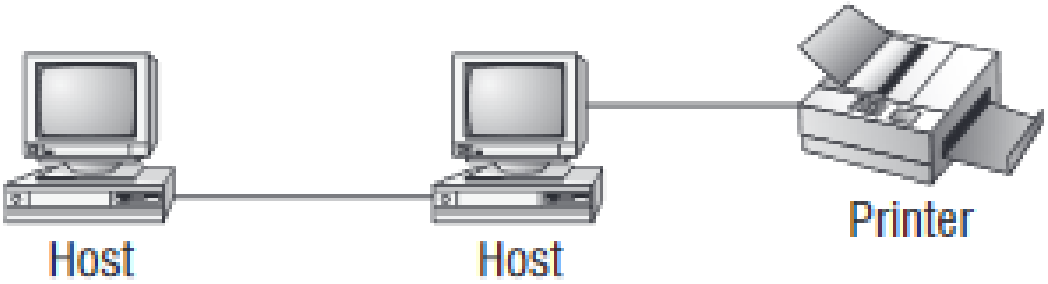
Lecture 1

What is Network

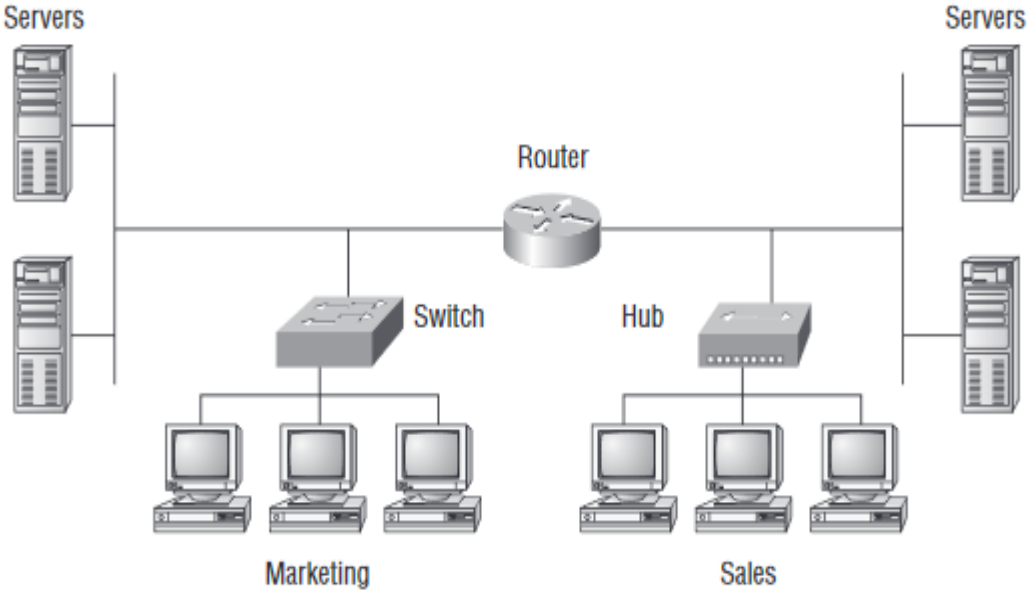
- The term network means two or more connected computers that can share resources like data and applications, office machines, an Internet connection, or some combination of these.
- Basic network made up of only two host computers connected; they share resources like files and even a printer hooked up to one of the hosts
- These two hosts “talk” to each other using a computer language called binary code, which consists of lots of 1s and 0s in a specific order that describes exactly what they want to “say.”

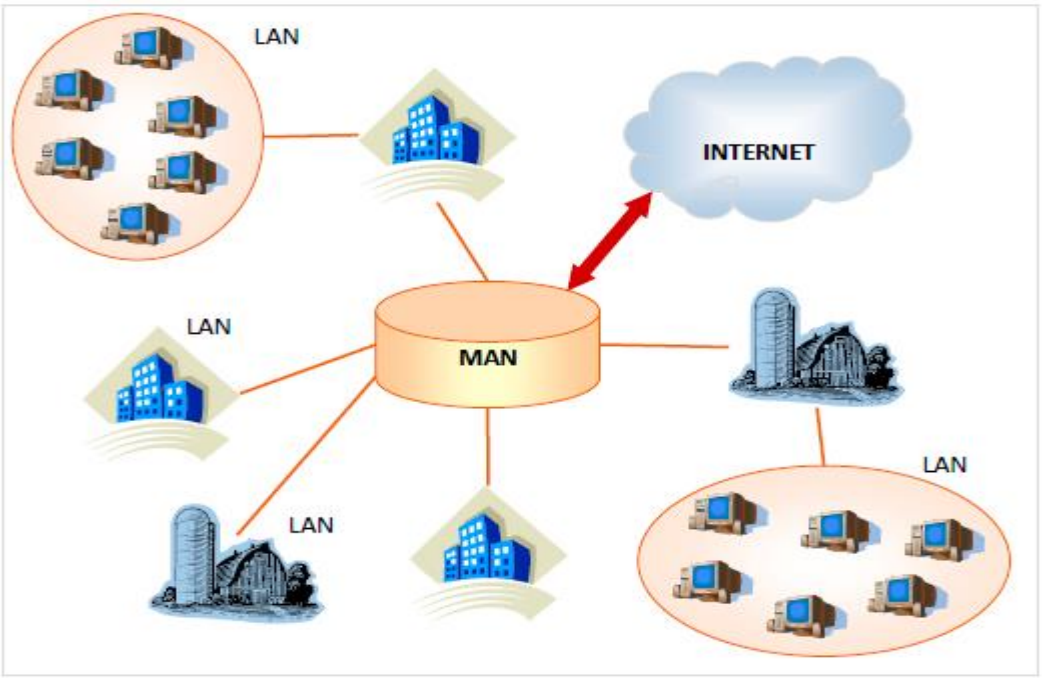


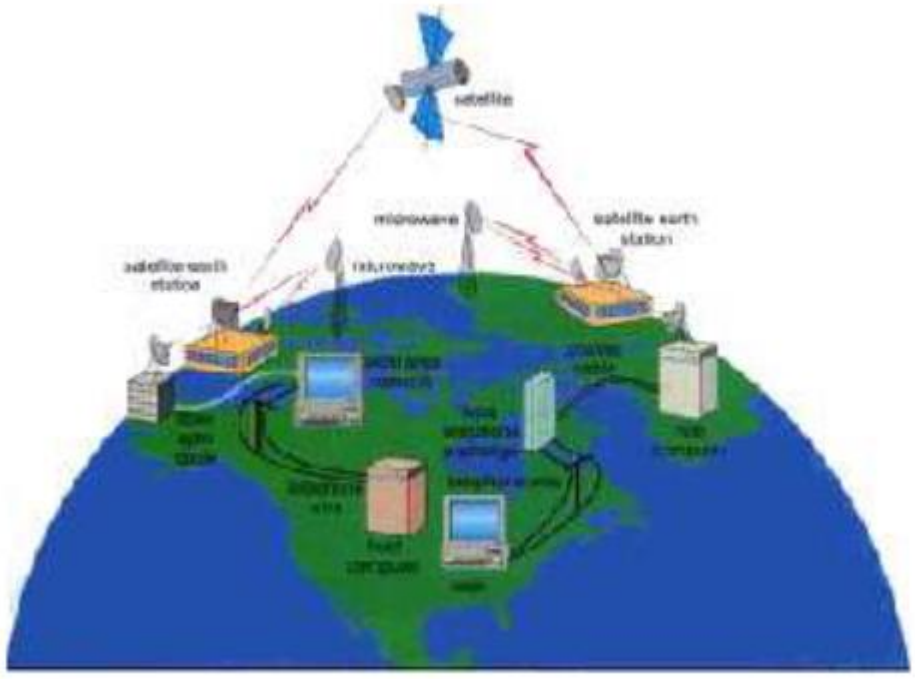
Types of Networks

BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns. Ex: Cable TV Network	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low

Congestion	**Less**	**More**	**More**
Used for	**College, School, Hospital.**	**Small towns, City.**	**Country/Continent.**
Allows	**Single pair of devices to communicate.**	**Multiple computers can simultaneously interact.**	**A huge group of computers communicate at the same time.**

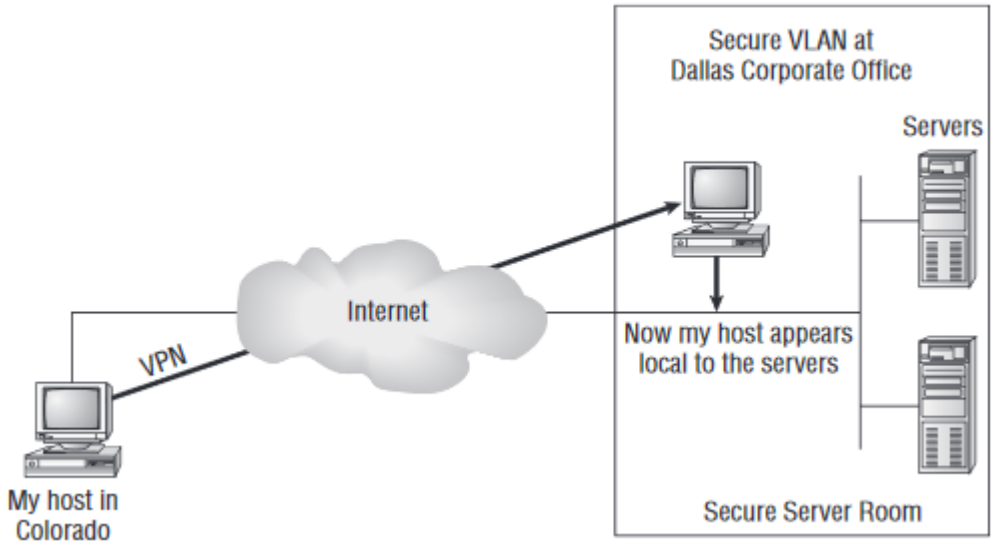






VPN (Virtual Private Network):

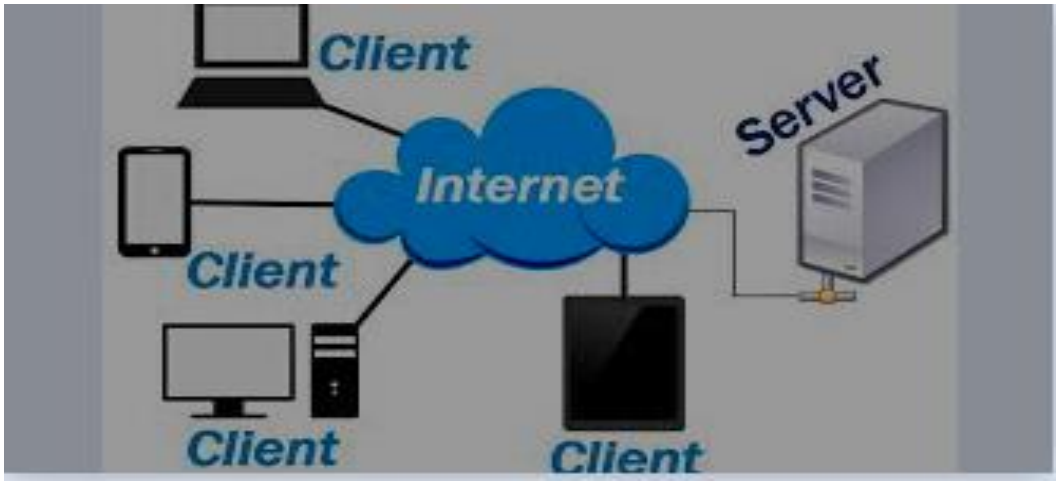
- A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet.
- VPNs can be used to access region-restricted websites.
- It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.



Common Network Component

- Workstations: A workstation is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems.

- Server: A server is a computer that serves information to other computers. These computers, called clients, can connect to a server through either a local area network or a wide area network, such as the internet.



Ports & Protocol

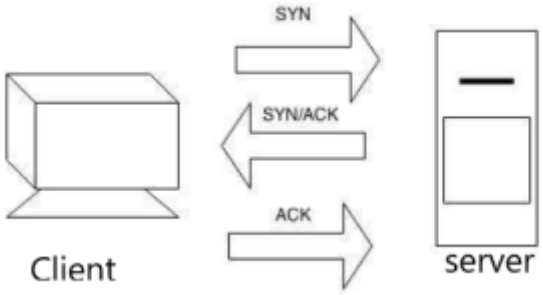
Ports	Protocols	Description
20,21	File Transfer Protocol (FTP) Data Transfer	For file transfer
22	SSH	SSH is also referred to as 'Secure Shell'. It operates on the port number 22 of the TCP protocol. It carries out the task of remotely connecting to a remote server or host. It will use for Linux secure data can transfer using this port.
23	Telnet	Telnet - Remote login service, unencrypted text messages, its main function is to establish a connection between a server and a remote computer.it is also used for troubleshooting problem and to check wether the connecting port is available
25	SMTP - Simple mail transfer protocol	SMTP is known as the Simple Mail Transfer Protocol. It is associated with the TCP port number 25. The primary purpose of this protocol is to make sure that email messages are communicated over the network securely. This port usually comes into being during the Application layer.
80	HTTP hypertext transfer protocol	Port 80 is associated with HTTP, Hypertext Transfer Protocol. It comes under the category of a TCP protocol. It is one of the most famous and widely used ports in the world. The main purpose of port 80 is to allow the browser to connect to the web pages on the internet
443	HTTP hypertext transfer protocol secure	HTTPS port 443 also lets you connect to the internet by establishing a connection between the webpages and the

		browser.
53	**Domain Name System (DNS) service**	**DNS makes use of relational databases to link the host names of the computers or networks to their respective IP Addresses. (Translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0. 2.44).)**
110	**POP3**	**POP3 is also referred to as Post Office Protocol Version 3. It operates on the port 110 of TCP Protocol. It allows the email messages to be retrieved from the SMTP servers.**
123	**NTP**	**The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.**
143	**Internet Message Access Protocol (IMAP) Management of Digital Mail**	**IMAP (Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages**
161	**Simple Network Management Protocol (SNMP)**	**Simple Network Management Protocol (SNMP) is a networking protocol used for the management and monitoring of network-connected devices in Internet Protocol networks.**
3389	**RDP**	**Remote desktop protocol, to use taking the access of windows machine**
1521	**Oracle**	**Data base type**
1443	**SQL**	**Data base type**
514	**Syslog**	**Sending the data towards another server.**
135-139	**NetBIOS**	**NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN).**
445	**SMB (simple mail block)**	**File shared internally then it will use**
389	**LDAP**	**LDAP (Lightweight Directory Access Protocol) is an open and cross platform protocol used for directory services authentication.**

Lecture 2

A 3-way Handshake:

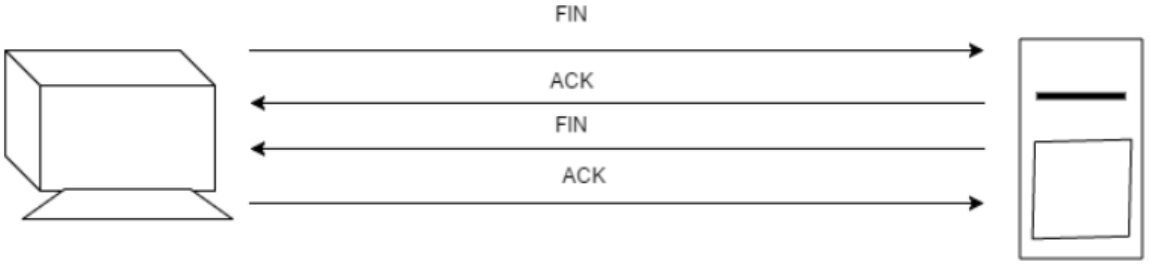
- The three-way handshake is the process in which two communicating devices synchronize during the establishment of a connection.
- Once the handshake is successful communication is initiated. It is a connection establishment process.



- The client will initiate the communication request by sending across a SYN data packet over an IP network to a server on the same or an external network. The objective of this packet is to ask if the server is open for new connection.
- The target server must have open ports that can accept and initiate new connections. When the server receives the SYN packet from the client node, it responds and returns a confirmation to the client saying connection can be started with the help of an acknowledgement packet-the ACK packet or SYN/ACK packet.
- The client receives the SYN/ACK from the server and responds with an ACK packet.
- Upon completion of this process, the connection is created and the host and server can communicate.

4-way Handshake:

It is a connection termination process.



- When the data transmission is complete and the client or any device wants to terminate the connection, the device initiating the termination, places a TCP segment the FIN flag set to one. The other device from the connection will acknowledge this by sending an ACK flag.

- Here one of the two connected devices indicated that the communication is done. But it is also important for the second device to indicate termination by confirming that its work is done, and communication can be stopped.
- The server or the second device will inform if it needs to terminate the connection by again sending a Fin packet to which the first device will acknowledge.

Transmission control protocol header (TCP):

TCP	UDP
Connection oriented protocol – When a message is sent it reaches the destination as it is. If there is a connection failure, the lost part of the message will be delivered when the connection is established. The message will not be corrupted or discarded.	**Connectionless protocol** – When a message is sent, it is not guaranteed that it will reach the destination as it is. If there is a connection failure, the lost part may be lost and the message at the receiving end will be corrupted even after the connection is established.
Ordered delivery – If you send two messages, they will reach the destination in the order in which they were sent.	**Unordered delivery**- If you send two messages, the packets will reach the destination in any sequence not necessary it will be in the order in which they were sent.
Speed – Since TCP has to re-establish connections during failures to guarantee ordered delivery of packets, TCP is slow as compared to UDP.	**Speed** – With UDP there is no ordering of messages, no tracking connections, therefore it is faster in comparison with TCP.
Header size - TCP header contains Sequence Number, Ack number, Window, Urgent Pointer, Source port, and Destination port.	**Header size** – UDP header contains Length, Source port, Destination port, and Check Sum.
Three way handshake for connection establishment.	No three way handshake for connection establishment (connectionless protocol).
Examples: IMAP, POP3	Examples: SNMP

TCP Header:

TCP segment header

Offsets	Octet	0								1								2								3							
Octet	Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	0	Source port																Destination port																
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																	Urgent pointer (if URG set)														
20	160	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.)																															
⋮	⋮																																
60	480																																

UDP Header:

UDP datagram header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port																
4	32	Length																Checksum																

TCP: Example

- World Wide Web (HTTP)
- E-mail (SMTP)
- File Transfer Protocol (FTP)
- Secure Shell (SSH)

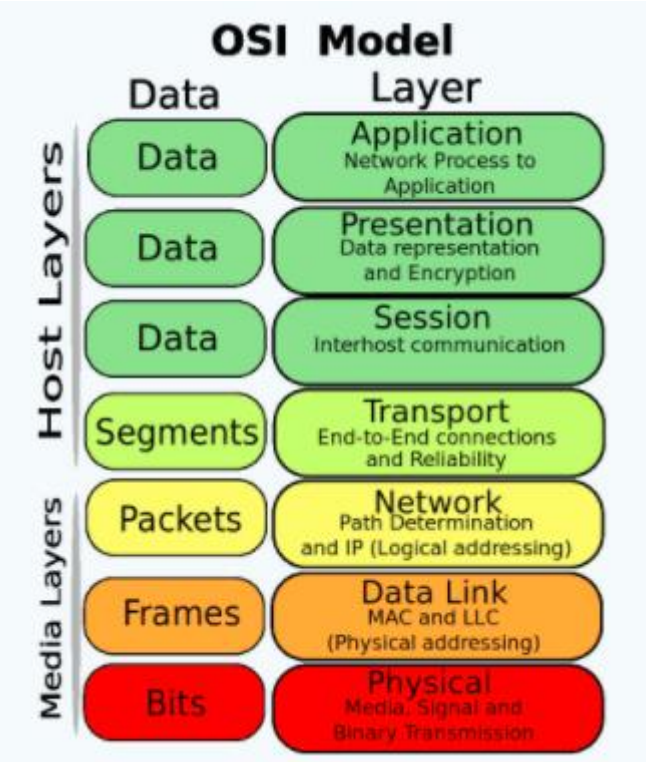
UDP: Example

- Domain Name System (DNS)
- Streaming media applications such as movies
- Online multiplayer games
- Voice over IP (VoIP)

Lecture-3

The OSI Model

- The OSI, or open system interconnect model, is a conceptual model for understanding data communications between any two networked systems.
- The OSI model is a reference model to understand the underlying network architecture.
- It provides a structured approach that specifies the sequence of processes required for network message transfer between applications running on different systems or networks.
- According to the standard OSI Model there are seven logical layers. Each layer takes care of a specific job and passes the output data to the next layer above it. At each layer, the data takes a different form as it travels (frames, segments, packets etc.)



All people seems to need data processing

APSTNDP

Please do not throw sandwich pizza away

1) Physical layer:
    - This is the lowest layer of the OSI model, it defines the physical topology.
    - It is concerned with the transmission and reception of raw bit (binary format) over a physical medium such as a copper or fiber optic cable.
    - It defines the transmission mode, simplex, full/half duplex.
    - Data encoding-It modifies the simple digital signal pattern (1s and 0s) used by the system to better accommodate the characteristics of the physical medium.

