Material – Network Concepts

1. IP Classification

What is IP Address: An internet protocol (IP) address allows computers to send and receive information. There are four types of IP addresses: public, private, static, and dynamic. An IP address allows information to be sent and received by the correct parties, which means they can also be used to track down a user's physical location

Static IP Addresses: As the name indicates, the static IP addresses usually never change but they may be changed as a result of network administration. They serve as a permanent Internet address and provide a simple and reliable way for the communication. From the static IP address of a system, we can get many details such as the continent, country, region and city in which a computer is located, The Internet Service Provider (ISP) that serves that particular computer and non-technical information such as precise latitude and longitude of the country, and the locale of the computer. There are many websites providing IP address lookups.

Dynamic IP Addresses: Dynamic IP address are the second category. These are temporary IP addresses. These IP addresses are assigned to a computer when they get connected to the Internet each time. They are borrowed from a pool of IP addresses, shared over various computers. Since limited number of static IP addresses are available, ISPs usually reserve the portion of their assigned addresses for sharing among their subscribers in this way.
Static IP addresses are considered as less secure than dynamic IP addresses because they are easier to track.

Class A private IP range: 10.0.0.0 to 10.255.255.255
Class B private IP range: 172.16.0.0 to 172.31.255.255
Class C private IP range: 192.168.0.0 to 192.168.255.255

2. OSI Layers:

OSI Layers uses: The Open Systems Interconnection (OSI) model defines a networking framework to implement protocols in layers, with control passed from one layer to the next. It is primarily used today as a teaching tool. It conceptually divides computer network architecture into 7 layers in a logical progression.
The Open Systems Interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides

a standard for different computer systems to be able to communicate with each other.

7. The Application Layer

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

6. The Presentation Layer

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

5. The Session Layer

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

4. The Transport Layer

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before

sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection does not overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete and requesting a retransmission if it isn't.

3. The Network Layer

The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.

2. The Data Link Layer

The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the SAME network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

1. The Physical Layer

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

How data flows through the OSI model

In order for human-readable information to be transferred over a network from one device to another, the data must travel down the seven layers of the OSI model on the sending device and then travel up the seven layers on the receiving end.

For example: Mr. Cooper wants to send Ms. Palmer an email. Mr. Cooper composes his message in an email application on his laptop and then hits 'send'. His email application will pass his email message over to the application layer, which will pick a protocol (SMTP) and pass the data along to the presentation layer. The presentation layer will then compress the data and then it will hit the session layer, which will initialize the communication session.

The data will then hit the sender's transportation layer where it will be segmented, then those segments will be broken up into packets at the network layer, which will be broken down even further into frames at the data link layer. The data link layer will then deliver those frames to the physical layer, which will convert the data into a bitstream of 1s and 0s and send it through a physical medium, such as a cable.

Once Ms. Palmer's computer receives the bit stream through a physical medium (such as her wifi), the data will flow through the same series of layers on her device, but in the opposite order. First the physical layer will convert the bitstream from 1s and 0s into frames that get passed to the data link layer. The data link layer will then reassemble the frames into packets for the network layer. The network layer will then make segments out of the packets for the transport layer, which will reassemble the segments into one piece of data.

The data will then flow into the receiver's session layer, which will pass the data along to the presentation layer and then end the communication session. The presentation layer will then remove the compression and pass the raw data up to the application layer. The application layer will then feed the human-readable data along to Ms. Palmer's email software, which will allow her to read Mr. Cooper's email on her laptop screen.

3. MAC/Switch/Router/Hub

MAC: MAC stands for Media Access Control, In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer. In this article, we will discuss about addressing in DLL, which is MAC Address.

Media Access Control (MAC) Address: MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

Logical Link Control (LLC) Sublayer

Media Access Control (MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.

Difference between MAC and IP:

S.no	MAC ADDRESS	IP ADDRESS
1	Media access control	Internet protocol
2	6 Bytes Address	IPV4 is 4Bytes, IPV6 is 6 Bytes
3	Used to ensure physical address	Used to ensure logical address
4	Operates on data link layer	Operates on Network layer
5	Helps in identifying device	Identifes connection of device
6	Cannot be changed with time	Can be modified with time
7	Cannot be found to 3rd party	Can be found to 3rd party

Switch: A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network. Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications.

Hub: A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN. A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.

Differences between Hub and Switch

S.no	Hub	Switch
1	Operate on Physical layer	Operates on data link layer
2	Non-intelligent network device	Intellgent network device
3	Primarily broadcasts messages	Supports Uni, multi and broadcasting
4	Collision may occurs in connection	Collision does not occur
5	Passive device	Actie device

Router: Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.

- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs,bridges and switches.

4. NAT/PAT: Basically, **NAT stands for Network Address Translation** and **PAT stands for Port Address Translation**

NAT, in which the Private IP address or local address are translated into the public IP address. NAT is used to slow down the rate of depletion of available IP address by translates the local IP or Private IP address into global or public ip address. NAT can be a one-to-one relation or many-to-one relation.

In PAT, Private IP addresses are translated into the public IP address via Port numbers. PAT also uses IPv4 address but with port number.

Network Address Translation (NAT) working – Generally, the border router is configured for NAT i.e the router which has one interface in local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Why mask port numbers?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does an only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies on the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

Static NAT – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organisations as there are many devices who will need Internet access and to provide Internet access, the public IP address is

needed. Suppose, if there are 3000 devices who need access to the Internet, the organisation have to buy 3000 public addresses that will be very costly.
Dynamic NAT – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses.
Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet is fixed. This is also very costly as the organisation have to buy many global IP addresses to make a pool.
Port Address Translation (PAT) – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

5. Ports and Protocols

Ports: ports are physical numbers use by tcp/ip to identify what services/application should handle data received by system. Tcp having 65536(0-65535) ports.

0-1023 are well known ports

Protocols: a protocol is a set of rules and guidelines for communicating data.

Well known ports and protocols:

Protocol	Port No
SSH(secure shell)	22
SCP (secure copy protocol)	22
SSL(secure socket layer)	22
TLS(transport layer security)	22
IPsec(internet protocol security)	500
HTTP(hypertext transfer protocol)	80
HTTPS(hypertext transfer protocol secure)	443
FTP(file transfer protocol)	20 & 21
SNMP(simple network management protocol)	161
DNS(domain name system)	53
DHCP(dyanamic host configuration protocol)	67 & 68
LDAP(leightweight directory access protocol)	389
RDP(remote desktop protocol)	3389
POP3(post office protocol)	110
IMAP(internet message access protocol)	143
MS SQL(Microsoft server)	1433
Kerberose(mutual authentication)	88

SMB(server message block)	445
Syslog	514
NTP Server	123

6. Network/Subnet:

Network: A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data. An example of a network is the Internet, which connects millions of people all over the world. To the right is an example image of a home network with multiple computers and other network devices all connected.

Examples of network devices: Desktops, computers, laptops, servers, routers, switches etc...

Subnet: A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

7. TCP/UDP: TCP Stands for **Transmission control protocol** and UDP stands for **User datagram protocol**

How TCP work?

A TCP connection is established with the help of three-way handshake. It is a process of initiating and acknowledging a connection. Once the connection is established, data transfer begins, and when the transmission process is finished, the connection is terminated by the closing of an established virtual circuit.

How UDP work?

UDP uses a simple transmission method without implied hand-shaking dialogues for ordering, reliability, or data integrity. UDP also assumes that error checking and correction is not important or performed in the application, to avoid the overhead of such processing at the network interface level. It is also compatible with packet broadcasts and multicasting.

Features of TCP:

Delivery Acknowledgements and Re-transmission

Delays transmission when the network is congested

Easy Error detection

Features of UDP:

Supports bandwidth-intensive applications that tolerate packet loss

Less delay

It sends the bulk quantity of packets.

Possibility of the Data loss

Allows small transaction (DNS lookup)

Difference between TCP and UDP

TCP	UDP
1. Connection oriented	1. connection less
2. Rearrange data packets in specific order	2. No Fixed order
3. TCP is slower	3. UDP is faster
4. Check errors and corrects	4. no error correction
5. Reliable	5. Un-reliable
6. Acknowledgement will be provided	6. No Acknowledgement

8. Network Topology:

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Types of network topologies:

1. Point-to-Point

   Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa. If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

2. Bus Topology:

   In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning. Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

3. Star Topology:

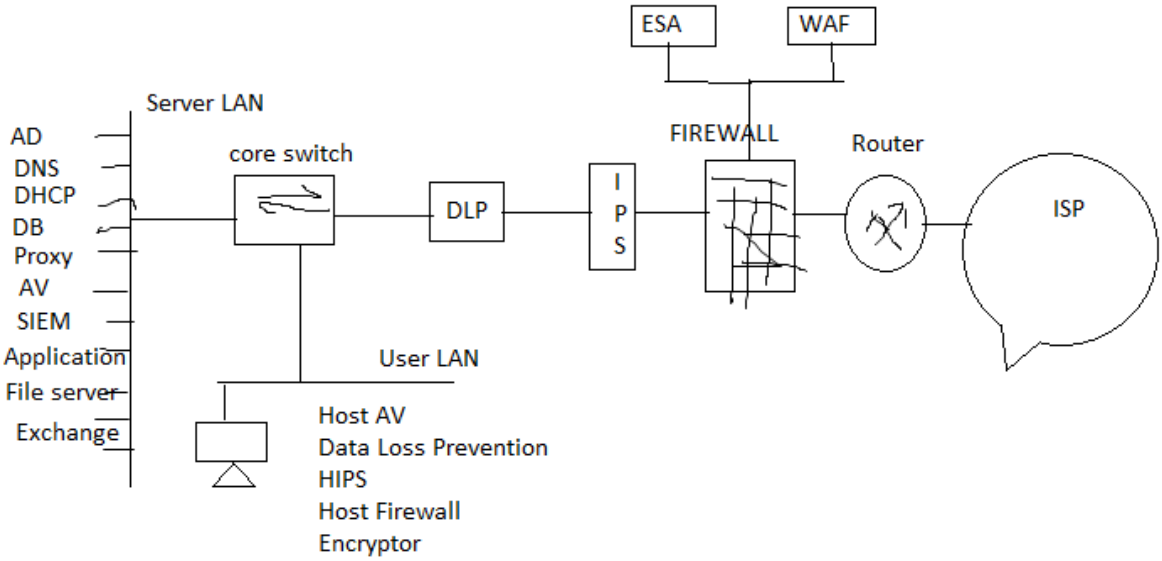
   All hosts in Star topology are connected to a central device, known as switch device, using a point-to-point connection. That is, there exists a point to point connection between hosts and switch. As in Bus topology, switch acts as single point of failure. If switch fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the switch. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

4. Ring Topology:

   In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.

