Module 3: Information & Network Detection

Chapter-1 Access Control & Intrusion detection

1. Overview of Identification & Authorization
2. Overview of IDS
3. Intrusion Detection Systems & Intrusion Prevention Systems

1. Overview of Identification & Authorization:

- **Identification:**
  - Identification is nothing more than claiming you are somebody.
  - Example: While talking on telephone, person specifies his/her identity that is I am Ram.
  - An **identity** is equivalent to the knowledge of a specific piece of data:

- **Authentication:**
  - Authentication is how one proves that they are who they say they are.
  - It is a secret between you and the system.
  - **Example: Logging to gmail Account.**

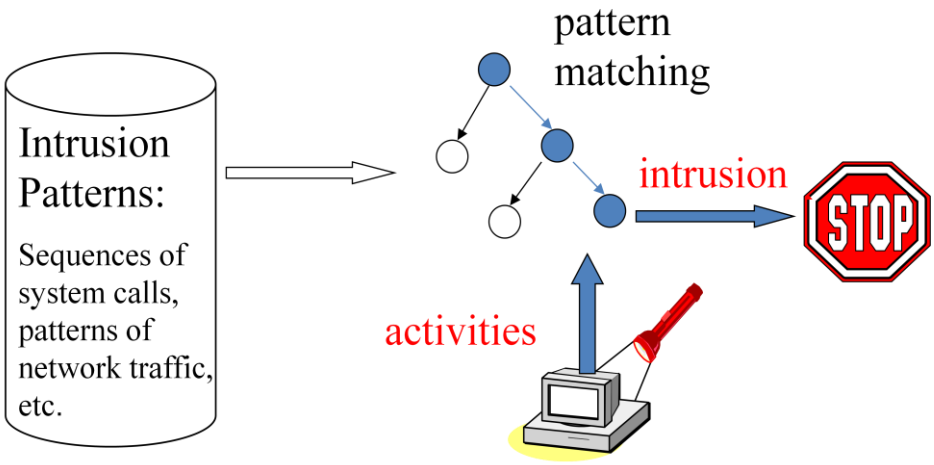
- **Authorization**
  - Authorization is what takes place after a person has been both identified and authenticated; it's the step determines what a person can then do on the system.
  - **Example: someone knocking on your door at night.**

- **Difference between identification, Authentication & Authorization:**
  - **Identification**: means **who**
  - **Authentication**: means **verification**
  - **Authorization:** means **rights the person has**

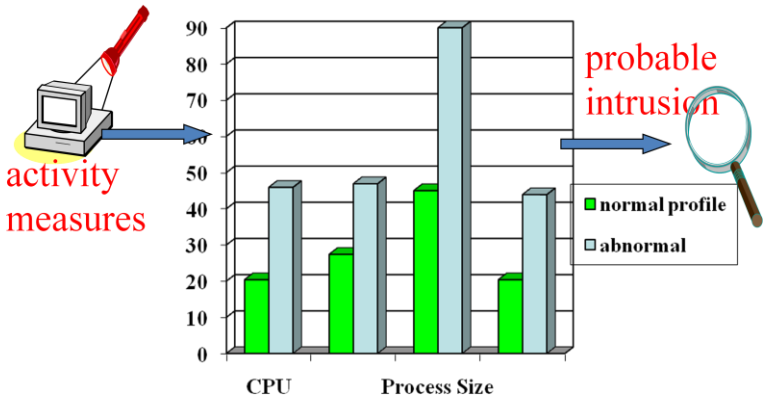
2. Overview of IDS:

- **IDS stand for Intrusion detection system.**
- **Intrusion** means an illegal act of entering, seizing, or taking possession of another's property.
- An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations.
- All Intrusion Detection Systems use one of two detection techniques:
  - Statistical anomaly-based IDS (Anomaly detection)
  - Signature-based IDS (Misuse detection)

- **Signature-based IDS (Misuse detection):**
  - **Example: Biometric attendance**
  - Disadvantage: signature database must be continually updated.



