This document is designed to refresh Cybersecurity concepts quickly. Information presented can be handy to prepare for job interviews. Document is divided into three sections with questions for Beginner, Intermediate & Advance levels.

BEGINNER LEVEL QUESTIONS

SET-I QUESTION FOR BEGINNERS

1) What is cybersecurity?

Cybersecurity refers to the protection of hardware, software, and data from attackers. The primary purpose of cyber security is to protect against cyberattacks like accessing, changing, or destroying sensitive information.

2) What are the elements of cybersecurity?

Major elements of cybersecurity are:

- Information security (aka data security)
- Network security
- Operational security
- Application security
- End-user education awareness
- Business continuity planning

3) What are the advantages of cyber security?

Benefits of cyber security are as follows:

- It protects the business against ransomware, malware, social engineering, and phishing.
- It protects end-users.
- It gives good protection for both data as well as networks.
- Increase recovery time after a breach.
- Cybersecurity prevents unauthorized users.

4) Define Cryptography.

It is a technique used to protect information from third parties called adversaries. Cryptography allows the sender and recipient of a message to read its details.

5) Differentiate between IDS and IPS.

Intrusion Detection System (IDS) detects intrusions. The administrator has to be careful while preventing the intrusion. In the Intrusion Prevention System (IPS), the system finds the intrusion and prevents it.

6) What is CIA?

Confidentiality, Integrity, and Availability (CIA) is a popular model which is designed to develop a security policy. CIA model consists of three concepts:

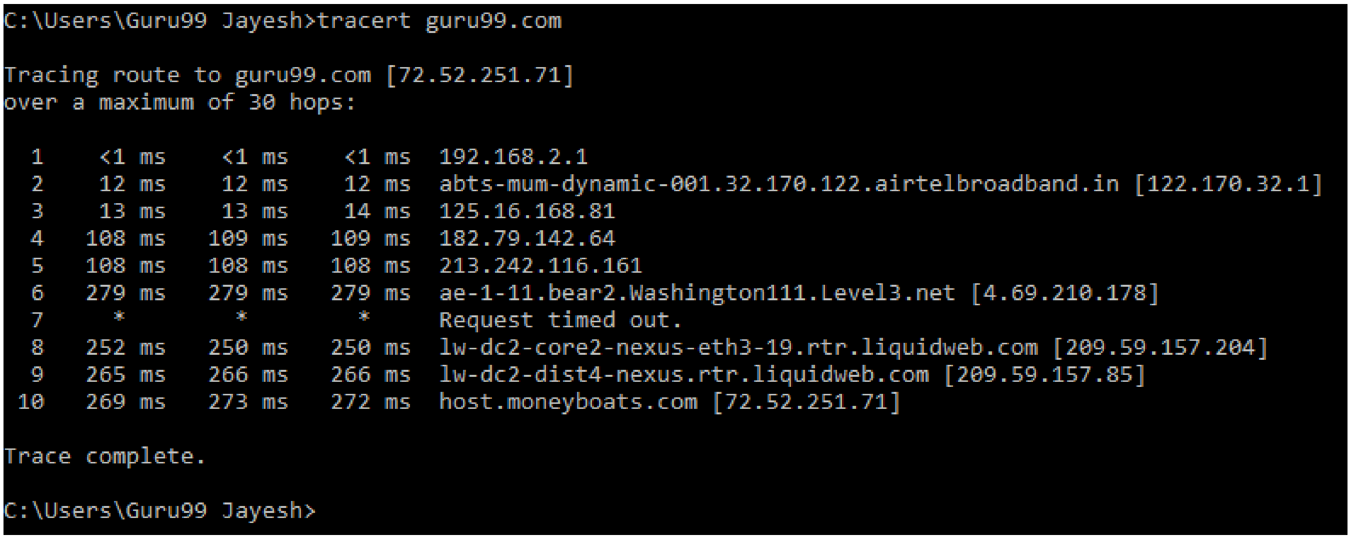
- Confidentiality: Ensure the sensitive data is accessed only by an authorized user.
- Integrity: Integrity means the information is in the right format.
- Availability: Ensure the data and resources are available for users who need them.

7) What is a Firewall?

It is a security system designed for the network. A firewall is set on the boundaries of any system or network which monitors and controls network traffic. Firewalls are mostly used to protect the system or network from malware, worms, and viruses. Firewalls can also prevent content filtering and remote access.

8) Explain Traceroute

It is a tool that shows the packet path. It lists all the points that the packet passes through. Traceroute is used mostly when the packet does not reach the destination. Traceroute is used to check where the connection breaks or stops or to identify the failure.



```
C:\Users\Guru99 Jayesh>tracert guru99.com

Tracing route to guru99.com [72.52.251.71]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2    12 ms    12 ms    12 ms  abts-mum-dynamic-001.32.170.122.airtelbroadband.in [122.170.32.1]
  3    13 ms    13 ms    14 ms  125.16.168.81
  4   108 ms   109 ms   109 ms  182.79.142.64
  5   108 ms   108 ms   108 ms  213.242.116.161
  6   279 ms   279 ms   279 ms  ae-1-11.bear2.Washington111.Level3.net [4.69.210.178]
  7     *        *        *     Request timed out.
  8   252 ms   250 ms   250 ms  lw-dc2-core2-nexus-eth3-19.rtr.liquidweb.com [209.59.157.204]
  9   265 ms   266 ms   266 ms  lw-dc2-dist4-nexus.rtr.liquidweb.com [209.59.157.85]
 10   269 ms   273 ms   272 ms  host.moneyboats.com [72.52.251.71]

Trace complete.

C:\Users\Guru99 Jayesh>
```

9) Differentiate between HIDS and NIDS.

