CHAP -3
INFRASTRUCTURE AND NETWORK SECURITY

INTRODUCTION TO SYSTEM SECURITY

- Computer/System Security is the protection of computing systems and the data that they store or access.
- Computer/system security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

WHY IS COMPUTER/SYSTEM SECURITY IMPORTANT?

- Computer Security allows the University to fufill its mission by:
  - Enabling people to carry out their jobs, education, and research activities
  - Supporting critical business processes
  - Protecting personal and sensitive information

WHY DO I NEED TO LEARN ABOUT COMPUTER/SYSTEM SECURITY? ISN'T THIS JUST AN IT PROBLEM?

- Good Security Standards follow the "90 / 10" Rule:
- 90% of security safeguards rely on an individual ("YOU") to adhere to good computing practices
- 10% of security safeguards are technical.
- Example: The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.

COMPUTER/SYSTEM SECURITY - ITS TYPES?

- One way to ascertain the similarities and differences among Computer Security is by asking what is being secured. For example,
- **Information security** is securing information from unauthorized access, modification & deletion
- **Application Security** is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.
- **Computer Security** means securing a standalone machine by keeping it updated and patched
- **Network Security** is by securing both the software and hardware technologies
- **Cybersecurity** is defined as protecting computer systems, which communicate over the computer networks

WHAT IS SERVER? AND ITS FUNCTIONS

- A server can be explained as a device or a computer program, providing a service to another computer program and its user generally referred to as the client. In a data center, the server program is run on a physical computer which is called as the server. Simply put, they just interconnect machines in a network. Traditionally, there are four types of servers,
- 1. FTP servers
- 2. Servers,
- 3. Online game servers
- 4. Web servers.
- **Functions of a Server**
- The key function of a computer server is to store, retrieve and send data and files to other computers in a network. The significance is understood when the concept is explained on a larger scale. The internet, the worldwide computer network relies on a large number of servers located around the world for easy exchange of data.

SERVER SECURITY

- As the server interconnect computers, they are the hub of a lot of valuable information that can be accessed. Protection of this accessible information assets from a Web Server is known as Server Security. A security rupture can harmfully affect the goodwill as well as the monetary status of an organization. Web server security becomes highly important when it is connected to the internet. The Websites facing the customers are really in need of layered security
- Server security covers the processes and tools used to protect the valuable data and assets held on an organization's servers, as well as to protect the server's resources. Due to the sensitive information they hold, servers are frequently targeted by cybercriminals looking to exploit weaknesses in server security for financial gain.

SOME COMMON SERVER SECURITY ISSUES FACED

- The most harmful mistakes which can cause the server less secure are as follows
- * Passwords
- * Open Network Ports
- * Old Software Version
- * Poor Physical Security
- * Insufficient security of CGIs
- * Old and Unnecessary Accounts
- * Procrastination

WHAT DOES OPERATING SYSTEM SECURITY (OS SECURITY) MEAN?

- Every computer system and software design must handle all security risks and implement the necessary measures to enforce security policies. At the same time, it's critical to strike a balance because strong security measures might increase costs while also limiting the system's usability, utility, and smooth operation. As a result, system designers must assure efficient performance without compromising security.
- The process of ensuring OS availability, confidentiality, integrity is known as operating system security. OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions. Operating system security comprises all preventive-control procedures that protect any system assets that could be stolen, modified, or deleted if OS security is breached.
- Security refers to providing safety for computer system resources like software, CPU, memory, disks, etc. It can protect against all threats, including viruses and unauthorized access. It can be enforced by assuring the operating system's **integrity, confidentiality**, and **availability**. If an illegal user runs a computer application, the computer or data stored may be seriously damaged.

WHAT DOES OPERATING SYSTEM SECURITY (OS SECURITY) MEAN?

- Security refers to providing safety for computer system resources like software, CPU, memory, disks, etc. It can protect against all threats, including viruses and unauthorized access. It can be enforced by assuring the operating system's **integrity, confidentiality**, and **availability**. If an illegal user runs a computer application, the computer or data stored may be seriously damaged.
- **The goal of Security System**
- **1. Integrity -** Unauthorized users must not be allowed to access the system's objects, and users with insufficient rights should not modify the system's critical files and resources.
- **2. Secrecy -** The system's objects must only be available to a small number of authorized users. The system files should not be accessible to everyone.
- **3. Availability -** All system resources must be accessible to all authorized users, i.e., no single user/process should be able to consume all system resources. If such a situation arises, service denial may occur. In this case, malware may restrict system resources and preventing legitimate processes from accessing them.