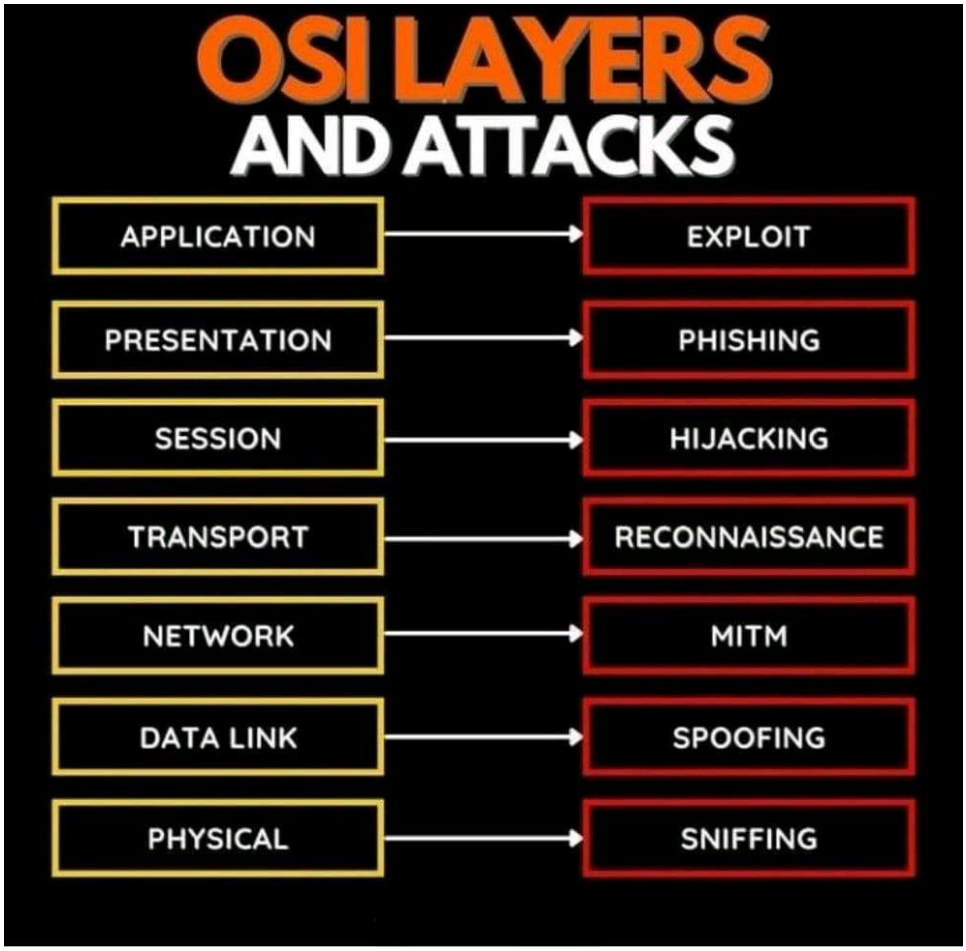
2) Data Link layer:
    - The data link layer provides error-free transfer of data frames from one node to another over the physical layer.
    - Link establishment and termination
    - Frame sequencing and acknowledgement
    - The data link layer is divided into two sub layers.
        - Logical Link Control (LLC) layer–It deals with establishment of logical links between devices, error checking and packet synchronization.
        - Media Access Control (MAC) layer-Responsible for physical addressing i.e.MAC addressing.
3) Network Layer:
    - The network layer knows the addresses of all the nodes in the network. It decides which physical path the data should take based on network conditions, priority of service, and other factors.
    - Logical-physical address mapping i.e., IP and MAC address.
    - Congestion control and packet sequencing.
4) Transport Layer:
    - The transport layer provides host to host communication.
    - The transport layer header includes information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries.
    - It acknowledges successful transmission of data and sends the next data if no errors have occurred.
    - The transport layer can accept large messages, but there are strict message size limits imposed by the network (or lower) layer. So, the transport layer must break up the messages into smaller frames prepending a header to each frame.
    - The transport layer are : Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
5) Session Layer:

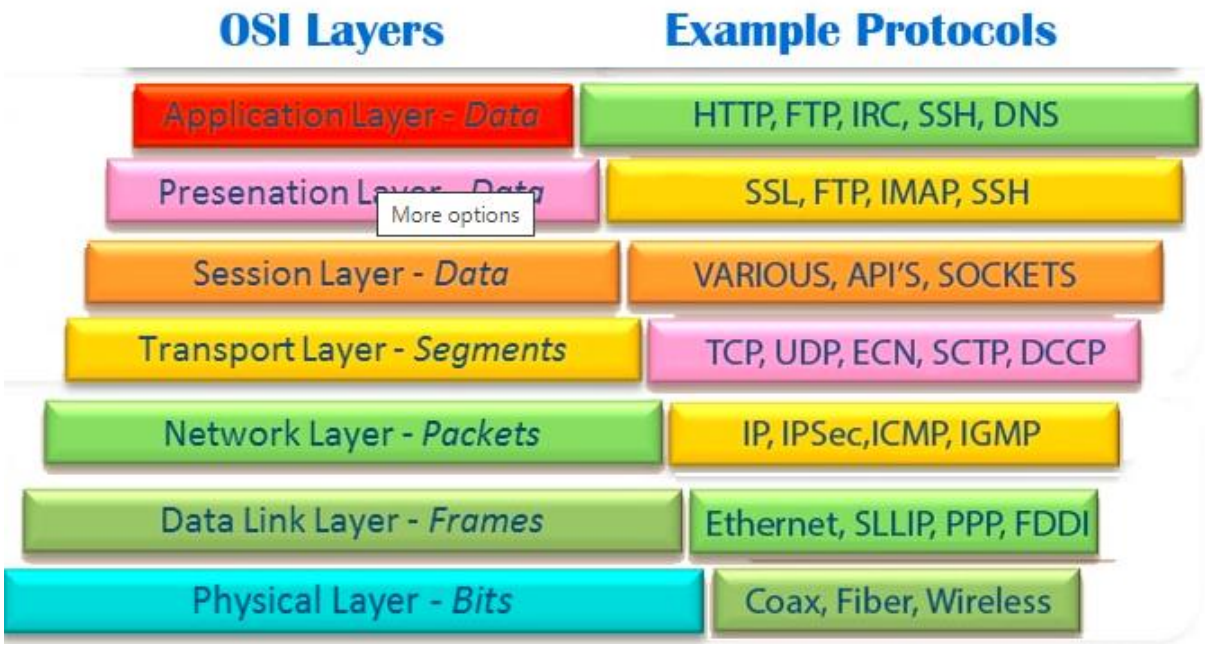
- The session layer allows session establishment and session termination between processes running on different computers.
- Manages the sessions between various hosts and applications.
- It keeps track of file downloads, web page retrievals, telnet connections etc.

6) Presentation Layer:
   - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network.
   - The presentation layer transforms data into the form that the application understands and accepts.
   - Data compression: reduces the number of bits that need to be transmitted on the network.
   - Data encryption: Encrypt data for security purposes. For example, password encryption

7) Application Layer:
   - At the application layer, the user interacts directly with the software application. Here the data is in visual format and not in binary (ones and zeroes).
   - Even when we open a web browser, an application is started.
   - The application layer has many protocols that help with information exchange. Like for example, HTTP, FTP, DNS and many more.
   - This layer provides the following services:
     - Remote file access
     - Remote printer access
     - Directory services
     - Electronic messaging
     - Telnet

Protocol	*Layers*
FTP, HTTP, SMTP, SNMP, telnet	*Application Layer*
SMB, ASN.1	*Presentation Layer*
SSL, TLS, NetBIOS	*Session Layer*
TCP, UDP	*Transport Layer*
IP, ICMP, RIP, ARP, OSPF	*Network Layer*
Ethernet, Token ring, FDDI, ATM	*Data Link Layer*
10BASE-T, 100BASE-T, SONET	*Physical Layer*

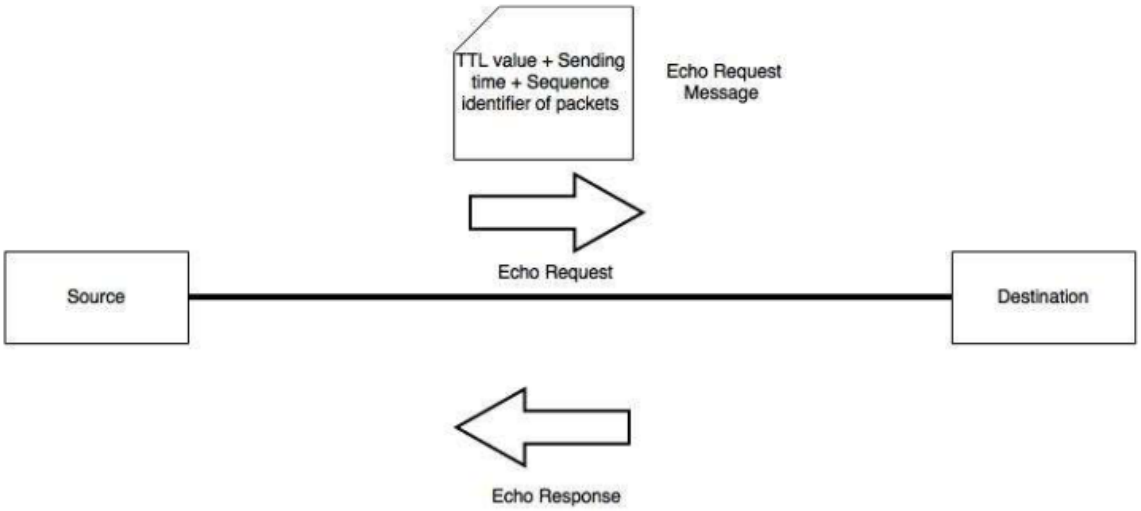

OSI LAYERS
AND ATTACKS
APPLICATION
EXPLOIT
PRESENTATION
PHISHING
SESSION
HIJACKING
TRANSPORT
RECONNAISSANCE
NETWORK
MITM
DATA LINK
SPOOFING
PHYSICAL
SNIFFING


OSI Layers
Example Protocols
Application Layer - Data
HTTP, FTP, IRC, SSH, DNS
Presenation Layer - Data
More options
SSL, FTP, IMAP, SSH
Session Layer - Data
VARIOUS, API'S, SOCKETS
Transport Layer - Segments
TCP, UDP, ECN, SCTP, DCCP
Network Layer - Packets
IP, IPSec,ICMP, IGMP
Data Link Layer - Frames
Ethernet, SLLIP, PPP, FDDI
Physical Layer - Bits
Coax, Fiber, Wireless

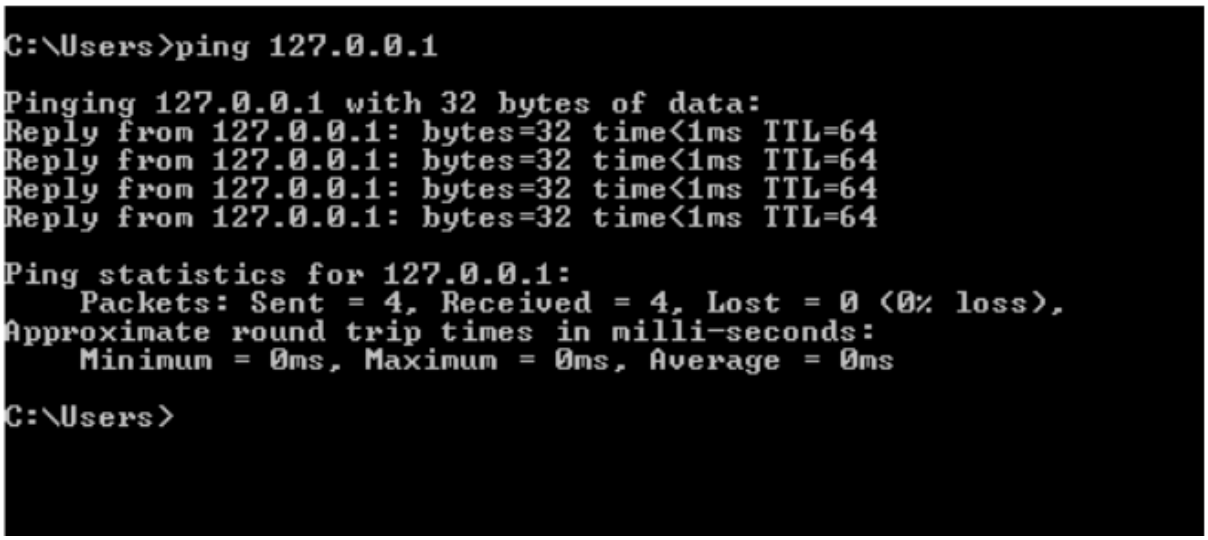
Lecture 4

ICMP Messages

- It is used by network devices to send error messages, for example, a requested service is not available, or a host or router could not be reached in the network. It is used for diagnostic purpose.
- **ICMP Ping**: We ping each other's or our own systems to determine its reachability. Sometimes when a website is not available, we try to ping it and determine if the packets are correctly sent and received i.e., to make sure if it is available or not. So, what exactly happens when we ping?
- Ping is a command. When we ping any host, ICMP echo request packets are sent to the target host and if it is reachable, we receive ICMP echo response packets. It measures the round-trip time and records any packet loss.



- The ICMP echo request message that is sent by the source to the target contains the TTL value of packet, the sequence identifier of the packet and the time when it sends the packet.
- The time when the ICMP echo response is sent by the target is noted by the source. Using the time when the request was sent, and when the response was received by the source, round trip time is calculated.
- Depending upon the number of echo requests set by the user or program, echo requests are sent to the target and round-trip times are calculated. The default is 4 requests. This can be set using the 'count 'option (-n).
- The sequence identifier is incremented with each echo request.
- **Request timed out** –if there is no response from the target this error message is displayed.
- Ping your own system and you can see the following output, syntax is Ping <host IP address/domain name>

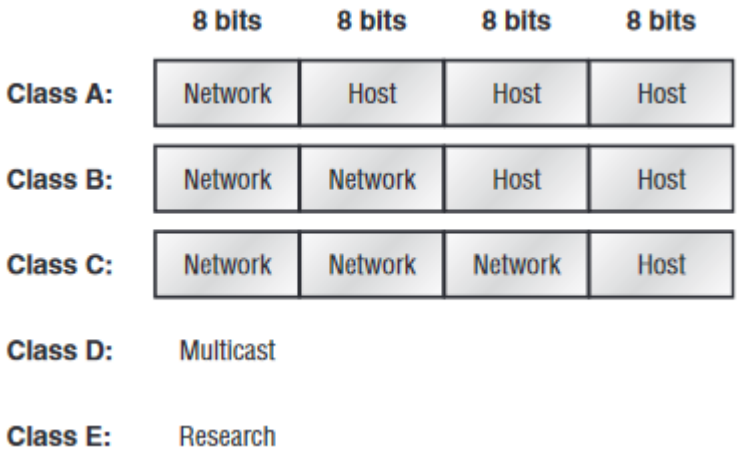


- Let us understand the output. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.
- As we can see the packets sent=4, received=4 and loss=0means the destination host is reachable as the packets were successfully sent.
- Pinging 127.0.0.1 with 32 bytes of data means we are trying to ping the destination 127.0.0.1 with 32 bytes of data sent with each packet.
- The TTL=64value determines the amount of time till which the packet can travel in the n/w

IP Addressing

- **Why do we need IP addresses?**
  - IP addresses uniquely identify our devices on a network and are used for communication.
  - MAC addresses also uniquely identify devices but on the local network, and hence using MAC addresses we can only communicate in the local network.
  - IP addresses are used so that we can communicate across different networks and the internet.
- **IPV4 vs IPV6**
  IPv4 is 32-Bit IP address whereas **IPv6** is a 128-Bit IP address.
  IPv4 is a numeric addressing method whereas **IPv6** is an alphanumeric addressing method.
  MAC address is of 48 bits
  IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas **IPv6** uses NDP (Neighbour Discovery Protocol) to map to MAC address.
- **IP Terminology:**
  Bit: A bit is one digit, either a 1 or a 0.
  Byte: A byte consist of 8 bits. (1 Byte = 8 bits)
  Octet: An octet, made up of 8 bits
  Network Address: This is the designation used in routing to send packets to a remote network—for example, 10.0.0.0, 172.16.0.0, and 192.168.10.0

- An IP address consists of 32 bits of information. These bits are divided into four sections, referred to as octets or bytes, and four octets sum up to 32 bits (8×4=32). You can depict an IP address as: 172.16.30.56
- The major advantage of this scheme is that it can handle a large number of addresses, namely 4.3 billion (a 32-bit address space with two possible values for each position—either 0 or 1—gives you 232, or 4,294,967,296).
- **Network ID and Host ID**
  - IP addresses are divided into two parts: Network ID and the Host ID.
  - The network ID determines the network portion of an IP address.
  - The Host ID determines the host portion of the IP address.
  - N = Network ID
  - H = Host ID
- **Types of IP Addresses**
  - Class A > 1-126 (Ex: 5.2.123.122)
  - Loop back:127.0.0.0 –127.255.255.255
  - Class B > 128-191 (Ex: 145.13.221.178)
    - APIPA Address : APIPA (Automatic private IP Address) assigns a class B IP address from 169.254. 0.0 to 169.254. 255.255 to the client when a DHCP server is either permanently or temporarily unavailable. Designed for small non-routable networks, if a DHCP server becomes available later, the APIPA address is replaced with one from the DHCP server.
  - Class C > 192-223 (Ex: 199.45.234.111)
  - Class D > 224-239 (Ex 228.125.189.213)
  - Class E > 240-254 (Ex: 241.129,221.155)



- **Class A**
  For class A IP addresses, the first byte is network ID and the other bytes are host ID.
  Syntax –N.H.H.H
  IP address -64.40.58.11
  Network ID –64.0.0.0
  Host ID –0.40.58.11
- **Class B**
  For class B IP addresses, the first two bytes are network IDs and the other bytes are host ID.

Syntax –N.N.H.H
IP address –160.200.226.204
Network ID –160.200.0.0
Host ID –0.0.226.204

- **Class C**
  For class C IP addresses, the first three bytes are network IDs and the last byte is host ID.
  Syntax –N.N.N.H
  IP address –192.168.1.2
  Network ID –192.168.1.0
  Host ID –0.0.0.2
- **Class D** – Multicast Address
  Multicast Addressing: To send data to a specific group of machines in a network we do multicasting. In IPv4, addresses 224.0.0.0 through 239.255.255.255 (Class D addresses) are designated as multicast addresses.

- **Class E**
  The Internet Engineering Task Force (IETF) reserves these addresses for its own research.

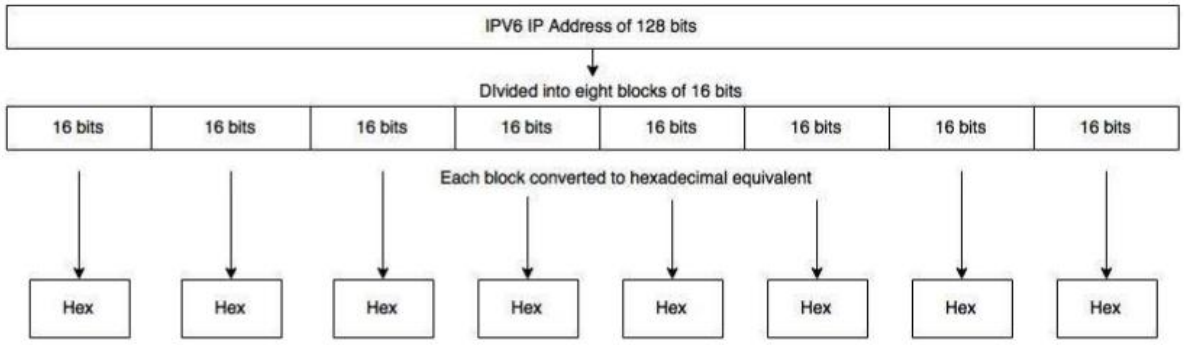
Modes of Addressing (Routing)

- **Unicast Addressing:** Here the data is sent from a source machine to a destination machine. The destination address field in the data packet contains the IP address of the destination machine. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient.
- **Broadcast Addressing:** In broadcast addressing, the data is sent from the sender to all the machines in the network. The sender sends data only once and all the machines receive a copy of it. 255.255.255.255 is the broadcast address of the network 0.0.0.0, when data is sent on this broadcast address it is forwarded to all machines in the local network but never forwarded by the routers connecting the local network to other networks.
  Example -140.176.0.0/16 class B network
  Broadcast address for this network -140.176.255.255
- **Multicast Addressing:** To send data to a specific group of machines in a network we do multicasting. In IPv4, addresses 224.0.0.0 through 239.255.255.255 (Class D addresses) are designated as multicast addresses
- **Private Vs Public IP Address:**
- **Private IP** address of a system is the IP address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.
  - Private IP provide security to end users on the network while accessing resources on the Internet.
  - They help with network administration.
  - Many homes have more than one Internet connected device, such as smartphones, tablets etc. In such situations, a network address translator (NAT) is usually used to provide Internet connectivity to multiple hosts.
  - They also help with scalability.

- **Public IP** address of a system is the IP address which is used to communicate outside the network. Public IP address is basically assigned by the ISP (Internet Service Provider)

IPV6:

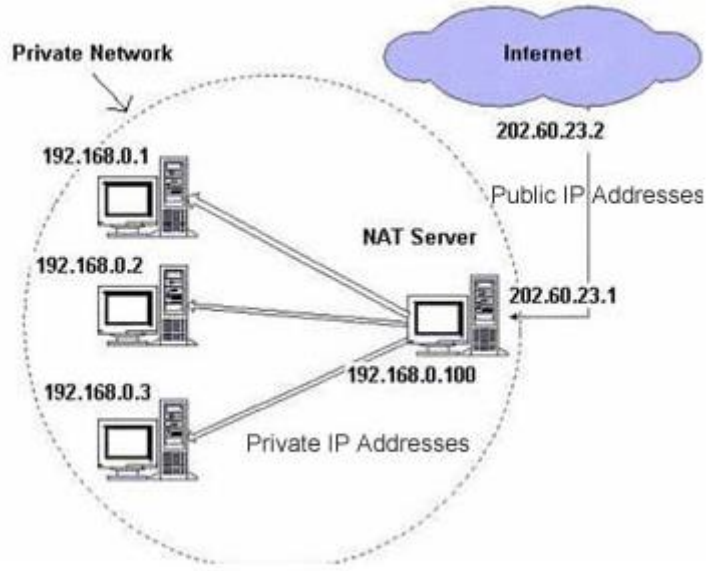
- There are currently two versions of Internet Protocol (IP): IPv4 and IPv6. Billions of devices are already sharing IP addresses.
- There will be a time when devices like watches might also need an IP address.
- IP v6 provides 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses.
- It should meet the world's IP addressing needs well into the future.
- Internet has grown exponentially, and the address space allowed by IPv4 will not be sufficient for the ever-increasing number of devices.
- An IPV6 address, like an IPV4 address, uniquely identifies a network interface of a computer on a network. It is made up of 128 bits and provides a large address space as compared to IPV4. It addresses the shortcoming of IPv4.
- An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.



The Hex values are then separated with ' : ' (colon) and we get a IPV6 address. Example: FE80:0000:0000:0000:0202:B3FF:FE1E:8329

Sr. No.	Key	Private IP Address	Public IP Address
1	Scope	Private IP address scope is local to present network.	Public IP address scope is global.
2	Communication	Private IP Address is used to communicate within the network.	Public IP Address is used to communicate outside the network.
3	Format	Private IP Addresses differ in a uniform	Public IP Addresses differ in

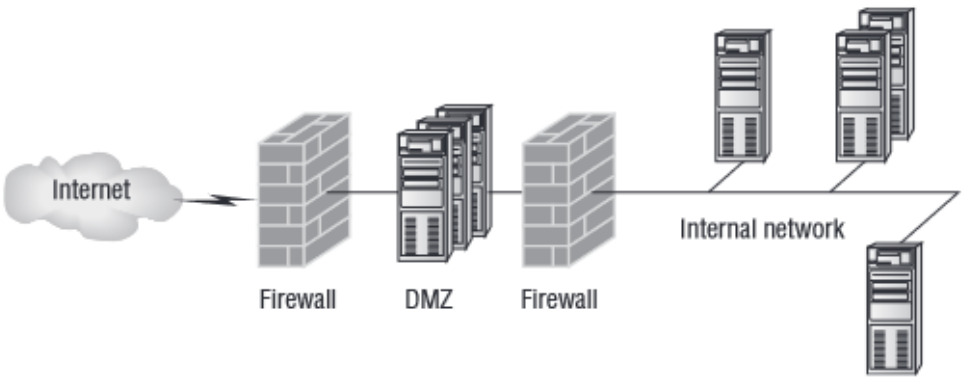
Sr. No.	Key	Private IP Address	Public IP Address
		manner.	varying range.
4	Provider	Local Network Operator creates private IP addresses using network operating system.	ISP, Internet Service Provider controls the public IP address.
5	Cost	Private IP Addresses are free of cost.	Public IP Address comes with a cost.
6	Locate	Private IP Address can be located using ipconfig command.	Public IP Address needs to be searched on search engine like google.
7	Range	Private IP Address range: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255	Except private IP Addresses, rest IP addresses are public.
8	Example	Private IP Address is like 192.168.11.50.	Public IP Address is like 17.5.7.8.



