A Document series by VIEH Group

Cybersecurity interview Q&A

Be interview ready with our guide

V.I.E.H GROUP

Think Secure, Think VIEH

Disclaimer

Dear readers,
This document is provided by VIEH Group for educational purposes only. While we strive for accuracy and reliability, we make no warranties or representations regarding the completeness, accuracy, or usefulness of the information presented herein. Any reliance you place on this document is at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. We acknowledge and appreciate the contribution of the source person.

also,
This document is not created by a professional content writer so any mistake and error is a part of great design

Happy learning !!!

This document is fully credited to **Unknown,** whose exceptional insights elevate its value. Their contribution is deeply appreciated, underscoring their significant role in its creation.

Our newsletter: **Cyber Arjun**

Scan QR:

Cyber Security Interview Questions & Answers

1) What is Cyber Security?

Cyber security is the process of protection of hardware, software and data from the hackers. The primary purpose of implementing these cyber security techniques is to protect against different cyberattacks such as changing, accessing or destroying sensitive data.

2) What are The Fundamental Elements of Cyber Security?

Following are the main elements of cyber security:

- Information security
- End-user education
- Operational security
- Application security
- Network security
- Business continuity planning

3) What are The Main Advantages of Cyber Security?

- Protects the business against unauthorized access including ransomware, social engineering, malware and phishing.
- Protects end-users and improve the business continuity management
- Improves stakeholder confidence
- Provide adequate protection for both data as well as networks
- Increase recovery time after any breach

4) What Do You Means By Cryptography?

Cryptography is the technique which is used to protect the confidential information from third parties called adversaries. It allows both sender and receiver of any message to read its details.

5) What is The Main Difference between IDS and IPS?

As the name indicates, IDS (Intrusion Detection System) detects the intrusions and an administrator prevent the intrusion carefully. Whereas in the IPS (Intrusion Prevention System), the system finds the intrusion and prevent it for better protection.

6) Explain The CIA Model?

CIA (Confidentiality, Integrity, and Availability) is a common model that is used to develop a security policy. It consists of the following concepts:

- Confidentiality: Ensure the confidential and private data is accessed only by the authorized users
- Integrity: It means the information is in the right format
- Availability: Ensure the data and other required resources are available to those users who need them

7) Define The Firewall?

In simple words, the firewall is a network security device which is mainly designed to monitor incoming and outgoing traffic and blocks data based on the security rules. Firewalls are considered the best option to protect the network from worms, malware, viruses, remote access and content filtering.

8) What is Traceroute and How Can We Check It?

Traceroute is the network diagnostic tool which is used to track the real path of any data packet on an IP address from its source to destination. It reports the all IP addresses of routers and records the time taken for each hop. Traceroute is mostly used to check out the connection breaks to identify the point of failure.

Go to command prompt (cmd), write “tracert” and enter any domain name after a single space as you can view in the picture given below:

9) What is The Difference between HIDS and NIDS?

Parameter	HIDS	NIDS
Usage	Detect the intrusions	Used for the network
Monitoring	It monitors suspicious system activities and traffic of any specific device.	It monitors the traffic of
Performance	Must be installed on every host	It can monitor multiple h

10) What is SSL and Why We Need To Use It?

SSL (Secure Sockets Layer) is a technology used to create encrypted connections between web servers and web browsers. It is now compulsory for every website to be ranked on the first page of google and commonly used to protect online transactions, user’s data and digital payments.

11) Define Data Leakage?

It is the name of unauthorized transmission of data from a network (within the organization) to an external network or destination. Data leakage can occur via email, optical media, USB keys or laptops.

12) What is The Brute Force Attack and How to Prevent it?

The brute force attack is based on trial-and-error to guess login information, encryption keys, or PIN. In this case, hackers make all the possible ways and try

one by one to guess the credentials. Brute force attacks are automated and use a password dictionary that contains millions of words that can be used as a password. So, you can try to minimize the brute force risk by adopting the following ways:

- Set password length
- Use a complex password
- Set limits on login failures

13) Define Port Scanning?

Port scanning is the name of identification of the open ports and services available on any particular host. So, attackers use this technique to find out information for malicious purposes.

14) Enlist The Names of OSI Model Layers

There are seven layers of OSI Model:

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 (Virtual Private Network) is a network connection method that is used for creating a secure and encrypted connection. VPN protects you from the snooping,

censorship and interference. Virtual Private Networks secure the public internet connection with the help of encryption techniques and provide shielding to your online activity from cybercriminals and even your own Internet Service Provider.

16) Who are The Black Hat Hackers?

Black hat hackers are those people who have good knowledge of breaching the network security and they are able to generate malware for personal financial gain or malicious activities. They are clever and break into a network to modify or destroy data and make it unavailable for authorized users.

17) Who are White Hat Hackers?

White hat hackers are also known as security specialists who are specialized in penetration testing and help the organization to protect their confidential and secure information from attackers.

18) Who are Grey Hat Hackers?

It is the combination of both white and black hat hacking techniques in which the grey hat hackers sometimes violate ethical standards but they don't have any malicious intent.

