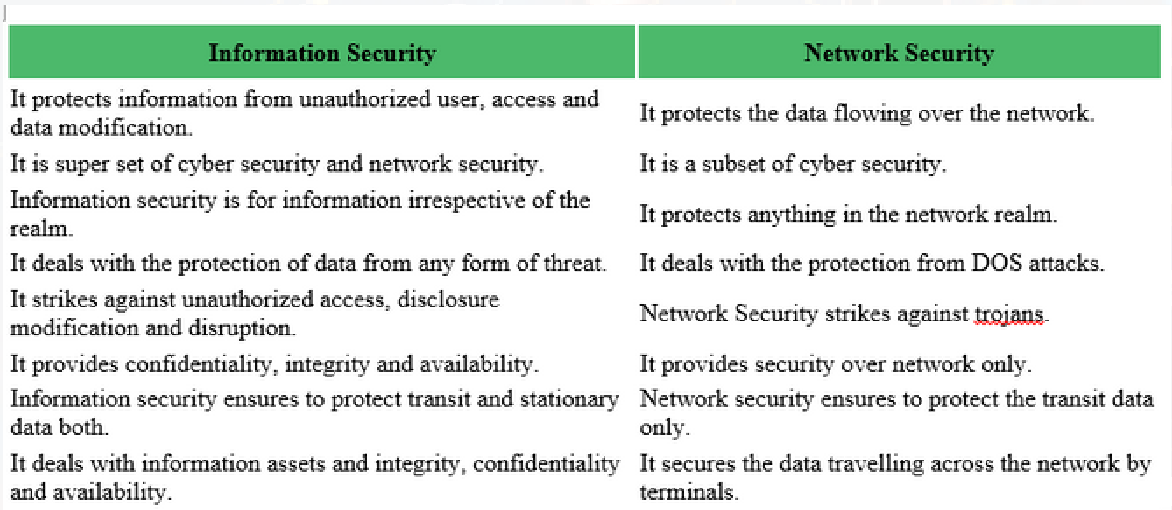
CYBER SECURITY
IMPORTANT NOTES

1. Diffrence between Information and Cyber Security?



Information Security	Network Security
It protects information from unauthorized user, access and data modification.	It protects the data flowing over the network.
It is super set of cyber security and network security.	It is a subset of cyber security.
Information security is for information irrespective of the realm.	It protects anything in the network realm.
It deals with the protection of data from any form of threat.	It deals with the protection from DOS attacks.
It strikes against unauthorized access, disclosure modification and disruption.	Network Security strikes against trojans.
It provides confidentiality, integrity and availability.	It provides security over network only.
Information security ensures to protect transit and stationary data both.	Network security ensures to protect the transit data only.
It deals with information assets and integrity, confidentiality and availability.	It secures the data travelling across the network by terminals.

2. What is the difference between IDS and IPS?

-- IDS is Intrusion Detection System and it only detects intrusions and the administrator has to take care of preventing the intrusion. Whereas, in IPS i.e., Intrusion Prevention System, the system detects the intrusion and also takes actions to prevent the intrusion.

3. How is Encryption different from Hashing?

--> Both Encryption and Hashing are used to convert readable data into an unreadable format. The difference is that the encrypted data can be converted back to original data by the process of decryption but the hashed data cannot be converted back to original data

4.What is a three-way handshake?

-- A three-way handshake is a method used in a TCP/IP network to create a connection between a host and a client. It’s called a three-way handshake because it is a three-step method in which the client and server exchanges packets. The three steps are as follows:

1. The client sends a SYN(Synchronize) packet to the server check if the server is up or has open ports.
2. The server sends SYN-ACK packet to the client if it has open ports
3. The client acknowledges this and sends an ACK(Acknowledgment) packet back to the server

5. What is a Firewall and why is it used?

-- A Firewall is a network security system set on the boundaries of the system/network that monitors and controls network traffic. Firewalls are mainly used to protect the system/network from viruses, worms, malware, etc. Firewalls can also be to prevent remote access and content filtering.