Lecture 5

Firewall

- Firewall is a network device which allow or denies traffic based on rules defined on it.
- A firewall is a device that protects a network from unauthorized access. It acts as a barrier between the internal network and the public network (internet).
- A firewall monitors the incoming traffic by applying a set of rules i.e. Access Control Rules. You can create or disable firewall filter rules, based on conditions as:
  •IP Addresses (which are to be allowed/blocked)
  •Domain names
  •Protocols(allowed/blocked)
  •Keywords(permit/deny)
- A firewall can be either a stand-alone "black box" or a software implementation placed on a server or router.



- one to the Internet (known as the public side) and one to the network (known as the private side)
- Sometimes, there is a second firewall. This firewall is used to connect servers and equipment that can be considered both public and private (like web and email servers). This intermediary network is known as a demilitarized zone (DMZ).
- Firewalls are the first line of defense for an Internet-connected network. Without them in place, any network that's connected to the Internet is essentially wide open to anyone.
- Types of Firewalls:
  - **Stateful Packet Inspection (SPI)**
  - **Proxy Server Firewalls**
  - **Packet Filter**

Firewall vendors: Checkpoint, CISCO ASA, FortiGate, SonicWALL, Palo Alto, IP tables, Windows defender

ZONES: DMZ, Database, Application, User etc

Intrusion Detection and Prevention System (IDS/IPS):

- A firewall filters traffic based on the access rules that are configured on a firewall. Intrusion detection and prevention systems analyze the traffic in more detail. They are intelligent as compared to a firewall.
- **Intrusion Prevention System (IPS):** Intrusion prevention systems examines network traffic that for any malicious activity. Intrusion prevention systems:
  •Identifies malicious activity (raises alarm)
  •Logs information about this activity
  •Tries to prevent it (dropping the malicious packets/blocking traffic from that particular IP)
  •Reports the activity to the network/firewall administrator
- **Intrusion Detection System (IDS):**An intrusion detection system monitors network traffic for malicious activity. It detect scan intrusion and does not block or stop it like an IPS. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection systems:
  •Identify malicious activity
  •Logs information aboutthis activity
  •May not block or stop the attack(depending on the IDS)
  •Report the activity
- There is network based (NIDS) and host based (HIDS) intrusion detection systems.
  Network IDS:
  - Network based IDS are placed at various locations in the network to monitor traffic to and from all devices on the network.
  - It monitors traffic to and froall devices on the network.
  - It analyzes the traffic on the subnet, and matches the traffic thatis passed on the subnets to a library of known attacks.The alerts are sent to the administrators.
  - Example: Snort

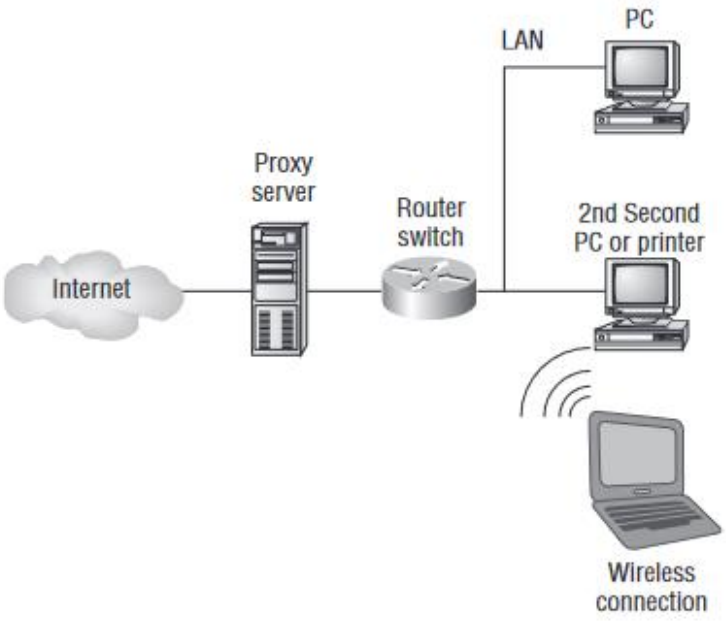
  Host based IDS:

  - Host based IDS are runs of individual hosts on the network.
  - it only monitors traffic to and from the device on which IDS is installed.
  - It takes a snapshot of existing system files and matches it to the system files previous snapshot and compares for any unusual change. Alerts are sent to the administrators.
  - Example: OSSEC -Open Source Host-based Intrusion Detection System

Firewall,IDS,IPS, Proxy,Load Balancer, WAF, Switch,Router, DHCP,DNS, NAT,NIC,AV, DLP, EDR

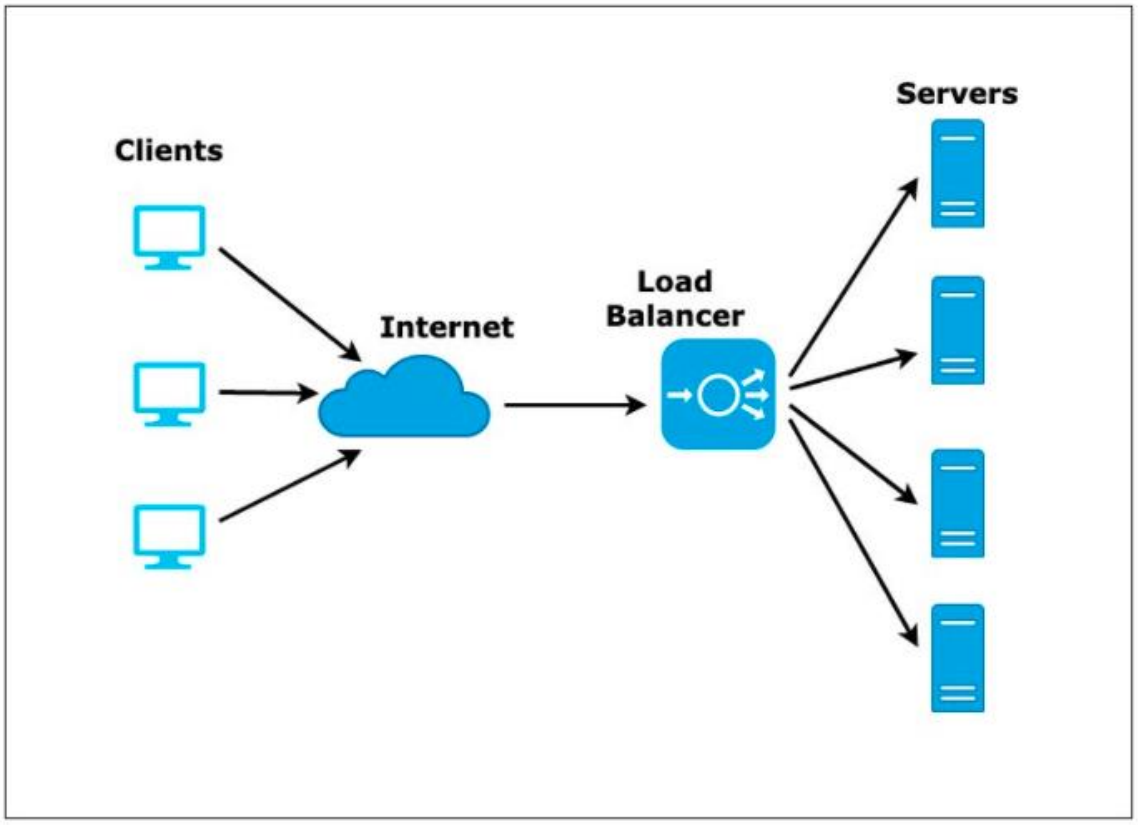
Proxy Server:

- A proxy server is basically a type of server that handles its client-machine requests by forwarding them on to other servers while allowing granular control over the traffic between the local LAN and the Internet.
- When it receives a request, the proxy will then connect to the specific server that can full fill the request for the client that wants it.
- Sometimes the proxy modifies the client's request or a server's response to it—or even handles the client's request itself.
- It will cache or "remember" the specific server that would have normally been contacted for the request in case it's needed another time.
- This behaviour really speeds up the network's function, thereby optimizing its performance.
- Proxy servers can also limit the availability of the types of sites that users on a LAN have access to, which is a benefit for an administrator of the network if users are constantly connected to non-work sites and using all the WAN bandwidth.



Load Balancer

Think about this scenario: Say you have a web site where people are placing orders for the stuff you have got for sale. Obviously, the orders placed vary in size and the rate at which that they come in; and you would not want your servers becoming so overloaded that they hose up and crash your site, causing you to lose lots of money, now would you? That's where balancing the load of traffic between a group of servers comes to the rescue, because even if one of them freezes, your customers will still be able to access your site and place orders.

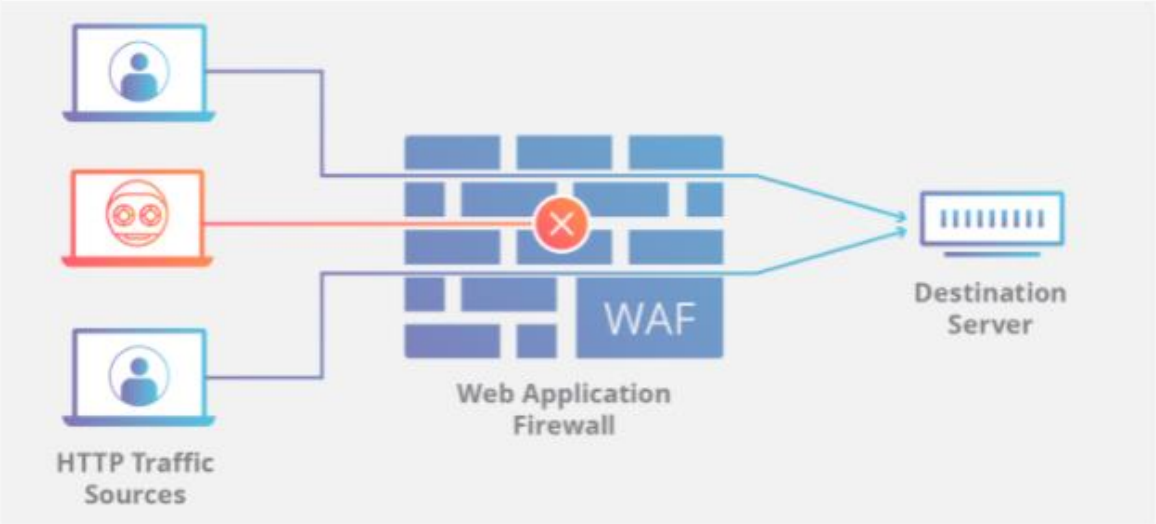


Load Balancer between client and the server

Web Application Firewall:

- A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

- It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.
- A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks.



Working:

- A WAF that operates based on a blocklist (negative security model) protects against known attacks.
- Think of a blocklist WAF as a club bouncer instructed to deny admittance to guests who don't meet the dress code.
- Conversely, a WAF based on an allow list (positive security model) only admits traffic that has been pre-approved.
- Both blocklists and allow lists have their advantages and drawbacks, which is why many WAFs offer a hybrid security model, which implements both.

Network-based, host-based, and cloud-based WAFs

A network-based WAF is generally hardware-based. Since they are installed locally they minimize latency, but network-based WAFs are the most expensive option and also require the storage and maintenance of physical equipment.

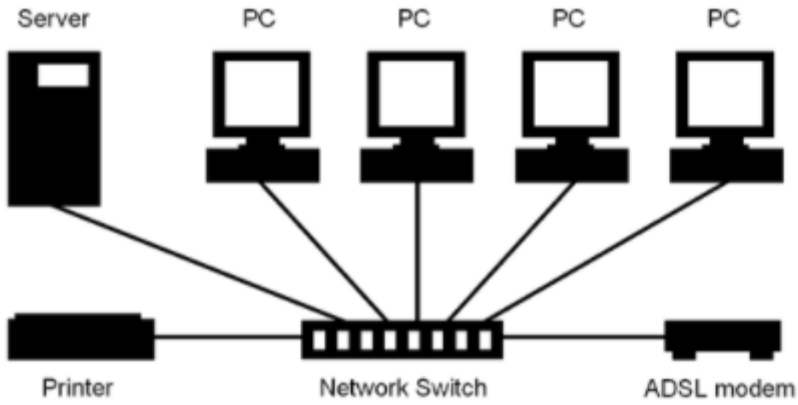
A host-based WAF may be fully integrated into an application's software. This solution is less expensive than a network-based WAF and offers more customizability. The downside of a host-based WAF is the consumption of local server resources, implementation complexity, and maintenance costs. These components typically require engineering time, and may be costly.

Cloud based WAFs offer an affordable option that is very easy to implement; they usually offer a turnkey installation that is as simple as a change in DNS to redirect traffic. Cloud-based WAFs also have a minimal upfront cost, as users pay monthly or annually for security as a service. Cloud-based WAFs can also offer a solution that is consistently updated to protect against the newest threats without any additional work or cost on the user's end. The drawback of a cloud-based WAF is that users hand over the responsibility to a third-party, therefore some features of the WAF may be a black box to them.

Ex: Akamai WAF

Switch:

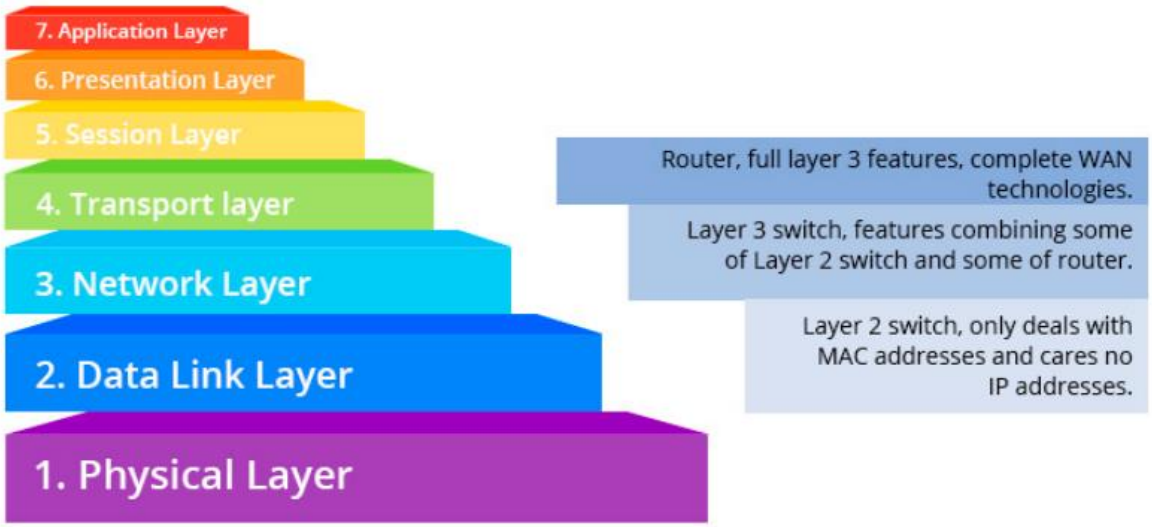

Avaya ERS 2550T-PWR, a 50-port Ethernet switch



- Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers, on the same network within a building or campus.
- A switch enables connected devices to share information and talk to each other.
- The basic function that any switch is supposed to perform is to receive information from any source connected to it and dispatch that information to the appropriate destination only.
- A switch is operated at the data link layer to develop a distinct collision domain for each port of the switch.
- Let us consider, there are four computers - A, B, C, and D connected to four ports of the switch, then any pair, say A and B, may transfer data in either

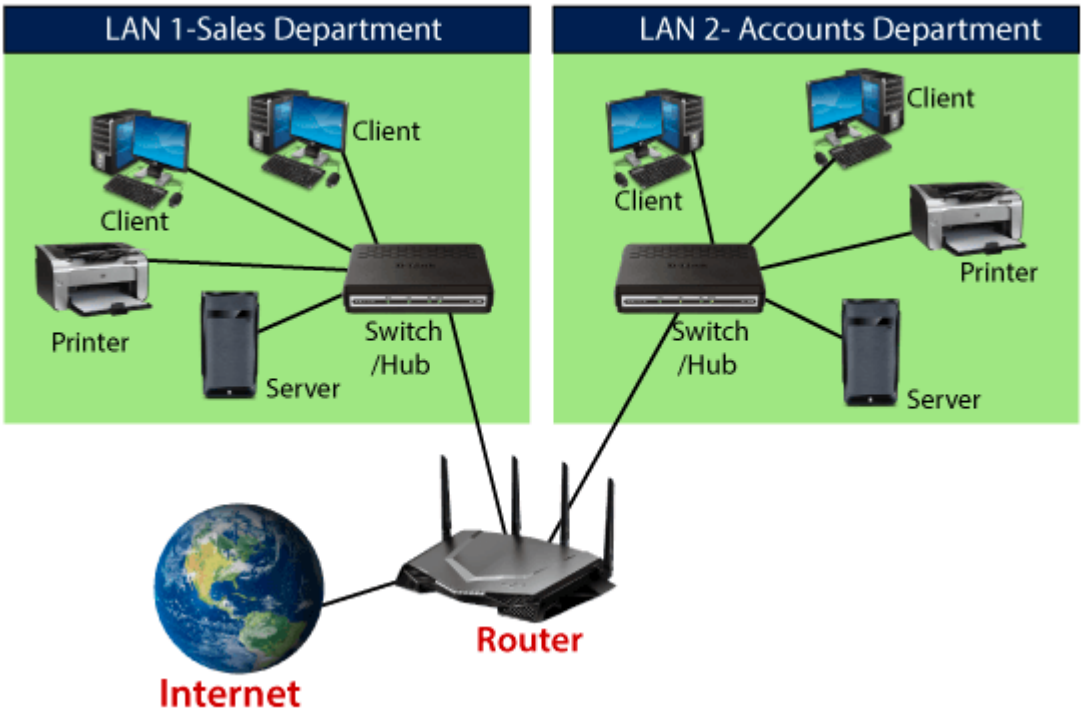
direction, at the same time, the other pair, C and D, can exchange their information simultaneously, and these two communications will not interrupt each other.

- Layer 2 switches perform the switching function to re-arrange the data frames from the source to its destination network. Layer 3 switch or multiplayer switch define paths based on logical addressing. Layer 2 switches are used to reduce traffic on the local network, whereas Layer 3 switches mostly used to Implement VLAN.

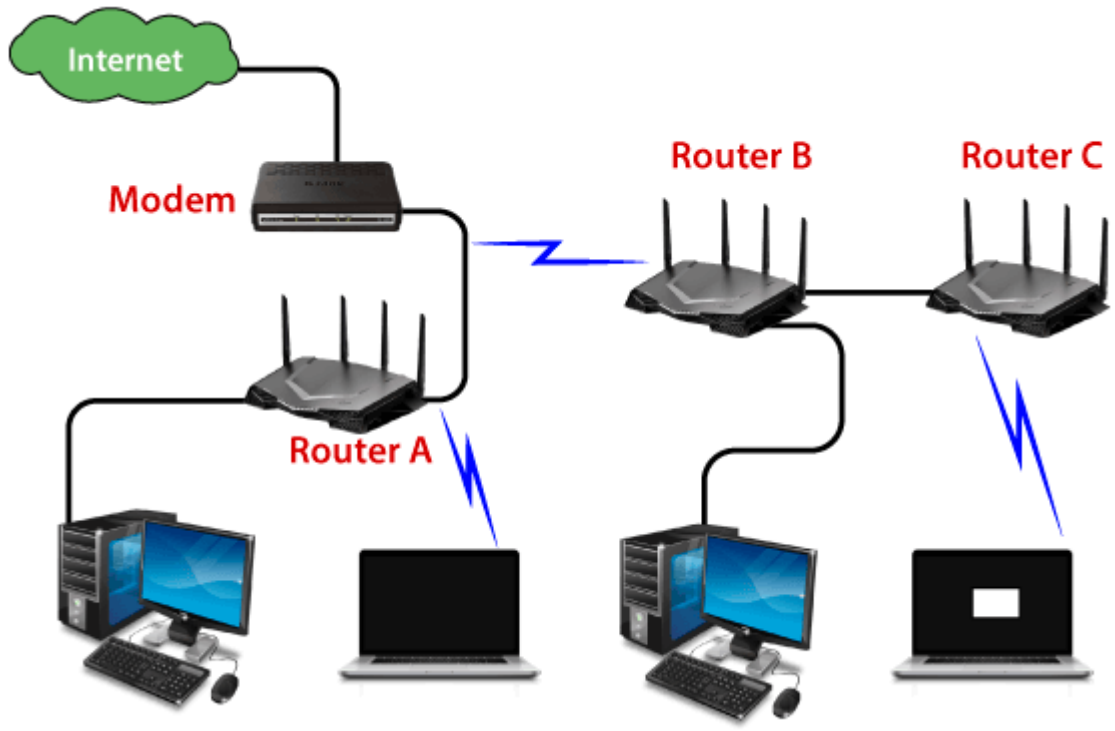


Router:

- A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet.
- The most familiar type of IP routers are home and small office routers that simply forward IP packets between the home computers and the Internet.



- A router works on the **third layer** of the OSI model, and it is based on the IP address of a computer.
- It uses protocols such as ICMP to communicate between two or more networks. It is also known as an intelligent device as it can calculate the best route to pass the network packets from source to the destination automatically.
- A router analyses a destination IP address of a given packet header and compares it with the routing table to decide the packet's next path.
- The list of routing tables provides directions to transfer the data to a particular network destination. They have a set of rules that compute the best path to forward the data to the given IP address.



- There are two types of tables in the router that are **static and dynamic**. The static routing tables are configured manually, and the dynamic routing tables are updated automatically by dynamic routers based on network activity.

Benefits of Router:

- **Security:** Router provides the security, as LANs work in broadcast mode. The information is transmitted over the network and traverses the entire cable system. Although the data is available to each station, but the station which is specifically addressed reads the data.
- **Performance enhancement:** It enhances the performance within the individual network. For example, if a network has 14 workstations, and all generate approximately the same volume of traffic. The traffic of 14 workstations runs through the same cable in a single network. But if the network is divided into two sub-networks each with 7 workstations, then a load of traffic is reduced to half. As each of the networks has its own servers and hard disk, so fewer PCs will need the network cabling system.
- **Reliability:** Routers provide reliability. If one network gets down when the server has stopped, or there is a defect in the cable, then the router services, and other networks will not be affected. The routers separate the affected network, whereas the unaffected networks remain connected, without interrupting the work and any data loss.

- **Networking Range:** In networking, a cable is used to connect the devices, but its length cannot exceed 1000 meters. A router can overcome this limitation by performing the function of a repeater (Regenerating the signals). The physical range can be as per the requirement of a particular installation, as long as a router is installed before the maximum cable range exceeds.