THERE ARE VARIOUS PROGRAM THREATS. SOME OF THEM ARE AS FOLLOWS:

- **1.Virus**
  - A virus may replicate itself on the system. Viruses are extremely dangerous and can modify/delete user files as well as crash computers. A virus is a little piece of code that is implemented on the system program. As the user interacts with the program, the virus becomes embedded in other files and programs, potentially rendering the system inoperable.
- **2. Trojan Horse**
  - This type of application captures user login credentials. It stores them to transfer them to a malicious user who can then log in to the computer and access system resources.
- **3. Logic Bomb**
  - A logic bomb is a situation in which software only misbehaves when particular criteria are met; otherwise, it functions normally.
- **4. Trap Door**
  - A trap door is when a program that is supposed to work as expected has a security weakness in its code that allows it to do illegal actions without the user's knowledge.

HOW TO ENSURE OPERATING SYSTEM SECURITY?

- **Authentication**
- The process of identifying every system user and associating the programs executing with those users is known as authentication. The operating system is responsible for implementing a security system that ensures the authenticity of a user who is executing a specific program. In general, operating systems identify and authenticate users in three ways.
- **1. Username/Password** Every user contains a unique username and password that should be input correctly before accessing a system.
- **2. User Attribution** These techniques usually include biometric verification, such as fingerprints, retina scans, etc. This authentication is based on user uniqueness and is compared to database samples already in the system. Users can only allow access if there is a match.
- **3. User card and Key** To login into the system, the user must punch a card into a card slot or enter a key produced by a key generator into an option provided by the operating system.

HOW TO ENSURE OPERATING SYSTEM SECURITY?

- **One Time passwords**
- Along with standard authentication, one-time passwords give an extra layer of security. Every time a user attempts to log into the One-Time Password system, a unique password is needed. Once a one-time password has been used, it cannot be reused. One-time passwords may be implemented in several ways.
- **1. Secret Key**
  - The user is given a hardware device that can generate a secret id that is linked to the user's id. The system prompts for such a secret id, which must be generated each time you log in.
- **2. Random numbers**
  - Users are given cards that have alphabets and numbers printed on them. The system requests numbers that correspond to a few alphabets chosen at random.
- **3. Network password**
  - Some commercial applications issue one-time passwords to registered mobile/email addresses, which must be input before logging in.

HOW TO ENSURE OPERATING SYSTEM SECURITY?

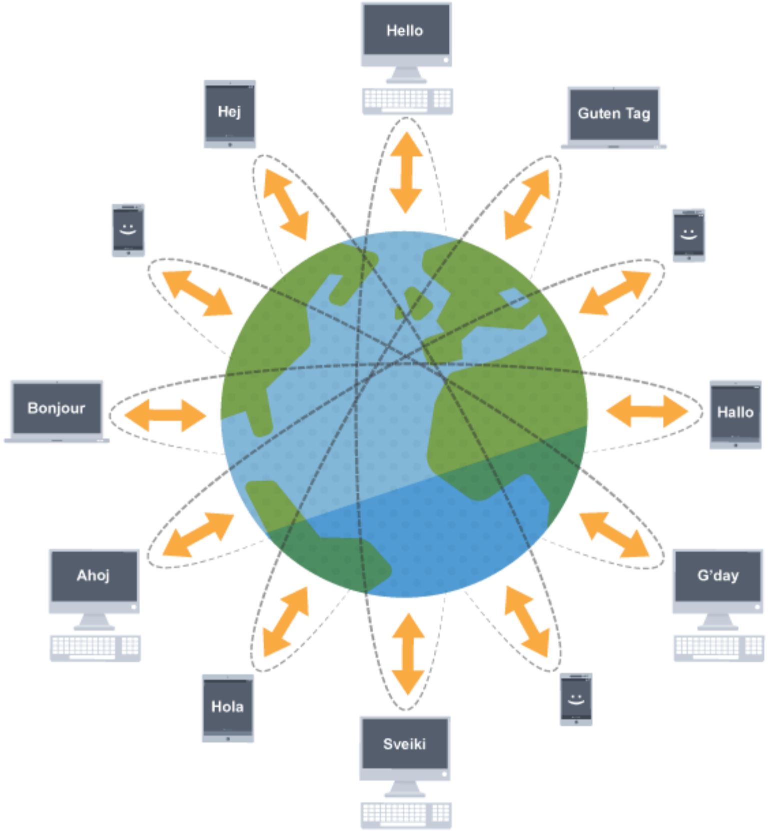
- **Firewalls**
- Firewalls are essential for monitoring all incoming and outgoing traffic. It imposes local security, defining the traffic that may travel through it. Firewalls are an efficient way of protecting network systems or local systems from any network-based security threat.
- ***Physical Security***
- The most important method of maintaining operating system security is physical security. An attacker with physical access to a system may edit, remove, or steal important files since operating system code and configuration files are stored on the hard drive.

