enterprise IT infrastructure. However, smaller attacks are used to target individuals and personal computing implementations.

Advanced persistent threats are sophisticated cyber attacks that might use a backdoor to attack a system on multiple fronts. With these sorts of attacks, the backdoor could remain in the system for a long time.

How do backdoors work?

In the context of an attack, backdoors are hidden mechanisms attackers use to access a system without authentication. However, vendors sometimes create backdoors for legitimate purposes, such as restoring a user's lost password or providing government entities with access to encrypted data. Other backdoors are created and installed nefariously by hackers. Developers sometimes use backdoors during the development process and don't remove them, leaving them as a potential vulnerability point.

Malware can also act as a backdoor. In some cases, malware is a first-line backdoor, where it provides a staging platform for downloading other malware modules that perform an actual attack. With this type of attack, threat actors install a web shell to establish a backdoor on targeted systems and obtain remote access to a server. The attacker uses a command-and-control server to send commands through the backdoor to sensitive data or otherwise cause harm.

Types of backdoor attacks

Various types of malware are used in backdoor attacks, including the following:

- **Cryptojacking** occurs when a victim's computing resources are hijacked to mine cryptocurrency. Cryptojacking attacks target all sorts of devices and systems.
- **DoS attacks** overwhelm servers, systems and networks with unauthorized traffic so that legitimate users can't access them.
- **Ransomware** is malware that prevents users from accessing a system and the files it contains. Attackers usually demand payment of a ransom for the resources to be unlocked.
- **Spyware** is malware that steals sensitive information and relays it to other users without the information owner's knowledge. It can steal credit card numbers, account login data and location information. Keyloggers are a form of spyware used to record a user's keystrokes and steal passwords and other sensitive data.
- **Trojan horse** is a malicious program that's often installed through a backdoor and appears harmless. A backdoor Trojan includes a backdoor that enables remote administrative control of a targeted system.

Various attack vectors are used to install backdoors, such as the following:

- **Federated learning.** This decentralized method of machine learning trains models locally on edge devices, as opposed to collecting data and training it in a centralized location. Edge devices have limited communication with the centralized servers. This lets threat actors poison a training data set and embed a backdoor on the central server when it does communicate with the edge device.
- **Hardware.** Attackers use modified chips, processors, hard drives and USBs to create backdoors.
- **Internet of things (IoT).** Components of these systems, such as security cameras, drones and smart thermostats, can act as backdoors and turn into security vulnerabilities. IoT devices often come equipped with default

passwords that function as a backdoor. Administrators often don't change them, and hackers can easily guess them.

- **Island hopping.** These types of attacks target an organization's third-party business partners to gain unauthorized access to the larger organization being targeted. Supply chains can be compromised using island hopping.
- **Phishing.** Seemingly legitimate emails are used to trick users into giving hackers sensitive information and can be used to install backdoor malware.
- **Steganography.** Malware is concealed in the bitmap of an image file. These files would normally not be considered a security threat, but steganography turns them into one.

Detection and prevention

Backdoors are designed to be hidden from most users. They are hidden using alias names, code obfuscation and multiple layers of encryption. This makes backdoors difficult to detect. Detection and prevention methods include the following tools and strategies:

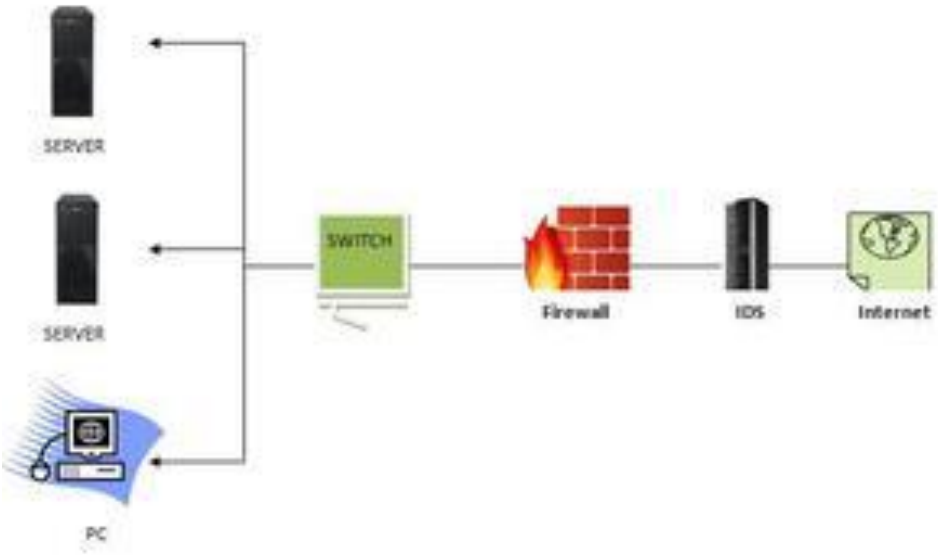
- **Antimalware.** Some antimalware software can detect and prevent a backdoor from being installed.
- **Firewalls.** Ensure a firewall protects every device on a network. Application firewalls and web application firewalls can help prevent backdoor attacks by limiting the traffic that can flow across open ports.
- **Honeypots.** These security mechanisms lure attackers to a fake target. Honeypots are used to protect the real network and study the behavior of an attacker without their knowledge.
- **Network monitoring.** IT professionals use a protocol monitoring tool or network analyzer to inspect network packets. Malicious traffic can contain signatures that indicate the presence of a backdoor, and abnormal spikes in traffic can signal suspicious activity.
- **Security best practices.** Standard security measures and a layered cybersecurity strategy help prevent attackers from creating backdoors. If a