- **Statistical anomaly-based IDS (Anomaly detection):**
  - An IDS which is anomaly based will monitor network traffic and compare it against an established baseline.
  - **Example: Credit card**



- **Network-based Intrusion Detection System (NIDS):**
  - A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.
  - A NIDS reads all inbound packets and searches for any suspicious patterns.
  - This is generally accomplished by placing the network interface card (NIC) to capture all network traffic that crosses its network.
  - It involves looking at the packets on the network as they pass by some sensor.

- The sensor can only see the packets that happen to be carried on the network segment it's attached to.
- Once the attack is identified, or abnormal behaviour is sensed, the alert can be sent to the administrator.

- **Host-based Intrusion Detection System (HIDS):**
  - Host intrusion detection systems run on individual hosts or devices on the network.
  - A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.
  - Use OS based monitoring to find intrusion.
  - Log all relevant system events (e.g., file/device accesses)
  - Monitor shell commands and system calls executed by user applications and system programs.

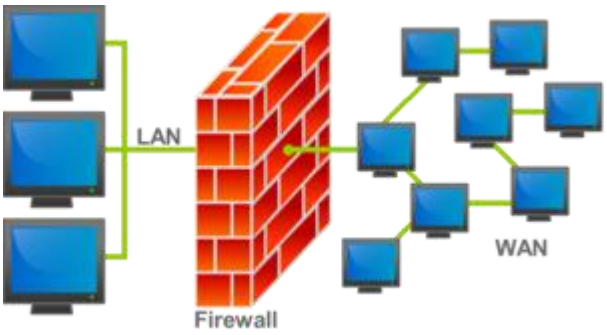
3. Intrusion Prevention Systems: (IPS)

- Intrusion prevention systems (**IPS**), also known as intrusion detection and prevention systems (**IDPS**).
- The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.
- Intrusion prevention systems can be classified into four different types:
  i. **Network-based intrusion prevention system (NIPS)**: monitors the entire network for suspicious traffic by analyzing protocol activity.
  ii. **Wireless intrusion prevention systems (WIPS)**: monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.
  iii. **Network behaviour analysis (NBA)**: examines network traffic to identify threats that generate unusual traffic flows, such as certain forms of malware and policy violations.
  iv. **Host-based intrusion prevention system (HIPS)**: an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Chapter-2 Server Management & Firewalls

1. User Management
2. Overview of firewalls
3. Types of firewalls
4. DMZ & firewall features

1. Overview of firewalls:



- It controls the incoming and outgoing network traffic based on an applied rule set.
- A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet).
- All messages entering or leaving the intranet pass through the firewall.
- Firewalls can be implemented in both hardware and software.

2. Types of firewalls:

- There are several types of firewall techniques that will prevent potentially harmful information from getting through:
  - packet filters
  - Stateful firewall
  - Application-layer firewall
  - Proxy firewall

1. Packet filters:

a. First firewall that inspecting the packets that are transferred between computers on the Internet.

b. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port number are checked against the firewall's rule set.

2. **Stateful firewall:**
    a. It records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection.
    b. If a packet does not match an existing connection, it's evaluated according to the rule set for new connections.

3. **Application-layer firewall:**
    a. The key benefit of application-layer filtering is the ability to block specific content, such as known malware or certain websites, and recognize when certain applications and protocols -- such as HTTP, FTP and DNS -- are being misused.

4. **Proxy firewall:**
    a. Intercepts all messages entering and leaving the network.
    b. The proxy server effectively hides the true network addresses.
    c. A proxy firewall prevents direct connections between either sides of the firewall.