WHAT IS A NETWORK?

- A network is two or more computers (or other electronic devices) that are **connected together**, usually by cables or Wi-Fi.
- Some computer networks will have a **server**. A server is a powerful computer that often acts as a central hub for services in a network, eg emails, internet access and file storage. Each computer connected to a server is called a **client**.
- A computer that is not connected to a network is called a **standalone computer**.

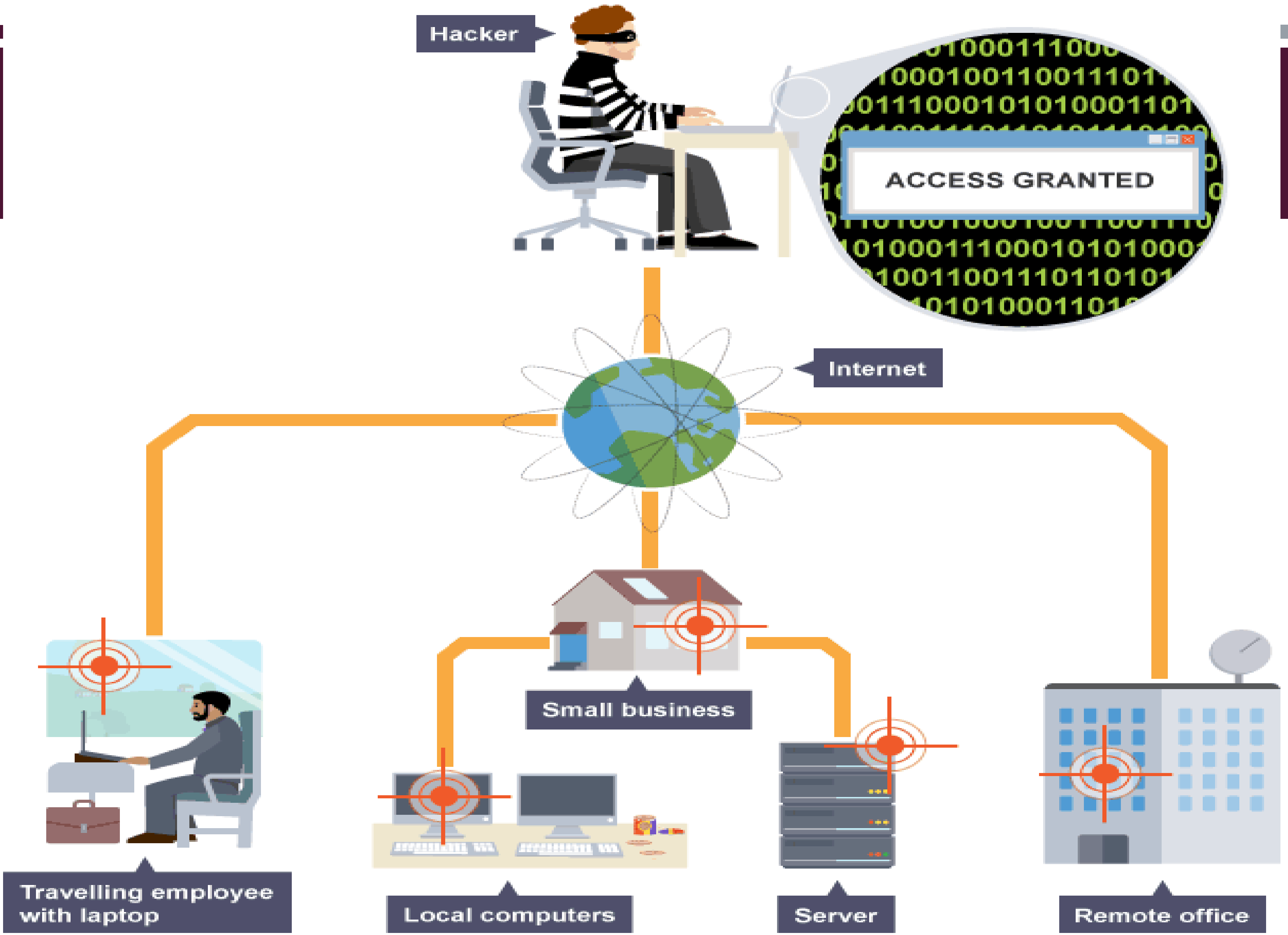
WHAT ARE THE BENEFITS OF A NETWORK?