backdoor is created for a legitimate purpose, its attack surface should be minimized. It also must be monitored and removed once its legitimate use is finished.

- **Allowlisting.** Use allowlisting to avoid untrusted software and only allow trusted user access with proper authentication. Choose applications and plugins with caution, as cybercriminals often hide backdoors in free applications and plugins.

3.6 Intrusion Detection System

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.



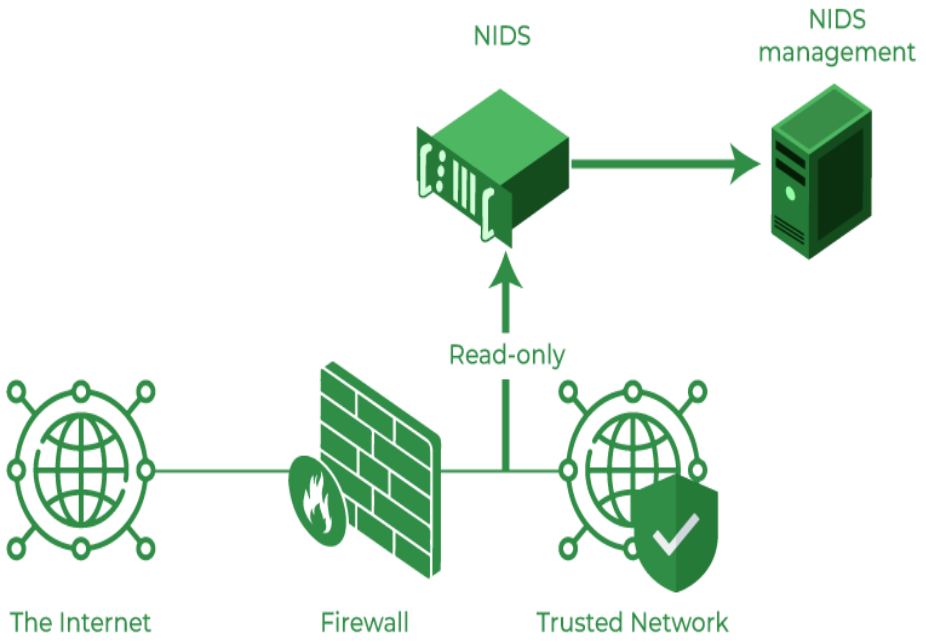
How does an IDS work?