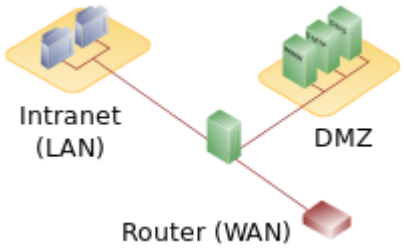
4. DMZ & firewall features:

- ## Firewall features:

1. Protects the user from unwanted incoming connection attempts.
2. Allows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt
3. Block or alert the user about outgoing connection attempts
4. Hide the computer from network traffic
5. Monitor applications that are listening for incoming connections
6. Monitor and regulate all incoming and outgoing Internet users
7. Prevent unwanted network traffic from locally installed applications

- **DMZ (De militarized Zone) or Perimeter Network**

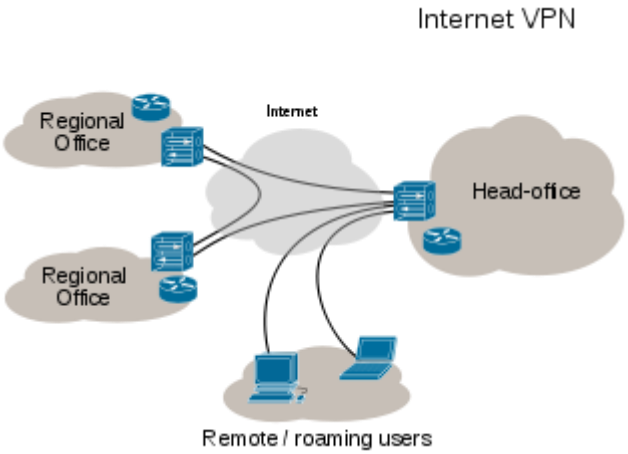
    - It is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network.
    - It prevents outside users from getting direct access to a server that has company data.
    - A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.
    - Hosts in the DMZ are permitted to have only limited connectivity to specific hosts in the internal network.
    - The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN).



Chapter-3 Security for VPN & Next Generation Techniques

1. VPN Security
2. Security in Multimedia Networks
3. Various Computing platforms: HPC, cluster & Computing Grids
4. Virtualization & cloud technology & security

1. VPN:



- VPN stand for Virtual private network.
- A firewall protects your data on your computer, VPNs protect it online.
- A virtual private network (VPN) extends a private network across a public network, such as the Internet.
- It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network.
- VPNs allow employees to securely access their company's intranet while travelling outside the office.
- VPNs securely connect geographically separated offices of an organization, creating one cohesive network.

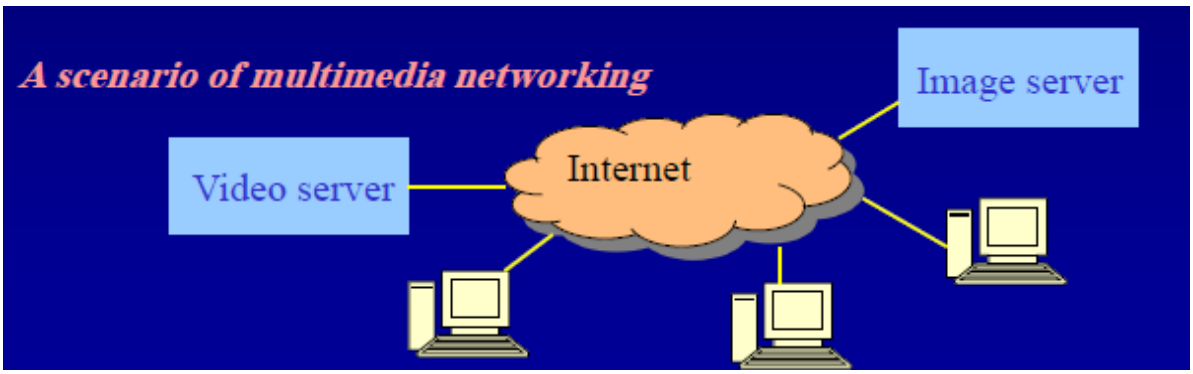
VPN Security:

- To prevent disclosure of private information, VPNs typically allow only authenticated remote access and make use of encryption techniques.
- The VPN security model provides:
  - **Confidentiality** : an attacker would only see encrypted data.
  - Sender **authentication** to prevent unauthorized users from accessing the VPN.
  - Message **integrity** to detect any instances of tampering with transmitted messages.