Parameter	HIDS	NIDS
Usage	HIDS is used to detect the intrusions.	NIDS is used for the network.
What does it do?	It monitors suspicious system activities and traffic of a specific device.	It monitors the traffic of all devices on the network.

10) Explain SSL

SSL stands for Secure Sockets Layer. It is a technology creating encrypted connections between a web server and a web browser. It is used to protect the information in online transactions and digital payments to maintain data privacy.

11) What do you mean by data leakage?

Data leakage is an unauthorized transfer of data to the outside world. Data leakage occurs via email, optical media, laptops, and USB keys.

12) Explain the brute force attack. How to prevent it?

It is a trial-and-error method to find out the right password or PIN. Hackers repetitively try all the combinations of credentials. In many cases, brute force attacks are automated where the software automatically works to login with credentials. There are ways to prevent Brute Force attacks. They are:

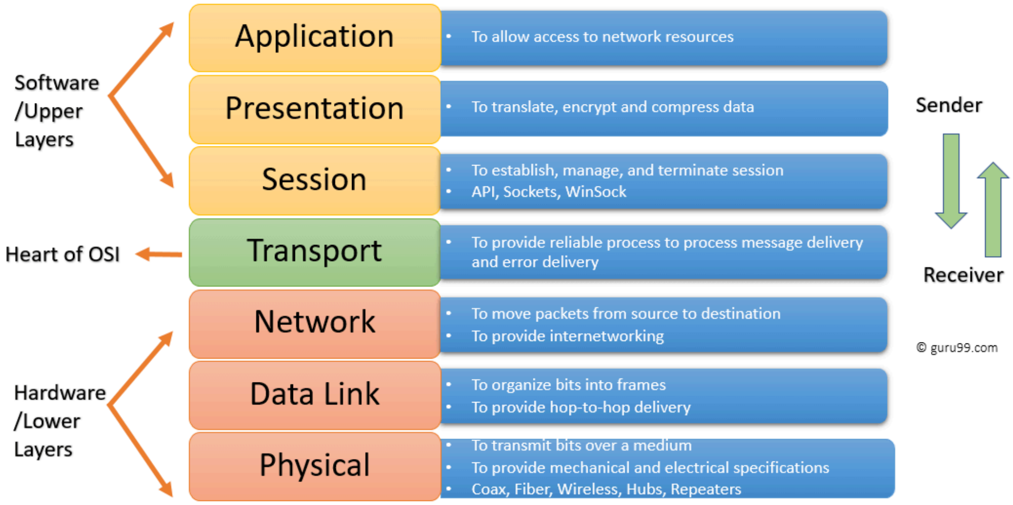
- Setting password length.
- Increase password complexity.
- Set limit on login failures.

13) What is port scanning?

It is the technique for identifying open ports and service available on a specific host. Hackers use port scanning technique to find information for malicious purposes.

14) Name the different layers of the OSI model.

Seven different layers of OSI models are as follows:



Application	To allow access to network resources
Presentation	To translate, encrypt and compress data
Session	To establish, manage, and terminate session API, Sockets, WinSock
Transport	To provide reliable process to process message delivery and error delivery
Network	To move packets from source to destination To provide internetworking
Data Link	To organize bits into frames To provide hop-to-hop delivery
Physical	To transmit bits over a medium To provide mechanical and electrical specifications Coax, Fiber, Wireless, Hubs, Repeaters

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

15) What is a VPN?

VPN stands for Virtual Private Network. It is a network connection method for creating an encrypted and safe connection. This method protects data from interference, snooping, and censorship.

16) What are black hat hackers?

Black hat hackers are people who have a good knowledge of breaching network security. These hackers can generate malware for personal financial gain or other malicious reasons. They break into a secure network to modify, steal, or destroy data so that the network can not be used by authorized network users.

17) What are white hat hackers?

White hat hackers or security specialist are specialized in Penetration testing. They protect the information system of an organization.

18) What are grey hat hackers?

Grey hat hackers are computer hacker who sometimes violate ethical standards, but they do not have malicious intent.

19) How to reset a password-protected BIOS configuration?

There are various ways to reset BIOS password. Some of them are as follows:

- Remove CMOS battery.
- By utilizing the software.
- By utilizing a motherboard jumper.
- By utilizing MS-DOS.

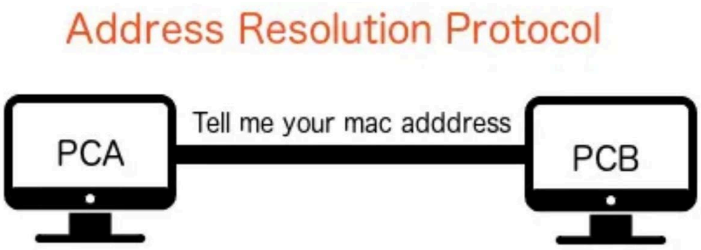
20) What is MITM attack?