- Using a network allows you to share:
- hardware, such as a printer
- software, allowing multiple users to run the same programs on different computers
- data, so that other people can access shared work and you can access your data from any computer on the network



WHAT PROBLEMS CAN OCCUR WITH A NETWORK?

- If we connect computers or devices together in a network we can expose ourselves to some problems.
- If the network breaks, this can make a number of tasks it is used for quite difficult. For example, it might not be possible to share photographs and opinions with friends.
- If computers and devices are networked together, we can expose ourselves to **hackers** and **viruses**. Most viruses are spread over a network and most hackers use a network to access other people’s computers. Without a network connection, a hacker would have to physically get to your computer.


Hacker
ACCESS GRANTED
Internet
Small business
Travelling employee with laptop
Local computers
Server
Remote office

NETWORK PACKET SNIFFING

- When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called *data packets* and reassembled at receiver's node in original format. It is the *smallest unit* of communication over a computer network. It is also called a block, a segment, a datagram or a cell. The act of capturing data packet across the computer network is called **packet sniffing**.
- It is similar to as wire tapping to a telephone network. It is mostly used by *crackers and hackers* to collect information illegally about network. It is also used by *ISPs, advertisers and governments*.

ISPS USE PACKET SNIFFING TO TRACK ALL YOUR ACTIVITIES SUCH AS:

- who is receiver of your email
- what is content of that email
- what you download
- sites you visit
- what you looked on that website
- downloads from a site
- streaming events like video, audio, etc.

PACKET SNIFFER

- **Packet Sniffer –**
  Packet sniffing is done by using tools called *packet sniffer*. It can be either *filtered or unfiltered*. Filtered is used when only *specific data packets* have to be captured and Unfiltered is used when *all the packets* have to be captured. WireShark, SmartSniff are examples of packet sniffing tools.
- **How to prevent packet sniffing –**

- Encrypting data you send or receive.
- using trusted Wi-Fi networks.
- Scanning your network for dangers or issues.

NETWORK DESIGN SIMULATION

- Network simulation is one kind of method in the research of a computer network where a software program forms the performance of a network by analyzing the relations between the various network entities such as links, Nswitched, routers, nodes, access points.
- The network performance, different applications, services & supports can be monitored in an analysis lab. Different features of the surroundings can also be changed in a controlled way to evaluate how the network or protocols would perform beneath different conditions.

NETWORK SIMULATOR

- Software that is used to predict the performance of a computer network is known as a network simulator. These are used when communication networks have turned into too difficult for fixed analytical techniques to offer a precise understanding of system performance.
- In a simulator, the computer network can be molded with the help of links, devices and applications and the performance of a network can be reported. These are available by using new networks and technologies which are used today like IoT, 5G, WLANs, ad hoc networks of mobile, WSNs, LTE, ad hoc networks of vehicles, etc.

NETWORK EMULATION

- This is one kind of method used to test the act of real applications over a virtual network. This is dissimilar compare with network simulation wherever only mathematical form of traffic, channels, protocols and network models are applied. The main function of this is to assess performance, estimate the impact of change, and otherwise optimize decision-making in technology.

DIFFERENT NETWORK SIMULATIONS

- The different types of network simulators/ network simulation tools are open source and commercial
- Network Simulator version 2 (NS-2)
- Ns3
- Netkit
- Marionnet
- JSIM (Java-based Simulation)
- OPNET
- QualNet
- The open-source simulators are Marrionet, Netkit, NS2, JSIM
- The commercial simulators are OPNET and QualNet

WHAT IS CYBERSECURITY ASSET MANAGEMENT?

- Cybersecurity asset management is the process of identifying, on a continuous, real-time basis, the IT assets that your organization owns and the potential security risks or gaps that affect each one.
- In this context, assets take many forms. They could be traditional devices, like PCs and servers. Or, they could be specialized IoT, IoMT, IIoT, or OT devices or software-defined resources, like a cloud-based database or a company-owned domain.
- Any device, resource or service that exists within your IT estate could be subject to risks or vulnerabilities that lead to a breach of the individual resource and your network as a whole, in the event that attackers use one compromised resource as a beachhead to launch a broader attack.