- Secure VPN protocols include the following:
  - **Internet Protocol Security (IPsec):**
    - It is developed for IPv6.
    - Its design meets most security goals: authentication, integrity, and confidentiality.
    - IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
  - **Secure Sockets Layer (SSL) and Transport Layer Security (TLS):**
    - These protocols operate using a handshake method.
    - This handshake produces the cryptographic parameters of the session."
    - These parameters, typically digital certificates, are the means by which the two systems exchange encryption keys, authenticate the session, and create the secure connection.
  - **Point-to-Point Tunnelling Protocol (PPTP):**
  - **Secure Shell (SSH):**
    - SSH creates both the VPN tunnel and the encryption that protects it.
    - This allows users to transfer unsecured data by routing the traffic from remote fileservers through an encrypted channel.
    - The data itself isn't encrypted but the channel it's moving through is.

2. Security in Multimedia Networks:

- **Definition of multimedia:**
  - Multimedia is an integration of text, graphics, still and moving images, animation, sounds, and any other medium where every type of information can be represented, stored, transmitted.
  - **It involves transmission and distribution of multimedia information on the network.**
  - Sample applications: videoconferencing, web video broadcasting, multimedia Email, etc.



4. Various Computing platforms: HPC, cluster & Computing Grids:

- **HPC: (High Performance Computing)**
  - High Performance Computing (HPC) allows scientists and engineers to solve complex science, engineering, and business problems using applications that require high bandwidth, low latency networking, and very high compute capabilities.
  - High performance computers of interest to small and medium-sized businesses today are really *clusters* of computers.
  - HPC people often refer to the individual *computers* in a cluster as *nodes*.
  - A cluster of interest to a small business could have as few as four nodes.
  - Task is carried out in distributed environment.
  - Sometimes HPC is also called as **parallel processing**.
  - HPC can be carried out in 2 ways:
    - Cluster Computing
    - Grid Computing
  - **Cluster Computing:**
    - Cluster is homogenous.
    - Cluster computers all have the same hardware and OS.
    - Computers in the cluster are normally contained in a single location.
    - In case of Cluster, the whole system (all nodes) behaves like a single system view and resources are managed by centralized resource manager.
  - **Grid Computing:**
    - Grids are heterogeneous.
    - The computers that are part of a grid can run different operating systems and have different hardware.
    - Grids are inherently distributed by its nature over a LAN, metropolitan or WAN.
    - In case of Grid, every node is autonomous i.e. it has its own resource manager and behaves like an independent entity.

5. Virtualization & cloud technology & security:

- **Virtualization:**
  i. Refers to the act of creating a virtual (rather than actual) version of something, including but not limited to a virtual computer hardware platform, operating system (OS), storage device, or computer network resources.
  ii. The term *virtual machine* essentially describes sharing the resources of one single physical computer into various computers within itself.
  iii. Virtualization differs from cloud computing because virtualization is software that manipulates hardware, while cloud computing refers to a service that results from that manipulation.
- **Cloud computing:**
  i. It is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources.
  ii. Example : Email Communication
  iii. Bringing VMs (virtual machines) onto the cloud.
  iv. Cloud computing relies on sharing of resources.
  v. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS)

- **Cloud Security:**
  - Cloud security is sub-domain of computer security, network security, and, information security.
  - **Identity management :**
    - Every enterprise will have its own identity management system to control access to information and computing resources.
  - **Physical security:**
    - Essential supplies (such as electricity), theft, fires, floods are sufficiently robust to minimize the possibility of disruption.
  - **Personnel security:**
    - Employment activities such as security monitoring and supervision, disciplinary procedures, service level agreements, codes of conduct, policies etc.
  - **Availability:**
  - **Application security:**
  - **Privacy**:
    - Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted (even better) and that only authorized users have access to data in its entirety.