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

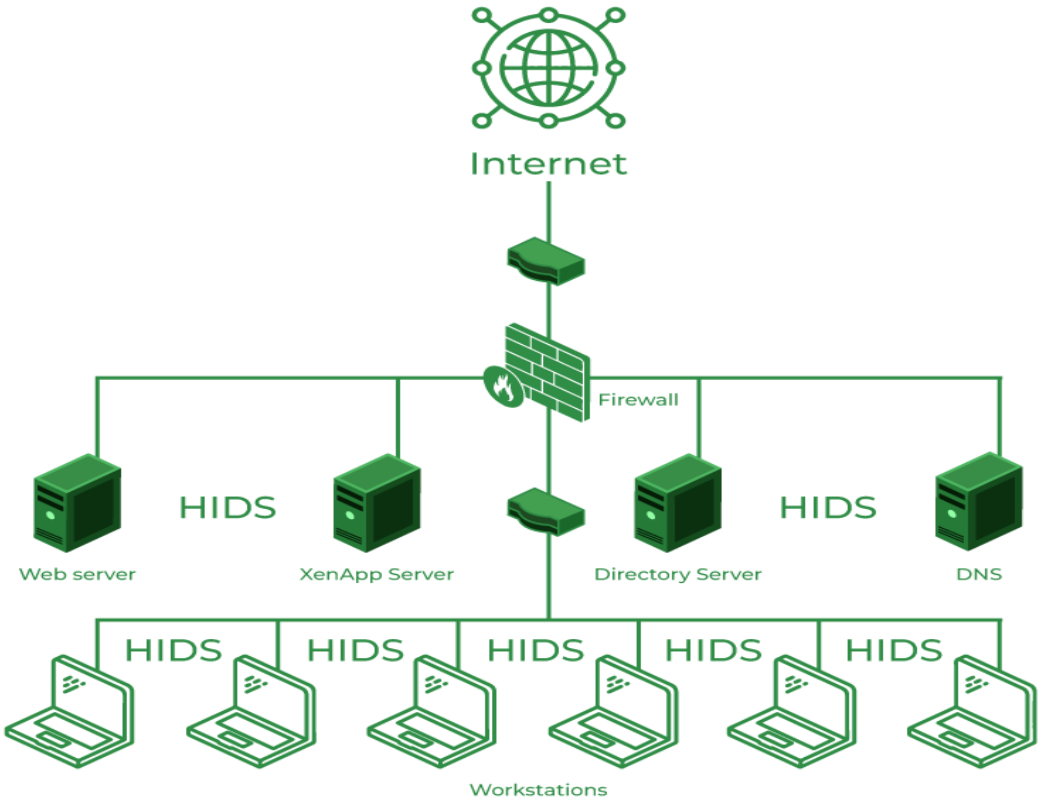
Classification of Intrusion Detection System

IDS are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.



- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.
- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Benefits of IDS

- **Detects malicious activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- **Improves network performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- **Compliance requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
- **Provides insights:** IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Detection Method of IDS

1. **Signature-based Method:** Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.
2. **Anomaly-based Method:** Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Placement of IDS

The most optimal and common position for an IDS to be placed is behind the firewall. Although this position varies considering the network. The 'behind-the-firewall' placement allows the IDS with high visibility of incoming network traffic and will not receive traffic between users and network. The edge of the network point provides the network the possibility of connecting to the extranet.

In cases, where the IDS is positioned beyond a network's firewall, it would be to defend against noise from internet or defend against attacks such as port scans and network mapper. An IDS in this position would monitor layers 4 through 7 of the OSI model and would use Signature-based detection method. Showing the number of attempted

breacheds instead of actual breaches that made it through the firewall is better as it reduces the amount of false positives. It also takes less time to discover successful attacks against network.

An advanced IDS incorporated with a firewall can be used to intercept complex attacks entering the network. Features of advanced IDS include multiple security contexts in the routing level and bridging mode. All of this in turn potentially reduces cost and operational complexity.

Another choice for IDS placement is within the network. This choice reveals attacks or suspicious activity within the network. Not acknowledging security inside a network is detrimental as it may allow users to bring about security risk, or allow an attacker who has broken into the system to roam around freely. Tight internal security makes it difficult for hackers who have gained entry inside system to maneuver freely and escalate their privileges

Conclusion:

Intrusion Detection System (IDS) is a powerful tool that can help businesses in detecting and prevent unauthorized access to their network. By analyzing network traffic patterns, IDS can identify any suspicious activities and alert the system administrator. IDS can be a valuable addition to any organization's security infrastructure, providing insights and improving network performance.

3.7 Honeypots

Honeypot is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

The **cost of a honeypot** is generally **high** because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources still preventing attacks at the backend and access to any production system. A **honeynet** is a combination of two or more honeypots on a network.

Types of Honeypot:

Honeypots are classified based on their deployment and the involvement of the intruder. Based on their deployment, honeypots are divided into:

1. **Research honeypots-** These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.
2. **Production honeypots-** Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

Based on interaction, honeypots are classified into:

1. **Low interaction honeypots:** Low interaction honeypots gives very little insight and control to the hacker about the network. It simulates only the services that are frequently requested by the attackers. The main operating system is not involved in the low interaction systems and therefore it is less risky. They require very fewer resources and are easy to deploy. The only disadvantage of these honeypots lies in the fact that experienced hackers can easily identify these honeypots and can avoid it.
2. **Medium Interaction Honeypots:** Medium interaction honeypots allows more activities to the hacker as compared to the low interaction honeypots. They can expect certain activities and are designed to give certain responses beyond what a low-interaction honeypot would give.
3. **High Interaction honeypots:** A high interaction honeypot offers a large no. of services and activities to the hacker, therefore, wasting the time of the hackers and trying to get complete information about the hackers. These honeypots involve the real-time operating system and therefore are comparatively risky if a hacker identifies the honeypot. High interaction honeypots are also very costly and are complex to implement. But it provides us with extensively large information about hackers.