A MITM or Man-in-the-Middle is a type of attack where an attacker intercepts communication between two persons. The main intention of MITM is to access confidential information.

21) Define ARP and its working process.

It is a protocol used for finding MAC addresses associated with IPv4 addresses. In simple terms, ARP is used to establish the IP:MAC mapping.

This protocol works as an interface between the OSI network and OSI link layer.



22) Explain Botnet.

It’s a number of internet-connected devices like servers, mobile devices, IoT devices, and PCs that are infected and controlled by malware.

23) What is the main difference between SSL and TLS?

The main difference between these two is that SSL verifies the identity of the sender. SSL helps you to track the person you are communicating to. TLS offers a secure channel between two clients.

24) What is the abbreviation of CSRF?

CSRF stands for Cross-Site Request Forgery.

25) What is 2FA? How to implement it for a public website?

TFA stands for Two Factor Authentication. It is a security process to identify the person who is accessing an online account. The user is granted access only after presenting evidence to the authentication device.

26) Explain the difference between asymmetric and symmetric encryption.

Symmetric encryption requires the same key for encryption and decryption. On the other hand, asymmetric encryption needs different keys for encryption and decryption.

27) What is the full form of XSS?

XSS stands for cross-site scripting.

28) Explain WAF

WAF stands for Web Application Firewall. WAF is used to protect the application by filtering and monitoring incoming and outgoing traffic between web application and the internet.

29) What is hacking?

Hacking is a process of finding weakness in computer or private networks to exploit its weaknesses and gain access.

For example, using password cracking technique to gain access to a system.

30) Who are hackers?

A Hacker is a person who finds and exploits the weakness in computer systems, smartphones, tablets, or networks to gain access. Hackers are well experienced computer programmers with knowledge of computer security.

31) What is network sniffing?

Network sniffing is a tool used for analyzing data packets sent over a network. This can be done by the specialized software program or hardware equipment. Sniffing can be used to:

- Capture sensitive data such as password.
- Eavesdrop on chat messages
- Monitor data package over a network

32) What is the importance of DNS monitoring?

Yong domains are easily infected with malicious software. You need to use DNS monitoring tools to identify malware.

33) Define the process of salting. What is the use of salting?

Salting is that process to extend the length of passwords by using special characters. To use salting, it is very important to know the entire mechanism of salting. The use of salting is to safeguard passwords. It also prevents attackers testing known words across the system.

For example, Hash(“QxLUF1bgIAdeQX”) is added to each and every password to protect your password. It is called as salt.

34) What is SSH?

SSH stands for Secure Socket Shell or Secure Shell. It is a utility suite that provides system administrators a secure way to access the data on a network.

35) Is SSL protocol enough for network security?

SSL verifies the sender’s identity, but it does not provide security once the data is transferred to the server. It is good to use server-side encryption and hashing to protect the server against a data breach.

36) What is black box testing and white box testing?

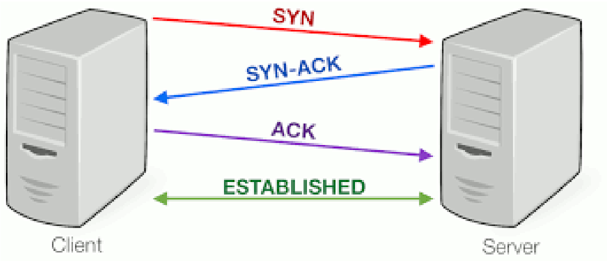
- Black box testing: It is a software testing method in which the internal structure or program code is hidden.
- White box testing: A software testing method in which internal structure or program is known by tester.

37) Explain vulnerabilities in network security.

Vulnerabilities refer to the weak point in software code which can be exploited by a threat actor. They are most commonly found in an application like SaaS (Software as a service) software.

38) Explain TCP Three-way handshake.

It is a process used in a network to make a connection between a local host and server. This method requires the client and server to negotiate synchronization and acknowledgment packets before starting communication.



39) Define the term residual risk. What are three ways to deal with risk?

It is a threat that balances risk exposure after finding and eliminating threats.
Three ways to deal with risk are:

1. Reduce it
2. Avoid it
3. Accept it.

40) Define Exfiltration.

Data exfiltration refers to the unauthorized transfer of data from a computer system. This transmission may be manual and carried out by anyone having physical access to a computer.

41) What is exploit in network security?

An exploit is a method utilized by hackers to access data in an unauthorized way. It is incorporated into malware.

42) What do you mean by penetration testing?

It is the process of checking exploitable vulnerabilities on the target. In web security, it is used to augment the web application firewall.

43) List out some of the common cyber-attack.

Following are the common cyber-attacks which can be used by hackers to damage network:

- Malware
- Phishing
- Password attacks
- DDoS
- Man in the middle
- Drive-by downloads
- Malvertising
- Rogue software

44) How to make the user authentication process more secure?

In order to authenticate users, they have to provide their identity. The ID and Key can be used to confirm the user’s identity. This is an ideal way how the system should authorize the user.

45) Explain the concept of cross-site scripting.

Cross-site scripting refers to a network security vulnerability in which malicious scripts are injected into websites. This attack occurs when attackers allow an untrusted source to inject code into a web application.

46) Name the protocol that broadcast the information across all the devices.