5. Mesh Topology: In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only. Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links.

9. Network Architecture:



What is Network Architecture: Network architecture is the design of a computer network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as communication protocols used.

10.Encoding and Decoding:

Encoding is the process of putting a sequence of characters such as letters, numbers, and other special characters into a specialized format for efficient transmission. Decoding is the process of converting an encoded format back into the original sequence of characters. It is completely different from Encryption which we usually misinterpret. Encoding and decoding are used in data communications and storage. Encoding should NOT be used for transporting sensitive information.

11.Encryption:

Encryption is the process of translating plain text data (*plaintext*) into something that appears to be random and meaningless (*ciphertext*). Decryption is the process of converting ciphertext back to plaintext.

Types of Encryption: There are two types of encryption in widespread use **symmetric** and **asymmetric** encryption.

What is symmetric encryption?

In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient. Symmetric encryption – Using the same key for encryption and decryption.

What is asymmetric encryption?

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key. The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large.
Data encrypted with the recipient's public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data. Asymmetric encryption – Using a different key for the encryption and decryption process.

12. Hashing:

Hashing is a technique that generates a fixed length value summarising a file or message contents. It is often incorrectly referred to as an encryption method. Hash functions are used with cryptography to provide digital signatures and integrity controls but as no secret key is used it does not make the message private as the hash can be recreated.

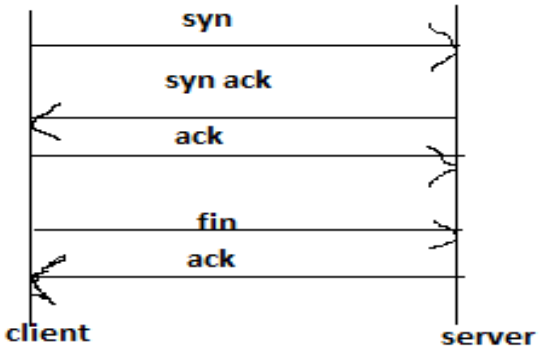
13. Unicasting/Multicasting/Broadcasting:

Unicast: From one source to one destination i.e. One-to-One. traffic, many streams of IP packets that move across networks flow from a single point, such as a website server, to a single endpoint such as a client PC. This is the most common form of information transference on networks. Traffic is sent from one host to another. A replica of each packet in the data stream goes to every host that requests it. The implementation of unicast applications is a bit easy as they use well-established IP protocols; however, they are particularly incompetent when there is a need for many-to-many communications. In the meantime, all packets in the data stream must be sent to every host requesting access to the data stream. However, this type of transmission is ineffective in terms of both network and server resource as it equally presents obvious scalability issues.
Multicast: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many In this method traffic recline between the boundaries of unicast (one point to one destination) and broadcast (one point to all destinations). And multicast is a "one source to many destinations" way of traffic distribution, means that only the destinations that openly point to their requisite to accept the data from a specific source to receive the traffic stream. On an IP network, destinations (i.e. clients) do not regularly communicate straight to sources (i.e. servers), because the routers between source and destination must be able to regulate the topology of the network from unicast or multicast side to avoid disordered routing traffic. Multicast routers replicate packets received on one input interface and send the replicas out on multiple output interfaces.
Broadcast: From one source to all possible destinations i.e. One-to-All. Here, traffic streams from a single point to all possible endpoints within reach on the network, which is generally a LAN. This is the easiest technique to ensure traffic reaches to its destinations. This mode is mainly utilized by television networks for video and audio distribution. Even if the television network is a cable television (CATV) system, the source signal reaches to all possible destinations, which is the key reason that some channels' content is scrambled. Broadcasting is not practicable on the public Internet due to the massive amount of unnecessary data that would continually reach at each user's device, the complications and impact of scrambling and related privacy issues.

14. TCP Three way Handshake:

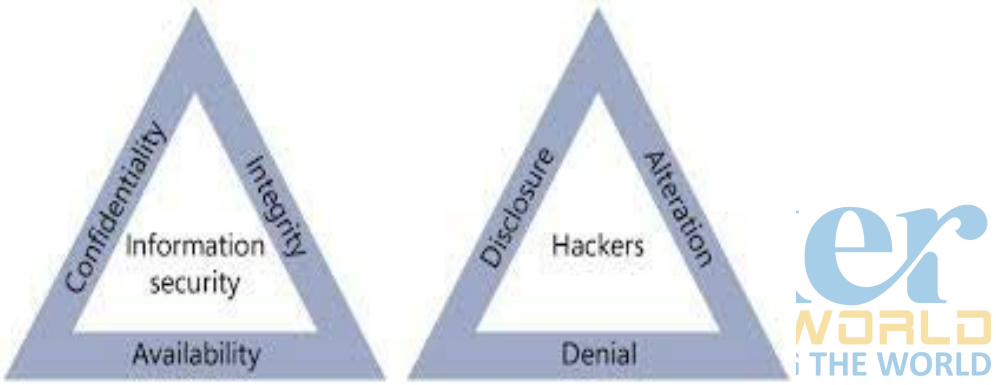
To start tcp session, the client sends a SYN packet and the server responds with SYN ACK packet, and the client completes the third part of handshake with ACK packet, at this point connection is established.

After completion of transmission of data client sends the FIN packet and server reply with ACK, at this point connection is terminated.



Pillars of Security

CIA: CIA stands for **Confidentiality, Integrity and Availability** and CIA in technical way can be pronounced as CIA Triad.



Confidentiality: Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people while making sure that authorized people can access it. It is common for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. Stringent measures can then be implemented according to those categories.

Sometimes safeguarding data confidentiality involves special training for that privy to sensitive documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods, to prevent users from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy form only.

Integrity: involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.

Availability: Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst-case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data blocked by malicious denial-of-service (DoS) attacks and network intrusions.

IAAA: IAAA stands for Identification, Authentication, Authorisation, Accountability

Key concepts to understanding identity and access management is knowing the IAAA (Identification, Authentication, Authorisation, Accountability) security principles.

Identification is the "who are you?" stage and could be any of the following:

- Name, username, ID, employee number etc.

Authentication is the (prove who you are) stage to verify the given identification:

- Something you know, such as a password or pin.
- Something you have, such as an identification device, smart-card or token.
- Something you are, such as biometrics e.g. fingerprint or facial recognition.
- Something you do, such as a mandatory action to complete authentication.
- Somewhere you are, such as your geolocation.

The common authentication types are single-factor authentication, two-factor authentication, and multi-factor authentication.

- Single-factor authentication is often the traditional username and password combination.
- Two-factor authentication is a secondary method in addition to the traditional credentials.
- Multi-factor authentication is similar to two-factor but it can refer to two or more authentication types.

Authorisation is the process of specifying user access rights and privelleges using models such as DAC (Discretionary Access Control), MAC (Mandatory Access Control) and RBAC (Role-based Access Control).

Accountability is ensuring the actions performed by a user are traceable to prove responsibility, this is also referred to as non-repudiation.

Security Solutions:

1. Firewall:

Firewall: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security.

Types of firewalls:

1. Proxy firewall: An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.
2. Stateful inspection firewall: Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

3. Unified threat management (UTM) firewall: A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.
4. Next-generation firewall (NGFW): Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks. According to Gartner, Inc.'s definition, a next-generation firewall must include:
    - Standard firewall capabilities like stateful inspection.
    - Integrated intrusion prevention.
    - Application awareness and control to see and block risky apps.
    - Upgrade paths to include future information feeds.
    - Techniques to address evolving security threats.
5. And Others Types like: Stateless firewall, Circuit level firewall, Application layer firewall, etc..

2. IPS/IDS: Initially IPS stands for **Intrusion Prevention System** and IDS Stands for **Intrusion Detection System.**

IPS: An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application. IPS technologies can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and vulnerability exploits. A vulnerability is a weakness in a software system and an exploit is an attack that leverages that vulnerability to gain control of a system. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System can be used in these cases to quickly block these attacks. Because IPS technologies watch packet flows, they can also be used to enforce the use of secure protocols and deny the use of insecure protocols such as earlier versions of SSL or protocols using weak ciphers.

Types of IPS:

1. Network Intrusion prevention system: It monitors the entire network for suspicious traffic by analyzing protocol activity.
2. Host Intrusion prevention system: It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Detection Method of Intrusion Prevention System (IPS):

1. Signature-based detection: Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.
2. Statistical anomaly-based detection: Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is

normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

3. Stateful protocol analysis detection: This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

IDS: An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms. Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity. Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

Types of IDS:

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

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

Detection Method of IDS:

1. Signature-based Method: Signature-based IDS detects the attacks based on the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects based on the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based Method: Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.

Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

What is the difference between IDS and IPS: Early implementations of the technology were deployed in detect mode on dedicated security appliances, As the technology has matured and moved into integrated Next Generation Firewall or UTM devices, the default action is set to prevent the malicious traffic. In some cases, the decision to detect and accept or prevent the traffic is based upon confidence in the specific IPS protection. When there is lower confidence in an IPS protection, then there is a higher likelihood of false positives. A false positive is when the IDS identifies an activity as an attack, but the activity is acceptable behavior. For this reason, many IPS technologies also can capture packet sequences from the attack event. These can then be analyzed to determine if there was an actual threat and to further improve the IPS protection.