WHY IS CYBERSECURITY ASSET MANAGEMENT IMPORTANT?

- **Cybersecurity is not a distraction**: With a strong cybersecurity asset management process in place, businesses can deploy new IT services or resources without letting security become a distraction or hindrance. They can make decisions based on business priorities, confident that whichever changes they make, their cybersecurity asset management process will catch potential vulnerabilities.
- **Proactive response**: Cybersecurity asset management helps ensure that security teams detect threats before they evolve into serious problems. By continuously monitoring the IT estate for new deployments and risks, teams don’t have to wait until they detect an active attack in order to respond.
- **Security visibility**: If an attack does occur, cybersecurity asset management provides the security team with an inventory of assets and risks that it can use to gain context on what went wrong and when. Instead of having to reconstruct the state of resource deployments and configurations in order to research the origins of a breach or vulnerability, teams have an up-to-date record that they can refer to immediately.

EXAMPLES OF CYBERSECURITY ASSET MANAGEMENT

- **Device discovery and protection:** By identifying network endpoints and assessing each one for security vulnerabilities, teams can take immediate steps to address problems by, for example, segmenting insecure endpoints from the rest of the network.
- **Vulnerability management:** Cybersecurity asset management helps detect and address active vulnerabilities, such as unpatched software running on a device.
- **Cloud security:** Modern clouds are complex, multilayered environments that consist of a range of services and resource types. Cybersecurity asset management includes the identification of cloud resources that are vulnerable due to insecure software or lack of access control.
- **Incident response:** When an incident warrants further investigation, cybersecurity asset management plays a role in providing the incident response (IR) team with the information it needs to determine the root cause and remediate.
- **Continuous policy enforcement:** In the event that a resource violates security policies that your team has defined, cybersecurity asset management enables the rapid discovery and remediation of the problem. When new devices are added to the network that match a particular device profile with an active policy, they are automatically protected.

WHAT IS AN INTRUSION DETECTION AND PREVENTION SYSTEM?

- Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.
- An intrusion detection system (IDS) is software that automates the intrusion detection process.
- An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.
- An Intrusion Detection and Prevention System (IDPS) monitors network traffic for indications of an attack, alerting administrators to possible attacks. IDPS solutions monitor traffic for patterns that match with known attacks. Traditionally, they used signature-based or statistical anomaly detection methods, but IDPS increasingly

WHAT IS AN INTRUSION DETECTION SYSTEM?

- Defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity.
- An IDS detects activity in traffic that may or may not be an intrusion.
- IDSes can detect and deal with insider attacks, as well as, external attacks, and are often very useful in detecting violations of corporate security policy and other internal threats.
- IDPSs are primarily focused on identifying possible incidents. For example, an IDPS could detect when an attacker has successfully compromised a system by exploiting a vulnerability in the system. The IDPS would log information on the activity and report the incident to security administrators so that they could initiate incident response actions to minimize damage.

INTRUSION DETECTION SYSTEM

- **Signature-based**: The signature-based IDS is used to match the signatures of known attacks that have already been stored in your database to detect attacks on your network.
- **Anomaly-based**: The anomaly-based IDS method identifies abnormal behavior in your organization's network.
- **Protocol-based**: The protocol-based IDS method monitors and analyzes protocols used by the computing system.

HOST BASED INTRUSION DETECTION

- Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.
- It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.
- Host-based IDS are often critical in detecting internal attacks directed towards an organization's servers such as DNS, Mail, and Web Servers.

NETWORK BASED INTRUSION DETECTION

- Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device.
- Instead of analyzing information that originates and resides on a host, Network-based IDS uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network.
- Most Network-based IDS log their activities and report or alarm on questionable events.
- Network-based IDS work best when located on the DMZ, on any subnets containing mission critical servers and just inside the firewall.

HOST BASED INTRUSION DETECTION

- Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.
- It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.
- Host-based IDS are often critical in detecting internal attacks directed towards an organization's servers such as DNS, Mail, and Web Servers.

NETWORK BASED INTRUSION DETECTION

- Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device.
- Instead of analyzing information that originates and resides on a host, Network-based IDS uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network.
- Most Network-based IDS log their activities and report or alarm on questionable events.
- Network-based IDS work best when located on the DMZ, on any subnets containing mission critical servers and just inside the firewall.