6. How is Encryption different from Hashing?

--> A Botnet is a number of devices connected to the internet where each device has one or more bots running on it. The bots on the devices and malicious scripts used to hack a victim. Botnets can be used to steal data, send spams and execute a DDOS attack.

https://www.linkedin.com/in/nidhi-bagde/

7. What are salted hashes?
Salt is a random data. When a properly protected password system receives a new password, it creates a hash value of that password, a random salt value, and then the combined value is stored in its database.

This helps to defend against dictionary attacks and known hash attacks.
Example: If someone uses the same password on two different systems and they are being used using the same hashing algorithm, the hash value would be same, however, if even one of the system uses salt with the hashes, the value will be different.

8. What are black hat, white hat and grey hat hackers?
Black hat hackers - are known for having vast knowledge about breaking into computer networks. They can write malware which can be used to gain access to these systems. This type of hackers misuse their skills to steal information or use the hacked system for malicious purpose.

White hat hackers - use their powers for good deeds and so they are also called Ethical Hackers. These are mostly hired by companies as a security specialist that attempts to find and fix vulnerabilities and security holes in the systems. They use their skills to help make the security better.

Grey hat hackers - are an amalgamation of a white hat and black hat hacker. They look for system vulnerabilities without the owner's permission. If they find any vulnerabilities, they report it to the owner. Unlike Black hat hackers, they do not exploit the vulnerabilities found.

9. What is a VPN?
Almost all Cybersecurity Interview Questions will have this question included. VPN stands for Virtual Private Network. It is used to create a safe and encrypted connection. When you use a VPN, the data from the client is sent to a point in the VPN where it is encrypted and then sent through the internet to another point. At this point, the data is decrypted and sent to the server. When the server sends a response, the response is sent to a point in the VPN where it is encrypted and this encrypted data is sent to another point in the VPN where it is decrypted. And finally, the decrypted data is sent to the client. The whole point of using a VPN is to ensure encrypted data transfer.

10. What do you understand by Risk, Vulnerability & Threat in a network?
Threat: Someone with the potential to harm a system or an organization
Vulnerability: weakness in a system that can be exploited by a potential hacker.
Risk: Potential for loss or damage when threat exploits a vulnerability.

11. How often should you perform Patch management?
Patch management should be done as soon as it is released. For windows, once the patch is released it should be applied to all machines, not later than one month. Same goes for network devices, patch it as soon as it is released. Proper patch management should be followed.

12. What is port blocking within LAN?
Restricting the users from accessing a set of services within the local area network is called port blocking.

Stopping the source to not to access the destination node via ports. As the application works on the ports, so ports are blocked to restricts the access filling up the security holes in the network infrastructure.

13. What are the steps to set up a firewall?

Following are the steps to set up a firewall:

1. Username/password: modify the default password for a firewall device
2. Remote administration: Disable the feature of the remote administration
3. Port forwarding: Configure appropriate port forwarding for certain applications to work properly, such as a web server or FTP server
4. DHCP server: Installing a firewall on a network with an existing DHCP server will cause conflict unless the firewall's DHCP is disabled
5. Logging: To troubleshoot firewall issues or potential attacks, ensure that logging is enabled and understand how to view logs
6. Policies: You should have solid security policies in place and make sure that the firewall is configured to enforce those policies.

14. What is a Brute Force Attack? How can you prevent it?

Brute Force is a way of finding out the right credentials by repetitively trying all the permutations and combinations of possible credentials. In most cases, brute force attacks are automated where the tool/software automatically tries to login with a list of credentials. There are various ways to prevent Brute Force attacks. Some of them are:

- **Password Length**: You can set a minimum length for password. The lengthier the password, the harder it is to find.
- **Password Complexity**: Including different formats of characters in the password makes brute force attacks harder. Using alpha-numeric passwords along with special characters, and upper and lower case characters increase the password complexity making it difficult to be cracked.
- **Limiting Login Attempts**: Set a limit on login failures. For example, you can set the limit on login failures as 3. So, when there are 3 consecutive login failures, restrict the user from logging in for some time, or send an Email or OTP to use to log in the next time. Because brute force is an automated process, limiting login attempts will break the brute force process.

11. How often should you perform Patch management?

Patch management should be done as soon as it is released. For windows, once the patch is released it should be applied to all machines, not later than one month. Same goes for network devices, patch it as soon as it is released. Proper patch management should be followed.