Routing Protocols:

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Exterior Gateway Protocol (EGP)
- Routing Information Protocol (RIP)

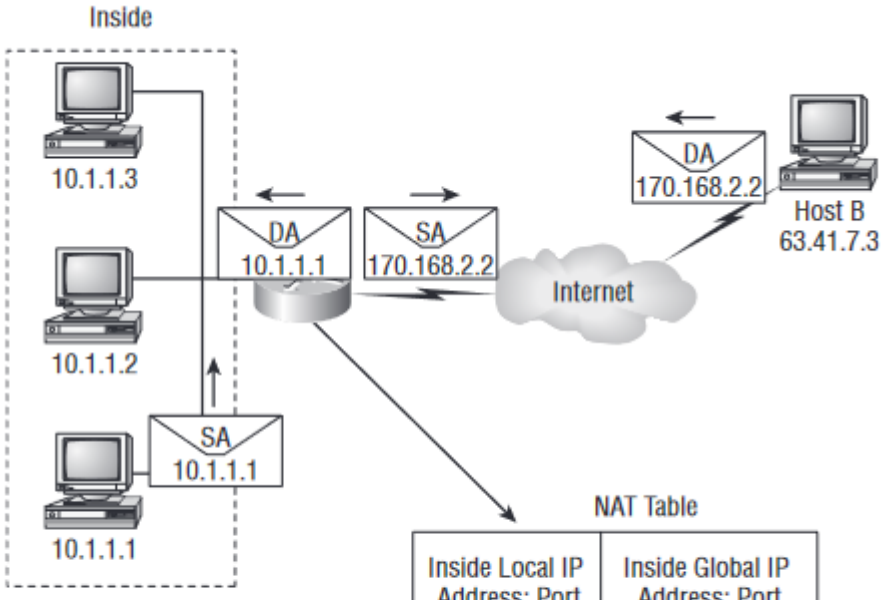
Difference Between Switch and Router:

Switch	**Router**
The switch works in data link layer of OSI Model.	Route works in the network layer of OSI Model.
The switch is a multicast device.	The router is a routing device.
Switch transfer data in the form of frames.	Router transfer data in the form of packets.
The switch is used to connect multiple LANs or multiple devices in the same network.	The router is used to connect two completely different network available in the different region.
Switch offers wired connectivity in a network.	The router offers both wired and wireless connectivity in a network.
The switches determine the destination address with the help of hardware-configured MAC address and transfer the data.	Routers use software-configured network address, to determine the address.
Switches transfer the data between LAN segments.	Routers transfer the data between LAN and WAN segments
The switch is basically placed in the	The router is basically placed in

network where all the devices are directly get connected to it.	the gateway of a network from where all the packets are coming in going out.
Whenever a user sends a data in the network, it will reach to switch first.	The router is the last device in a network to receive the data.
The switch does not use any routing table to transfer data.	The router uses a routing table to find the perfect route to send the data.
Cannot configure path manually to send data.	Can configure multiple paths for sending data in a network.
Cannot configure protocols such as RIP, IGRP, OSPF, etc.	Can be configured protocols such as RIP, IGRP, OSPF, etc according to network requirement.

Network Address Translation:

- An IP address is a very important information that identifies devices on a network. There are two types of IP addresses, public and private.
- The Public address is the one that is given by the Internet Service Provider as soon as the computer is connected to the network and which is unique and the private IP address is the one reserved by The Internet Assigned Numbers Authority (IANA) for private networks (local networks)
- 10.0.0.0 –10.255.255.255
  172.16.0.0 –172.31.255.255
  192.168.0.0 –192.168.255.255



NAT Table

Inside Local IP Address: Port	Inside Global IP Address: Port
10.1.1.3	170.168.2.4
10.1.1.2	170.168.2.3
10.1.1.1	170.168.2.2

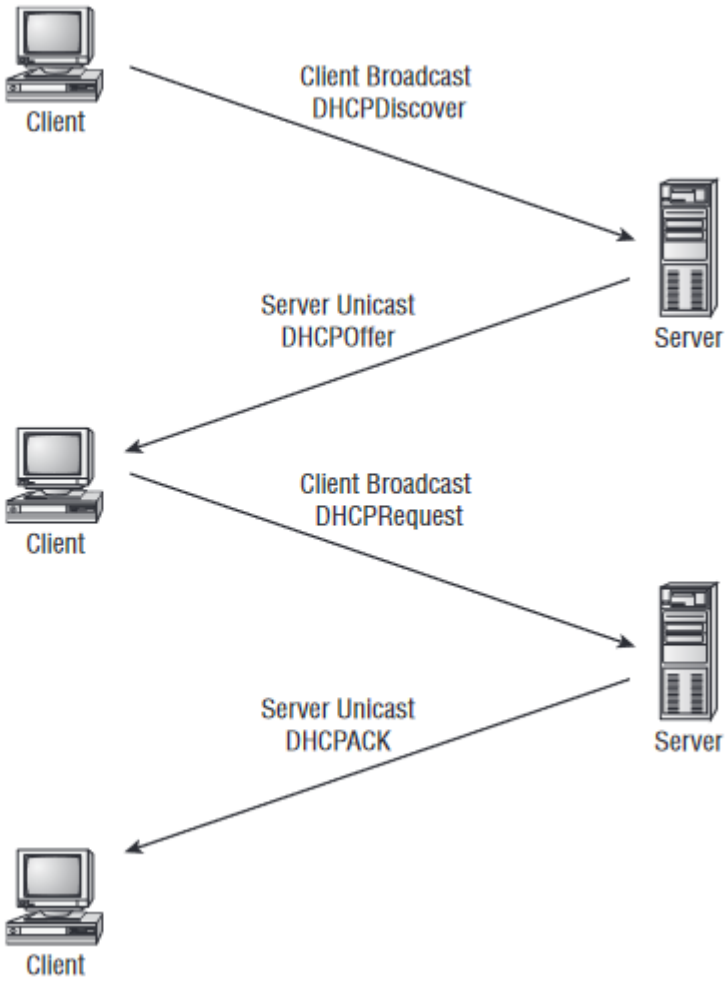
- Host 10.1.1.1 sends an outbound packet to the router configured with NAT. The router identifies the IP address as an inside local IP address destined for an outside network, translates the address, and documents the translation in the NAT table.
- The packet is sent to the outside interface with the new translated source address. The external host returns the packet to the destination host, and the NAT router translates the inside global IP address back to the inside local IP address using the NAT table.

PAT

- A port address translation (PAT) is a kind of dynamic NAT protocol, a subgroup of a NAT, that allows multiple devices on a single private network to connect to the public internet using the same public IP address.
- Information sent and received through the PAT connection receives a port number at the end of the IP address. This distinguishes the different devices on the network without requiring multiple public IP address connections

DHCP:

- Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to hosts with information provided by a server. It allows easier administration and works well in small to even very large network environments.
- DHCP server provide below mentioned information to a host when the host is requesting an IP address from the DHCP server.
    - IP address
    - Subnet mask
    - Domain name
    - Default gateway (routers)
    - DNS
    - Windows Internet Naming Service (WINS) information



1. The DHCP client broadcasts a DHCP Discover message looking for a DHCP server (Port 67).
2. The DHCP server that received the DHCP Discover message sends a unicast DHCP Offer message back to the host
3. The client then broadcasts to the server a DHCP Request message asking for the offered IP address and possibly other information.
4. The server finalizes the exchange with a unicast DHCP Acknowledgment message.

DNS:

- Domain Name Service (DNS) resolves hostnames—specifically, Internet names, such as www.google.com, to their corresponding IP addresses.
- What would hap-pen if you wanted to move your web page to a different service provider? The IP address would change, and no one would know what the new one was. DNS allows you to use a domain name to specify an IP address. You can change the IP address as often as you want, and no one will know the difference.

- Aero Airlines and aerospace companies
- biz Businesses or firms
- com Commercial Organizations
- coop Cooperative business Organizations
- edu educational institutions
- gov Government institutions
- info Information service providers
- int International Organizations
- mil Military groups
- museum Museum & other nonprofit organizations
- name Personal names
- net Network Support centers
- org Nonprofit Organizations
- pro Professional individual Organizations

Country Domain

- The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

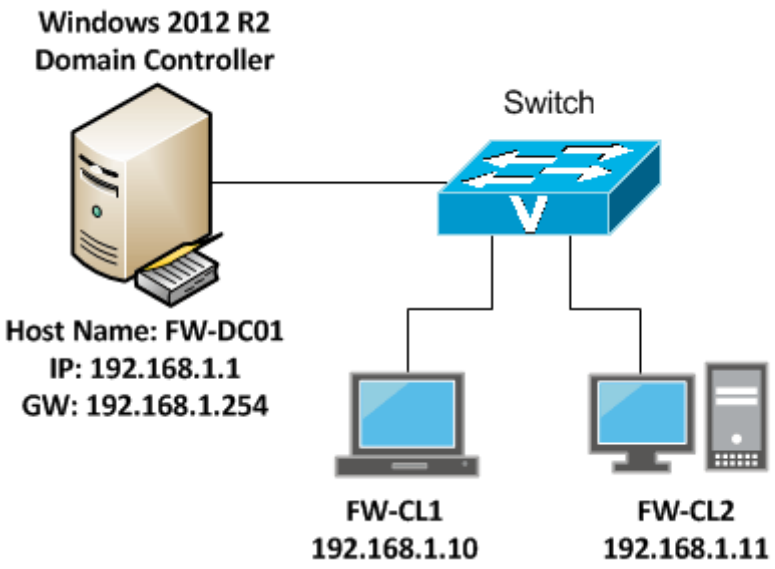
Active Directory:

- Microsoft windows Laptop/Desktop OS: Windows XP, Windows 7, Windows 10, Windows 11
- Microsoft windows server OS: Windows 2003, Windows 2008, Windows 2012, Windows 2016 , windows server 2019
- Server/Laptop/desktop imp config: Processor, OS, RAM, Hard Disk
- Linux OS: RHEL (Red hat), Cent OS, Kali Linux, Ubuntu
- Local User vs Domain User
- Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.
- A server running the Active Directory Domain Service (AD DS) role is called a domain controller.
- It authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers, and installing or updating software.
- For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.
- Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services.

Domain Services

Active Directory Domain Services (AD DS) is the foundation stone of every Windows domain network. It stores information about members of the domain, including devices and users, verifies their credentials and defines their access rights.

The server running this service is called a domain controller. A domain controller is contacted when a user logs into a device, accesses another device across the network, or runs a line-of-business Metro-style app sideloaded into a device



What is Vulnerability:

- Vulnerability can be defined as an issue in the software code that a hacker can exploit to harm the systems. It can be a gap in the implementation of cybersecurity procedures or a weakness in the controls.
- A vulnerability is a flaw that could lead to the compromise of the confidentiality, integrity, or availability of an information system.
- Android was the most vulnerable OS in 2019, but things are improving. A total of 414 security vulnerabilities were reported for the Android operating system in 2019, higher than Debian Linux, Windows 10, and Ubuntu.
- There are various authentic sources of documented vulnerabilities, including the following:
  CVE (Common Vulnerabilities and Exposures): This is managed by the MITRE Corporation and sponsored by the U.S.

  https://www.cvedetails.com/vulnerability-list/

OWASP (Open Web Application Security Project): OWASP manages a list of vulnerabilities in a project known as the OWASP Top 10 https://owasp.org/www-project-top-ten/

Types of Hackers:

A hacker is a person who breaks into computer systems to gain unauthorized access to data. It could be for malicious purpose or with good intentions. Let us understand the types of hackers.

Black Hat

- A Black hat hacker is one who breaks into computer system for illegal purposes, often for personal gain.
- When a black hat hacker gets access to a system, he may misuse the information and take advantage of the break-in by destroying files or stealing data.

White Hat

- A white hat hacker is an ethical hacker who breaks into computer system with no malicious intent.
- He is an ethical hacker who has the required permission to hack into computer system to discover vulnerabilities so that they can be patched before the system is compromised.
- For example, a black hat hacker would compromise a computer system without permission, stealing information for their own personal gain or vandalizing the system. (E.g., breaking into a bank's vault) A white-hat hacker would ask for permission before testing the system's security and alert the organization after compromising it.

Gray Hat

- A Gray-hat hacker falls in between a black hat and a white hat hacker. A Gray hat hacker can illegally hack into a system but not for personal gains.
- The Gray hat hacker will hack to show his hacking skills or to prove that a particular system has vulnerabilities. A Gray-hat hacker might attempt to compromise a computer system without permission, but informs the organization later allowing them to fix the problem.
- While the Gray-hat hacker did not use their access for bad purposes, they compromised a security system without permission, which is illegal. A Gray hat hacker could also publish the vulnerability publicly allowing criminals to take advantage.

Hacktivism:

- Derived from combining the words 'Hack' and 'Activism', hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes. The individual who performs an act of hacktivism is said to be a hacktivist.

  https://www.cybersecuritydegrees.com/faq/the-most-inspiring-cases-of-hacktivism/

Patch Tuesday:

- Patch Tuesday (also known as Update Tuesday) is an unofficial term used to refer to when Microsoft, Adobe, Oracle, and others regularly releases software patches for their software products. It is widely referred to in this way by the industry. Microsoft formalized Patch Tuesday in October 2003.
- Although patches are sent out every second Tuesday of the month, critical code fixes are sent out any time.

Zero Day Attacks:

- A zero-day vulnerability is a vulnerability that is not known to the vendor yet but has been discovered by some attackers. When attackers exploit such vulnerabilities for which the patch has not been released, to break into a system, it is known as a zero-day attack.

Penetration Testing Vs Ethical Hacking:

Penetration Testing: Deals with the process of finding vulnerabilities in a target environment. Target is a single system.

Ethical Hacking: Encompasses all hacking techniques and attacks to find security flaws. Target is entire network.

Understanding Access Control

Identification vs. Authentication:

- Identification means finding out who someone is.
- Authentication is a mechanism of verifying that identification.
- In another way, identification is claiming an identity; authentication is proving it.

Examples: A password or PIN, A smart card, token, or identification device. your fingerprints or retinal pattern (often called biometrics). Action you must take to complete authentication. Your geolocation.

Authentication and Authorization:

Authentication is the process of verifying the identity of a user by obtaining some sort of credentials and using those credentials to verify the user's identity. If the credentials are valid, the authorization process starts. Authentication process always proceeds to Authorization process.

You were probably already familiar with the process of authentication, because most of us perform it most every day, whether at work (logging onto your PC) or at home (logging into a website).

Authorization is the process of allowing an authenticated users to access the resources by checking whether the user has access rights to the system. Authorization helps you to control access rights by granting or denying specific permissions to an authenticated user.

In simple terms, authorization determines your ability to access the system and up to what extent. Once your identity is verified by the system after successful authentication, you are then authorized to access the resources of the system.

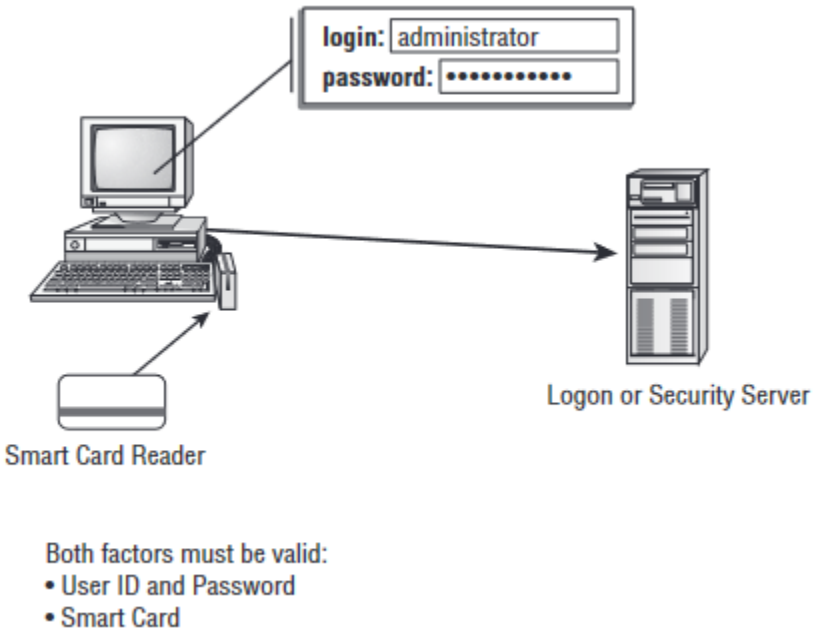
Authentication	Authorization
Authentication confirms your identity to grant access to the system.	Authorization determines whether you are authorized to access the resources.
It is the process of validating user credentials to gain user access.	It is the process of verifying whether access is allowed or not.
It determines whether user is what he claims to be.	It determines what user can and cannot access.
Authentication usually requires a username and a password.	Authentication factors required for authorization may vary, depending on the security level.
Authentication is the first step of authorization so always comes first.	Authorization is done after successful authentication.
For example, students of a particular university are required to authenticate themselves before accessing the student link of the university's official website. This is called authentication.	For example, authorization determines exactly what information the students are authorized to access on the university website after successful authentication.

Multifactor Authentication:

When two or more access methods are included as part of the authentication process, it is called a multifactor authentication system.

A system that uses smart cards and passwords is referred to as a two-factor authentication system.

Two-factor authentication is shown in Figure. This example requires both a smart card and a logon password process.



A multifactor system can consist of a two-factor system, three-factor system, and so on. If more than one factor is involved in the authentication process, it is considered a multifactor system. But the two or more factors employed should not be from the same category.

Authentication Protocols:

A variety of authentication protocols are used to aid in authenticating a user (or another system) to a system:

- PAP (Password Authentication Protocol) is an older system that is no longer used. PAP sends the username and password to the authentication server in plain text.
- SPAP (Shiva Password Authentication Protocol) replaced PAP. The main difference is that SPAP encrypts the username and password.
- The TOTP (Time-Based One-Time Password) algorithm uses a time-based factor to create unique passwords.
- The HOTP (HMAC-Based One-Time Password) algorithm is based on using a Hash Message Authentication Code (HMAC) algorithm.

Account Policy Enforcement:

The account policy determines the security parameters regarding who can and cannot access the system.

Password Length and Complexity:

- The more difficult a user's password is, the more difficult it becomes for a miscreant to break it and log in as that user, and the more difficult it becomes, as well, for the user to remember it.
- Choosing this option requires users to create passwords that meet the following requirements:
- They cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- They must be at least eight characters long.
- They must contain characters from at least three of the following four sets:
  - A–Z
  - a–z
  - 0–9
  - Non-alpha characters (!, $, #, %, and so forth)

Password Expiration

- Every password must expire because the longer the same value is used, the more likely it is to be broken.
- Ninety days is acceptable for many organizations, but Microsoft often recommends setting this value to 42 days if you want to enforce strong password usage throughout the organization.
- To keep users from changing their password to the same value as the old one, or to one they used the last time around, you should enable password history.

Password Recovery

- One of the certainties in life is that users will occasionally forget their password. This often occurs shortly after they've changed it from one value to another, but it can often occur after a long weekend.

Password Disablement and Lockout

- When a user will be gone from a company for a while (maternity leave, for example), their account should be disabled until they return. When a user will be gone from a company forever (termination), their account should be removed from the system immediately.
- Lockout occurs when a user is attempting to log in but giving incorrect values; locking this account is necessary to prevent a would-be attacker from repeatedly guessing at password values until they find a match. You can configure the lockout policies at the local level on the workstation (Local Security Policy) as well as at

the domain level (Group Policies), and the values you configure are the same:

Account Lockout Duration When the system locks the account, this is the duration before it is unlocked. With Windows, this value can range from 0 minutes to 99,999 minutes.

Account Lockout Threshold This setting determines how many incorrect attempts a user can give before the account is locked. In Windows, this value can range from 0 to 999.

Users with Multiple Accounts/Roles: Analyst, Senior Analyst, Lead Analyst

Generic Account Prohibition: A generic account is any account that is shared—allowing multiple users to log in and use the system/network/resource.

Implementing Access Controlling Best Practices:

How you implement access control makes all the difference in the security of your systems.

Least Privileges:

- This is one of the most critical concepts in access control. Implementing least privileges means that any given user (or system) is given the minimum privileges necessary to accomplish his or her job.
- Example, if sales managers need to run reports from a database, they will be given privileges only allowing the running of reports. They won't be given privileges to delete data, alter the database tables, add users, and so forth.

Separation of Duties:

- The principle of separation of duties says that no user should have all the privileges necessary to complete a critical business function by themselves.
- Instead, the critical business function should be divided into discrete tasks and the appropriate privilege granted to different users. By requiring the involvement of more than one employee, separation of duties helps prevent fraud and abuse.

Time of Day Restrictions:

- if you are the administrator for an office, and workers use the systems only from 8:00 to 5:00 Monday through Friday, then you can configure their accounts to allow access only from 7:00 to 6:00 (offering an extra hour at each end for work they need to do outside of normal) on those days and not allow access outside of those parameters.

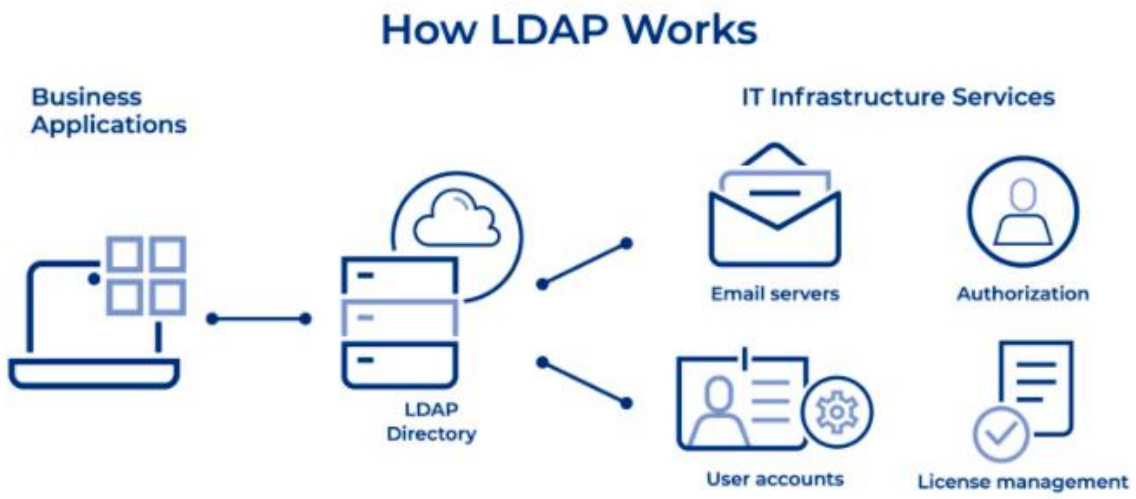
- What you have accomplished by making the accounts valid for only 55 hours each week is to prevent them from being used by attackers the other 113 hours.