COMPARISON

Host Based

- Narrow in scope (watches only **specific** host activities)
- More complex setup
- Better for detecting attacks from the **inside**
- **More expensive** to implement
- Detection is based on what any **single host** can record
- Does not see packet headers
- Usually only responds **after** a suspicious log entry has been made
- OS-specific
- Detects local attacks before they hit the network
- Verifies success or failure of attacks

Network Based

- Broad in scope (watches **all** network activities)
- Easier setup
- Better for detecting attacks from the **outside**
- **Less expensive** to implement
- Detection is based on what can be recorded on the **entire network**
- Examines packet headers
- Near **real-time** response
- OS-independent
- Detects network attacks as payload is analyzed
- Detects unsuccessful attack attempts

HYBRID INTRUSION DETECTION

- Are systems that combine both Host-based IDS, which monitors events occurring on the host system and Network-based IDS, which monitors network traffic, functionality on the same security platform.
- A Hybrid IDS, can monitor system and application events and verify a file system's integrity like a Host-based IDS, but only serves to analyze network traffic destined for the device itself.
- A Hybrid IDS is often deployed on an organization's most critical servers.

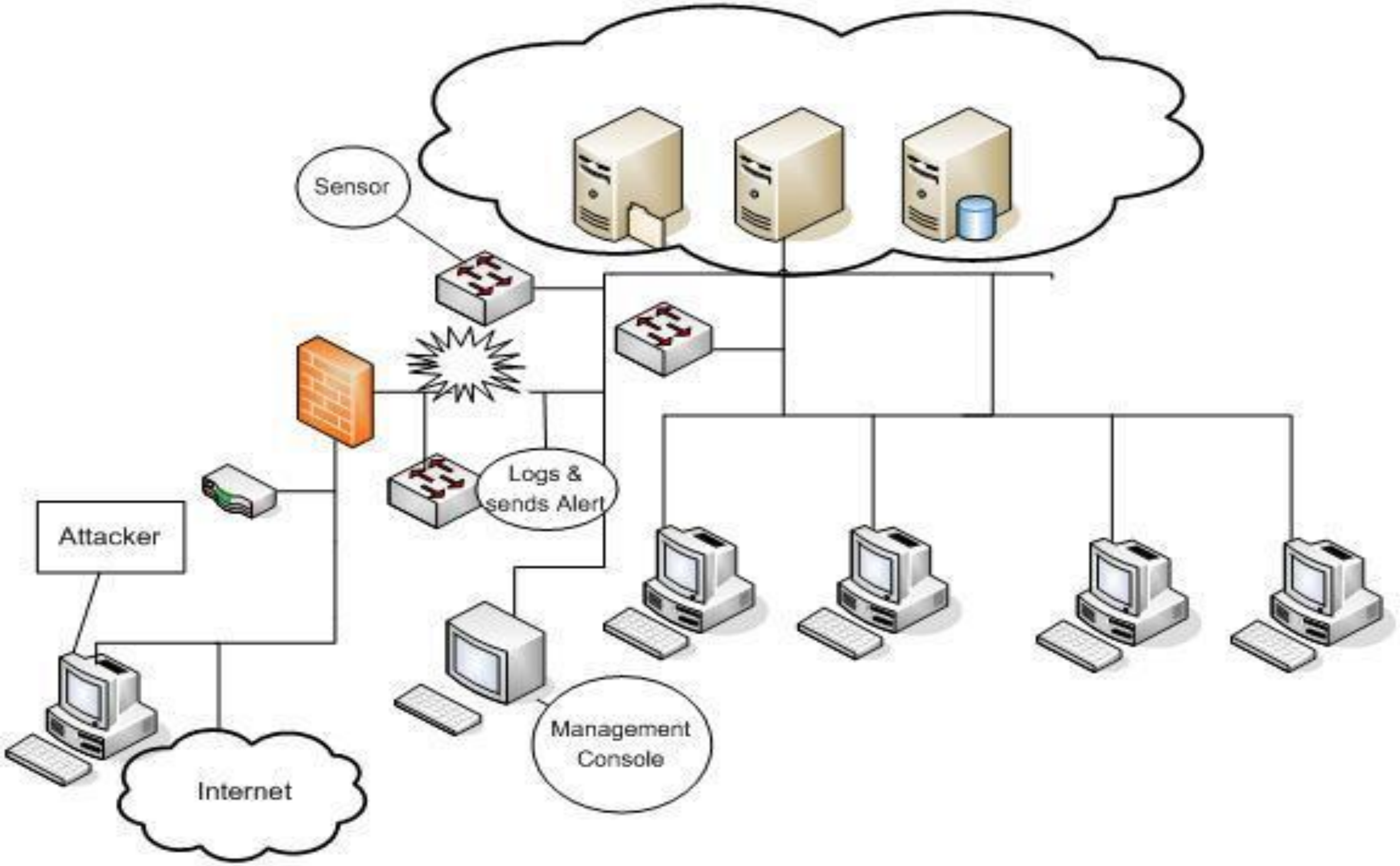
HONEYPOTS

- Are decoy servers or systems setup to gather information regarding an attacker of intruder into networks or systems.
- Appear to run vulnerable services and capture vital information as intruders attempt unauthorized access.
- Provide you early warning about new attacks and exploitation trends which allow administrators to successfully configure a behavioral based profile and provide correct tuning of network sensors.
- Can capture all keystrokes and any files that might have been used in the intrusion attempt.

PASSIVE SYSTEMS

- Detects a potential security breach
- Logs the information
- Signals an alert on the console
- Does not take any preventive measures to stop the attack