Firewall	IPS	IDS
1. FW is network security device that filters incoming and outgoing network traffic based on rules defined	1. IPS inspects traffic detects, classifies, and proactively stops malicious traffic from attack	1. IDS inspects traffic for malicious activity or policy voilation and sends alerts on detection
2. Filters traffic based on IP Address and port	2. Filters traffic based on pattern, signature of attack and then prevents the attack on detection	2. Detects traffic and looks for pattern or signature of attack and then generates Alerts
3. Works in layer 3	Inline mode, generally works in layer 2	Inline mode in machine
4. Placed at Perimeter level in network	4. Placed after Firewall	4. Placed inline with machine
5. Block the traffic	5. Prevents the traffic on anomaly detection	5. Alerts/Alarms on detection of anomaly

3.Proxy: A Proxy or Proxy server is an intermediary server between client and the internet. Proxy servers offers the following basic functionalities:

1. Firewall and network data filtering.
2. Network connection sharing
3. Data caching

Proxy servers allow to hide, conceal and make your network id anonymous by hiding your IP address.

Following are the reasons to use proxy servers:

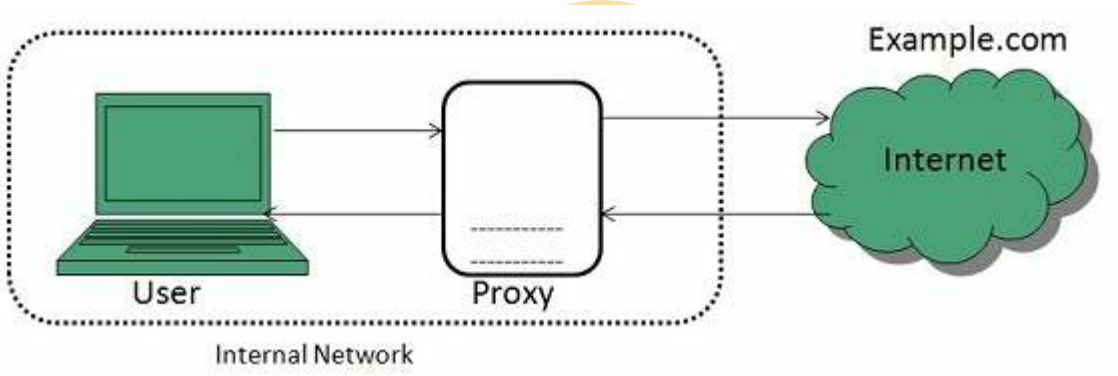
Monitoring and Filtering
Improving performance
Translation
Accessing services anonymously
Security

Proxy servers allow us to do several kinds of filtering such as:

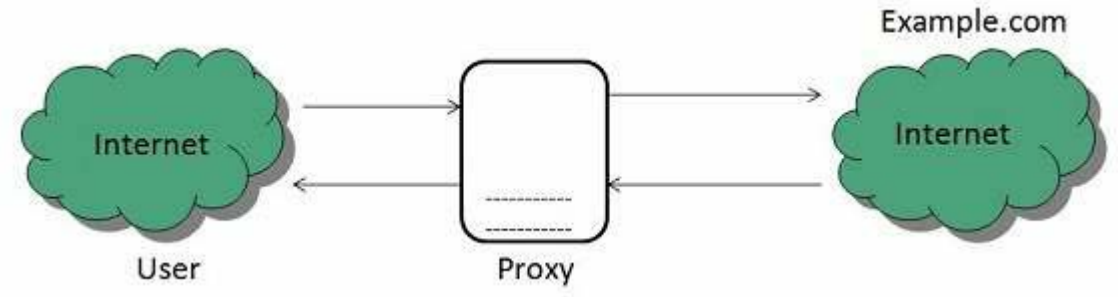
Content Filtering
Filtering encrypted data
Bypass filters
Logging and eavesdropping

Type of Proxies:

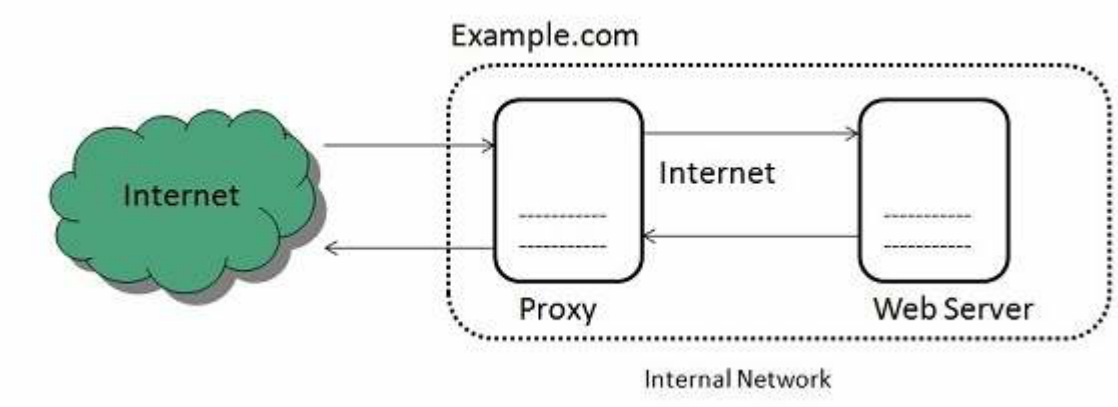
Forward Proxies: In this the client requests its internal network server to forward to the internet.



Open Proxies: Open Proxies helps the clients to conceal their IP address while browsing the web.



Reverse Proxies: In this the requests are forwarded to one or more proxy servers and the response from the proxy server is retrieved as if it came directly from the original Server.



Difference Between Firewall and Proxy:

Firewall	Proxy
1. Firewall can monitor and filter all the incoming and outgoing traffic on a given local network	1. Proxy server connects an eternal client with a server to communicate with each other
2. It blocks connections from unauthorised network	2. it facilitates connections over network
3. It filters data by monitoring IP packets that are traversed	3. It filters the client-side requests that are made to coonects to the network
4. It involves network and transport layer data	4. It works on application layer data
5. it is used to protect an internal network against attacks	5. It is used for anonymity and to bypass restrictions

4.Email Gateway: Secure Email Gateways provide predelivery protection by blocking email-based threats before they reach a mail server, whether on-premises or on Office 365 / G-Suite. They protect businesses from spam, viruses, malware, and denial of service attacks. The gateway scans all incoming, outbound, and internal email communications, including attachments and URLs for signs of malicious or harmful content. Email Gateways will also offer protection from social engineering attacks such as phishing, or business email compromise. The gateway can check the domain of incoming emails, as

well as scan for suspicious content within the email, to stop harmful content from coming into the network. Emails that have been marked as malicious are quarantined or rejected. Some systems allow the quarantined emails to be accessed by admins if necessary. Alongside blocking incoming threats, Email Gateways will also scan outgoing content. This can help protect businesses from data loss.

Key Secure Email Gateway Features:

Spam Filters: Billions of unsolicited email messages are sent by marketers every day. Email security software enables companies to minimize the disruptions caused by spam by allowing them to set pre-determined criteria to detect, filter, and/or block messages that have a high probability of being irrelevant, non-permission-based promotions.

Anti-Virus Protection: Viruses can be detrimental to email systems, as well as to the other files and components within a company's network. Once a virus has permeated an email server, there is almost no stopping the damage it can do to a technology infrastructure. That's why anti-virus protection is the cornerstone of most email security software packages. With email security software, all incoming and outgoing messages, as well as their attachments, are scanned for the latest and greatest viruses. When an infection is identified, the message will be blocked from distribution or receipt, or the corrupted files will be automatically cleaned before being sent or received.

Content and Image Control: With email security software, companies can proactively block content based on pre-defined conditions. For example, they can prevent large images – either embedded or attached – from being received and negatively impacting email server traffic, or they can prohibit emails that contain offensive language or pictures from hitting company inboxes.

Data Encryption: The sharing of private and proprietary information via email is part of every company's day-to-day activities. Therefore, email security software solutions are designed to protect that data from being intercepted by hackers and falling into the wrong hands. They accomplish this by dynamically encrypting all email message data before it is transmitted from the server.

5.AntiVirus:

Antivirus software is a type of program designed and developed to protect computers from malware like viruses, computer worms, spyware, botnets, rootkits, keyloggers and such. Antivirus programs function to scan, detect and remove viruses from your computer.

Advantages of an Effective Antivirus:

Protection from viruses and their transmission
Block spam and ads
Defense against hackers and data thieves
Ensures protection from removable devices
Protects your data and files
Supercharge your PC
Firewall protection from spyware and phishing attacks
Limit the access of websites to enhance web protection

Protects your password

6.DLP (Data Loss Prevention):

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations. The DLP term refers to defending organizations against both data loss and data leakage prevention. Data loss refers to an event in which important data is lost to the enterprise, such as in a ransomware attack. Data loss prevention focuses on preventing illicit transfer of data outside organizational boundaries.

Organizations typically use DLP to:

Protect Personally Identifiable Information (PII) and comply with relevant regulations
Protect Intellectual Property critical for the organization
Achieve data visibility in large organizations
Secure mobile workforce and enforce security in Bring Your Own Device (BYOD) environments
Secure data on remote cloud systems

7.End Point Protection:

What is an Endpoint: An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples of endpoints include:

- Desktops
- Laptops
- Smartphones
- Tablets
- Servers
- Workstations
- Internet-of-things (IoT) devices

Endpoints represent key vulnerable points of entry for cybercriminals. Endpoints are where attackers execute code and exploit vulnerabilities, as well as where there are assets to be encrypted, exfiltrated or leveraged. With organizational workforces becoming more mobile and users connecting to internal resources from off-premises endpoints all over the world, endpoints are increasingly susceptible to cyberattacks. Objectives for targeting endpoints include, but are not limited to:

- Use an endpoint as an entry and exit point to access high-value assets and information on an organization's network.
- Access assets on the endpoint to exfiltrate or hold hostage, either for ransom or purely for disruption.
- Take control of the device and use it in a botnet to execute a DoS attack.