Internet Group Management Protocol or IGMP is a communication protocol that is used in game or video streaming. It facilitates routers and other communication devices to send packets.

47) How to protect email messages?

Use cipher algorithm to protect email, credit card information, and corporate data.

48) What are the risks associated with public Wi-Fi?

Public Wi-Fi has many security issues. Wi-Fi attacks include karma attack, sniffing, war-driving, brute force attack, etc.

Public Wi-Fi may identify data that is passed through a network device like emails, browsing history, passwords, and credit card data.

49) What is Data Encryption? Why it is important in network security?

Data encryption is a technique in which the sender converts the message into a code. It allows only authorized user to gain access.

50) Explain the main difference between Diffie-Hellman and RSA.

Diffie-Hellman is a protocol used while exchanging key between two parties while RSA is an algorithm that works on the basis two keys called private and public key.

51) What is a remote desktop protocol?

Remote Desktop Protocol (RDP) is developed by Microsoft, which provides GUI to connect two devices over a network.

The user uses RDP client software to serve this purpose while other device must run RDP server software. This protocol is specifically designed for remote management and to access virtual PCs, applications, and terminal servers.

52) Define Forward Secrecy.

Forward Secrecy is a security measure that ensures the integrity of unique session key in event that a long term key is compromised.

53) Explain the concept of IV in encryption.

IV stands for the initial vector is an arbitrary number that is used to ensures that identical text encrypted to different ciphertexts. Encryption program uses this number only once per session.

54) Explain the difference between stream cipher and block cipher.

Parameter	Stream Cipher	Block Cipher
How does it work?	Stream cipher operates on small plaintext units	Block cipher works on large data blocks.
Code requirement	It requires less code.	It requires more code.
Usage of key	Key is used only once.	Reuse of key is possible.
Application	Secure Socket layer.	File encryption and database.
Usage	Stream cipher is used to implement hardware.	Block cipher is used to implement software.

55) Give some examples of a symmetric encryption algorithm.

Some examples of symmetric encryption algorithm include DES, RCx, Blowfish

56) What is the abbreviation of ECB and CBC?

The full form of ECB is Electronic Codebook, and the full form of CBC is Cipher Block Chaining.

57) Explain a buffer overflow attack.

Buffer overflow attack is an attack that takes advantage of a process that attempts to write more data to a fixed-length memory block.

58) Define Spyware.

Spyware is a malware that aims to steal data about the organization or person. This malware can damage the organization’s computer system.

59) What is impersonation?

It is a mechanism of assigning the user account to an unknown user.

60) What do you mean by SRM?

SRM stands for Security Reference Monitor provides routines for computer drivers to grant access rights to objects.

61) What is a computer virus?

A virus is a malicious software that is executed without the user's consent. Viruses can consume computer resources, such as CPU time and memory. Sometimes, the virus makes changes in other computer programs and insert its own code to harm the computer system.

A computer virus may be used to:

- Access private data like user id and passwords
- Display annoying messages to the user
- Corrupt data in your computer
- Log the user's keystrokes

62) What do you mean by Authenticode?

Authenticode is a technology that identifies the publisher of Authenticode sign software. It allows users to ensure that the software is genuine and not contain any malicious program.

63) Define CryptoAPI

CryptoAPI is a collection of encryption APIs which allows developers to create a project on a secure network.

64) Explain steps to secure web server.

Follow the following steps to secure your web server:

- Update ownership of file.
- Keep your webserver updated.
- Disable extra modules in the webserver.
- Delete default scripts.

65) What is Microsoft Baseline Security Analyzer?

Microsoft Baseline Security Analyzer or MBSA is a graphical and command-line interface that provides a method to find missing security updates and misconfigurations.

66) What is Ethical hacking?

Ethical hacking is a method to improve the security of a network. In this method, hackers fix vulnerabilities and weakness of computer or network. Ethical hackers use software tools to secure the system.

67) Explain social engineering and its attacks.

Social engineering is the term used to convince people to reveal confidential information.

There are mainly three types of social engineering attacks: 1) Human-based, 2) Mobile-based, and 3) Computer-based.

- Human-based attack: They may pretend like a genuine user who requests higher authority to reveal private and confidential information of the organization.
- Computer-based attack: In this attack, attackers send fake emails to harm the computer. They ask people to forward such emails.
- Mobile-based attack: Attacker may send SMS to others and collect important information. If any user downloads a malicious app, then it can be misused to access authentication information.

68) What are IP and MAC Addresses?

IP Address is the acronym for Internet Protocol address. An internet protocol address is used to uniquely identify a computer or device such as printers, storage disks on a computer network.

MAC Address is the acronym for Media Access Control address. MAC addresses are used to uniquely identify network interfaces for communication at the physical layer of the network.

69) What do you mean by a worm?
A Worm is a type of malware which replicates from one computer to another.

70) State the difference between virus and worm

Parameter	Virus	Worm
How do they infect a computer?	It inserts malicious code into a specific file or program.	Generate it's copy and spread using email client.
Dependency	Virus need a host program to work	They do not require any host to function correctly.
Linked with files	It is linked with .com, .xls, .exe, .doc, etc.	It is linked with any file on a network.
Affecting speed	It is slower than worm.	It is faster compared to a virus.

71) Name some tools used for packet sniffing.