Authentication Services:

LDAP (Lightweight directory access protocol):

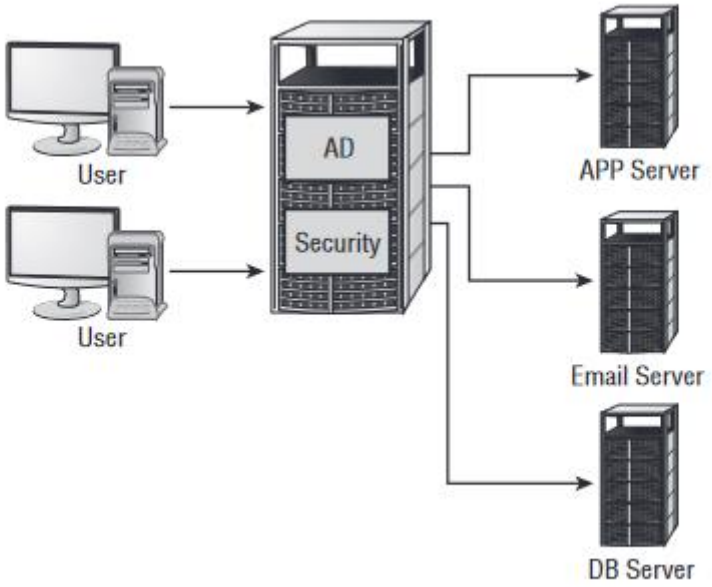
- LDAP (Lightweight Directory Access Protocol) is an open and cross platform protocol used for directory services authentication.
- LDAP provides the communication language that applications use to communicate with other directory services servers.
- Directory services store the users, passwords, and computer accounts, and share that information with other entities on the network
- LDAP is a protocol, so it doesn't specify how directory programs work. Instead, it's a form of language that allows users to find the information they need very quickly.

-



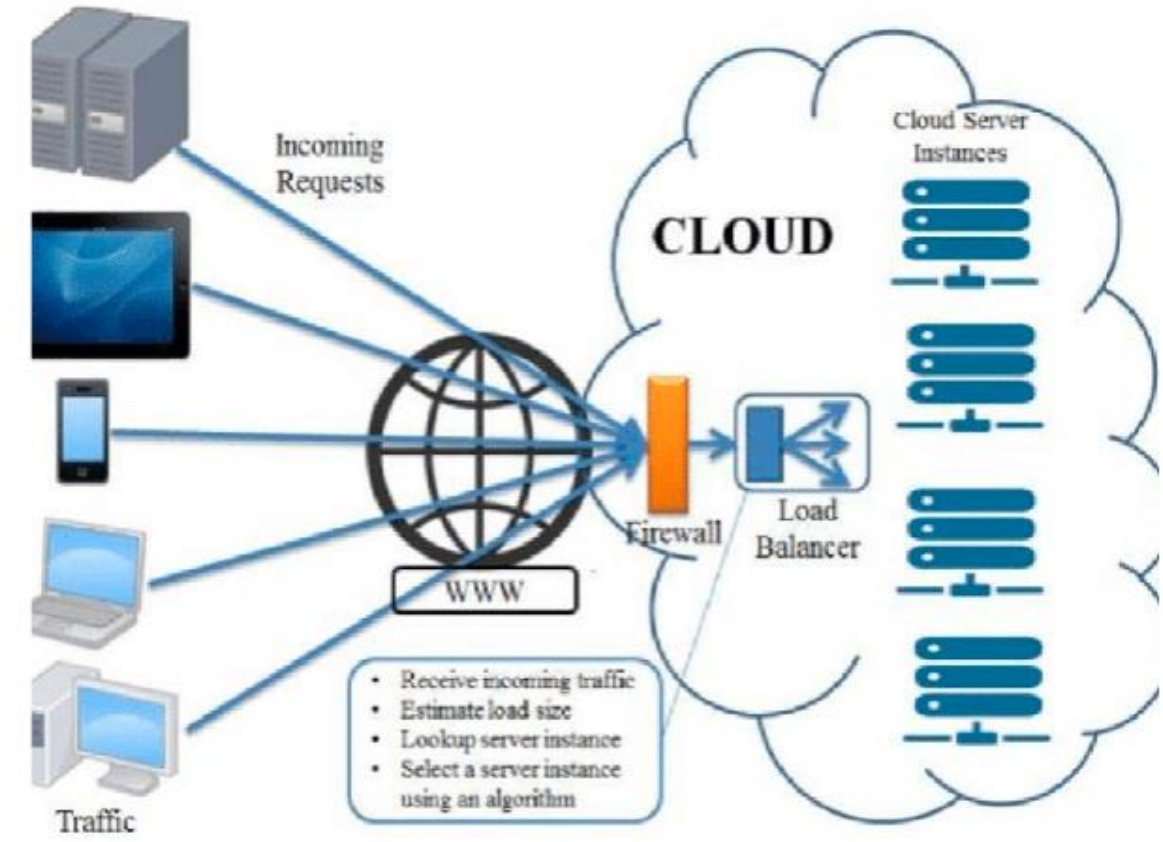
Single Sign-On:

- One of the big problems that larger systems must deal with is the need for users to access multiple systems or applications.
- This may require a user to remember multiple accounts and passwords. The purpose of a single sign-on (SSO) is to give users access to all the applications and systems they need when they log on.



What is Cloud server:

- Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet.
- Cloud servers have all the software they require to run and can function as independent units.



Advantages:

Easy implementation. Cloud hosting allows business to retain the same applications and business processes without having to deal with the backend technicalities. Readily manageable by the Internet, a cloud infrastructure can be accessed by enterprises easily and quickly.

Accessibility. Access your data anywhere, anytime. An Internet cloud infrastructure maximizes enterprise productivity and efficiency by ensuring your application is always accessible. This allows for easy collaboration and sharing among users in multiple locations.

No hardware required. Since everything will be hosted in the cloud, a physical storage center is no longer needed. However, a backup could be worth looking into in the event of a disaster that could leave your company's productivity stagnant.

Cost per head. Overhead technology costs are kept at a minimum with cloud hosting services, enabling businesses to use the extra time and resources for improving the company infrastructure.

Flexibility for growth. The cloud is easily scalable so companies can add or subtract resources based on their needs. As companies grow, their system will grow with them. Efficient recovery. Cloud computing delivers faster and more

accurate retrievals of applications and data. With less downtime, it is the most efficient recovery plan.

Risk vs. Threat vs. Vulnerability

Vulnerability: A vulnerability is a weakness in hardware, software, personnel, or procedures, which may be exploited by threat actors to achieve their goals.

- Vulnerabilities can be physical, such as a publicly exposed networking device, software-based, like a buffer overflow vulnerability in a browser, or even human, which includes an employee susceptible to phishing attacks.
- The process of discovering, reporting, and fixing vulnerabilities is called vulnerability management. A vulnerability, to which fix is not yet available, is called a zero-day vulnerability.

Threat: A threat is any type of danger, which can damage or steal data, create a disruption, or cause a harm in general. Common examples of threats include malware, phishing, data breaches and even rogue employees.

- Threats are manifested by threat actors, who are either individuals or groups with various backgrounds and motivations.
- Understanding threats is critical for building effective mitigations and helps to make the right decisions in cybersecurity. Information about threats and threat actors is called threat intelligence.

Risk: The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

- Risk is a combination of the threat probability and the impact of a vulnerability.
- In other words, risk is the probability of a threat agent successfully exploiting a vulnerability, which can also be defined by the following formula:

  Risk = Threat Probability * Vulnerability Impact.

- Identifying all potential risks, analysing their impact, and evaluating appropriate response is called risk management.

Understanding Malware

- Malware (A malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network.
- A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware.
- Malware can be used against individuals to gain information such as personal identification numbers or details, bank or credit card numbers, and passwords.

Spyware:

- Spyware is defined as malicious software designed to enter your computer device, gather data about you, and forward it to a third-party without your consent.
- it is gathering information about the user to pass on to marketers or intercepting personal data such as credit card numbers.
- One thing separating spyware from most other malware is that it almost always exists to provide commercial gain. The operating systems from Microsoft are the ones most affected by spyware.

Some of the most common ways for computers to become infected include the following:

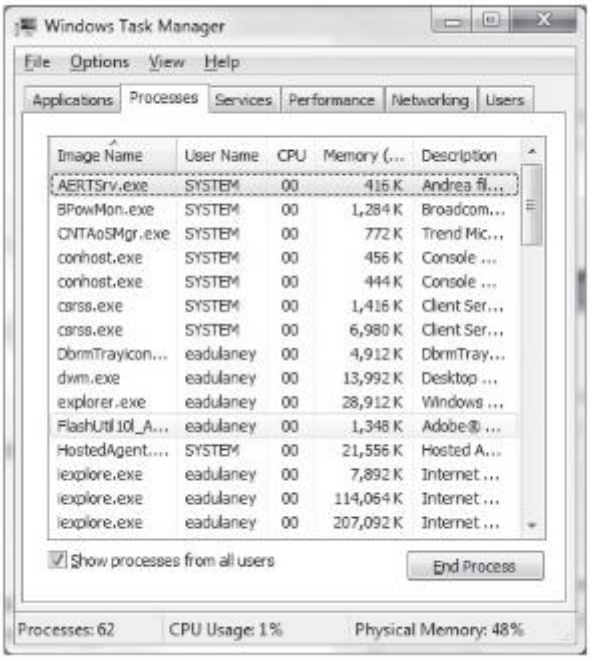
- Pirating media, including games, videos and music
- Downloading materials from unreliable or unknown sources
- Accepting a pop-up advertisement or prompt without reading the content
- Accepting and opening email attachments from unrecognized senders.

Adware:

- If the primary purpose of the malware application is to deliver ads, then it is classified as Adware.
- Adware can have the same qualities as spyware, but the primary purpose of adware is to display ads and generate revenue for the creator.
- Windows Defender can be used as a first line of defense.

Rootkits:

- Rootkits are software programs that have the ability to hide certain things from the operating system.
- With a rootkit, there may be a number of processes running on a system that do not show up in Task Manager or connections established or available that do not appear in a netstat display



Trojan Horses:

Trojan horses are programs that enter a system or network under the guise of another program.

A Trojan horse may be included as an attachment or as part of an installation program.

Trojan horses can be used to compromise the security of your system, and they can exist on a system for years before they're detected.

One of the most important measures you can take to combat software attacks proactively is to know common fi le extensions and the applications with which they're associated.

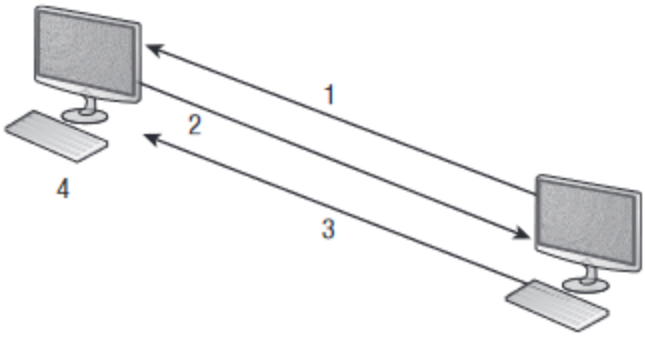
Should be allowed	Should *not* be allowed
.doc/docx	.bat
.pdf	.com
.txt	.exe
.xls/xlsx	.hlp
	.pif
	.scr

Logic Bombs:

Logic bombs are programs or code snippets that execute when a certain predefined event occurs.

A bomb may send a note to an attacker when a user is logged on to the Internet and is using a word processor. This message informs the attacker that the user is ready for an attack.

a logic bomb in operation. Notice that this bomb doesn't begin the attack, but it tells the attacker that the victim has met the needed criteria or state for an attack to begin. Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs.



1. Attacker implants logic bomb.
2. Victim reports installation.
3. Attacker sends attack message.
4. Victim does as logic bomb indicates.

Backdoors:

Backdoor refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker.

The program may allow a certain user ID to log on without a password or to gain administrative privileges.

A backdoor attack is usually either an access or modification attack. A number of tools exist to create backdoor attacks on systems.

Two popular ones are Back Orifice and NetBus. Fortunately, most conventional antivirus software will detect and block these types of attacks.

Botnets:

- Botnets are networks of computers infected by malware (such as computer viruses, key loggers and other malicious software) and controlled remotely by criminals, usually for financial gain or to launch attacks on websites or networks.
- That means the actor can have all the computers in the infected network carry out the same instructions at the same time.
- This power to perform actions at massive scale, to coordinate the behaviour of hundreds of thousands of internet-connected machines, is what makes botnets so fearsome.

Ransomware:

Ransomware is a type of malware that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.

Ransomware delivered through a Trojan—it takes control of a system and demands that a third party be paid.

The “control” can be accomplished by encrypting the hard drive, by changing user password information.

Viruses:

A virus is a piece of software designed to infect a computer system.

a virus may do nothing more than reside on the computer, but it may also damage the data on your hard disk drive (HDD), destroy your operating system, and possibly spread to other systems.

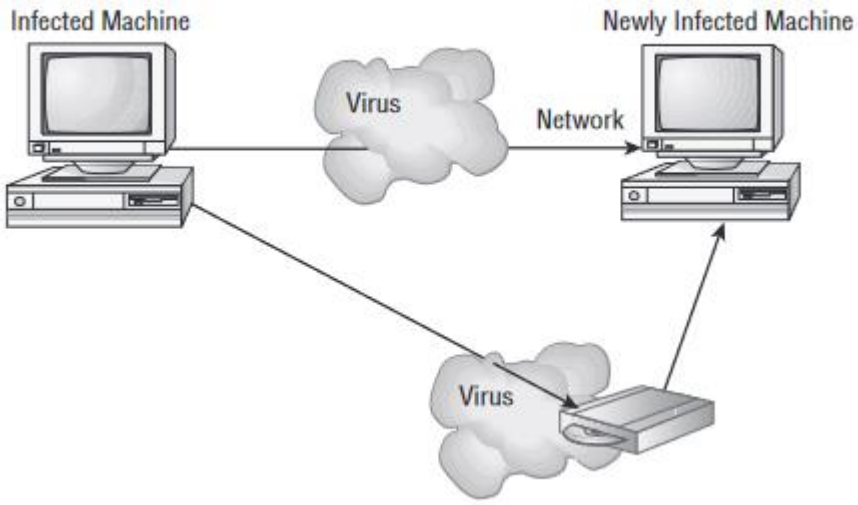
Viruses get into your computer in one of three ways:▪On contaminated media (DVD, USB drive, or CD-ROM)▪Through email and social networking sites▪As part of another program

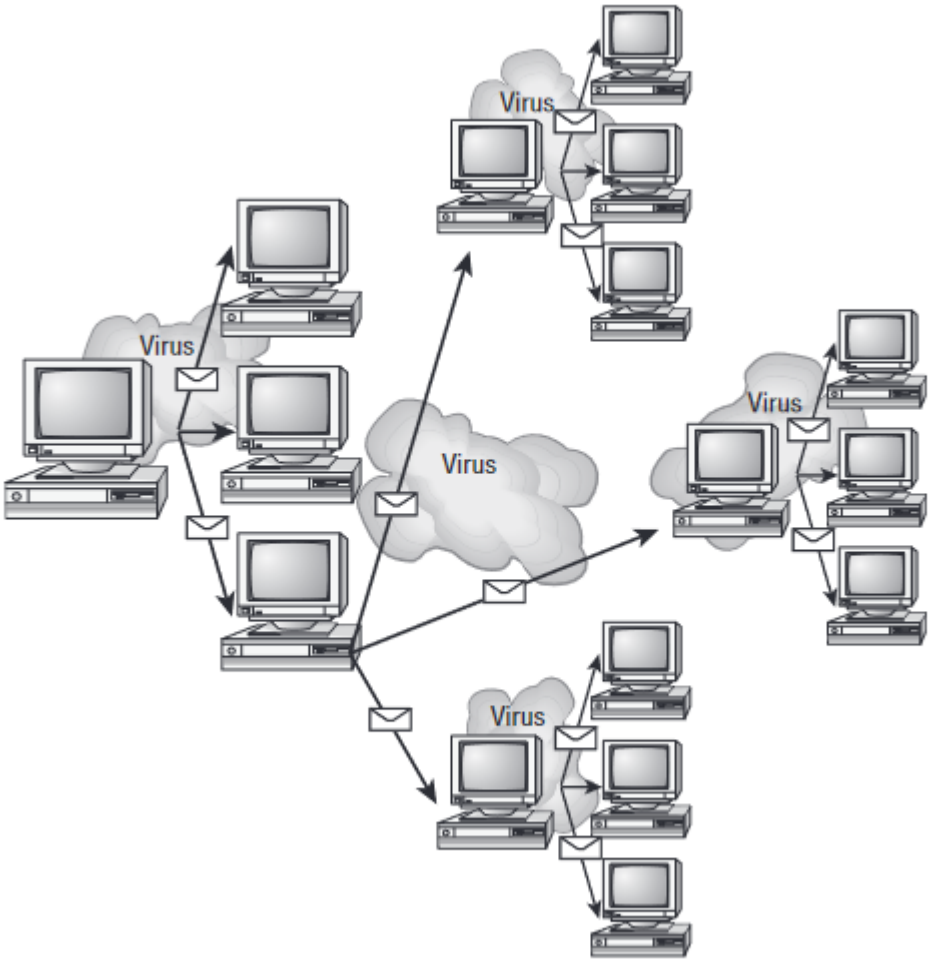
some of the following symptoms when determining if a virus infec-tion has occurred:

The programs on your system start to load more slowly. This happens because the virus is spreading to other files in your system or is taking over system resources.

▪Unusual files appear on your hard drive, or files start to disappear from your system. Many viruses delete key files in your system to render it inoperable.

▪Program sizes change from the installed versions. This occurs because the virus is attaching itself to these programs on your disk.





Antivirus Software

- The primary method of preventing the propagation of malicious code involves the use of antivirus software.
- Antivirus software is an application that is installed on a system to protect it and to scan for viruses as well as worms and Trojan horses. Most viruses have characteristics that are common to families of virus.
- Thousands of known viruses, worms, logic bombs, and other malicious code have been defi ned. New ones are added all the time. Your antivirus software manufacturer will usually work very hard to keep the definition database fi les current.
- The second method of preventing viruses is user education. Teach your users not to open suspicious fi les and to open only those fi les that they’re reasonably sure are virus-free. They need to scan every disk, email, and document they receive before they open them.

Antivirus Software

- The primary method of preventing the propagation of malicious code involves the use of antivirus software.
- Antivirus software is an application that is installed on a system to protect it and to scan for viruses as well as worms and Trojan horses. Most viruses have characteristics that are common to families of virus.
- Thousands of known viruses, worms, logic bombs, and other malicious code have been defi ned. New ones are added all the time. Your antivirus software manufacturer will usually work very hard to keep the definition database files current.
- The second method of preventing viruses is user education. Teach your users not to open suspicious files and to open only those files that they're reasonably sure are virus-free. They need to scan every disk, email, and document they receive before they open them.

Denial-of-Service and Distributed Denial-of-Service Attacks

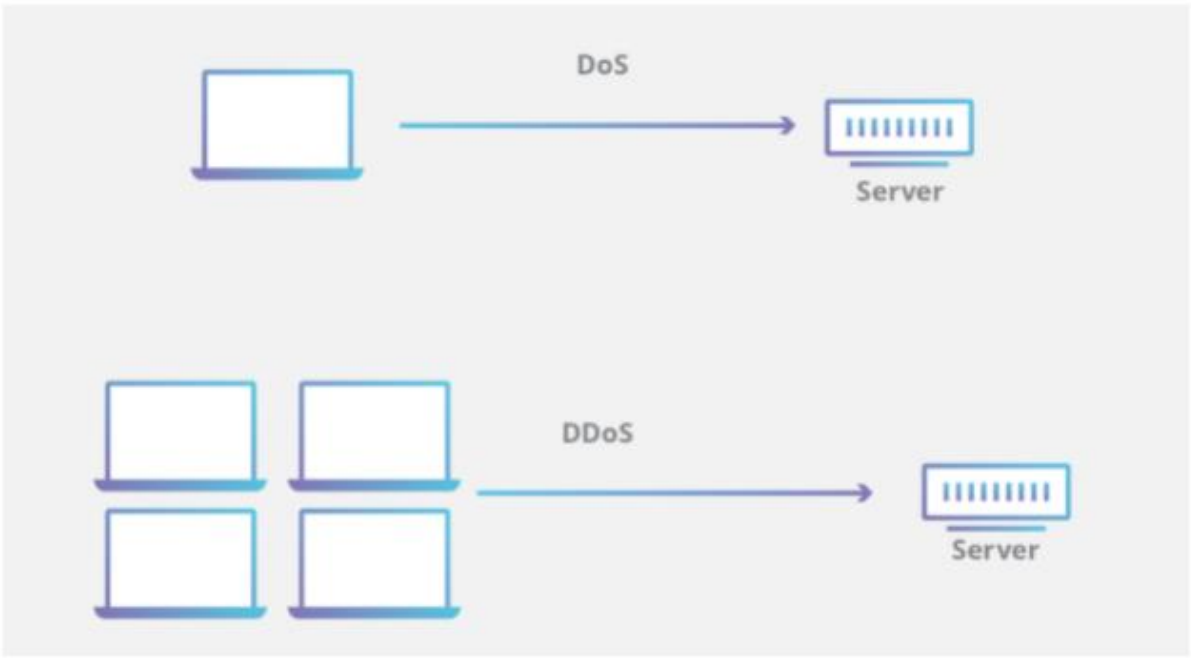
- Denial-of-service (DoS) attacks prevent access to resources by users authorized to use those resources.
- An attacker may attempt to bring down an e-commerce website to prevent or deny usage by legitimate customers.
- Most simple DoS attacks occur from a single system, and a specific server or organization is the target.

Several types of attacks can occur in this category. These attacks can do the following:

- Deny access to information, applications, systems, or communications.
- Bring down a website while the communications and systems continue to operate.
- crash the operating system (a simple reboot may restore the server to normal operation).
- Fill the communications channel of a network and prevent access by authorized users.
- Open as many TCP sessions as possible; this type of attack is called a TCP SYN flood DoS attack.

Two of the most common types of DoS attacks are the ping of death and the buffer overflow.

- The ping of death crashes a system by sending Internet Control Message Protocol (ICMP) packets that are larger than the system can handle.
- Buffer flow attacks, as the name implies, attempt to put more data (usually long input strings) into the buffer than it can hold.

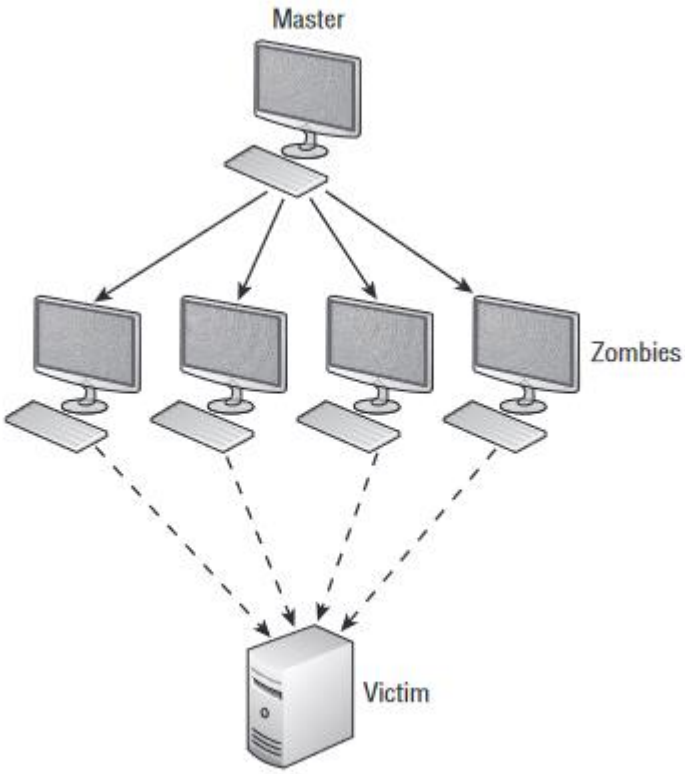


A distributed denial-of-service (DDoS) attack is similar to a DoS attack. A DDoS attack amplifies the concepts of a DoS attack by using multiple computer systems (often through botnets) to conduct the attack against a single organization.