What is end point security: Endpoint security is the process of securing the various endpoints on a network, often defined as end-user devices such as mobile devices, laptops, and desktop PCs, although hardware such as servers in a data center are also considered endpoints. Precise definitions vary among thought leaders in the security space, but essentially, endpoint security addresses the risks presented by devices connecting to an enterprise network.

8.WAF (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. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors. By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server. A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

What are network-based, host-based, and cloud-based WAFs?

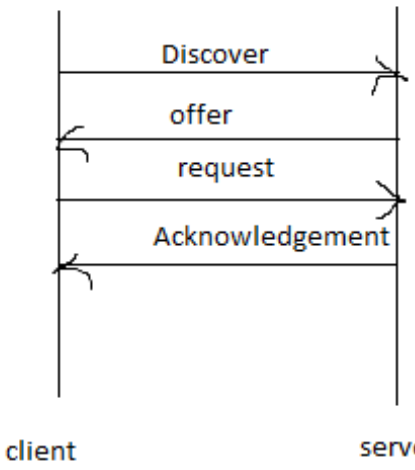
A network-based WAF is generally hardware-based. Since they are installed locally, they minimize latency, but network-based WAFs are the most expensive option and also require the storage and maintenance of physical equipment.

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. Learn about Cloudflare's cloud based WAF solution.

9.DHCP (Dynamic Host Configuration Protocol):

The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters such as IP address for interface and server. The process of assigning the IP address by the DHCP server is also known as DORA.
DORA stands for - Discover, Offer, Request, Acknowledgement.



Components of DHCP:

- DHCP server: A networked device running the DCHP service that holds IP addresses and related configuration information. This is most typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- DHCP client: The endpoint that receives configuration information from a DHCP server. This can be a computer, mobile device, IoT endpoint or anything else that requires connectivity to the network. Most are configured to receive DHCP information by default.
- IP address pool: The range of addresses that are available to DHCP clients. Addresses are typically handed out sequentially from lowest to highest.
- Subnet: IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.
- Lease: The length of time for which a DHCP client holds the IP address information. When a lease expires, the client must renew it.
- DHCP relay: A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. This can be used to centralize DHCP servers instead of having a server on each subnet.

10.DNS (Domain Name System):

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

How does DNS work: The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

Main Types of DNS Records:

A Record: The A record is a DNS record that relates a domain name to an IP address. This is how your website's home server can be found on the internet. It is the A record that associates the website (the content) with its designated domain name (address).

AAAA records: The AAAA records are exactly the same as the A records, but instead of using IPv4 addresses, they use IPv6, which is already a necessity. When the internet was created, the amount of 4 billion addresses provided by IP version 4 seemed orders of magnitude greater than what would ever be needed. However, with the exponential growth of the internet and the explosion of devices connected to it, this is no longer the case. IPv6 was

introduced to battle the exhaustion of the IPv4 pool without changing much how DNS works as a whole.

CNAME Record: The CNAME record is quite similar to the A record, but it binds a domain name to another domain name. This way you can hook subdomains of your domain to external domains without worrying about changing their IP addresses – you will be referenced directly to the other domain name instead.

MX Record: The MX record is the one that directs where the mail server, and quite often "servers" are located. In order for your website to open, there needs to be a web server which serves the website data; however, the emails are sent and received by a mail server, hence the purpose of existence of the MX record. MX records have a specific property called priority. The MX server priority is designated with digits, starting with zero. This is done for redundancy reasons, mostly, so that several mail servers can be associated with a single domain name. If the server with priority 0 doesn't reply to the request, the one with the next number is being queried and so on.

SPF Records: SPF records is a TXT record (a text-based record) used for determining the authenticity of the mail services. As the mail protocol is quite old and hasn't seen many (if any) updates over the last decades, additional security measures are introduced every now and again. Most of them help determine whether the sender of the email is the person he claims to be. SPF records are one of those mechanisms.

PTR records: PTR records are reverse DNS records which are the exact opposite of A records. They bind IPs to domains. This way when you query an IP, you can get meaningful information as to what domain name it's associated with.

NS Records: The nameserver records are one of the most important ones as they tell the domain name which DNS zone to use. Generally, you can create a DNS zone in any DNS server and have different records for it. For example, you can create a valid DNS zone for "google.com" and send it to your website. Does this mean that all the traffic for Google is now yours? Well, no, because the authentic Google.com NS (nameserver) records are saying which exact nameservers are containing the **correct** DNS zone. Quite handy.

11.DMZ:

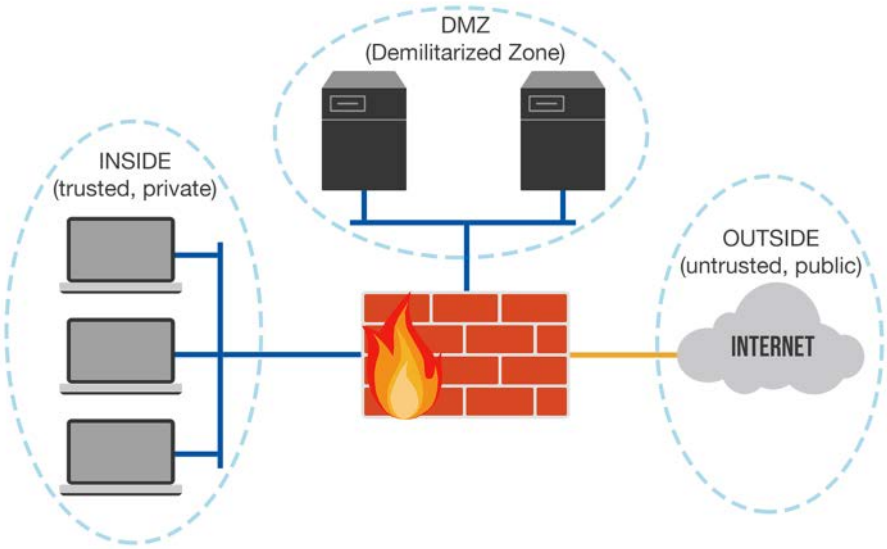
In computer security, a DMZ Network (sometimes referred to as a "demilitarized zone") functions as a subnetwork containing an organization's exposed, outward-facing services. It acts as the exposed point to an untrusted network, commonly the Internet. The goal of a DMZ is to add an extra layer of security to an organization's local area network. A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ, while the rest of the organization's network is safe behind a firewall. When implemented properly, a DMZ Network gives organizations extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

Purpose of a DMZ: The DMZ Network exists to protect the hosts most vulnerable to attack. These hosts usually involve services that extend to users outside of the local area network, the most common examples being email, web servers, and DNS servers. Because of the increased potential for attack, they are placed into the monitored subnetwork to help protect the rest of

the network if they become compromised. Hosts in the DMZ have tightly controlled access permissions to other services within the internal network, because the data passed through the DMZ is not as secure. On top of that, communications between hosts in the DMZ and the external network are also restricted to help increase the protected border zone. This allows hosts in the protected network to interact with the internal and external network, while the firewall separates and manages all traffic shared between the DMZ and the internal network. Typically, an additional firewall will be responsible for protecting the DMZ from exposure to everything on the external network.

DMZ Designs: There are numerous ways to construct a network with a DMZ. The two major methods are a single firewall (sometimes called a three-legged model), or dual firewalls. Each of these systems can be expanded to create complex architectures built to satisfy network requirements:

- **Single firewall:** A modest approach to network architecture involves using a single firewall, with a minimum of 3 network interfaces. The DMZ will be placed Inside of this firewall. The tier of operations is as follows: the external network device makes the connection from the ISP, the internal network is connected by the second device, and connections within the DMZ is handled by the third network device.
- **Dual firewall:** The more secure approach is to use two firewalls to create a DMZ. The first firewall (referred to as the "frontend" firewall) is configured to only allow traffic destined for the DMZ. The second firewall (referred to as the "backend" firewall) is only responsible for the traffic that travels from the DMZ to the internal network. An effective way of further increasing protection is to use firewalls built by separate vendors, because they are less likely to have the same security vulnerabilities. While more effective, this scheme can be more costly to implement across a large network.



Cyber Security Concepts

1. What is Security and types of security:

Security: Simply keeping us away from threat.

Types of security in Cyber world:

Cyber Security: Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. And **Importance of cyber security:** It is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices while doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information.

- Network security: The process of protecting the network from unwanted users, attacks and intrusions.
- Application security: Apps require constant updates and testing to ensure these programs are secure from attacks.
- Endpoint security: Remote access is a necessary part of business but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company's network.
- Data security: Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.
- Identity management: Essentially, this is a process of understanding the access every individual has in an organization.
- Database and infrastructure security: Everything in a network involve databases and physical equipment. Protecting these devices is equally important.
- Cloud security: Many files are in digital environments or "the cloud". Protecting data in a 100% online environment presents a large amount of challenges.
- Mobile security: Cell phones and tablets involve virtually every type of security challenge in and of themselves.
- Disaster recovery/business continuity planning: In the event of a breach, natural disaster or other event data must be protected and business must go on. For this, you'll need a plan. End-user education: Users may be employees accessing the network or customers logging on to a company app. Educating good habits (password changes, 2-factor authentication, etc.) is an important part of cybersecurity.

- Internet of things (IoT) security: IoT refers to a wide variety of critical and non-critical cyber physical systems, like appliances, sensors, televisions, wifi routers, printers, and security cameras.

2.Technologies and Tools:

SIEM Technology: First SIEM stands for Security Information and Event Management. SIEM tools provide:

- Real-time visibility across an organization's information security systems.
- Event log management that consolidates data from numerous sources.
- A correlation of events gathered from different logs or security sources, using if-then rules that add intelligence to raw data.
- Automatic security event notifications. Most SIEM systems provide dashboards for security issues and other methods of direct notification.