Advantages of honeypot:

1. Acts as a rich source of information and helps collect real-time data.
2. Identifies malicious activity even if encryption is used.
3. Wastes hackers' time and resources.
4. Improves security.

Disadvantages of honeypot:

1. Being distinguishable from production systems, it can be easily identified by experienced attackers.
2. Having a narrow field of view, it can only identify direct attacks.
3. A honeypot once attacked can be used to attack other systems.
4. Fingerprinting (an attacker can identify the true identity of a honeypot).

3.8 Sniffers

A sniffer, also known as a packet analyzer or network analyzer, is a tool used to capture and analyze network traffic. It is a software or hardware tool that intercepts and records data packets transmitted between computers or devices on a network.

Packet sniffers are commonly used for network troubleshooting, security analysis, and network optimization. They can be used to identify network problems such as congestion, packet loss, or improper configurations, and they can also be used to detect security threats such as network intrusions or unauthorized access attempts.

Packet sniffers work by capturing packets of data as they are transmitted on the network. These packets are then analyzed and displayed to the user in a human-readable format, allowing them to examine the contents of the packets and extract information from them.

Packet sniffers can be used on both wired and wireless networks, and they can capture data from a variety of network protocols, including TCP/IP, HTTP, FTP, and SMTP.

However, it is important to note that packet sniffers can also be used for malicious purposes, such as intercepting sensitive information such as passwords, credit card numbers, or personal information. Therefore, the use of packet sniffers should be regulated and used only for legitimate purposes with appropriate consent and legal authority.

A **Sniffer** is a program or tool that captures information over a network. There are 2 types of Sniffers: Commercial Sniffers and Underground Sniffers.

1. **Commercial Sniffers –**
   Commercial sniffers are used to maintain and monitor information over the network. These sniffers are used to detect network problems. Network General Corporation (NGC) is a company that offers commercial sniffers. These can be used for:
   1. Fault analysis to detect problems in a network.
   2. Performance analysis to detect network bottlenecks.

2. **Underground Sniffers –**
   Underground sniffers are malicious programs used by hackers to capture information over a network when underground sniffers are installed on the router, it can breach security of any network that passes through the router. It can capture:
   1. Confidential messages like email.
   2. Financial data like debit card details.

Components of a Sniffer:
To capture the information over the network sniffer uses the following components:

1. **Hardware –**
   Sniffers use standard network adapters to capture network traffic.

2. **Capture Driver –**
   Capture Driver captures network traffic from Ethernet wire, filters that network traffic for information that you want, and then stores the filtered information in a buffer.

3. **Buffer –**
   When a sniffer captures data from a network, it stores data in a buffer. There are 2 ways to store captured data –
   1. You can store data until the buffer is filled with information

   2. It is the round-robin method in which data in the buffer is always replaced by new data that is captured.

4. **Decoder –**
   The information that travels over the network is in binary format, which is not readable. you can use a decoder to interpret this information and display it in a readable format. A decoder helps you analyze how information is passed from one computer to other.

Placement of Sniffer:
The most common places where you can place sniffers are:
1. Computer
2. Cable wires
3. Routers
4. Network segments connected to the internet

3.9 Wiresharks

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.

The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer networking-related professional.

There are many reasons why Wireshark is so popular :

1. It has a great GUI as well as a conventional CLI(T Shark).
2. It offers network monitoring on almost all types of network standards (ethernet, wlan, Bluetooth etc)
3. It is open-source with a large community of backers and developers.
4. All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.

3.10 Keyloggers

Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware. **Working:** Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.

1. **Software key-loggers :** Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.
   a) **JavaScript based key logger –** It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.
   b) **Form Based Key loggers –** These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers : These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

a) **USB key logger –** There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.
b) **Smartphone sensors –** Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

Prevention from key-loggers : These are following below-

1. **Anti-Key-logger –** As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.
2. **Anti-Virus –** Many anti-virus software also detects key loggers and delete them from the computer system. These are software anti-software so these cannot get rid from the hardware key-loggers.
3. **Automatic form filler –** This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed.

4. **One-Time-Passwords –** Using OTP's as password may be safe as every time we login we have to use a new password.
5. **Patterns or mouse-recognition –** On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.
6. **Voice to Text Converter** – This software helps to prevent Keylogging which targets a specific part of our keyboard.