Following are some tools used for packet sniffing.

- Tcpdump
- Wireshark
- Kismet
- NetworkMiner
- Dsniff

72) Explain antivirus sensor systems

Antivirus is a software tool that is used to identify, prevent, or remove the viruses present in the computer. They perform system checks and increase the security of the computer regularly.

73) List out the types of sniffing attacks.

Various types of sniffing attacks are:

- Protocol Sniffing
- Web password sniffing
- Application-level sniffing
- TCP Session stealing
- LAN Sniffing
- ARP Sniffing/Spoofing

74) What is a distributed denial-of-service attack (DDoS)?

It is an attack in which multiple computers attack website, server, or any network resource.

75) Explain the concept of session hijacking.

TCP session hijacking is the misuse of a valid computer session. IP spoofing is the most common method of session hijacking. In this method, attackers use IP packets to insert a command between two nodes of the network.

76) List out various methods of session hijacking.

Various methods of session hijacking are:

- Using packet Sniffers
- Cross-Site Scripting (XSS Attack)
- IP Spoofing
- Blind Attack

77) What are Hacking Tools?

Hacking Tools are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers, and networks. There are varieties of such tools available on the market. Some of them are open source, while others are a commercial solution.

78) Explain honeypot and its Types.

Honeypot is a decoy computer system which records all the transactions, interactions, and actions with users.

Honeypot is classified into two categories: 1) Production honeypot and 2) Research honeypot.

- Production honeypot: It is designed to capture real information for the administrator to access vulnerabilities. They are generally placed inside production networks to increase their security.
- Research Honeypot: It is used by educational institutions and organizations for the sole purpose of researching the motives and tactics of the back-hat community for targeting **different networks.**

79) Name common encryption tools.

Tools available for encryptions are as follows:

- RSA
- Twofish
- AES
- Triple DES

80) What is Backdoor?

It is a malware type in which security mechanism is bypassed to access a system.

81) Is it right to send login credentials through email?

It is not right to send login credentials through email because if you send someone userid and password in the mail, chances of email attacks are high.

82) Explain the 80/20 rule of networking?

This rule is based on the percentage of network traffic, in which 80% of all network traffic should remain local while the rest of the traffic should be routed towards a permanent VPN.

83) Define WEP cracking.

It is a method used for a security breach in wireless networks. There are two types of WEP cracking: 1) Active cracking and 2) Passive cracking.

84) What are various WEP cracking tools?

Well known WEP cracking tools are:

- Aircrack
- WebDecrypt
- Kismet
- WEPCrack

85) What is a security auditing?

Security auditing is an internal inspection of applications and operating systems for security flaws. An audit can also be done via line by line inspection of code.

86) Explain phishing.

It is a technique used to obtain a username, password, and credit card details from other users.

87) What is Nano-scale encryption?

Nano encryption is a research area which provides robust security to computers and prevents them from hacking.

88) Define Security Testing?

Security Testing is defined as a type of Software Testing that ensures software systems and applications are free from any vulnerabilities, threats, risks that may cause a big loss.

89) Explain Security Scanning.

Security scanning involves identifying network and system weaknesses and later provides solutions for reducing these risks. This scanning can be performed for both Manual as well as Automated scanning.

90) Name the available hacking tools.

Following is a list of useful hacking tools.

- Acunetix
- WebInspect
- Probably
- Netsparker

- Angry IP scanner:
- Burp Suite
- Savvius

91) What is the importance of penetration testing in an enterprise?

Here are two common applications of Penetration testing.

- Financial sectors like stock trading exchanges, investment banking, want their data to be secured, and penetration testing is essential to ensure security.
- In case if the software system is already hacked and the organization would like to determine whether any threats are still present in the system to avoid future hacks.

92) What are the disadvantages of penetration testing?

Disadvantages of penetration testing are:

- Penetration testing cannot find all vulnerabilities in the system.
- There are limitations of time, budget, scope, skills of penetration testers.
- Data loss and corruption
- Down Time is high which increase costs

93) Explain security threat

Security threat is defined as a risk which can steal confidential data and harm computer systems as well as organization.

94) What are physical threats?

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

95) Give examples of non-physical threats

Following are some examples of non-physical threat:

- Loss of sensitive information
- Loss or corruption of system data
- Cyber security Breaches
- Disrupt business operations that rely on computer systems
- Illegal monitoring of activities on computer systems

96) What is Trojan virus?

Trojan is a malware employed by hackers and cyber-thieves to gain access to any computer. Here attackers use social engineering techniques to execute the trojan on the system.

97) Define SQL Injection

It is an attack that poisons malicious SQL statements to database. It helps you to take benefit of the design flaws in poorly designed web applications to exploit SQL statements to execute malicious SQL code. In many situations, an attacker can escalate SQL injection attack in order to perform other attack, i.e. denial-of-service attack.

98) List security vulnerabilities as per Open Web Application Security Project (OWASP).

Security vulnerabilities as per open web application security project are as follows:

- SQL Injection
- Cross-site request forgery
- Insecure cryptographic storage
- Broken authentication and session management
- Insufficient transport layer protection
- Unvalidated redirects and forwards
- Failure to restrict URL access

99) Define an access token.

An access token is a credential which is used by the system to check whether the API should be granted to a particular object or not.