SIEM works by combining two technologies: a) Security information management (SIM), which collects data from log files for analysis and reports on security threats and events, and b) security event management (SEM), which conducts real-time system monitoring, notifies network admins about important issues and establishes correlations between security events.
The security information and event management process can be broken down as follows:

- **Data collection** – All sources of network security information, e.g., servers, operating systems, firewalls, antivirus software and intrusion prevention systems are configured to feed event data into a SIEM tool. Most modern SIEM tools use agents to collect event logs from enterprise systems, which are then processed, filtered and sent them to the SIEM. Some SIEMs allow agentless data collection. For example, Splunk offers agentless data collection in Windows using WMI.
- **Policies** – A profile is created by the SIEM administrator, which defines the behavior of enterprise systems, both under normal conditions and during pre-defined security incidents. SIEMs provide default rules, alerts, reports, and dashboards that can be tuned and customized to fit specific security needs.
- **Data consolidation and correlation** – SIEM solutions consolidate, parse and analyze log files. Events are then categorized based on the raw data and apply correlation rules that combine individual data events into meaningful security issues.
- **Notifications** – If an event or set of events triggers a SIEM rule, the system notifies security personnel.

SIEM Tools Different Vendors:
Microfocus - ArcSight
Splunk
IBM – Qradar
LogRhythm
DNIF
McAfee Nitro ESM etc etc..

Vulnerability Assessment: A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

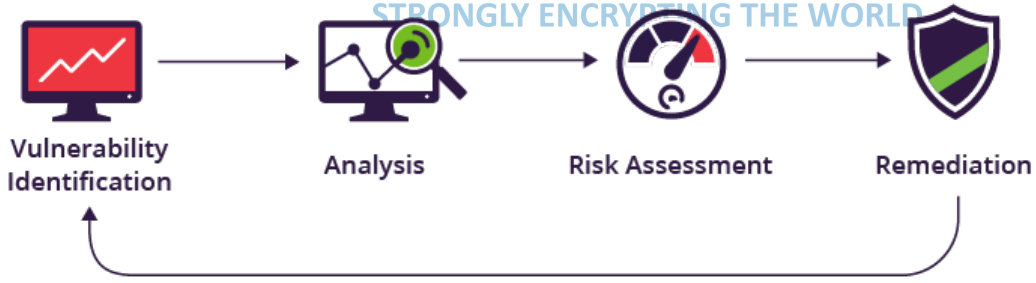
Examples of threats that can be prevented by vulnerability assessment include:

- SQL injection, XSS and other code injection attacks.
- Escalation of privileges due to faulty authentication mechanisms.
- Insecure defaults – software that ships with insecure settings, such as a guessable admin password.

There are several types of vulnerability assessments. These include:

1. **Host assessment** – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
2. **Network and wireless assessment** – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources**.**
3. **Database assessment** – The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.
4. **Application scans** – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

Vulnerability assessment Security scanning process consists of four steps:



1.Vulnerability identification (testing): The objective of this step is to draft a comprehensive list of an application's vulnerabilities. Security analysts test the security health of applications, servers or other systems by scanning them with automated tools or testing and evaluating them manually. Analysts also rely on vulnerability databases, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses.

2. Vulnerability analysis: The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one. It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability. For example, the root cause of a vulnerability could be an old version of an open source library. This provides a clear path for remediation – upgrading the library.

3. Risk assessment: The objective of this step is the prioritizing of vulnerabilities. It involves security analysts assigning a rank or severity score to each vulnerability, based on such factors as:

- Which systems are affected?
- What data is at risk.
- Which business functions are at risk?
- Ease of attack or compromise.
- Severity of an attack.
- Potential damage because of the vulnerability.

4. Remediation: The objective of this step is the closing of security gaps. It's typically a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.

Specific remediation steps might include:

- Introduction of new security procedures, measures or tools.
- The updating of operational or configuration changes.
- Development and implementation of a vulnerability patch.

Vulnerability Tools:
Nmap
Qualys Guard
Nessus
Nexpose etc. etc.

Data Loss Prevention: For More info please refer to Security Solutions
DLP Tools:
McAfee
Digital Guardian
Symantec
Force point etc etc.

Endpoint Security: For More info please refer to Security Solutions
Endpoint Security Tools:
Symantec
Check point
Forcepoint
Carbon Black etc etc.

Intrusion Prevention system and Intrusion Detection System: For More info please refer to Security Solutions.
IPS Tools:
Solar Winds
OSSEC
Sagan
Snort etc etc.

Antivirus: For More info please refer to Security Solutions.
Antivirus Tools:
McAfee
Kaspersky
Symantec
F-Secure etc etc..

3.Incident Investigation: I will Explain the investigation process on multiple scenario's and attack(s).

4.Log Source Integration: I will Explain the Integration process.

5. Vulnerability, Threat, Exploit and Risk:

Vulnerability: A vulnerability, in information technology (IT), is a flaw in code or design that creates a potential point of security compromise for an endpoint or network. Vulnerabilities create possible attack vectors, through which an intruder could run code or access a target system's memory. The means by which vulnerabilities are exploited are varied and include code injection and buffer overruns; they may be conducted through hacking scripts, applications and free hand coding. A zero-day exploit, for example, takes place as soon as a vulnerability becomes generally known.

Threat: A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors.
Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

Some Common types of security Vulnerabilities and Threats:

1. **Unpatched Software –** Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly.

2. **Misconfiguration –** System misconfigurations (e.g. assets running unnecessary services, or with vulnerable settings such as unchanged defaults) can be exploited by attackers to breach your network. The adversary will try to probe your environment looking for systems that can be compromised due to some misconfiguration, and then attack them directly or indirectly.
3. **Weak Credentials –** An attacker may use dictionary or brute force attacks to attempt to guess weak passwords, which can then be used to gain access to systems in your network.
4. **Phishing, Web & Ransomware –** Phishing is used by attackers to get users to inadvertently execute some malicious code, and thereby compromise a system, account or session. The adversary will send your users a link or malicious attachment over email (or other messaging system), often alongside some text/image that entices them to click.
5. **Zero-days & Unknown Methods –** Zero days are specific software vulnerabilities known to the adversary but for which no fix is available, often because the bug has not been reported to the vendor of the vulnerable system. The adversary will try to probe your environment looking for systems that can be compromised by the zero day exploit they have, and then attack them directly or indirectly.

Exploit: An exploit is a code that takes advantage of a software vulnerability or security flaw. It is written either by security researchers as a proof-of-concept threat or by malicious actors for use in their operations. When used, exploits allow an intruder to remotely access a network and gain elevated privileges or move deeper into the network. In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor Trojans and spyware that can steal user information from the infected systems. An exploit is any attack that takes advantage of vulnerabilities in applications, networks, operating systems, or hardware. Exploits usually take the form of software or code that aims to take control of computers or steal network data.

Risk: The potential for loss, damage, or destruction of an asset because of a threat exploiting a vulnerability. Cybersecurity risk is the probability of exposure or loss resulting from a cyber-attack or data breach on your organization. A better, more encompassing definition is the potential loss or harm related to technical infrastructure, use of technology or reputation of an organization.

Few Common Cyber Attacks

1. DOS/DDOS: First initially DOS stands for Denial-of-Service and DDOS stands for Distributed Denial-of-Service. A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack. A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

DoS attacks typically fall in 2 categories:

Buffer overflow attacks: An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.

Flood attacks: By saturating a targeted server with an overwhelming number of packets, a malicious actor can oversaturate server capacity, resulting in denial-of-service. For most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

DoS and DDoS attacks can be divided into three types:

Volume Based Attacks: Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

Protocol Attacks: Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).

Application Layer Attacks: Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second (Rps).

DDoS attacks types:

UDP Flood: A UDP flood, by definition, is any DDoS attack that floods a target with User Datagram Protocol (UDP) packets. The goal of the attack is to flood random ports on a

remote host. This causes the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP 'Destination Unreachable' packet. This process saps host resources, which can ultimately lead to inaccessibility.

ICMP (Ping) Flood: Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.

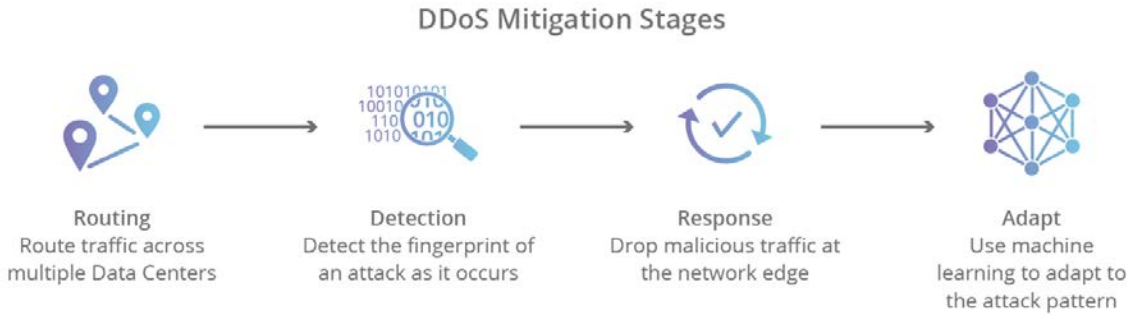
SYN Flood: A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the "three-way handshake"), wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

Ping of Death: A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size – for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

Slowloris: Slowloris is a highly targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool and leads to denial of additional connections from legitimate clients.