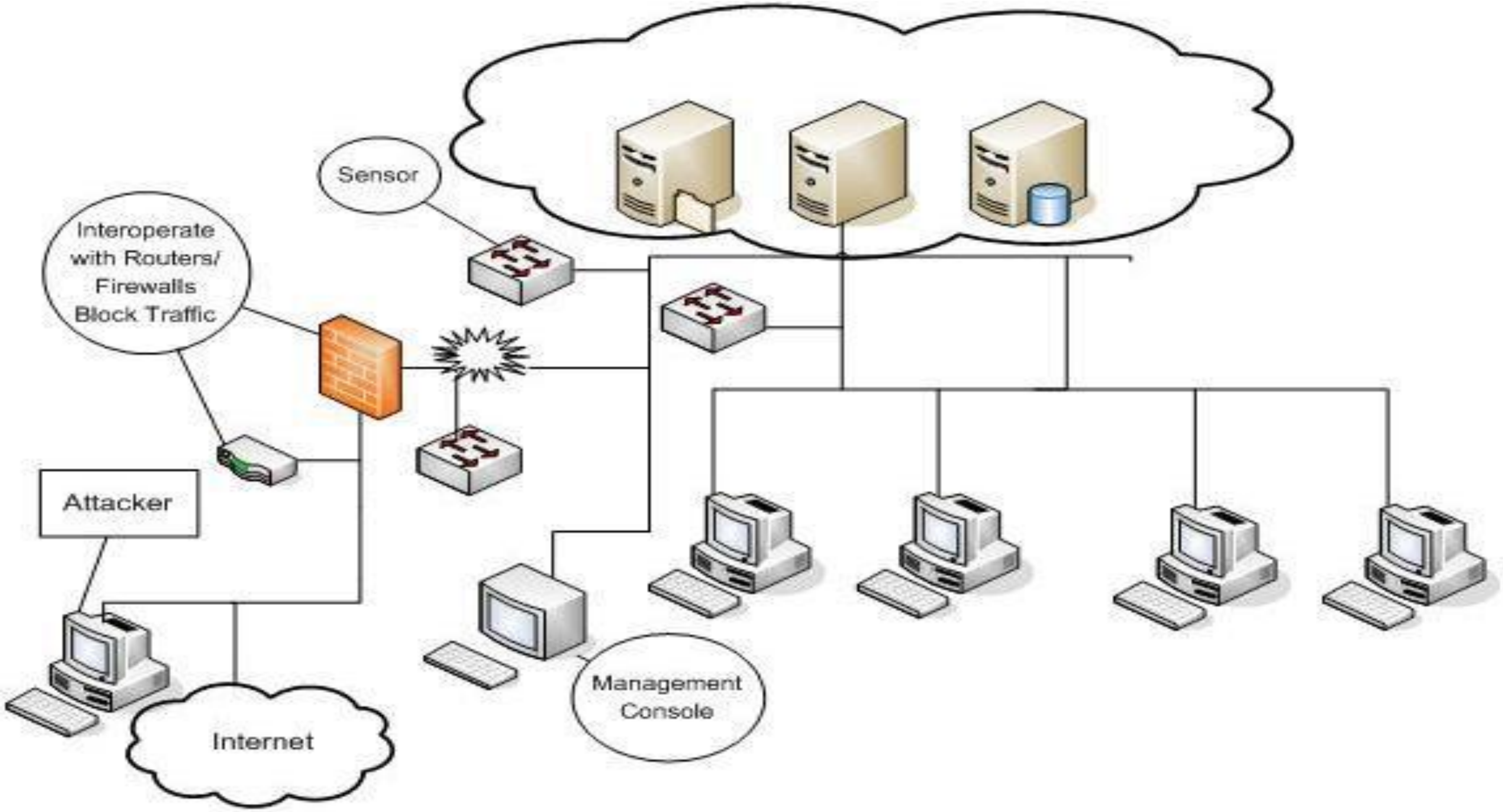
PASSIVE SYSTEMS



REACTIVE/ACTIVE SYSTEMS

- Responds to the suspicious activity like a passive IDS by logging, alerting and recording, but offers the additional ability to take action against the offending traffic.

REACTIVE/ACTIVE SYSTEMS



SIGNATURE BASED IDS

- Monitor network or server traffic and match bytes or packet sequences against a set of predetermined attack lists or signatures.
- Should a particular intrusion or attack session match a signature configured on the IDS, the system alerts administrators or takes other pre-configured action.
- Signatures are easy to develop and understand if you know what network behavior you're trying to identify.
- However, because they only detect known attacks, a signature must be created for every attack.
- New vulnerabilities and exploits will not be detected until administrators develop new signatures.
- Another drawback to signature-based IDS is that they are very large and it can be hard to keep up with the pace of fast moving network traffic.

ANOMALY BASED IDS

- Use network traffic baselines to determine a "normal" state for the network and compare current traffic to that baseline.
- Use a type of statistical calculation to determine whether current traffic deviates from "normal" traffic, which is either learned and/or specified by administrators.
- If network anomalies occur, the IDS alerts administrators.
- A new attack for which a signature doesn't exist can be detected if it falls out of the "normal" traffic patterns.
- High false alarm rates created by inaccurate profiles of "normal" network operations.

ISSUES

False Negatives

- When an IDS fails to detect an attack
- False negatives occur when the pattern of traffic is not identified in the signature database, such as new attack patterns.
- False negatives are deceptive because you usually have no way of knowing if and when they occurred.
- You are most likely to identify false negatives when an attack is successful and wasn't detected by the IDS.

False Positives

- Described as a false alarm.
- When an IDS mistakenly reports certain "normal" network activity as malicious.
- Administrators have to fine tune the signatures or heuristics in order to prevent this type of problem.

WHY ARE IDS IMPORTANT?