100) Explain ARP Poisoning

ARP (Address Resolution Protocol) Poisoning is a type of cyber-attack which is used to convert IP address to physical addresses on a network device. The host sends an ARP broadcast on the network, and the recipient computer responds back with its physical address.

ARP poisoning is sending fake addresses to the switch so that it can associate the fake addresses with the IP address of a genuine computer on a network and hijack the traffic.

101) Name common types of non-physical threats.

Following are various types of non-physical threats:

- Trojans
- Adware
- Worms
- Spyware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Virus
- Key loggers
- Unauthorized access to computer systems resources
- Phishing

102) Explain the sequence of a TCP connection.

The sequence of a TCP connection is SYN-SYN ACK-ACK.

103) Define hybrid attacks.

Hybrid attack is a blend of dictionary method and brute force attack. This attack is used to crack passwords by making a change of a dictionary word with symbols and numbers.

104) What is Nmap?

Nmap is a tool which is used for finding networks and in security auditing.

105) What is the use of EtterPeak tool?

EtterPeak is a network analysis tool that is used for sniffing packets of network traffic.

106) What are the types of cyber-attacks?

There are two types of cyberattacks: 1) Web-based attacks, 2) System based attacks.

107) List out web-based attacks

Some web-based attacks are: 1) SQL Injection attacks, 2) Phishing, 3) Brute Force, 4) DNS Spoofing, 4) Denial of Service, and 5) Dictionary attacks.

108) Give examples of System-based attacks

Examples of system-based attacks are: Virus, Backdoors, Bots, Worm

109) List out the types of cyber attackers

There are four types of cyber attackers. They are: 1) cybercriminals, 2) hacktivists, 3) insider threats, 4) state-sponsored attackers.

110) Define accidental threats

They are threats that are accidently done by organization employees. In these threats, an employee unintentionally deletes any file or shares confidential data with outsiders or a business partner going beyond the policy of the company.

SET-II OF QUESTION FOR BEGINNERS

1. What is cybersecurity, and why is it important?

Cybersecurity protects computer systems, networks, and data from theft, damage, or unauthorized access. It's important to safeguard sensitive information, maintain privacy, prevent financial losses, and protect critical infrastructure from cyber threats.

2. Define the terms Virus, Malware, and Ransomware.

- Virus: A program that replicates itself and spreads to other files or systems, often causing harm.
- Malware: A broader term encompassing any malicious software that disrupts or gains unauthorized access to computer systems.
- Ransomware: A malicious software encrypting files or computer systems and requesting a ransom for their decryption.

3. Explain the difference between a Threat, Vulnerability, and Risk in cybersecurity.

- Threat: Any potential danger or harmful event that can exploit vulnerabilities and negatively impact security.
- Vulnerability: Weaknesses or gaps in security measures that threats can exploit.
- Risk: The probability of a threat capitalizing on a vulnerability and the potential consequences or damage it may inflict.

4. What is Phishing? Provide an example.

Phishing: A cyberattack in which malicious actors employ deceptive emails or messages to deceive individuals into disclosing sensitive information.

Example: An email claiming to be from a bank, requesting the recipient to provide their login credentials by clicking a link that leads to a fake website.

5. How do firewalls protect network security?

Firewalls serve as protective barriers, overseeing and screening both inbound and outbound network traffic in accordance with established security regulations.

They block unauthorized access and help prevent malicious data from entering or leaving a network.

6. What is a VPN and why is it used?

A Virtual Private Network encrypts and secures internet connections, ensuring privacy and anonymity.

It protects data from eavesdropping, accesses restricted content, and enhances public Wi-Fi security.

7. Explain the concept of a secure Password.

A secure password is complex, lengthy, and difficult to guess.

It comprises a combination of uppercase and lowercase letters, numbers, and special characters, with the requirement that this combination should be distinct for every individual account.

8. What are the common techniques for securing a computer network?

Techniques include using strong passwords, regular updates and patch management, implementing firewalls, using intrusion detection systems, and conducting security audits.

9. What is two-factor authentication, and why is it important?

Two-factor authentication enhances security by necessitating users to furnish two distinct forms of verification, typically a password and a temporary code, thereby bolstering protection.

It's important because even if a password is compromised, unauthorized access is prevented without the second factor.

10. Define the terms Encryption and Decryption.

Encryption: Converting plaintext data into a coded format to protect it from unauthorized access.

Decryption: Converting encrypted data back into its original, readable form.

11. What is SSL encryption?

SSL (Secure Sockets Layer) encryption is a protocol that ensures secure data transmission between a user's web browser and a website server, protecting data during transit.

12. What is the difference between IDS and IPS?

IDS (Intrusion Detection System): Monitors network traffic and generates alerts when suspicious activity is detected.

IPS (Intrusion Prevention System): Not only detects but also actively blocks or prevents suspicious network activity.

13. Explain what a security audit Is.

A security audit systematically evaluates an organization's information systems and security policies to assess their effectiveness, identify vulnerabilities, and recommend improvements.

14. What steps would you take if you discovered a security breach?

Isolate affected systems, contain the breach, notify relevant parties, investigate the incident, remediate vulnerabilities, and implement measures to prevent future breaches.

15. What is social engineering? Give an example.

Social engineering manipulates individuals to disclose confidential information or perform actions for malicious purposes.