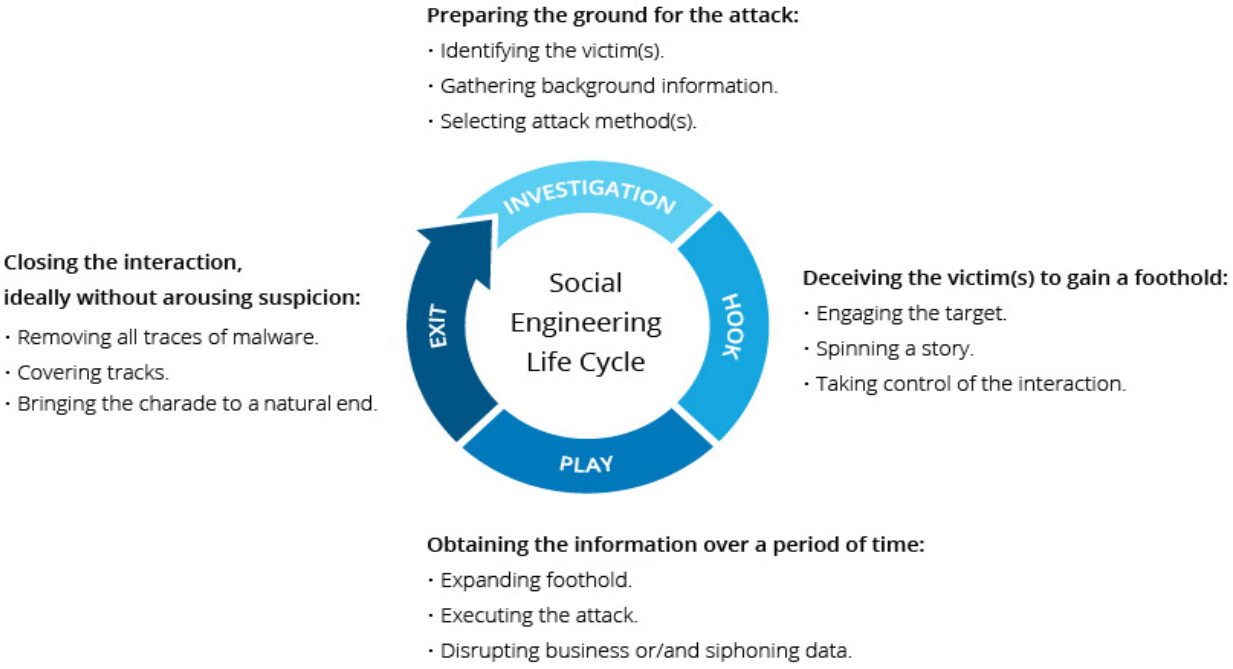
NTP Amplification: In NTP amplification attacks, the perpetrator exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm a targeted server with UDP traffic. The attack is defined as an amplification assault because the query-to-response ratio in such scenarios is anywhere between 1:20 and 1:200 or more. This means that any attacker that obtains a list of open NTP servers (e.g., by a using tool like Metasploit or data from the Open NTP Project) can easily generate a devastating high-bandwidth, high-volume DDoS attack.

DoS/DDoS Mitigation steps:



2. Social Engineering, Piggybacking etc.

Social Engineering: Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.



Social engineering prevention:

- Don't open emails and attachments from suspicious sources.
- Use multifactor authentication
- Be wary of tempting offers
- Keep your antivirus/antimalware software updated

Piggybacking: Piggybacking, also called tailgating, is when an unauthorized person physically follows an authorized person into a restricted corporate area or system. One tried-and-true method of piggybacking is when a hacker calls out to an employee to hold a door open for them as they have forgotten their ID card. Another method involves a person asking an employee to "borrow" his or her laptop for a few minutes, during which the criminal can quickly install malicious software.

Shoulder Surfing: Shoulder surfing refers to the act of obtaining personal or private information through direct observation by, for example, looking over a person's shoulder. It is also possible to observe a target using binoculars, video cameras (hidden or visible), and other optical devices. Typically, the objective of shoulder surfing is to catch things like username and password combinations that can be later used to access a user's account. Credit card numbers, personal identification numbers (PIN), important personal information (like middle name and birth date used in password recovery) are also targeted.

Dumpster Diving: Dumpster diving is the process of searching trash to obtain useful information about a person/business that can later be used for the hacking purpose. This

attack mostly targets large organizations or business to carry out phishing (mostly) by sending fake emails to the victims that appear to have come from a legitimate source. The information obtained by compromising the confidentiality of the victim is used for Identity frauds.

Impersonating: An impersonation attack typically involves an email that seems to come from a trusted source. Sometimes the email attack may start with a message that looks like it comes from a CEO, CFO or another high-level executive – these scams are also called whaling email attacks. An impersonation attack may also involve a message that appears to be from a trusted colleague, a third-party vendor or other well-known Internet brands. The message may request that the recipient initiate a transfer to a bank account or vendor that later proves to be fraudulent, or it may ask the recipient to send along information like W-2 files, bank information or login credentials that give hackers access to business finances and systems.

Tailgating: Piggybacking and Tailgating are equally same.

Credential stuffing: Credential stuffing is the automated injection of stolen username (typically emails) and password pairs to gain unauthorized access to user accounts. Using automation tools, large numbers of compromised credentials are automatically entered into an application (typically a Web application) until success is achieved. Once account takeover is achieved, account data can be stolen, fraudulent transactions initiated, or the account can be used for other nefarious activities. An important enabler for credential stuffing is the tendency of users to reuse passwords across more than one application. As a result, compromised credentials from one application can be used to access other applications. Credential stuffing attacks can involve the use of botnets that use automated scripts to try to access an account until a legitimate set of credentials permit the hijacking of at least one account.

3. Brute force attack etc. Brute-force attack is an attempt to guess a secret – e.g. password or encryption key – by systematically checking every possible option. A brute force attack against an encryption system attempts to decrypt encrypted data by exhaustively enumerating and trying encryption keys. Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. Well designed and implemented cryptosystems make the brute force attack option infeasible, as they ensure that probability of success is negligibly small by using long encryption keys that are difficult to successfully guess. A brute force attack against a password system attempts to exhaustively enumerate and try all password combinations. The increasing computational power of computers makes it computationally practical to guess longer and longer passwords. To overcome this, password length and complexity requirements can be introduced, making guessing impractical again. Brute-force attacks can take place offline or online. In case of an offline attack, the attacker has access to the encrypted material or a password hash and tries different key without the risk of discovery

or interference. In an online attack, the attacker needs to interact with a target system. In such cases, the system can counteract the attack by, for example, limiting the number of attempts that a password can be tried, introducing time delays between successive attempts, increasing the answer's complexity (e.g. by requiring a CAPTCHA answer or verification code sent to a cell phone), and/or locking accounts out after reaching a threshold of unsuccessful logon attempts. Introducing the second factor of authentication is another countermeasure.

Password Spray: Password spraying is an attack that attempts to access many accounts (usernames) with a few commonly used passwords. Traditional brute-force attacks attempt to gain unauthorized access to a single account by guessing the password. This can quickly result in the targeted account getting locked-out, as commonly used account-lockout policies allow for a limited number of failed attempts (typically three to five) during a set period. Password spray campaigns typically target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. Targeting federated authentication can help mask malicious traffic. Additionally, targeting SSO applications helps maximize access to intellectual property if the attack succeeds.

Pass-the-Hash attack: A Pass-the-Hash (PtH) attack is a technique whereby an attacker captures a password hash (as opposed to the password characters) and then simply passes it through for authentication and potentially lateral access to other networked systems. The threat actor does not need to decrypt the hash to obtain a plain text password. PtH attacks exploit the authentication protocol, as the passwords hash remains static for every session until the password is rotated. Attackers commonly obtain hashes by scraping a system's active memory and other techniques.

What is a Rainbow Table: A rainbow table is a precomputed table for reversing cryptographic hash functions. They are used for cracking password hashes. Using a rainbow table requires less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt. Salting the password hash renders the rainbow table attack infeasible.

What is password Hash Salting: Password hash salting is when random data – a salt – is used as an additional input to a hash function that hashes a password. The goal of salting is to defend against dictionary attacks or attacks against hashed passwords using a rainbow table. To salt a password hash, a new salt is randomly generated for each password. The salt and the password are concatenated and then processed with a cryptographic hash function. The resulting output (but not the original password) is stored with the salt in a database.

Man in the Middle Attack: In a Man-in-the-Middle (MitM) attack an attacker is able to insert himself into the communications channel between two trusting parties for the purpose of eavesdropping, data theft and/or session tampering. There are multiple ways an attacker can carry out the attack depending on the setup and type

of communications channel established. One common example for a MitM attack is when an attacker on the internet intercepts communications between a client and a server, causing both sides to think they are communicating with one another, when in fact they are both communicating with an attacker. The attacker transparently relays data traversing the communications channel to the respective parties after reading it and/or tampering with it.

Another common example is what is referred to as Man-in-the-Browser (MitB) attack, a form of MitM, where the attacker compromises the client web browser, typically with the aid of a malware. Once the browser is controlled by the attacker, it can steal data that is sent and received through it and alter what is being presented to the user and what is being communicated to the server. MitB attacks are commonly used to attack online banking services by stealing credentials and/or carrying out fraudulent transactions once the user is logged into his account.

There are 8 types of man in the middle attack: DNS Spoofing, IP Spoofing, Wi-Fi eavesdropping, HTTPS Spoofing, SSL Hijacking, Email Hijacking, Session Hijacking and Man in the Browser.

DNS Spoofing (DNS Cache Poisoning): DNS spoofing is a type of attack in which a malicious actor intercepts DNS request and returns the address that leads to its own server instead of the real address. Hackers can use DNS spoofing to launch a man-in-the-middle attack and direct the victim to a bogus site that looks like the real one, or they can simply relay the traffic to the real website and silently steal the information.

IP Spoofing: Every computer in a network is identified with an internet protocol (IP) address, which it uses to communicate with other devices on the same network. IP addresses come in different forms, the more common form, known as IPv4, gives each computer a 32bit identifier (e.g. 192.168.34.12). On some networks, security of digital assets and applications is maintained by specifying which IP addresses can access which resources. An IP spoofing attack happens when a malicious actor masks their identity by presenting themselves with the IP address of a legitimate device to gain access to resources that would otherwise be beyond their reach. For instance, access to a server might be limited to a specific set or range of IP addresses. A hacker manipulates its network packets so that the sender's address reads as that of a legitimate computer. By doing this, the attacker tricks the server into thinking the packets are coming from an authorized device.