These attacks exploit the inherent weaknesses of dedicated networks such as DSL and cable.

An attacker can load an attack pro-gram onto dozens or even hundreds of computer systems that use DSL or cable modems. The attack program lies dormant on these computers until they get an attack signal from a master computer.

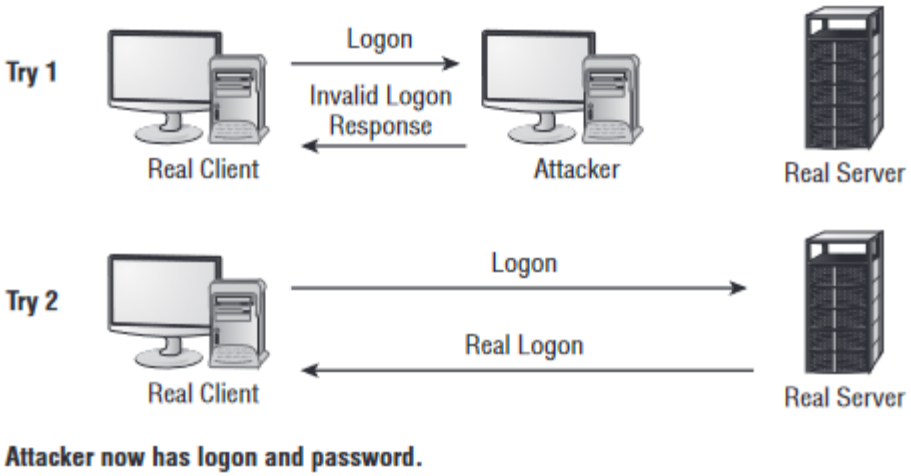
The signal triggers the systems, which launch an attack simultaneously on the target network or system.



Spoofing Attack:

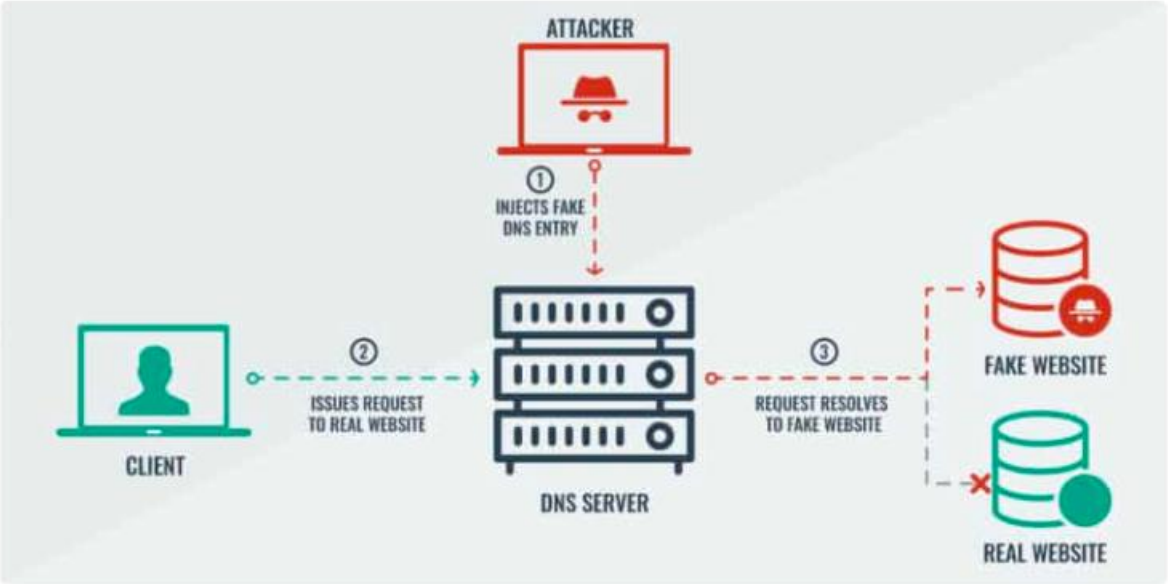
- A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.
- The most popular spoofing attacks today are IP spoofing, ARP spoofing, and DNS spoofing.
- **IP spoofing**, the goal is to make the data look as if it came from a trusted host when it did not (thus spoofing the IP address of the sending host).
- **ARP spoofing** (ARP poisoning), the MAC (Media Access Control) address of the data is faked. By faking this value, it is possible to make it look as if the data came from a network that it did not.
- **DNS spoofing**, the DNS server is given information about a name server that it thinks is legitimate when it is not.
- This can send users to a website other than the one to which they wanted to go, reroute mail, or do any other type of redirection wherein data from a DNS server is used to determine a destination.
- Another name for this is DNS poisoning

Figure shows a spoofing attack occurring as part of the logon process on a computer network. The attacker in this situation impersonates the server to the client attempting to log in. No matter what the client attempts to do, the impersonating system will fail the login. When this process is finished, the impersonating system disconnects from the client. The client then logs into the legitimate server. In the meantime, the attacker now has a valid user ID and password.



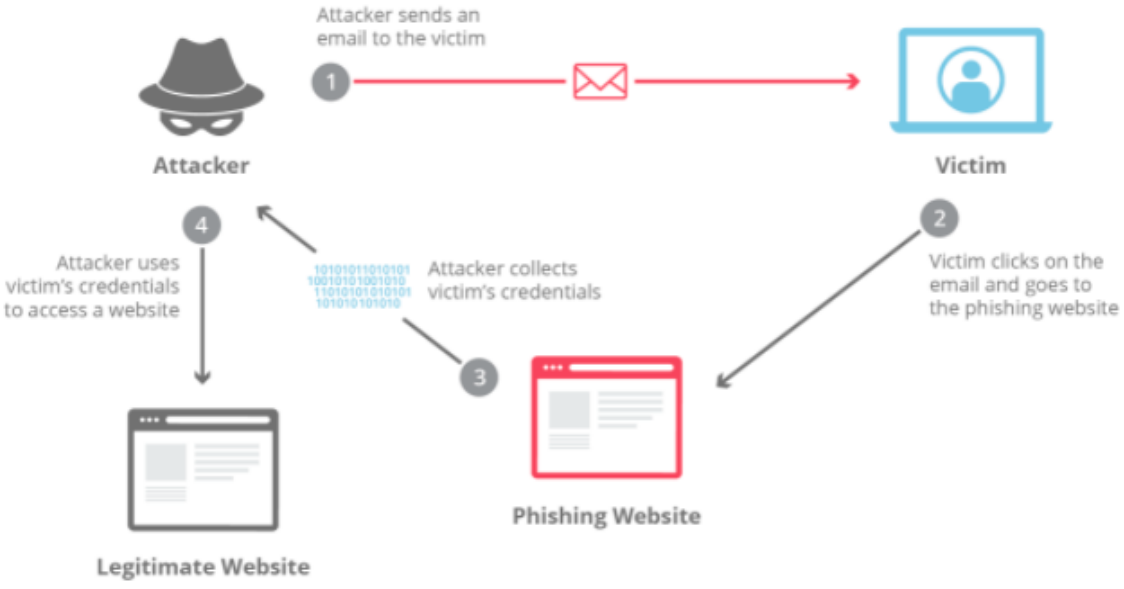
Pharming Attack:

- Pharming is a form of redirection in which traffic intended for one host is sent to another. This can be accomplished on a small scale by changing entries in the hosts file and on a large scale by changing entries in a DNS server (the poisoning mentioned earlier).
- In either case, when a user attempts to go to a site they are redirected to another.
- An example of this would be Illegitimate Company ABC creating a site to look exactly like the one for Giant Bank XYZ.
- The pharming is done (using either redirect method), and users trying to reach Giant Bank XYZ are tricked into going to Illegitimate Company ABC's site, which looks enough like what they are used to seeing that they provide username and password data.
- As soon as Giant Bank XYZ realizes that the traffic is being redirected, they will immediately move to stop it. Although Illegitimate Company ABC will be closed, they were able to collect data for the length of time the redirection occurred, which could vary from minutes to days.



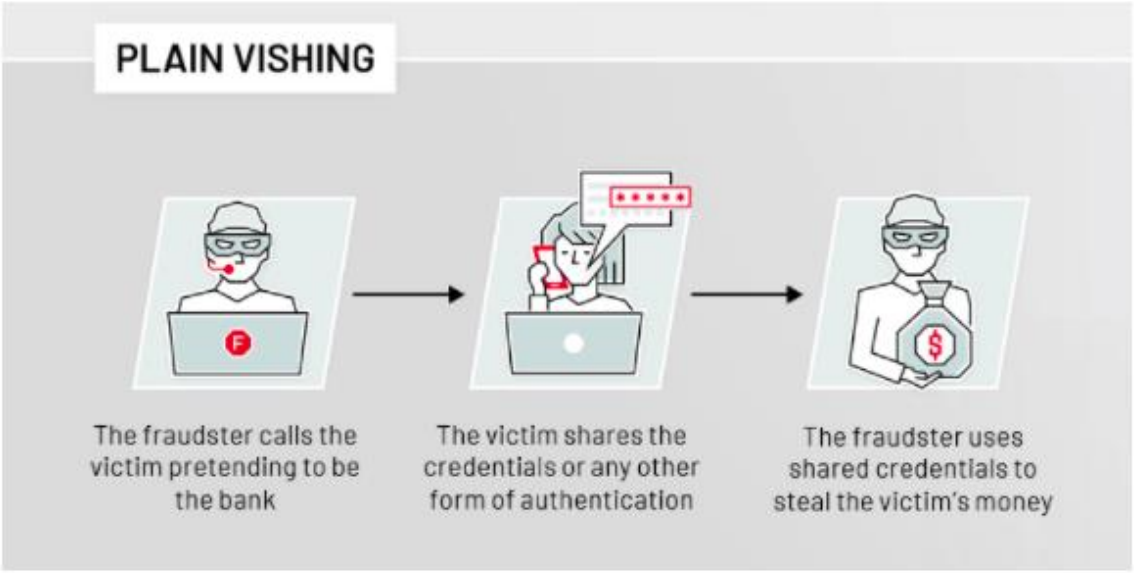
Phishing:

- Phishing is a form of social engineering in which you ask someone for a piece of information that you are missing by making it look as if it is a legitimate request.
- An email might look as if it is from a bank and contain some basic information, such as the user's name. In the email, it will often state that there is a problem with the person's account or access privileges.
- The user will be told to click a link to correct the problem. After they click the link—which goes to a site other than the bank's—they are asked for their username, password, account information, and so on.
- The person instigating the phishing can then use the values entered there to access the legitimate account.



- **Spear phishing** is a unique form of phishing in which the message is made to look as if it came from someone you know, and trust as opposed to an informal third party.
- With spear phishing, you might get a message that appears to be from your boss telling you that there is a problem with your direct deposit account and that you need to access this HR link right now to correct it.
- Spear phishing works better than phishing because it uses information that it can find about you from email databases, friends list, and the like.

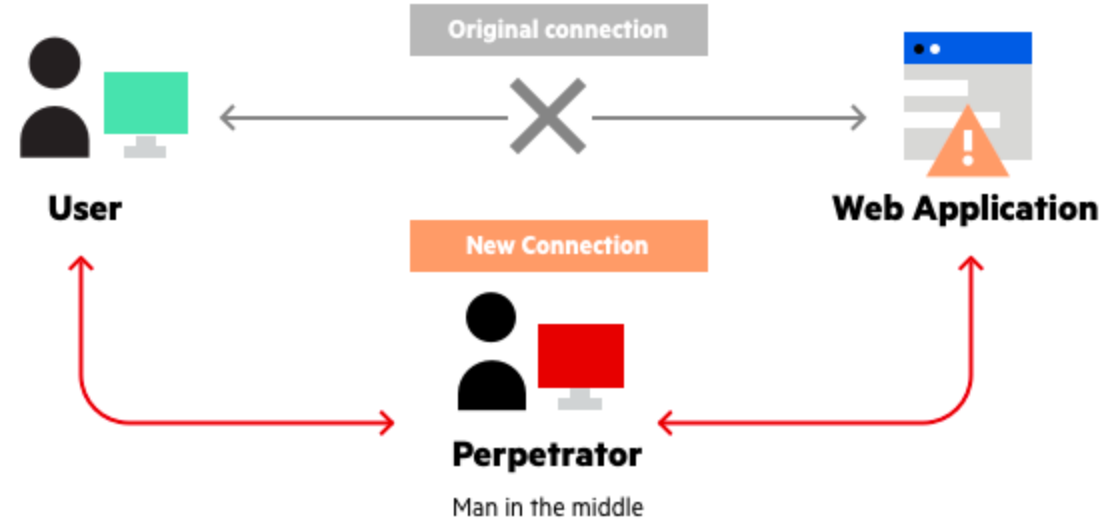
- **Vishing** is a cybercrime that uses the phone to steal personal confidential information from victims. Often referred to as voice phishing, cybercriminals use savvy social engineering tactics to convince victims to act, giving up private information and access to bank accounts.
- vishing relies on convincing victims that they are doing the right thing by responding to the caller. Often the caller will pretend to be calling from the government, tax department, police, or the victim's bank.



A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer.

After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants.

This enables an attacker to intercept information and data from either party while also sending malicious links or other information to both legitimate participants in a way that might not be detected until it is too late.



Man in the middle attack example

Password Attacks

- Password attacks occur when an account is attacked repeatedly. This is accomplished by using applications known as password crackers, which send possible passwords to the account in a systematic manner.
- The attacks are initially carried out to gain passwords for an access or modification attack. There are several types of password attacks:
- **A brute-force attack** is an attempt to guess passwords until a successfull guess occurs. As an example of this type of attack, imagine starting to guess with “A” and then going through “z”; when no match is found, the next guess series goes from “AA” to “zz” and then adds a third value (“AAA” to “zzz”).
- **A dictionary attack** uses a dictionary of common words to attempt to find the user’s password. Dictionary attacks can be automated, and several tools exist in the public domain to execute them. As an example of this type of attack, imagine guessing words and word combinations found in a standard English-language dictionary.

Privilege Escalation

- Privilege escalation involves a user gaining more privileges than they should have. With their elevated permissions, they can perform tasks they should not be allowed to do (such as delete files or view data).
- This condition is often associated with bugs left in software. When creating a software program, developers will occasionally leave a backdoor in the program that allows them to become a root user should they need to fix something during the debugging phase.

- To understand privilege escalation, think of cheat codes in video games. Once you know the game's code, you can enter it and become invincible. Similarly, someone might take advantage of a hidden cheat in a software application to become root.

Malicious Insider Threats

- One of the most dangerous threats to any network is an insider who is intent on doing harm.
- By being an insider, they have already gotten past your first defense and they might be motivated by a desire to make someone pay for passing them over for a promotion, bored and looking for something to do, or driven by any of a plethora of other motivations.
- People can be bribed to give away information, and one of the toughest challenges is someone on the inside who is displeased with the company and not afraid to profit from it.
- This is known as a malicious insider threat, and it can be far more difficult to contend with than any outside threat since they already have access—both physical and login—to your systems.

Social Engineering:

Social engineering is the process by which intruders gain access to your facilities, your network, and even your employees by exploiting the generally trusting nature of people.

It is often difficult to determine whether the individual is legitimate or has bad intentions.

Example: Someone enters your office building wearing a white lab jacket with a logo on it. He also has a toolkit. He approaches the receptionist and identifies himself as a copier repairman from a major local copier company. He indicates that he is here to do preventive service on your copier. In most cases, the receptionist will let him pass and tell him the location of the copier. Once the "technician" is out of sight, the receptionist probably will not give him a second thought. Your organization has just been the victim of a social engineering attack. The attacker has now penetrated your first and possibly even your second layer of security.

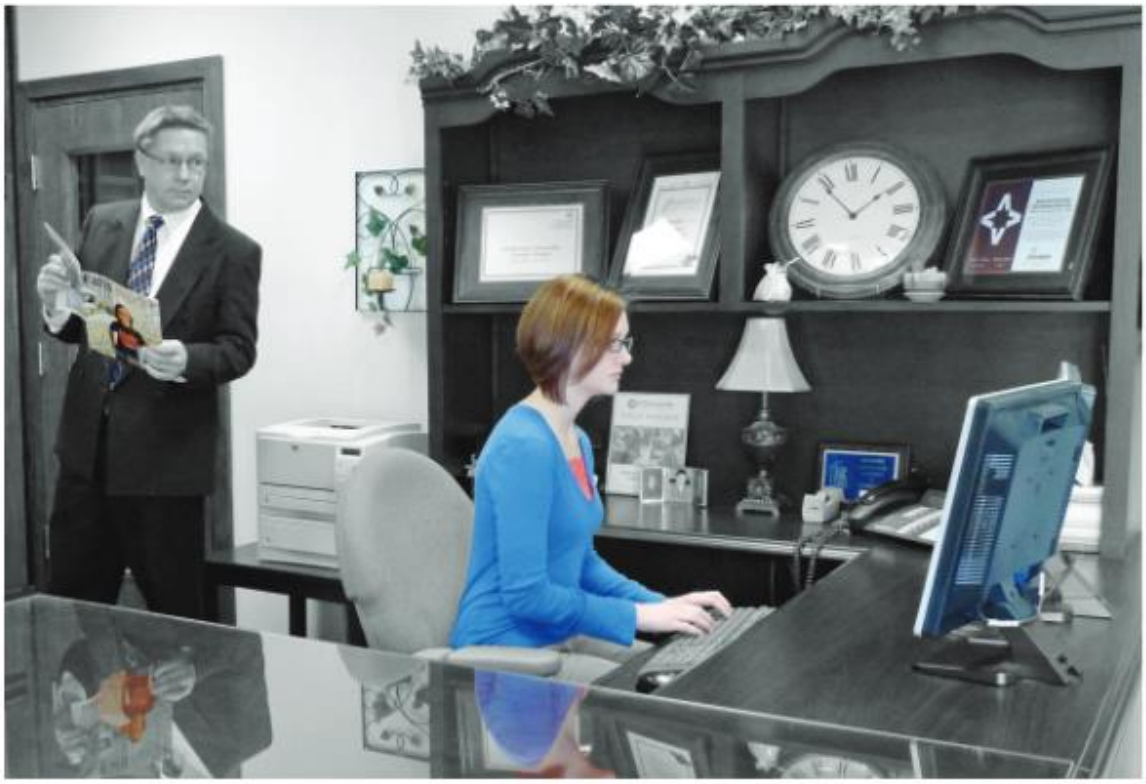
Types of Social Engineering Attacks:

Preventing social engineering attacks involves more than just providing training on how to detect and prevent them. It also involves making sure that people stay alert.

Shoulder Surfing One popular form of social engineering is known as shoulder surfing, and it involves nothing more than watching someone "over their shoulder" when they enter their sensitive data.

They can see you entering a password, typing in a credit card number, or entering any other pertinent information.

The best defense against this type of attack is to survey your environment before entering personal data. For ex" In any public location where they sit with their laptops, at business travel centers in hotels, at ATMs, and so on.



Dumpster Diving is a common physical access method. Companies normally generate a huge amount of paper, most of which eventually winds up in dumpsters or recycle bins. Dumpsters may contain information that is highly sensitive in nature. In high-security and government environments, sensitive papers are either shredded or burned. Most businesses do not do this.

Tailgating A favourite method of gaining entry to electronically locked systems is to follow someone through the door they just unlocked, a process known as tailgating. Many people don't think twice about this event—it happens all the time—as they hold the door open for someone behind them who is carrying heavy boxes or is disabled in some way.

Impersonation: it involves any act of pretending to be someone you are not. This can be a service technician, a pizza delivery driver, a security guard, or anyone else who might be allowed unfettered access to the grounds, network, or system. Impersonation can be done in person, over the phone, by email, and so forth.

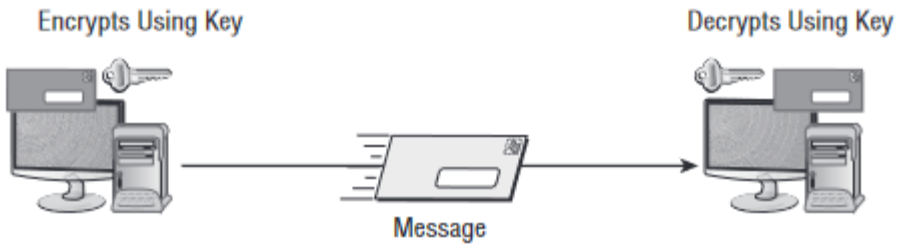
Cryptography

Steganography

Steganography is the process of hiding a message in a medium such as a digital image, audio file, or other fi le. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that fi le to hide your message.

Modern cryptography is divided into three major areas: symmetric cryptography, asymmetric cryptography, and hashing algorithms.

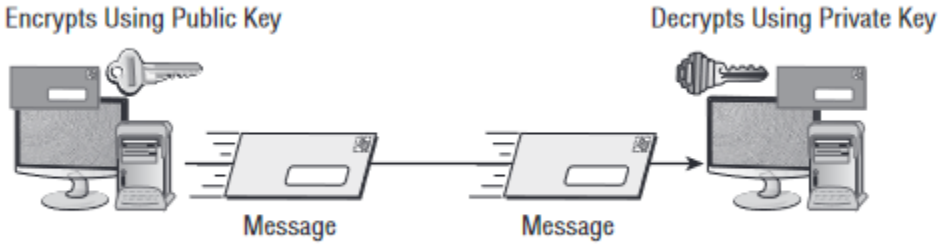
Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that is not disclosed to people who are not authorized to use the encryption system. The disclosure of a private key breaches the security of the encryption system. If a key is lost or stolen, the entire process is breached.



Data Encryption Standard (DES), 3-DES, Advanced Encryption Standard (AES), AES256

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message.

The public key may be truly public, or it may be a secret between the two parties. The private key is kept private, and only the owner (receiver) knows it. If someone wants to send you an encrypted message, they can use your public key to encrypt the message and then send you the message. You can use your private key to decrypt the message. The private key is always kept protected. If both keys become available to a third party, the encryption system won't protect the privacy of the message.



RSA (RSA is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman)

Diffie-Hellman

Elliptic Curve Cryptography

Hashing Algorithms

The hashes used to store data, such as hash tables, are very different from cryptographic hashes. In cryptography, a hash function must have three characteristics:

■It must be one-way. This means that it is not reversible. Once you hash something, you cannot unhash it.

■Variable-length input produces fixed-length output. This means that whether you hash two characters or two million, the hash size is the same.

■The algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output.

Secure Hash Algorithm The secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol.

This algorithm produces a 160-bit hash value. SHA-2 has several sizes: 224, 256, 334, and 512 bit. SHA-2 is the most widely used.

Message Digest Algorithm The Message Digest Algorithm (MD) also creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

Cryptography Standards and Protocols

What is an SSL?