Example: Pretending to be a trusted colleague and asking for login credentials over the phone.

16. What are cookies in a web browser?

Cookies are stored by websites on a user's device. They are used to track user preferences, session information, and provide a personalized browsing experience.

17. What is a DDoS attack and how does it work?

A Distributed Denial of Service (DDoS) attack inundates a target server or network with excessive traffic originating from numerous sources, making it inaccessible to genuine users.

18. Explain what a security policy is.

A security policy comprises a collection of formally documented regulations, recommendations, and protocols that delineate an organization's methods to safeguard its information, assets, and technological resources.

19. What is the difference between symmetric and asymmetric encryption?

Symmetric Encryption uses a similar key for encryption and decryption.

Asymmetric Encryption employs a pair of keys, one public and one private. Data that is encrypted with one key can only be deciphered using the complementary key.

20. How can you prevent a Man-In-The-Middle attack?

Use secure communication protocols, verify digital certificates, and avoid public Wi-Fi for sensitive transactions. Implementing strong encryption also helps.

21. What is a honeypot in cybersecurity?

A honeypot is a decoy system or network designed to attract attackers. It allows security professionals to study their tactics, techniques, and motivations.

22. Explain the concept of a digital signature.

A digital signature employs cryptographic methods to confirm the genuineness and unaltered state of a digital document or message, assuring both the sender's authenticity and the content's integrity.

23. What is a brute force attack?

It involves attackers employing a trial-and-error approach to find a password or encryption key by systematically testing every conceivable combination until they discover the correct one.

24. What are the common cyber threats today?

Common threats include malware, ransomware, phishing, DDoS attacks, insider threats, and zero-day vulnerabilities.

25. What is the role of patch management in maintaining security?

Patch management regularly applies updates and patches to software and systems to fix security vulnerabilities. It's crucial for preventing the exploitation of known weaknesses by attackers.

INTERMEDIATE LEVEL QUESTIONS

1. Explain the concept of Public Key Infrastructure (PKI).
PKI is a system of cryptographic techniques that enables secure communication over an insecure network. A public key and a private key pair are employed for various cryptographic operations such as encryption, decryption, the creation of digital signatures, and the validation of public keys through the use of certificate authorities (CAs) to ensure their authenticity.

2. What are the key elements of a strong security policy?
A strong security policy includes elements like access control, encryption, regular updates, user training, incident response plans, and compliance with relevant regulations.

3. How does a rootkit work and how would you detect it?
A rootkit is malicious software that gives attackers unauthorized access to a computer or network. Detection involves using specialized anti-rootkit tools and monitoring for suspicious system behavior.

4. Explain cross-site scripting and SQL injection.
XSS involves injecting malicious scripts into web applications, which can compromise user data. SQL Injection exploits vulnerabilities in SQL queries to manipulate a database. Both are forms of web application vulnerabilities.

5. What is a zero-day vulnerability?
It refers to a security vulnerability present in software or hardware that is undisclosed to the vendor and lacks an existing solution. This loophole can be leveraged by malicious actors before a remedy is created.

6. Discuss the ISO 27001/27002 standards.
It is a framework for information security management systems (ISMS), while ISO 27002 provides guidelines for implementing security controls and practices within an organization.

7. How do threat detection systems work?
Threat detection systems monitor network traffic and system logs to identify suspicious activities or potential security threats using predefined rules and machine learning algorithms.

8. Explain the principles of ethical hacking.
Ethical hacking involves testing systems and networks for vulnerabilities to strengthen security. Principles include obtaining proper authorization, maintaining confidentiality, and responsible disclosure of findings.

9. What are the different types of network security?
Network security includes perimeter security, firewall protection, intrusion detection systems, VPNs, and network segmentation to safeguard data and resources.

10. Discuss the concept of risk assessment in cybersecurity.
Risk assessment in cybersecurity involves identifying, assessing, and prioritizing potential threats and vulnerabilities to make informed decisions on security measures.

11. What is incident response, and how is it managed?
Incident response encompasses a methodical strategy for handling and diminishing security incidents, encompassing key phases such as preparation, detection, containment, eradication, recovery, and knowledge acquisition.

12. Explain the principle of least privilege.
The Least Privilege principle limits the access of users and processes to the bare minimum required for their specific tasks, thereby minimizing the potential for unauthorized actions.

13. How does Secure Socket Layer (SSL) work?
SSL protocol ensures secure data transmission between web browsers and servers using encryption, authentication, and data integrity checks.

14. What is network sniffing?
Network sniffing is the practice of intercepting and analyzing network traffic to gather information, potentially for malicious purposes. It can be used for monitoring or attacks.

15. Discuss the importance of disaster recovery planning in cybersecurity.
Disaster recovery planning encompasses the proactive preparation and responsive actions required to safeguard against data loss or system failures, ultimately ensuring the uninterrupted operation of a business.

16. What is a Security Information and Event Management (SIEM) System?
SIEM systems gather, correlate, and scrutinize security-relevant data from diverse origins to identify and react to security events.

17. How do you manage cryptographic keys?
Cryptographic keys should be securely generated, stored, rotated, and protected to maintain the confidentiality and integrity of encrypted data.

18. What are the common methods for secure data disposal?
Common methods include data shredding, overwriting, degaussing, and physical destruction to ensure that sensitive information cannot be recovered from storage media.