Wi-Fi Eavesdropping (Also Evil Twin attack): Also known as an "evil twin" attack, hackers perform Wi-Fi eavesdropping is a type of man-in-the-middle attack that tricks unsuspecting victims into connecting to a malicious Wi-Fi network. To perform Wi-Fi eavesdropping, a hacker sets up a Wi-Fi hotspot near a location where people usually connect to a public Wi-Fi network. This can be a hotel, a restaurant, or your local Starbucks. The hacker then names the hotspot after the actual public network that people use in that location (thus the name "evil twin"). Since people usually set their devices to remember and automatically reconnect to known Wi-Fi networks, as

soon as they come in the vicinity of the malicious hotspot, they automatically connect to it. The user will then think they have been connected to the legitimate network.

Please help yourself on other left types.

4. Buffer Overflow Vulnerability: Initially Buffer is nothing, but Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

In Buffer overflow vulnerability, Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems. If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

5. Phishing: Phishing is a common tactic used by online scammers and hackers to trick users into sharing their online credentials or other sensitive information. It is a type of "Social Engineering" that is usually done by sending a genuine and trustworthy looking message (E-mail, SMS, social media etc.) containing a link to a deceptive website. Once there, users are asked to provide their authentication credentials to log in, without suspecting they are proving an attacker with their precious password. Once the attacker has the credentials in hand, it can immediately be used to login to the real service and easily steal data or funds, damage online assets, impersonate the victim and so on. Since this "hack" is done without ever employing sophisticated cyber-attacks against the breached system, it can take a while to detect and by the time it is, irreparable has been done to the user and/or the organization.

Spear Phishing: Spear phishing, as its name suggests, is a phishing attack targeting a specific person (or sometimes a small group). Unlike standard phishing campaigns, that are trying to deceit as many victims as possible (due to the naturally low success rates), these are intended to gain very specific credentials, often as part of a broader attack against an organization.

Spam: Spam refers to unsolicited bulk messages being sent through email, instant messaging or other digital communication tools. It is generally used by advertisers because there are no operating costs beyond that of managing their

mailing lists. It could also take place in chat rooms, in blogs and more recently within voice over internet conversation (such as Skype). Beyond being a simple nuisance, spam can also be used to collect sensitive information from users and has also been used to spread viruses and other malware.

Vishing: 'Vishing' is over the phone phishing where scammers will try to persuade people to share information by posing as bank staff or other financial service employees.

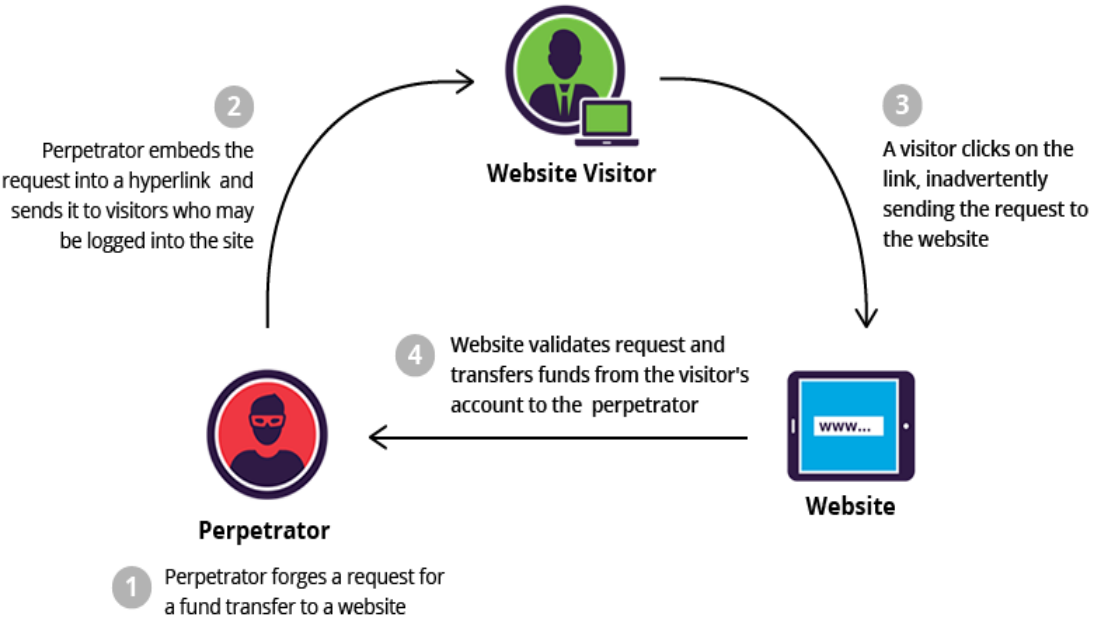
Smishing: 'Smishing' is SMS phishing where text messages are sent trying to encourage people to pay money out or click on suspicious links. Sometimes attackers try to get victims on the phone by sending a text message asking them to call a number, to persuade them further.

Whaling: A whaling attack is a method used by cybercriminals to masquerade as a senior player at an organization and directly target senior or other important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes. Also known as CEO fraud, whaling is similar to phishing in that it uses methods such as email and website spoofing to trick a target into performing specific actions, such as revealing sensitive data or transferring money. (Similar to Spear phishing).

6. Cross-Site Request Forgery:

Cross site request forgery (CSRF), also known as XSRF, Sea Surf or Session Riding, is an attack vector that tricks a web browser into executing an unwanted action in an application to which a user is logged in. A successful CSRF attack can be devastating for both the business and user. It can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft—including stolen session cookies. CSRFs are typically conducted using malicious social engineering, such as an email or link that tricks the victim into sending a forged request to a server. As the unsuspecting user is authenticated by their application at the time of the attack,

it's impossible to distinguish a legitimate request from a forged one



7. Watering Hole Attack:

A watering hole attack is a targeted attack designed to compromise users within a specific industry or group of users by infecting websites they typically visit and luring them to a malicious site. The end goal is to infect the users computer and gain access to the organizations network. Watering Hole attacks, also known as strategic website compromise attacks, are limited in scope as they rely on an element of luck. They do however become more effective, when combined with email prompts to lure users to websites. Attackers that are attempting opportunistic watering hole attacks for financial gain or to build their botnet can achieve this by compromising popular consumer websites. But the targeted attackers that are after more than financial gains tend to focus on public websites that are popular in a particular industry, such as an industry conference, industry standards body, or a professional discussion board. They will look for a known vulnerability on the website, compromise the site, and infect it with their malware before they lie in wait for baited users. Attackers will even prompt users to visit the sites by sending them 'harmless' and highly contextual emails directing them to specific parts of the compromised website. Often, these emails do not come from the attackers themselves, but through the compromised website's automatic email notifications and newsletters that go out on a constant basis. This makes detection of the email lures particularly problematic. As with targeted website attacks, typically the user's machine is transparently compromised via a drive-by download attack that provides no clues to the user that his or her machine has been attacked.

8. ARP Poisoning/MAC Flooding: Address Resolution Protocol (ARP) poisoning is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is linked to an authentic IP address, the attacker can receive any messages directed to the legitimate MAC address. As a result, the attacker can intercept, modify or block communicates to the legitimate MAC address. The term address resolution refers to the process of finding a MAC address that belongs to an assigned IP address for a computer in a network. The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is implemented over Ethernet.

What is ARP Spoofing: ARP spoofing is a type of attack in which an attacker sends false ARP (Address Resolution Protocol) messages over a local network (LAN). This results in the linking of an attacker's MAC address with the IP address of a legitimate machine on the network. Once the attacker's MAC address is linked to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address, assuming the identity of the legitimate MAC address. ARP spoofing can enable malicious parties to intercept, modify or even stop data being transmitted between parties. ARP spoofing attacks only occur on local area networks that utilize the Address Resolution Protocol.

MAC Flooding: The MAC Flooding is an attacking method intended to compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located. As we've already seen, the hubs broadcast the data to the entire network allowing the data to reach all hosts on the network but switches send the data to the specific machine(s) which the data is intended to be sent. This goal is achieved by the use of MAC tables The aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports. MAC Address Table is full, and it is unable to save new MAC addresses. It will lead the switch to enter a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting. Let us see what the benefits of the attacker with the MAC Flooding attack are. As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine. So that the attacker

will be able to steal sensitive data from the communication of the victim and other computers. Usually a packet analyzer is used to capture these sensitive data. After launching a MAC Flood attack successfully, the attacker can also follow up with an ARP spoofing attack. This will help the attacker retaining access to the privileged data even after the attacked switches recover from the MAC Flooding attack.

9. Zero-Day Vulnerability: A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection ... at first. If a zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence "zero-day."

10. Top 10 OWASP: First OWASP stands for the Open Web Application Security Project, an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security. And OWASP Top 10 is the list of the 10 most common application vulnerabilities. It also shows their risks, impacts, and countermeasures.

The Top 10 OWASP vulnerabilities in 2020 are:

1. Injection: Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. For example, an attacker could enter SQL database code into a form that expects a plaintext username. If that form input is not properly secured, this would result in that SQL code being executed. This is known as an SQL injection attack. Injection attacks can be prevented by validating and/or sanitizing user-submitted data. (Validation means rejecting suspicious-looking data, while sanitization refers to cleaning up the suspicious-looking parts of the data.) In addition, a database admin can set controls to minimize the amount of information an injection attack can expose.

2. Broken Authentication

Vulnerabilities in authentication (login) systems can give attackers access to user accounts and even the ability to compromise an entire system using an admin account. For example, an attacker can take a list containing thousands of known username/password combinations obtained during a data breach and use a script to try all those combinations on a login system to see if there are any that work. Some strategies to mitigate authentication vulnerabilities are requiring two-factor authentication (2FA) as well as limiting or delaying repeated login attempts using rate limiting.

3. Sensitive Data Exposure: If web applications don't protect sensitive data such as financial information and passwords, attackers can gain access to that data and sellor utilize it for nefarious purposes. One popular method for stealing sensitive information is using an on-path attack. Data exposure risk can be minimized by encrypting all sensitive data as well as disabling the caching* of any sensitive information. Additionally, web application developers should take care to ensure that they are not unnecessarily storing any sensitive data.

*Caching is the practice of temporarily storing data for re-use. For example, web browsers will often cache webpages so that if a user revisits thosepages within a fixed time span, the browser does not have to fetch the pages from the web.