- SSL stands for Secure Sockets Layer and, it is the standard technology for keeping an internet connection secure, and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading, and modifying any information transferred, including potential personal details.
- The two systems can be a server and a client (for example, a shopping website and browser) or server to server.
- It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection.
- There are two types of SSL handshakes described as one-way SSL and two-way SSL (Mutual SSL).
- The difference between those two is that in one -way SSL, only the client validates the identity of the server whereas in two-way SSL, both server and client validate the identity of each other.
- Usually, when we browse an HTTPS website, one-way SSL is being used where only our browser (client) validates the identity of the website (server). Two-way SSL is mostly used in server-to-server communication where both parties need to validate the identity of each other.

What is TLS?

- TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet.
- It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established.
- However, it can and indeed should also be used for other applications such as e-mail, file transfers, video/audioconferencing, instant messaging, and voice-over-IP, as well as Internet services such as DNS and NTP.
- TLS evolved from Secure Socket Layers (SSL) which was originally developed by Netscape Communications Corporation in 1994 to secure web sessions.

S.NO	SSL	TLS

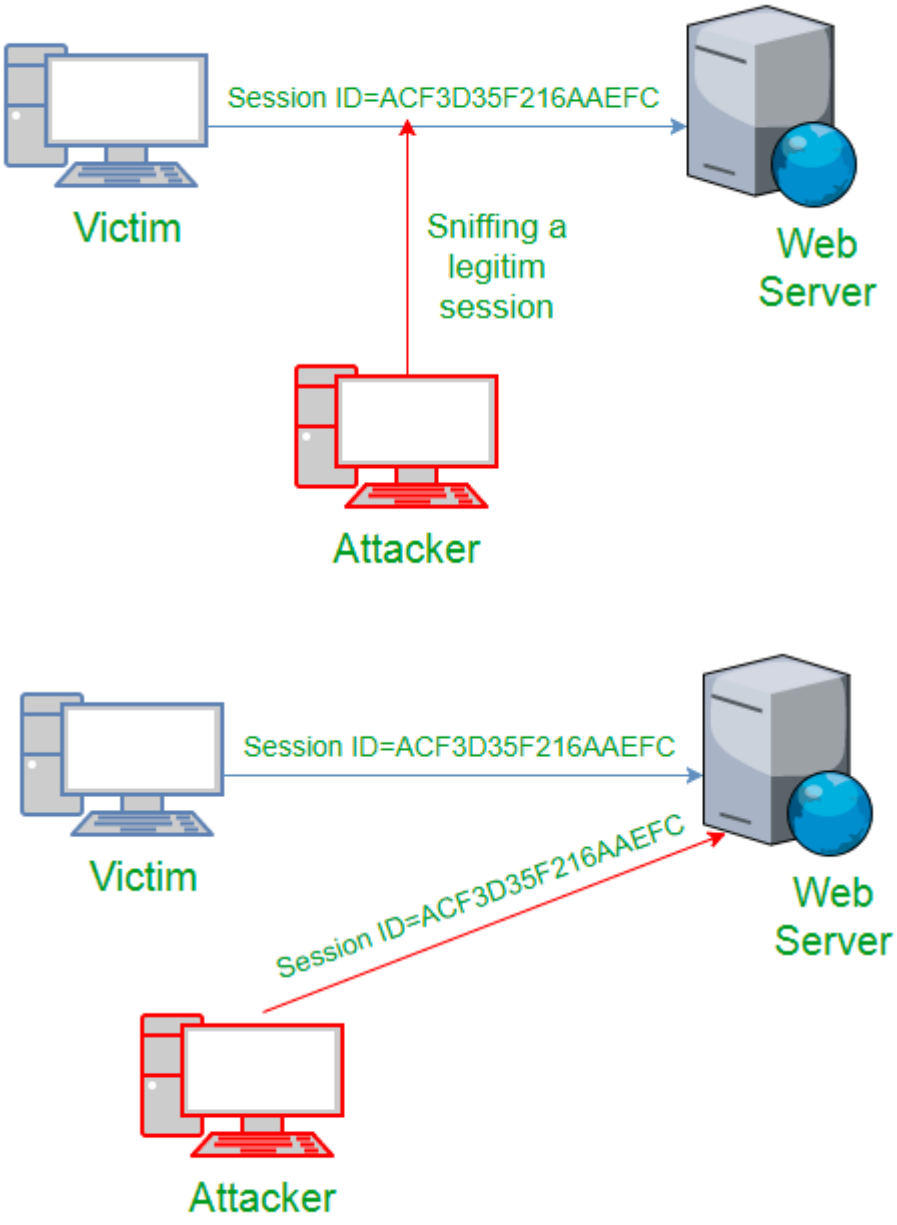
1.	SSL stands for Secure Socket Layer.	TLS stands for Transport Layer Security.
2.	SSL (Secure Socket Layer) supports **Fortezza** algorithm.	TLS (Transport Layer Security) does not supports **Fortezza** algorithm.
3.	SSL (Secure Socket Layer) is the 3.0 version.	TLS (Transport Layer Security) is the 1.0 version.
4.	In SSL(Secure Socket Layer), Message digest is used to create master secret.	In TLS(Transport Layer Security), Pseudo-random function is used to create master secret.
5.	In SSL(Secure Socket Layer), Message Authentication Code protocol is used.	In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used.
6.	SSL (Secure Socket Layer) is complex than TLS(Transport Layer Security).	TLS (Transport Layer Security) is simple.
7.	SSL (Secure Socket Layer) is less secured as compared to TLS(Transport Layer Security).	TLS (Transport Layer Security) provides high security.

Cookies

- Cookies are text files that a browser maintains on the user's hard disk to provide a persistent, customized web experience for each visit.
- A cookie typically contains information about the user. For example, a cookie can contain a client's history to improve customer service. If a bookstore wants to know your buying habits and what types of books you last viewed at its site, it can load this information into a cookie on your system.
- The next time you return to that store, the server can read your cookie and customize what it presents to you.
- Cookies can also be used to timestamp a user to limit access. A financial institution may send your browser a cookie once you have authenticated. The server can read the cookie to determine when a session is expired.

Session Hijacking

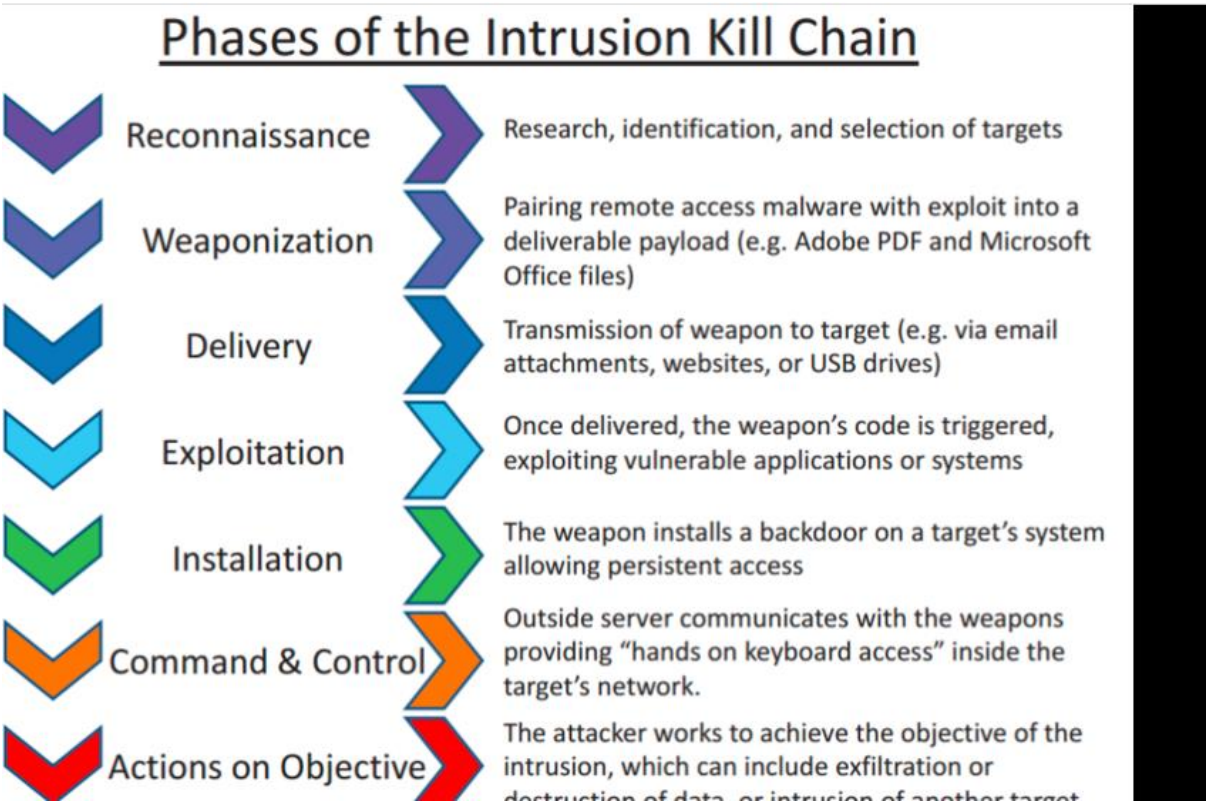
- The term session hijacking describes when the item used to validate a user's session, such as a cookie, is stolen and used by another to establish a session with a host that thinks it is still communicating with the first party.
- To use an overly simplistic analogy, imagine that you just finished a long phone conversation with a family member and then accidentally left your smartphone in the room while stepping outside. If Jim were to pick up that phone and press redial, the family member would see the caller ID, know that they had just been talking with you, and falsely assume that you were calling back. If Jim could imitate your voice, he could rattle off numerous nasty comments that would jeopardize your relationship with that family member.



Cyber Kill Chain (CKC)

The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).

Lockheed Martin derived the kill chain framework from a military model – originally established to identify, prepare to attack, engage, and destroy the target. Since its inception, the kill chain has evolved to better anticipate and recognize insider threats, social engineering, advanced ransomware and innovative attacks.



CYBER KILL CHAIN STAGES.

- **Reconnaissance:** Starting point, attackers choses there targets and gather information (name, email, etc.,) and do depth research on the targets to find the vulnerability.
- **Weaponization:** In this stage attacker creates a malware weapon like virus, worm, and other which contains a malicious payload in order to exploit the vulnerability of targets.
- **Delivery:** It involves transmiting the weapons to the target, use different methods like phishing emails.
- **Exploitation:** In this stage malware is triggered to exploit the weakness of the targets.
- **Installation:** In this stage the attackers install the malicious payload on the infected targets machine.
- **Command and Control:** In this stage attacker control and manipulate the targets.
- **Action of Objective:** In this stage attacker achieve his goal by Encryption or by deletes the data.

A cyber adversary is someone or a group that intends to perform malicious actions against other cyber resources.

Reconnaissance:

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting.

Such information may include details of the victim organization, infrastructure, or staff/personnel.

This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

Resource Development:

Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities.

These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.

Initial Access:

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.

Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Execution:

Execution consists of techniques that result in adversary-controlled code running on a local or remote system.

Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data.

For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

Persistence:

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding start-up code.

Privilege Escalation:

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.

Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.

Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Defense Evasion:

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise.

Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts.

Adversaries also leverage and abuse trusted processes to hide and masquerade their malware.

Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses

Credential Access:

Credential Access consists of techniques for stealing credentials like account names and passwords.

Techniques used to get credentials include keylogging or credential dumping.

Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Discovery:

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network.

These techniques help adversaries observe the environment and orient themselves before deciding how to act.

They also allow adversaries to explore what they can control and what is around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

Lateral Movement:

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network.

Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it.

Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

Collection:

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.

Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

Command and Control:

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.

Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.

There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defense.

Exfiltration:

Exfiltration consists of techniques that adversaries may use to steal data from your network.

Once they've collected data, adversaries often package it to avoid detection while removing it.

This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command-and-control channel or an alternate channel and may also include putting size limits on the transmission.

Impact:

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals.

These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

Risk Assessment

Risk assessment is also known as risk analysis or risk calculation.

Risk assessment deals with the threats, vulnerabilities, and impacts a loss of information.

A vulnerability is a weakness that could be exploited by a threat. Each risk that can be identified should be outlined, described, and evaluated for the likelihood of it occurring.

The key components of a risk-assessment process are,

Risks to Which the Organization Is Exposed:

This component allows you to develop scenarios that can help you evaluate how to deal with these risks if they occur.

An operating system, server, or application may have known risks in certain environments. You should create a plan for how your organization will best deal with these risks and the best way to respond.

Risks That Need Addressing:

The risk-assessment component also allows an organization to provide a reality check on which risks are real and which are unlikely.

This process helps an organization focus on its resources as well as on the risks that are most likely to occur.

For example, industrial espionage and theft are likely, but the risk of a hurricane damaging the server room in Indiana is very low. Therefore, more resources should be allocated to prevent espionage or theft as opposed to the latter possibility.

Coordination with BIA:

The risk-assessment component, in conjunction with the business impact analysis (BIA), provides an organization with an accurate picture of the situation facing it.

It allows an organization to make intelligent decisions about how to respond to various scenarios.

Acting on Your Risk Assessment

Risk Avoidance: A company may decide that many risks are associated with email attachments and choose to forbid any email attachments from entering the network.

Risk Transference: Risk transference, contrary to what the name may imply, does not mean that you shift the risk completely to another entity. What you do instead is share some of the burden of the risk with someone else, such as an insurance company. A typical policy would pay you a cash amount if all of the steps were in place to reduce risk and your system was still harmed.

Risk Mitigation:

Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on.

Risk Deterrence Risk deterrence involves understanding something about the enemy and letting them know the harm that can come their way if they cause harm to you. This can be as simple as posting prosecution policies on your login pages and convincing them that you have steps in place to identify intrusions and to act on them.

Risk Acceptance

Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition.

To truly qualify as acceptance, it cannot be a risk where the administrator or manager is unaware of its existence; it has to be an identified risk for which those involved understand the potential cost or damage and agree to accept it.

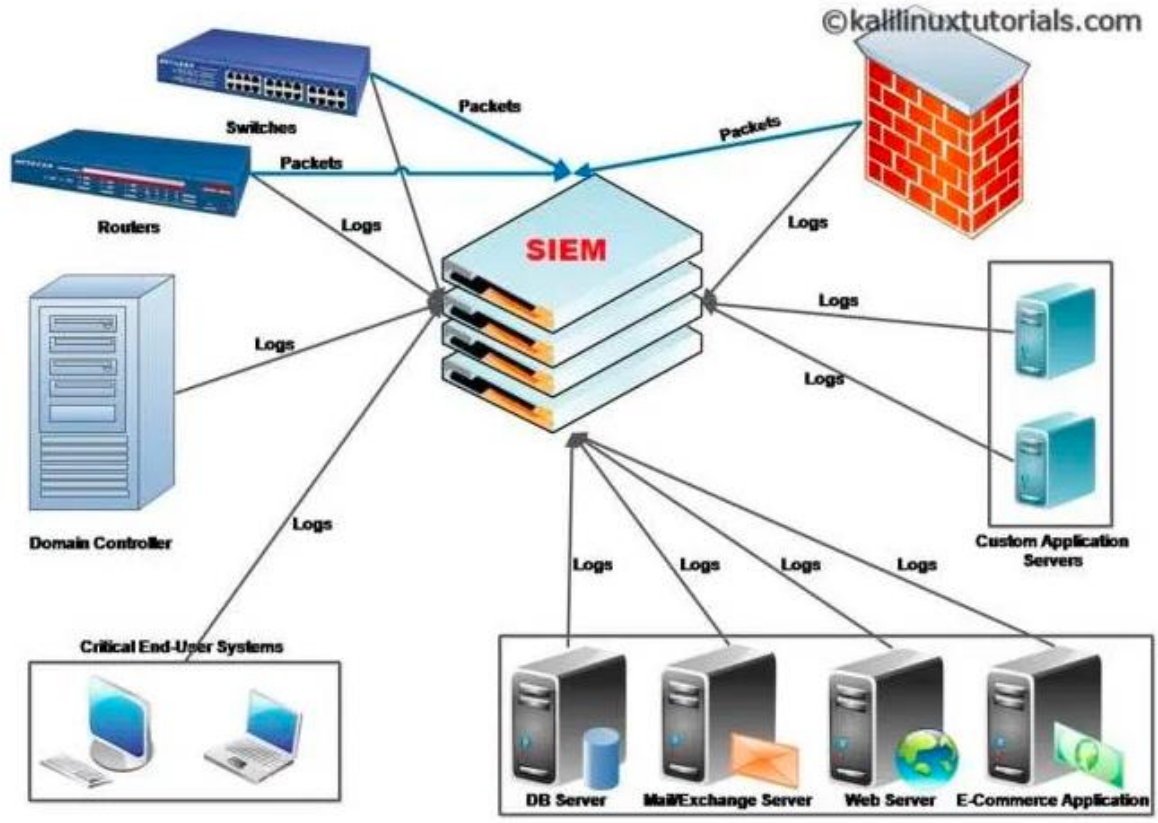
Security Operation Centre

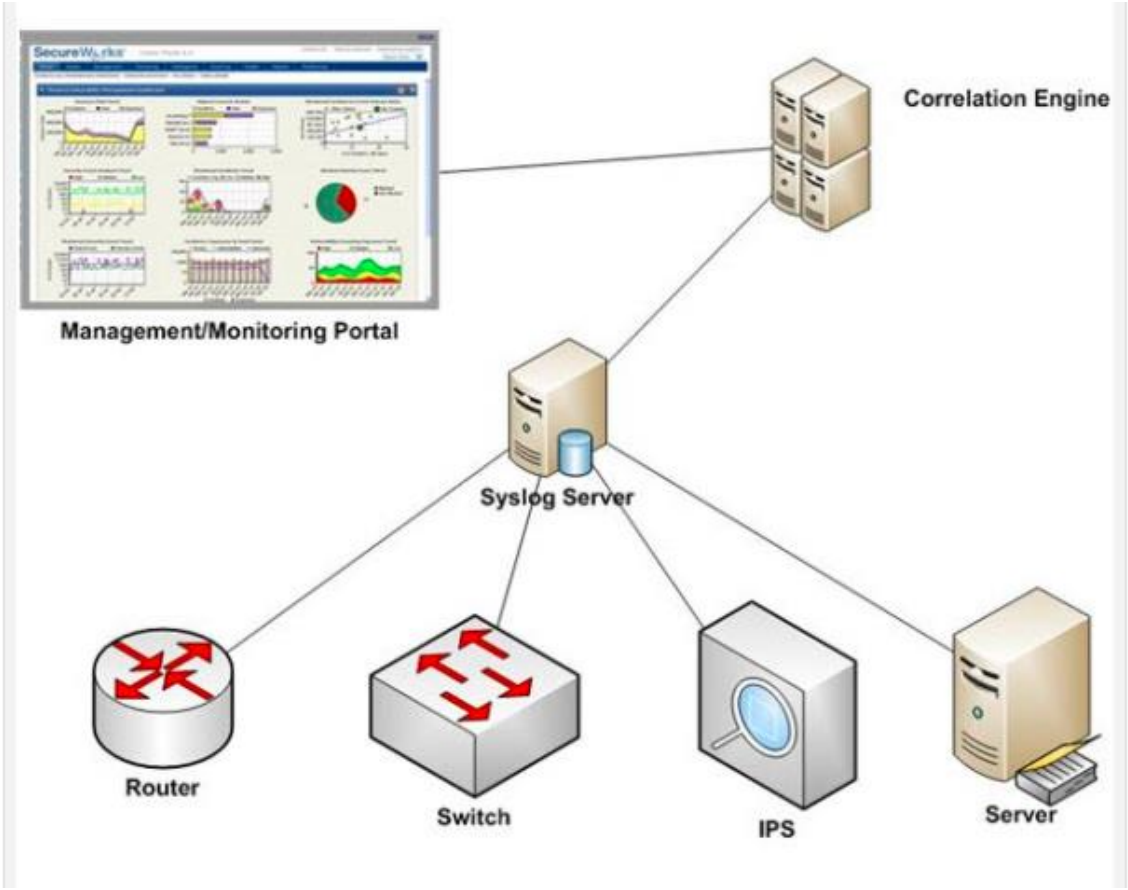
A Security Operation Centre (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analysing, and responding to cybersecurity incidents.

The function of a security operations team of a security operations centre (SOC), is to monitor, detect, investigate, and respond to cyberthreats around the clock.

A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside.

SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.





SOC Capabilities:

A SOC provides the following capabilities:

- ☑ Real-time threat detection and response. The SOC staff determines the best method or technologies for threat detection and response. The SOC itself includes all of the human and machine intelligence needed to collect and analyze machine data in real time, detect threats, and remediate them.
- ☑ 24x7 monitoring of system log data and network traffic. Continuous monitoring ensures that anomalous and malicious activity from either outsiders or insiders is detected in real time. Staff identifies malicious activity as it occurs, enabling teams to respond immediately and help eliminate—or at least reduce—its damage.

- ☑ A comprehensive and centralized view of a company's security posture. A SOC integrates the data coming from your tools to provide a snapshot of your current security posture.
- ☑ Threat hunting and investigation. The SOC staff proactively searches through your networks and data to identify threats that have evaded your perimeter controls and are hiding, undetected, on the network.

Roles & Responsibilities of SOC Member:

- ☑ **Security operators** help oversee SOC operations. They serve as the focal point for managing and coordinating a response to incidents.
- ☑ **Security analysts** are typically on the front lines of the SOC. They are the first to review alerts and determine their relevance and urgency. They are also responsible for investigating threats and determining appropriate steps for remediation.
- ☑ **Security researchers** study new strains of malware, take them apart, determine how they work, and share that information with others. They might also use the information they glean to better understand cyberattackers and their attack methods and behavior profiles.
- ☑ **Security managers** supervise the SOC team and handle higher-level tasks, like running reports, managing the escalation process, and reviewing incident reports. Managers also monitor the SOC's performance and communicate with business leaders.
- ☑ **An incident response team** consists of a manager, security analysts, and security researchers. The team is responsible for analyzing and responding to security breaches in an effort to minimize the impact to the business.
- ☑ **A forensics team** investigates breaches to determine root cause and, ideally, preserve evidence so that it can be used in a court of law. The team must practice proper planning, documentation, chain of custody, and rules of evidence.

☑ **A compliance audit team** performs periodic, comprehensive reviews of the IT environment to validate the organization's compliance with regulatory requirements. The team also performs risk assessments, understands applicable laws and regulations, monitors compliance efforts, and educates staff on audit findings.

☑ **A development team** maintains log source connections, API integrations, parsers, custom workflow tools, etc. A SOC leverages a development lifecycle against its platform, similar to the development process used to write software.

SOC Processes:

A SOC must implement the following processes:

- ☑ **Security training** processes ensure that training is ongoing and comprehensive, rather than an ad hoc effort. Security personnel need regular professional certifications and vendor training to ensure that their skills stay current. They must be trained on the technologies deployed in the IT environment and SOC, as well as on advances in cyberthreats.