12. What is Port Scanning?

Port Scanning is the technique used to identify open ports and service available on a host. Hackers use port scanning to find information that can be helpful to exploit vulnerabilities. Administrators use Port Scanning to verify the security policies of the network. Some of the common Port Scanning Techniques are:

1. Ping Scan
2. TCP Half-Open
3. TCP Connect
4. UDP
5. Stealth Scanning

13. What is Cryptography?

Cryptography is the practice and study of techniques for securing information and communication mainly to protect the data from third parties that the data is not intended for.

14. What is an ARP and how does it work?

Address Resolution Protocol (ARP)is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address.

The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.
If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

15. Explain Data Leakage

Data Leakage is an intentional or unintentional transmission of data from within the organization to an external unauthorized destination. It is the disclosure of confidential information to an unauthorized entity. Data Leakage can be divided into 3 categories based on how it happens:

1. **Accidental Breach**: An entity unintentionally send data to an unauthorized person due to a fault or a blunder
2. **Intentional Breac**h: The authorized entity sends data to an unauthorized entity on purpose
3. **System Hack:** Hacking techniques are used to cause data leakage
4.

Data Leakage can be prevented by using tools, software, and strategies known as **DLP(Data Leakage Prevention) Tools.**

16. What is the difference between IDS and IPS?

IDS is Intrusion Detection System and it only detects intrusions and the administrator has to take care of preventing the intrusion. Whereas, in IPS i.e., Intrusion Prevention System, the system detects the intrusion and also takes actions to prevent the intrusion.

17. Explain CIA triad.

CIA stands for Confidentiality, Integrity, and Availability. CIA is a model that is designed to guide policies for Information Security. It is one of the most popular models used by organizations.

Confidentiality

The information should be accessible and readable only to authorized personnel. It should not be accessible by unauthorized personnel. The information should be strongly encrypted just in case someone uses hacking to access the data so that even if the data is accessed, it is not readable or understandable.

Integrity

Making sure the data has not been modified by an unauthorized entity. Integrity ensures that data is not corrupted or modified by unauthorized personnel. If an authorized individual/system is trying to modify the data and the modification wasn't successful, then the data should be reversed back and should not be corrupted.

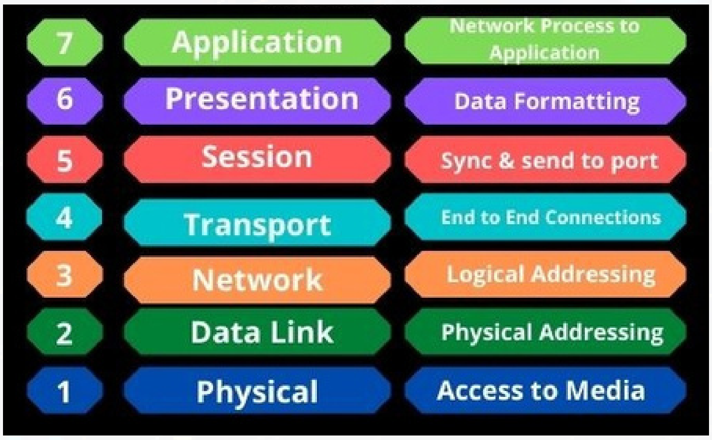
Availability

The data should be available to the user whenever the user requires it. Maintaining of Hardware, upgrading regularly, Data Backups and Recovery, Network Bottlenecks should be taken care of.

18. What are the different layers of the OSI model?

An OSI model is a reference model for how applications communicate over a network. The purpose of an OSI reference is to guide vendors and developers so the digital communication products and software programs can interoperate.

Following are the OSI layers:



7	Application	Network Process to Application
6	Presentation	Data Formatting
5	Session	Sync & send to port
4	Transport	End to End Connections
3	Network	Logical Addressing
2	Data Link	Physical Addressing
1	Physical	Access to Media

Physical Layer: Responsible for transmission of digital data from sender to receiver through the communication media,

Data Link Layer: Handles the movement of data to and from the physical link. It is also responsible for encoding and decoding of data bits.

Network Layer: Responsible for packet forwarding and providing routing paths for network communication.

Transport Layer: Responsible for end-to-end communication over the network. It splits the data from the above layer and passes it to the Network Layer and then ensures that all the data has successfully reached at the receiver's end.