- The ability to know when an intruder or attacker is engaged in reconnaissance or other malicious activity can mean the difference between being compromised and not being compromised.
- An IDS can alert the administrator of a successful compromise, allowing them the opportunity to implement mitigating actions before further damage is caused
- As Corporations and other Institutions are being legally compelled to disclose data breaches and compromises to their affected customers, this can have profound effects upon a compromised company, in the way of bad press, loss of customer trust, and the effects on their stock.

HOW DOES IT FIT INTO YOUR SECURITY PLAN?

- As a network security expert you should know you cannot just rely on one or a few tools to secure your network. You need to have a defense in depth mindset and layer your network defenses.
- Through the use of inside and outside firewalls, DMZs, Routers and Switches, an IDS is a great addition to your security plan.
- You can use them to identify vulnerabilities and weaknesses in your perimeter protection devices, such as: firewalls, switches and routers. The firewall rules and router access control lists can be verified regularly for compliance.
- You can use IDSes to enforce security policies, such as: unauthorized Internet access, downloads of executable files, use of file sharing programs like Kazza, or Instant Messenger use.
- IDSes are also an invaluable source of evidence. Logs from an IDS can become an important part of computer forensics and incident handling efforts.

PROS

- Can detect external hackers, as well as, internal network-based attacks
- Scales easily to provide protection for the entire network
- Offers centralized management for correlation of distributed attacks
- Provides defense in depth
- Gives administrators the ability to quantify attacks
- Provides an additional layer of protection

CONS

- Generates false positives and negatives
- Reacts to attacks rather than preventing them
- Requires full-time monitoring and highly skilled staff dedicated to interpreting the data
- Requires a complex incident response process
- Cannot monitor traffic at higher network traffic rates
- Generates an enormous amount of data to be analyzed
- Cannot deal with encrypted network traffic
- It is expensive

Thank you