3.11 Network forensics analysis tools and Software

Network forensic tools are incredibly useful when it comes to evidence collection, especially in a day and age when most people are constantly within reach of a cell phone, laptop and other technology. In this blog post we explore nearly two dozen types of network forensics tools and techniques that cybersecurity professionals are using to aid in investigations.

- **AccessData FTK**
  This computer forensic software is recognized as the standard toolkit for cyber defense forensic analysts. Features include full-disk forensic images, as well as the ability to decrypt files, crack passwords, parse registry files and more. A 10-day free trial and a variety of pricing and plans are available.
- **Bulk Extractor**
  Extract structured information — email addresses, credit card numbers, JPEGs and JSON snippets — with this high-performance digital forensic exploitation tool. The software works by rapidly scanning any kind of input, like disk images, files, directories and more.
- **CAINE**
  CAINE, or Computer Aided Investigative Environment, integrates existing software tools as modules to provide a user-friendly graphical interface. This is an open-source software, designed to be publicly accessible.
- **Cellebrite UFED**
  Use this platform to access a broad range of mobile devices, including smartphones, drones, SIM cards and GPS devices. Collections are made possible with multiple data methods, including full file system and physical extraction.
- **EnCase**
  This court-accepted evidence format had found digital evidence to assist law enforcement and government agencies for more than two decades. Its intent is to reduce case backlogs by closing cases faster. Report templates are easily customized for a comprehensive view of findings.
- **HackerCombat**
  Organizations are able to detect and respond to cyber threats efficiently with this web-based console. An open-source software, HackerCombat offers a free Endpoint Detection and Response solution.
- **HELIX3**
  Reveal Internet abuse, data sharing and harassment without detection using HELIX3. This software integrates into your network, providing visibility across the entire infrastructure. Features include compliance management, protection from employee malicious behavior, litigation support and more.
- **NetworkMiner**

Extract files, images, emails, passwords and the like with NetworkMiner, an open source tool with free and professional editions. The software can also be used to capture live network traffic.

- **Paraben**
  E3 Digital Forensic Software from Paraben can be used for all types of digital data processing, including support for smartphone and computer forensics as well as email investigations. Digital investigative training is offered.
- **ProDiscover Forensic**
  This comprehensive digital forensic software empowers investigators to capture key evidence from computer systems. Features include collection, preservation, filtering and analyzing. ProDiscover was one of the first products to offer remote capabilities. Customers include — NASA, Microsoft, Sony Pictures, New York State Police and the National Institute of Standards and Technology, to name a few.
- **Registry Recon**
  Choose from one, three and five-year subscription plans to comb through registry data with a focus on changes over time. Access deleted registry data and even view keys and their values at particular points in time.
- **SANS SIFT**
  Take advantage of free and open-source incident response and forensic tools with SANS SIFT. The latest techniques are incorporated as they become available.
- **Sleuth Kit (+ Autopsy)**
  Law enforcement, military and corporate examiners take advantage of this digital forensics platform and graphical interface. Features include timeline analysis, hash filtering, keyword search, data carving and more. Installation is easy and the software is free to use.
- **Splunk**
  Splunk products — Splunk SOAR, Splunk Enterprise Security and Splunk Intelligence Threat — allow users to combat threats with advanced analytics. Keep your system secure and reliable, addressing threats before they are major problems.
- **Snort**
  This open source detection software uses rules to define malicious network activity and generate alerts quickly when threats arise.
- **Tcpdump**
  Capture and analyze network traffic with Tcpdump. This software is free and often used to help troubleshoot network issues.
- **Volatility**
  The Volatility Foundation is an independent non-profit organization that promotes open source memory forensics with the Volatility Framework. The program is written in Python.

- **WindowsSCOPE**
  WindowsSCOPE Cyber Forensics 3.2 is graphical user interface-based memory forensic capture and analysis toolkit. It has advanced search capabilities with applications including digital forensics, crime investigation, cyber defense and attack detention. WindowsSCOPE serves varying markets — incident response, law enforcement, reverse engineering, education and more.
- **Wireshark**
  This widely-used network protocol analyzer features live capture and offline analysis, decryption support, standard three-pane packet browser and more.
- **Xplico**
  A major benefit of Xplico is that multiple users on your team can take advantage of this open source network forensic analysis tool at the same time.
- **XRY**
  This forensics and data recovery software runs on a Windows operating system to provide powerful, intuitive and efficient mobile data recovery capabilities.
- **X-Way Forensics**
  This integrated computer forensics software has a long list of features and options — disk cloning and imaging, data interpretation, remote capabilities and more.