Session Layer: Controls connection between the sender and the receiver. It is responsible for starting, ending, and managing the session and establishing, maintaining and synchronizing interaction between the sender and the receiver.

Presentation Layer: It deals with presenting the data in a proper format and data structure instead of sending raw datagrams or packets.

Application Layer: It provides an interface between the application and the network. It focuses on process-to-process communication and provides a communication interface.

18. How can identity theft be prevented?

Here's what you can do to prevent identity theft:

- Ensure strong and unique password
- Avoid sharing confidential information online, especially on social media
- Shop from known and trusted websites
- Use the latest version of the browsers
- Install advanced malware and spyware tools
- Use specialized security solutions against financial data
- Always update your system and the software
- Protect your SSN (Social Security Number)

19. How would you reset a password-protected BIOS configuration?

Since BIOS is a pre-boot system it has its own storage mechanism for settings and preferences. A simple way to reset is by popping out the CMOS battery so that the memory storing the settings lose its power supply and as a result, it will lose its setting.

20.Explain MITM attack and how to prevent it?

A **MITM(Man-in-the-Middle)** attack is a type of attack where the hacker places himself in between the communication of two parties and steal the information. Suppose there are two parties A and B having a communication. Then the hacker joins this communication. He impersonates as party B to A and impersonates as party A in front of B. The data from both the parties are sent to the hacker and the hacker redirects the data to the destination party after stealing the data required. While the two parties think that they are communicating with each other, in reality, they are communicating with the hacker.

You can prevent MITM attack by using the following practices:

- Use VPN
- Use strong WEP/WPA encryption
- Use Intrusion Detection Systems
- Force HTTPS

Public Key Pair Based Authentication

21. Explain DDOS attack and how to prevent it?

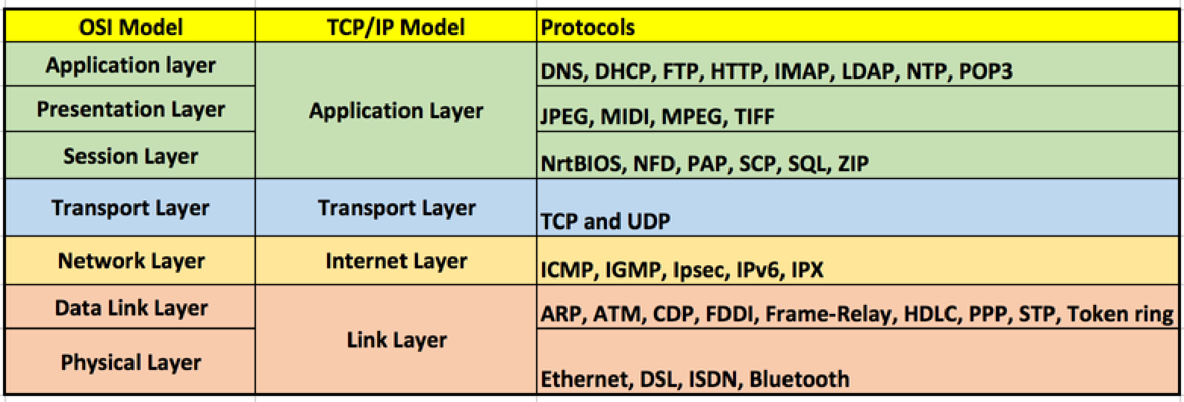
This again is an important Cybersecurity Interview Question. A DDOS(Distributed Denial of Service) attack is a cyberattack that causes the servers to refuse to provide services to genuine clients. DDOS attack can be classified into two types:

1. **Flooding attacks:** In this type, the hacker sends a huge amount of traffic to the server which the server can not handle. And hence, the server stops functioning. This type of attack is usually executed by using automated programs that continuously send packets to the server.
2. **Crash attacks:** In this type, the hackers exploit a bug on the server resulting in the system to crash and hence the server is not able to provide service to the clients.