4. XML External Entities (XEE): This is an attack against a web application that parses XML* input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An 'external entity' in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker. The best ways to prevent XEE attacks are to have web applications accept a less complex type of data, such as JSON**, or at the very least to patch XML parsers and disable the use of external entities in an XML application.

*XML or Extensible Markup Language is a markup language intended to be both human-readable and machine-readable. Due to its complexity and security vulnerabilities, it is now being phased out of use in many web applications.

**JavaScript Object Notation (JSON) is a type of simple, human-readable notation often used to transmit data over the internet. Although it was originally created for JavaScript, JSON is language-agnostic and can be interpreted by many different programming languages.

5. Broken Access Control: Access control refers a system that controls access to information or functionality. Broken access controls allow attackers to bypass authorization and perform tasks as though they were privileged users such as administrators. For example a web application could allow a user to change which account they are logged in as simply by changing part of a url, without any other verification. Access controls can be secured by ensuring that a web application uses authorization tokens* and sets tight controls on them.

*Many services issue authorization tokens when users log in. Every privileged request that a user makes will require that the authorization token be present. This is a secure way to ensure that the user is who they say they are, without having to constantly enter their login credentials.

6. Security Misconfiguration: Security misconfiguration is the most common vulnerability on the list and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could show a user overly descriptive errors which may reveal vulnerabilities in the application. This can be mitigated by removing any unused features in the code and ensuring that error messages are more general.

7. Cross-Site Scripting: Cross-site scripting vulnerabilities occur when web applications allow users to add custom code into a url path or onto a website that will be seen by other users. This vulnerability can be exploited to run malicious JavaScript code on a victim's browser. For example, an attacker could send an email to a victim that appears to be from a trusted bank, with a link to that bank's website. This link could have some malicious JavaScript code tagged onto the end of the url. If the bank's site is not properly protected against cross-site scripting, then that malicious code will be run in the victim's web browser when they click on the link. Mitigation strategies for cross-site scripting include escaping untrusted HTTP requests as well as validating and/or sanitizing user-generated content. Using modern web development frameworks like ReactJS and Ruby on Rails also provides some built-in cross-site scripting protection.

8. Insecure Deserialization: This threat targets the many web applications which frequently serialize and deserialize data. Serialization means taking objects from the application code and converting them into a format that can be used for another purpose, such as storing the data to disk or streaming it. Deserialization is just the opposite: converting serialized data

back into objects the application can use. Serialization is sort of like packing furniture away into boxes before a move, and deserialization is like unpacking the boxes and assembling the furniture after the move. An insecure deserialization attack is like having the movers tamper with the contents of the boxes before they are unpacked.
An insecure deserialization exploit is the result of deserializing data from untrusted sources, and can result in serious consequences like DDoS attacks and remote code execution attacks. While steps can be taken to try and catch attackers, such as monitoring deserialization and implementing type checks, the only sure way to protect against insecure deserialization attacks is to prohibit the deserialization of data from untrusted sources.
9. Using Components with Known Vulnerabilities
Many modern web developers use components such as libraries and frameworks in their web applications. These components are pieces of software that help developers avoid redundant work and provide needed functionality; common example include front-end frameworks like React and smaller libraries that used to add share icons or a/b testing. Some attackers look for vulnerabilities in these components which they can then use to orchestrate attacks. Some of the more popular components are used on hundreds of thousands of websites; an attacker finding a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit. Component developers often offer security patches and updates to plug up known vulnerabilities, but web application developers do not always have the patched or most-recent versions of components running on their applications. To minimize the risk of running components with known vulnerabilities, developers should remove unused components from their projects, as well as ensuring that they are receiving components from a trusted source and ensuring they are up to date.
10. Insufficient Logging and Monitoring: **Take this topic as assignment and prepare your own points.**

11.Cyber Kill Chain:

OLD Version: Cyber kill chain defines the steps used by cyber attackers in today's cyber-based attacks. The theory is that by understanding each of these stages, defenders can better identify and stop attackers at each of the respective stages. There are 7 stages involved in cyber kill chain process.
1.Reconnaissance: The attacker gathers information on the target before the actual attack starts. Many security professionals feel that there is nothing that can be done about this stage, but that's beyond wrong. Quite often, cyber attackers collect information on their intended targets by searching internet sites like LinkedIn or Instagram. They may also try to gather intel through techniques such as calling employees, email interactions, or dumpster diving.
2.Weaponization: The cyber attacker does not interact with the intended victim. Instead, they create their attack. For example, the attacker may create an infected Microsoft Office document paired with a customized phishing email, or perhaps they create a new strain of self-replicating malware to be distributed via USB drive. There are few security controls, including security awareness, that may impact or neutralize this stage, unless the cyber attacker does some limited testing on the intended target.
3.Delivery: Transmission of the attack to the intended victim(s). For example, this would be sending the actual phishing email or distributing the infected USB drives at a local coffee

shop or cafe. While there is an entire technical industry dedicated to stopping this stage, people also play a critical role.

4.Exploitation: This implies actual 'detonation' of the attack, such as the exploit running on the system. Trained people ensure the systems they are running are updated and current. They ensure they have anti-virus running and enabled. They ensure that any sensitive data they are working with is on secured systems, making them far more secure against exploitation.

5.Installation: The attacker installs malware on the victim. Not all attacks require malware, such as a CEO fraud attack or harvesting login credentials. However, just like exploitation when malware is involved, a trained and secure workforce can help ensure they are using secure devices that are updated, current, and have anti-virus enabled, which would stop many malware installation attempts.

6.Command & Control: This implies that once a system is compromised and/or infected, the system must call home to a Command and Control (C&C) system for the cyber attacker to gain control. Therefore 'hunting' has become so popular. They are looking for abnormal outbound activities like this.

7.Actions on Objectives: Once the cyber attacker establishes access to the organization, they can then execute actions to achieve their objectives. Motivations vary greatly depending on the threat actor. It may include political, financial, or military gain, so it is very difficult to define what those actions will be.

New Version: The new version of Cyber kill chain process has 8 phases/stages.

1. Reconnaissance: At the reconnaissance stage, the attacker gathers information about the target organization. They can use automated scanners to find vulnerabilities and weak points that may allow penetration. Attackers will try to identify and investigate security systems that are in place, such as firewalls, intrusion prevention systems and authentication mechanisms.

2. Intrusion: At the intrusion stage, attackers are attempting to get inside the security perimeter. Attackers commonly inject malware into a system to get a foothold. Malware could be delivered by social engineering emails, a compromised system or account, an "open door" representing a gap in security, such as an open port or unsecured endpoint, or an insider accomplice.

Example attacks in the intrusion stage:

External remote services
Spearphishing attachments
Supply chain compromise.

3. Exploitation: At the exploitation stage, attackers seek additional vulnerabilities or weak points they can exploit inside the organization's systems. For example, from the outside, the attacker may have no access to an organization's databases, but after the intrusion, they can see a database uses an old version and is exposed to a well-known vulnerability.

Example attacks in the exploitation stage:

PowerShell
Local job scheduling
Scripting

Dynamic data exchange

4. Privilege Escalation: In the privilege escalation stage, the goal of the attacker is to gain privileges to additional systems or accounts. Attackers may attempt brute force attacks, look for unsecured repositories of credentials, monitor unencrypted network traffic to identify credentials, or change permissions on existing compromised accounts.

Example attacks in the privilege escalation stage:
Access token manipulation
Path interception
Sudo attack
Process injection

5. Lateral Movement: In the lateral movement stage, attackers connect to additional systems and attempt to find the organization's most valuable assets. Attackers move laterally from one system to another to gain access to privileged accounts, sensitive data, or access to critical assets. Lateral movement is a coordinated effort that may span multiple user accounts and IT systems.

Example attacks in the lateral movement stage:
SSH hijacking
Internal spear phishing
Shared webroot
Windows remote management

6. Obfuscation: At the obfuscation stage the attacker tries to cover their tracks. They may try to delete or modify logs, falsify timestamps, tamper with security systems, and take other actions to hide previous stages in the kill chain and make it appear that sensitive data or systems were not touched.

Example attacks in the obfuscation stage:
Binary padding
Code signing
File deletion
Hidden users
Process hollowing

7. Denial of Service: At the denial of service (DoS) stage, attackers attempt to disrupt an organization's operations. Usually the aim is to draw the attention of security and operational staff and cause a distraction, enabling the attackers to achieve their real goal, which is data exfiltration. DoS can be waged against networks and production systems, including websites, email servers, or customer-facing applications.

Example attacks in the DoS stage:
Endpoint denial of service
Network denial of service
Resource hijacking
Service stop
System shutdown

8. Exfiltration: At the exfiltration stage, an advanced attacker finally “hits home”, getting their hands on the organization’s most sensitive data. Attackers will find a mechanism, typically some sort of protocol tunneling, to copy the data outside the organization, in order to sell the sensitive data, use it for additional attacks (for example, in the case of customer personal data or payment details), or openly distribute it to damage the organization.

Example attacks in the exfiltration stage

Data compressed
Data encrypted
Exfiltration over alternative protocol
Exfiltration over a physical medium
Scheduled transfer

12. Malware and Its types:

Malware is derived from the term’s malicious software. Hackers develop malicious software to infect and gain access to the victim computer without the user’s consent. There are different types of malware they are spyware, ransomware, viruses, adware, worms, Trojan horses, or any other kind of malware program that can get into the system. Typically, a program is called malware depending on the intention of the developer and not on the actual features. Originally, malware was developed just to prank the end user, however it eventually evolved with more and advanced technology implementation to target victim machines and gain monetary benefits. The objective of any hacker through malware infection is to steal confidential information or encrypt files and demand money to unlock files.

Types of Malware attacks:

Viruses: A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless, or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

Worms: Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

Spyware: Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

Trojan horse: A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.

Logic Bombs: A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the

hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

Ransomware: Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.

Backdoors: A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

Rootkits: A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

Keyloggers: Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Etc Etc…..