19. Explain the concept of endpoint security.
Endpoint security focuses on securing individual devices (endpoints) like computers and mobile devices by using antivirus, anti-malware, and intrusion detection systems.

20. Discuss the role of artificial intelligence in cybersecurity.
AI is used for threat detection, pattern recognition, and anomaly detection to improve cybersecurity defenses and automate incident response.

21. What are the challenges in cloud security?
Challenges include data breaches, compliance, data loss prevention, and securing shared responsibility models in cloud environments.

22. How do penetration testing and vulnerability assessments differ?
Penetration testing replicates real-world attack scenarios to discover vulnerabilities, whereas vulnerability assessments concentrate on scanning systems to detect recognized weaknesses.

23. What is a Security Operations Center (SOC)?
SOC is a centralized team responsible for real-time monitoring, detecting, and responding to security incidents.

24. Discuss the importance of compliance in cybersecurity.
Compliance ensures that an organization follows relevant laws and regulations, helping protect data and avoid legal consequences.

25. What Is multi-factor authentication and how does it enhance security?
MFA bolsters security by necessitating users to furnish multiple authentication factors, typically a combination of something they possess (e.g., a mobile token) and something they are aware of (e.g., a password).

ADVANCED LEVEL QUESTIONS

1. Discuss the challenges and strategies of securing IoT devices.

- Challenges: Device diversity, limited resources, and vulnerabilities.
- Strategies: Regular updates, strong authentication, network segmentation, and IoT security frameworks.

2. Explain Advanced Persistent Threats (APT).
APTs are long-term, targeted cyberattacks by skilled adversaries. They use stealth, persistence, and sophisticated techniques to breach systems.

3. Discuss the role of blockchain in cybersecurity.
Blockchain can enhance security through decentralized consensus, data integrity, and immutable records. It's used in secure transactions and identity management.

4. How do you approach securing a large, distributed network?
Employ segmentation, strong access controls, regular audits, and network monitoring to protect against threats across a vast network.

5. What is the importance of forensics in cybersecurity?
Forensics helps investigate incidents, gather evidence, and understand attack vectors, aiding in incident response and legal actions.

6. Discuss the intricacies of network protocol security.
Secure protocols are essential for data confidentiality and integrity. Use encryption and authentication, and keep protocols updated to mitigate risks.

7. How do you manage security in a DevOps environment?
Implement security into the development pipeline with automation, continuous monitoring, and collaboration between development and security teams.

8. Explain the concept of micro-segmentation in network security.
Micro-segmentation isolates network segments for finer control and security. It limits the lateral movement of threats within a network.

9. Discuss the challenges of securing big data environments.
Challenges include data volume and diversity. Strategies involve encryption, access controls, monitoring, and data classification.

10. What are your strategies for managing supply chain risks in cybersecurity?
Assess third-party vendors, enforce security standards, conduct audits, and maintain a supply chain risk management program.

11. Explain the concept of container security.
Secure containerized applications with image scanning, access controls, and runtime protection to prevent vulnerabilities.

12. How do you ensure compliance with international data protection laws (like GDPR)?
Implement data protection policies, conduct privacy impact assessments, and ensure compliance with consent and data subject rights.

13. Discuss the future trends in cybersecurity.
Trends include AI/ML for threat detection, zero-trust architecture, cloud security, and increased focus on IoT and 5G security.

14. What are the ethical considerations in cybersecurity?
Ethical concerns involve privacy, responsible disclosure, and avoiding harm to individuals and organizations.

15. How do you measure the effectiveness of a cybersecurity program?
Use metrics like risk assessments, incident response times, and security posture evaluations to measure program effectiveness.

16. Discuss the challenges in securing wireless networks.
Challenges include rogue access points and eavesdropping. Solutions include strong encryption, network monitoring, and user education.

17. What is quantum cryptography and its implications for security?
Quantum cryptography uses quantum mechanics to secure communication. It has the potential to resist quantum attacks, ensuring long-term security.

18. Explain the concept of federated identity management.
Federated identity allows users to access multiple systems with a single set of credentials, enhancing convenience and security.

19. What are the latest developments in cybersecurity threats?
Threats evolve with new attack vectors, such as supply chain attacks, ransomware, and AI-driven attacks.

20. How do you manage security in a hybrid cloud environment?
Secure hybrid cloud environments with consistent security policies, identity management, and data protection across on-premises and cloud resources.

21. Discuss the impact of artificial intelligence on cybersecurity threats.
AI can automate threat detection, enhance incident response, and improve security analytics. However, it can also be exploited by attackers.

22. What is the role of machine learning in detecting cyber threats?
ML algorithms analyze large datasets to detect anomalies and patterns associated with cyber threats, enabling proactive security measures.

23. Explain the concept of threat intelligence and its application.
Threat intelligence is the collection and analysis of data to identify and respond to emerging threats, enabling proactive cybersecurity.

24. What strategies would you implement for securing mobile applications?
Secure mobile apps with encryption, code reviews, secure APIs, and regular updates to protect against vulnerabilities and data breaches.

25. Discuss the challenges and solutions in endpoint detection and response (EDR).
EDR solutions monitor and respond to endpoint threats in real-time, providing visibility and incident response capabilities.