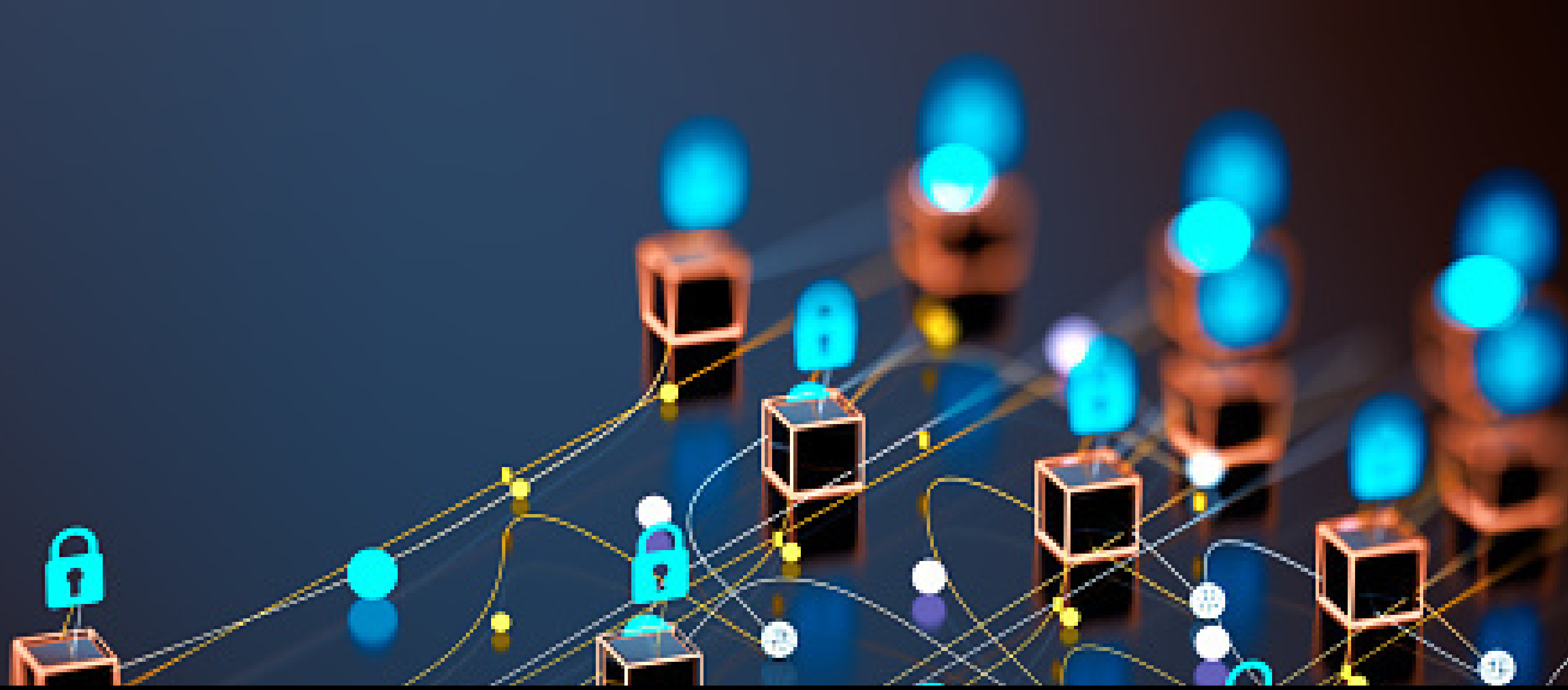
You can prevent DDOS attacks by using the following practices:

- Use Anti-DDOS services
- Configure Firewalls and Routers
- Use Front-End Hardware
- Use Load Balancing
- Handle Spikes in Traffic

22. What protocols fall under TCP/IP internet layer?



OSI Model	TCP/IP Model	Protocols
Application layer	Application Layer	DNS, DHCP, FTP, HTTP, IMAP, LDAP, NTP, POP3
Presentation Layer		JPEG, MIDI, MPEG, TIFF
Session Layer		NrtBIOS, NFD, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP and UDP
Network Layer	Internet Layer	ICMP, IGMP, Ipsec, IPv6, IPX
Data Link Layer	Link Layer	ARP, ATM, CDP, FDDI, Frame-Relay, HDLC, PPP, STP, Token ring
Physical Layer		Ethernet, DSL, ISDN, Bluetooth



Thank you!

For more content like this please follow --

https://www.linkedin.com/in/nidhi-bagde/