  Training processes help ensure that staff members are able to effectively carry out their roles and responsibilities at all times.
- ☑ **Threat hunting and investigation** processes are critical for ensuring that threat hunting and investigation efforts are consistent and repeatable. Where possible, repeatable steps should be automated.
- ☑ **Trouble ticketing** processes address how trouble tickets are escalated and tracked. The processes can and should be automated. Otherwise, the task of taking care of tickets manually can be a full-time job in a large SOC.
- ☑ **Incident response** processes ensure that the incident response team identifies, investigates, and responds to incidents in a timely manner that minimizes their impact and facilitates a rapid recovery. The processes should be repeatable and carried out consistently.
- ☑ **Threat intelligence** feeds are used properly to build correlation rules to help detect threats more accurately and reduce false positives.

SIEM (Security Information and Event Management)

LMS, SLM/SEM, SIM, SEM, SEC, SIEM

- **LMS "Log Management System**" – A system that collects and stores log files (from operating systems, applications, and more) from multiple hosts and systems into a single location, allowing centralized access to logs instead of accessing them from each system individually.
- **SLM /SEM "Security Log/Event Management"** – An LMS but marketed towards security analysts instead of system administrators. SEM is about highlighting log entries more significant to security.
- **SIM "Security Information Management**" – An asset management system, but with features to incorporate security information. Hosts may have vulnerability reports listed in their summaries, and intrusion detection and antivirus alerts may be shown mapped to the systems involved.

- **SEC "Security Event Correlation"** – To a particular piece of software, 3 failed login attempts to the same user account from 3 different clients, are just 3 lines in their logfile. To an analyst, that is a peculiar sequence of events worthy of investigation, and log correlation (looking for patterns in logfiles) is a way to raise alerts when these things happen.
- **SIEM "Security Information and Event Management" –** SIEM is the "all of the above" option. As the above technologies merged into single products, SIEM became the generalized term for managing information generated from security controls and infrastructure. We'll use the term SIEM for the rest of this presentation.

How SIEM Works

Data Collection

Most SIEM systems collect data by deploying collection agents on end-user devices, servers, network equipment, or other security systems like firewalls and antivirus, or via protocols syslog forwarding, SNMP or WMI. Advanced SIEMs can integrate with cloud services to obtain log data about cloud-deployed infrastructure or SaaS applications, and can easily ingest other non-standard data sources. Pre-processing may happen at edge collectors, with only some of the events and event data passed to centralized storage.

Data Storage

Traditionally, SIEMs relied on storage deployed in the data center, which made it difficult to store and manage large data volumes. As a result, only some log data was retained. Next-generation SIEMs are built on top of modern data lake technology such as Amazon S3 or Hadoop, allowing nearly unlimited scalability of storage at low cost. This makes it possible to retain and analyze 100% of log data across even more platforms and systems.

Policies and Rules

The SIEM allows security staff to define profiles, specifying how enterprise systems behave under normal conditions.

They can then set rules and thresholds to define what type of anomaly is considered a security incident. Increasingly, SIEMs leverage machine learning and automated behavioral profiling to automatically detect anomalies, and autonomously define rules on the data, to discover security events that require investigation.

Data Consolidation and Correlation

The central purpose of a SIEM is to pull together all the data and allow correlation of logs and events across all organizational systems.

An error message on a server can be correlated with a connection blocked on a firewall, and a wrong password attempted on an enterprise portal. Multiple data points are combined into meaningful

security events, and delivered to analysts by notifications or dashboards. Next-gen SIEMs are getting better and better at learning what is a “real” security event that warrants attention.

What are SIEMs Used For

Security Monitoring

SIEMs help with real-time monitoring of organizational systems for security incidents. A SIEM has a unique perspective on security incidents, because it has access to multiple data sources – for example, it can combine alerts from an IDS with information from an antivirus product. It helps security teams identify security incidents that no individual security tool can see, and help them focus on alerts from security tools that have special significance.

Advanced Threat Detection

SIEMs can help detect, mitigate and prevent advanced threats, including:

Malicious insiders – a SIEM can use browser forensics, network data, authentication and other data to identify insiders planning or carrying out an attack

Data exfiltration (sensitive data illicitly transferred outside the organization) – a SIEM can pick up data transfers that are abnormal in their size, frequency or payload

Outside entities, including Advanced Persistent Threats (APTs) – a SIEM can detect early warning signals indicating that an outside entity is carrying out a focused attack or long-term campaign against the organization

Forensics and Incident Response

SIEMs can help security analysts realize that a security incident is taking place, triage the event and define immediate steps for remediation.

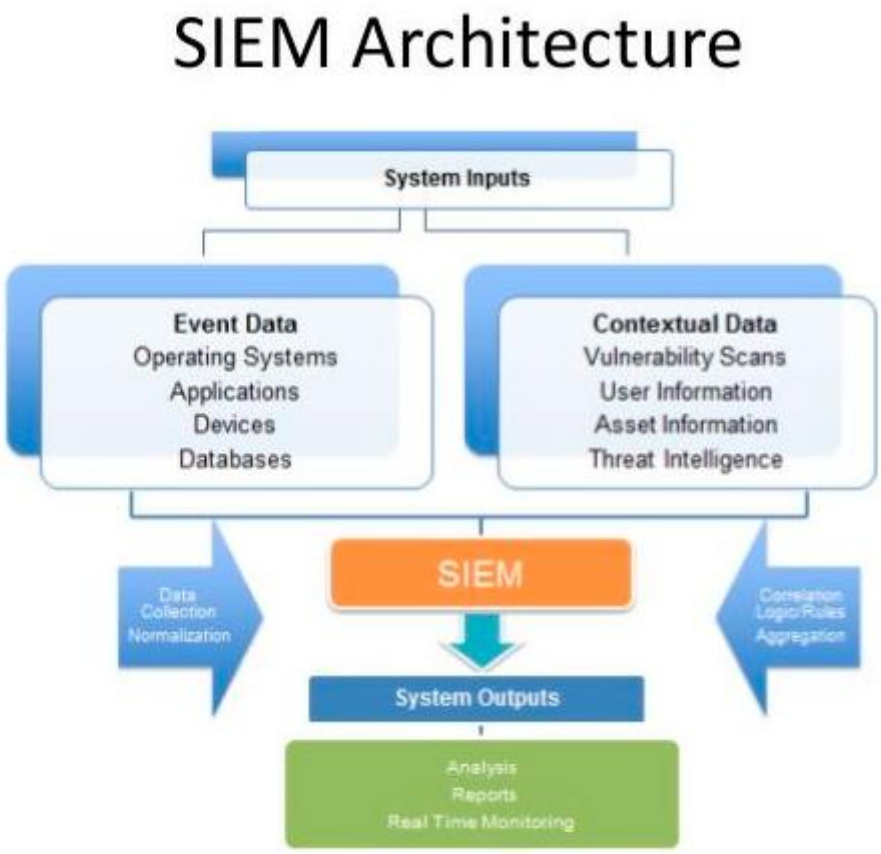
Even if an incident is known to security staff, it takes time to collect data to fully understand the attack and stop it – SIEM can automatically collect this data and significantly reduce response time. When security staff discover a historic breach or security incident that needs to be investigated, SIEMs provide rich forensic data to help uncover the kill chain, threat actors and mitigation.

Compliance Reporting and Auditing

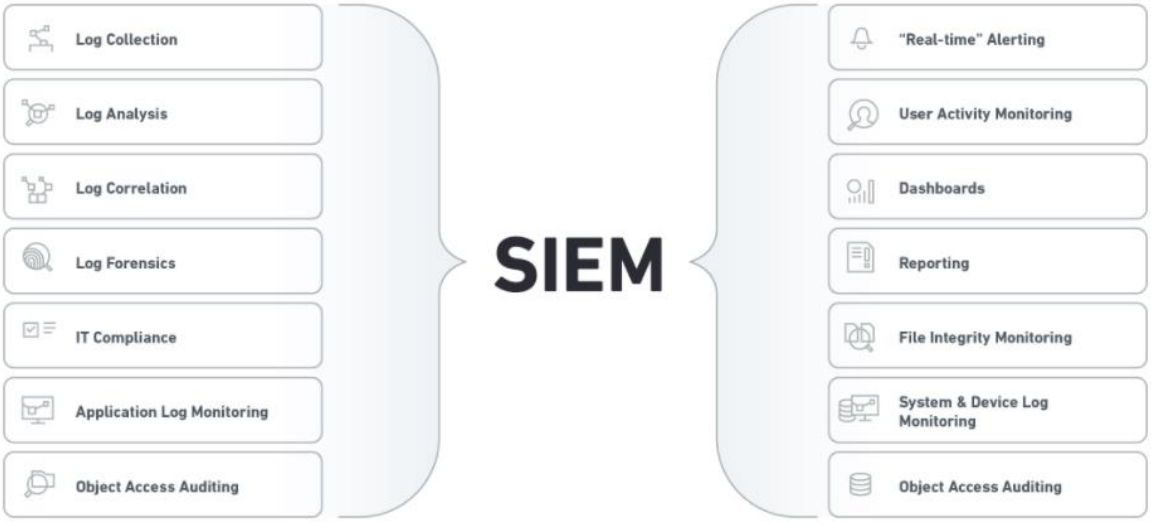
SIEMs can help organizations prove to auditors and regulators that they have the proper safeguards in place and that security incidents are known and contained.

Many early adopters of SIEMs used it for this purpose – aggregating log data from across the organization and presenting it in audit-ready format. Modern SIEMs automatically provide the monitoring and reporting necessary to meet standards like HIPAA, PCI/DSS, SOX, FERPA and HITECH**.**

SIEM architecture



Components and Capabilities in a SIEM Architecture



Data aggregation

Collects and aggregates data from security systems and network devices

Compliance

Gathers log data for standards like HIPAA, PCI/DSS, HITECH, SOX and GDPR and generates reports

Threat intelligence feeds

Combines internal data with third-party data on threats and vulnerabilities

Retention

Stores long-term historical data, useful for compliance and forensic investigation.

Correlation and security monitoring

Links events and related data into security incidents, threats or forensic findings

Forensic analysis

Enables exploration of log and event data to discover details of a security incident

Analytics

uses statistical models and machine learning to identify deeper relationships between data elements

Threat hunting

Enables security staff to run queries on log and event data to proactively uncover threats

Alerting

Analyses events and sends alerts to notify security staff of immediate issues

Incident response

Helps security teams identify and respond to security incidents, bringing in all relevant data rapidly

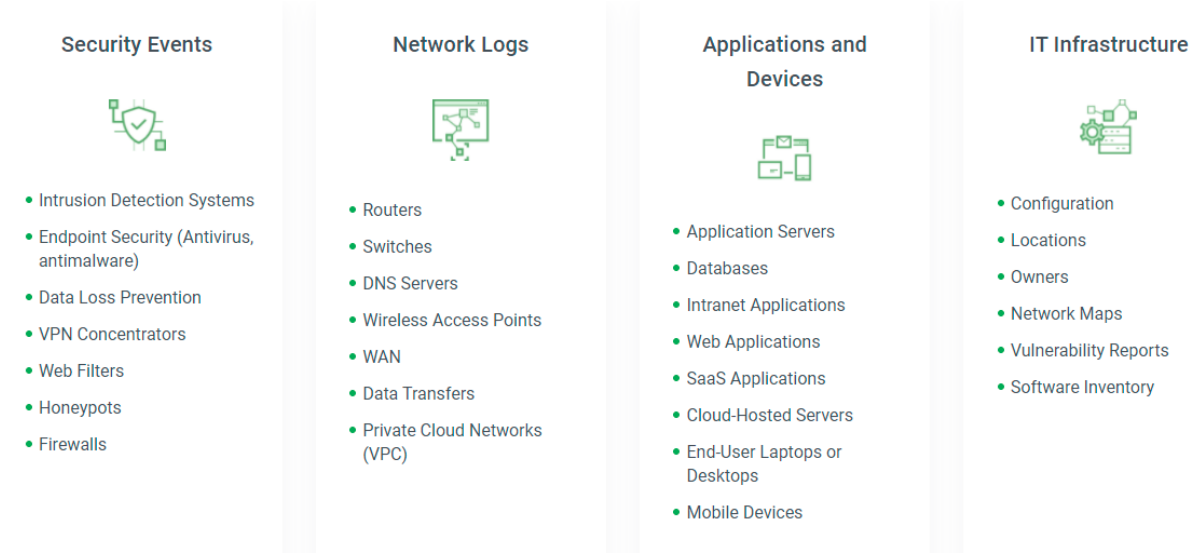
Dashboards

Creates visualizations to let staff review event data, identify patterns and anomalies

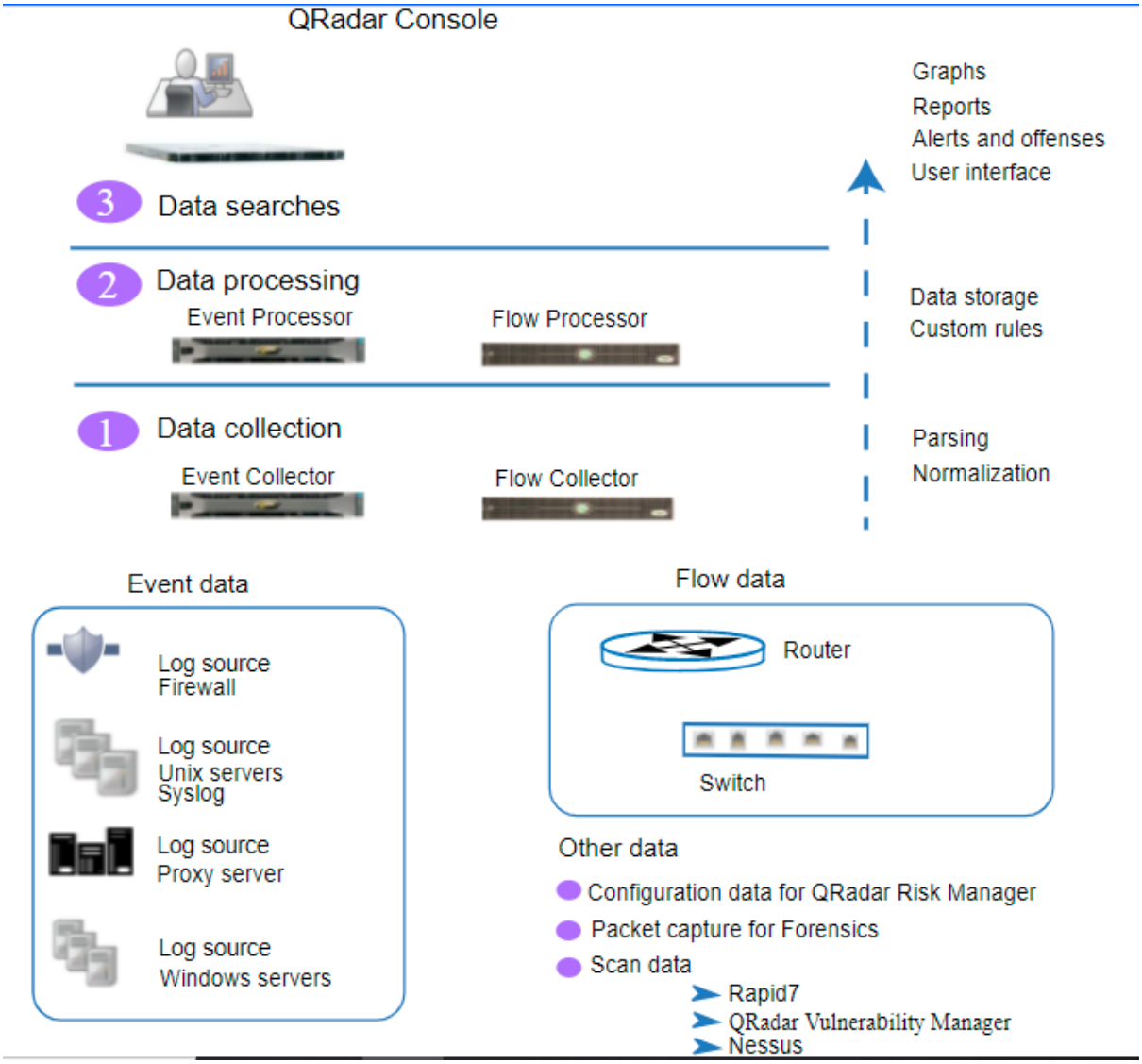
SOC automation

Advanced SIEMs can automatically respond to incidents by orchestrating security systems in an approach known as security orchestration and response (SOAR)

SIEM Integrations:



https://www.ibm.com/docs/en/qsip/7.4?topic=deployment-qradar-architecture-overview



- IBM QRadar collects, processes, aggregates, and stores network data in real time. QRadar uses that data to manage network security by providing real-time information and monitoring, alerts and offenses, and responses to network threats.
- IBM QRadar SIEM (Security Information and Event Management) is a modular architecture that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization. You can scale QRadar to meet your log and flow collection, and analysis needs. You can add integrated modules to your QRadar platform, such as QRadar Risk Manager, QRadar Vulnerability Manager, and QRadar Incident Forensics.

Data collection

- Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data.
- The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.
- The core functionality of QRadar SIEM is focused on event data collection, and flow collection.
- Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs.
- Flow data is network activity information or session information between two hosts on a network, which QRadar translates in to flow records. QRadar translates or normalizes raw data into IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

Data processing

- After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.
- Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.
- Other features such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), or QRadar Incident Forensics collect different types of data and provide more functions.
- QRadar Risk Manager collects network infrastructure configuration, and provides a map of your network topology. You can use the data to manage risk by simulating various network scenarios through altering configurations and implementing rules in your network.
- Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from other scanners such as Nessus, and Rapid7. The vulnerability data that is collected is used to identify various security risks in your network.
- Use QRadar Incident Forensics to perform in-depth forensic investigations, and replay full network sessions.

Data searches

- In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search and manage the security admin tasks for their network from the user interface on the QRadar Console.
- In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance.
- In distributed environments, the QRadar Console does not perform event and flow processing, or storage. Instead, the QRadar Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.

QRadar Console

- The QRadar Console provides the QRadar user interface, and real-time event and flow views, reports, offenses, asset information, and administrative functions.
- In distributed QRadar deployments, use the QRadar Console to manage hosts that include other components.

QRadar Event Collector

The Event Collector collects events from local and remote log sources, and normalizes raw log source events to format them for use by QRadar. The Event Collector bundles or coalesces identical events to conserve system usage and sends the data to the Event Processor.

- The Event Collector is assigned to an EPS license that matches the Event Processor that it is connected to.

QRadar Event Processor

- The Event Processor processes events that are collected from one or more Event Collector components.
- The Event Processor processes events by using the Custom Rules Engine (CRE). If events are matched to the CRE custom rules that are predefined on the Console, the Event Processor executes the action that is defined for the rule response.
- Each Event Processor has local storage, and event data is stored on the processor, or it can be stored on a Data Node.
- The processing rate for events is determined by your events per second (EPS) license.
- If you exceed the EPS rate, events are buffered and remain in the Event Collector source queues until the rate drops. However, if you continue to exceed the EPS license rate, and the queue fills up, your system drops events, and QRadar issues a warning about exceeding your licensed EPS rate.

QRadar QFlow Collector

- The Flow Collector collects flows by connecting to a SPAN port, or a network TAP.
- The IBM QRadar QFlow Collector also supports the collection of external flow-based data sources, such as NetFlow from routers.
- QRadar QFlow Collectors are not designed to be full packet capture systems. For full packet capture, review the QRadar Incident Forensics option.

QRadar Flow Processor

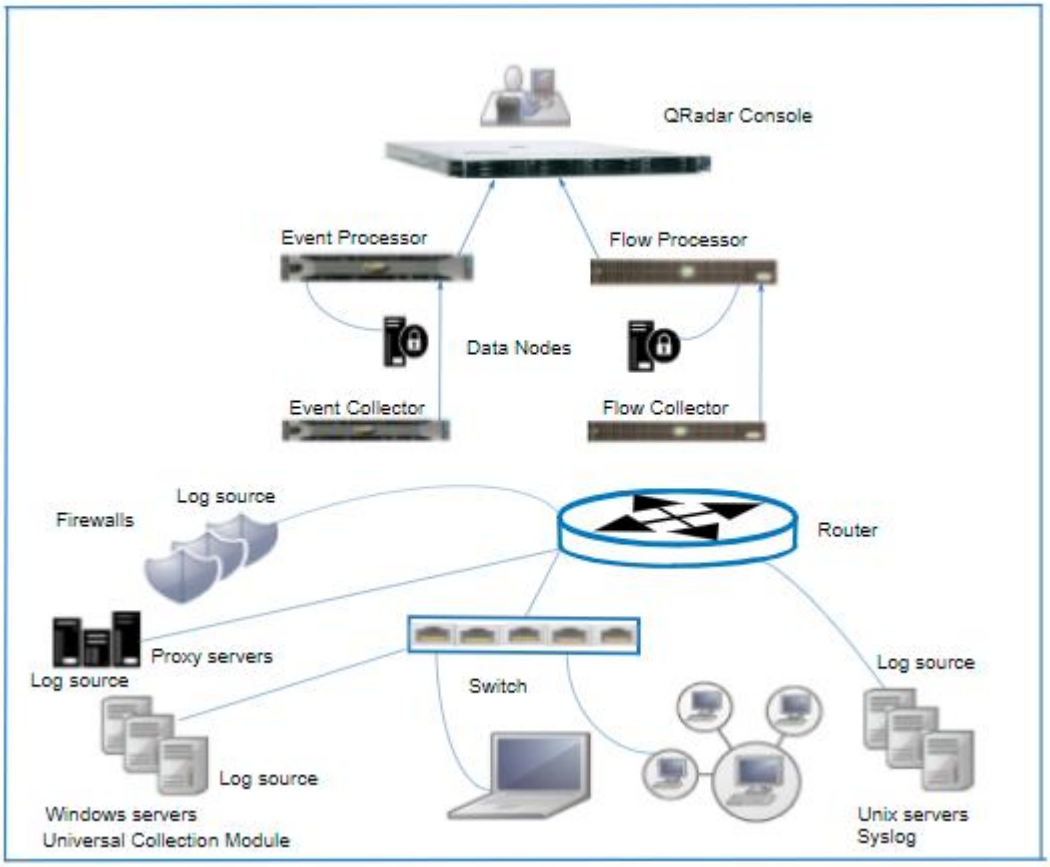
- The Flow Processor processes flows from one or more QRadar QFlow Collector appliances.
- The Flow Processor appliance can also collect external network flows such as NetFlow, J-Flow, and sFlow directly from routers in your network.
- You can use the Flow Processor appliance to scale your QRadar deployment to manage higher flows per minute (FPM) rates.
- Flow Processors include an on-board Flow Processor, and internal storage for flow data. When you add a Flow Processor to an All-in-One appliance, the processing function is moved from the All-in-One appliance to the Flow Processor.

QRadar Data Node

- Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required.
- Data Nodes help to increase the search speed in your deployment by providing more hardware resources to run search queries on.

QRadar App Host

- An App Host is a managed host that is dedicated to running apps.
- App Hosts provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console.
- Apps such as User Behavior Analytics with Machine Learning Analytics require more resources than are currently available on the Console.


QRadar Console
Event Processor
Flow Processor
Data Nodes
Event Collector
Flow Collector
Log source
Firewalls
Router
Proxy servers
Log source
Switch
Log source
Log source
Windows servers
Universal Collection Module
Unix servers
Syslog