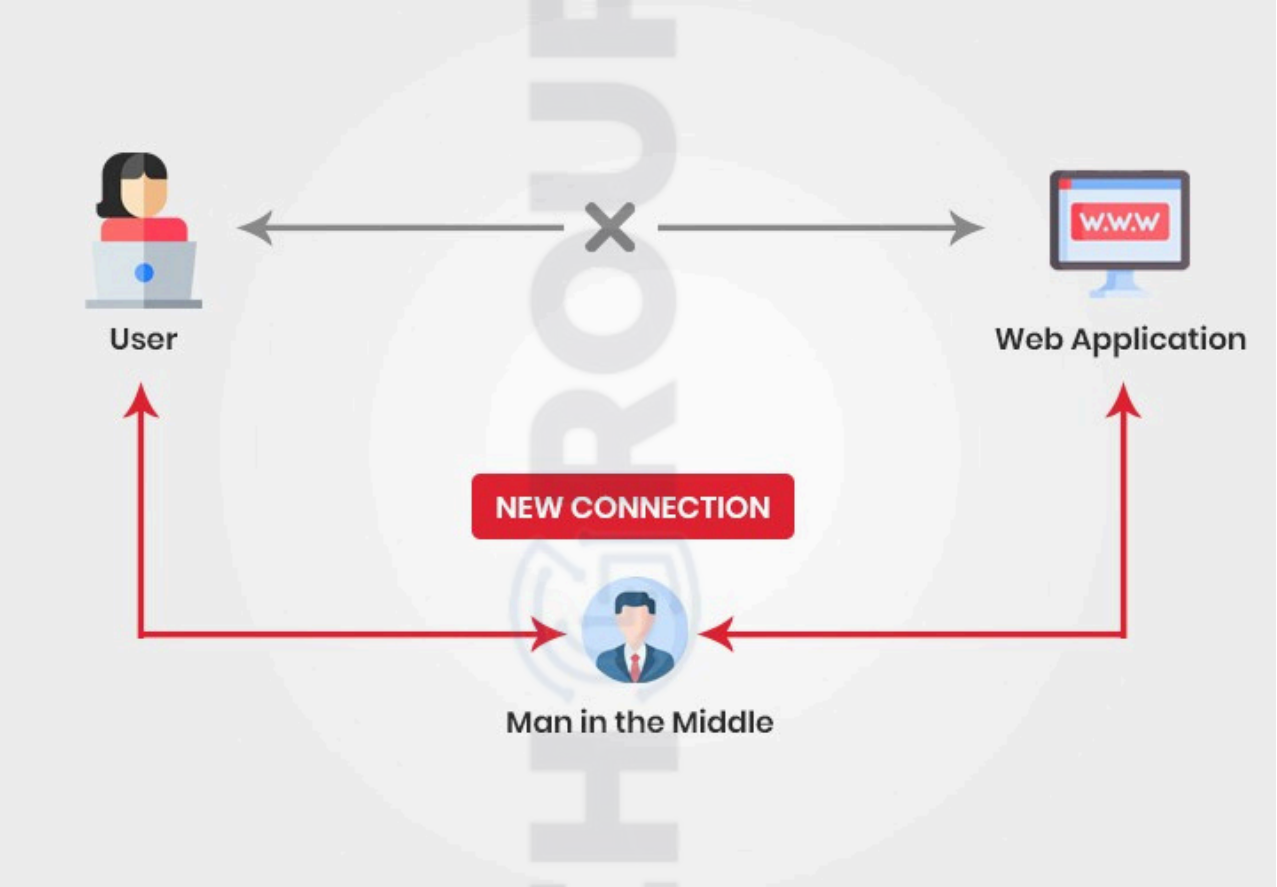
19) How To Reset The Password-protected BIOS Configuration?

There are different ways to reset the BIOS password but few of them are given below:

- Remove CMOS battery
- By utilizing the software
- Using a motherboard jumper

- By utilizing MS-DOS

20) Do You Know About MITM Attack?



MITM (Man In The Middle) is a type of attack in which the attacker intercepts the communication between two networks or persons. MITM is worked on the primary intent to access confidential information.

21) What is ARP and How it works?

ARP is a protocol that works as an interface between the OSI network and OSI link layer and used to find out the MAC address associated with IPv4 address.

22) Define Botnet

A botnet is the number of all internet-connected devices like laptops, servers, IoT, mobile devices and PCs that are controlled or infected by malware.

23) What are The Major Differences Between SSL and TLS?

TLS is a secure channel between two clients, whereas SSL helps to track the person we are communicating with because it verifies the sender's identity.

24) What is The Abbreviation of CSRF?

Cross-Site Request Forgery

25) What is 2FA? How To Implement It For A Public Website?

2FA stands for two-factor authentication and it is a security process that is used to identify the person who is accessing an online account. The user will get access after giving evidence to the authentication device.

26) What Is The Difference Between Asymmetric And Symmetric Encryption?

Asymmetric encryption uses a different key for encryption and decryption, whereas symmetric requires the same key for both encryption and decryption.

27) XSS Stands For?

cross-site scripting

28) Do You Know About WAF?

Web Application Firewall (WAF) is used to protect the application by filtering and monitoring all incoming and outgoing traffic between the application and internet.

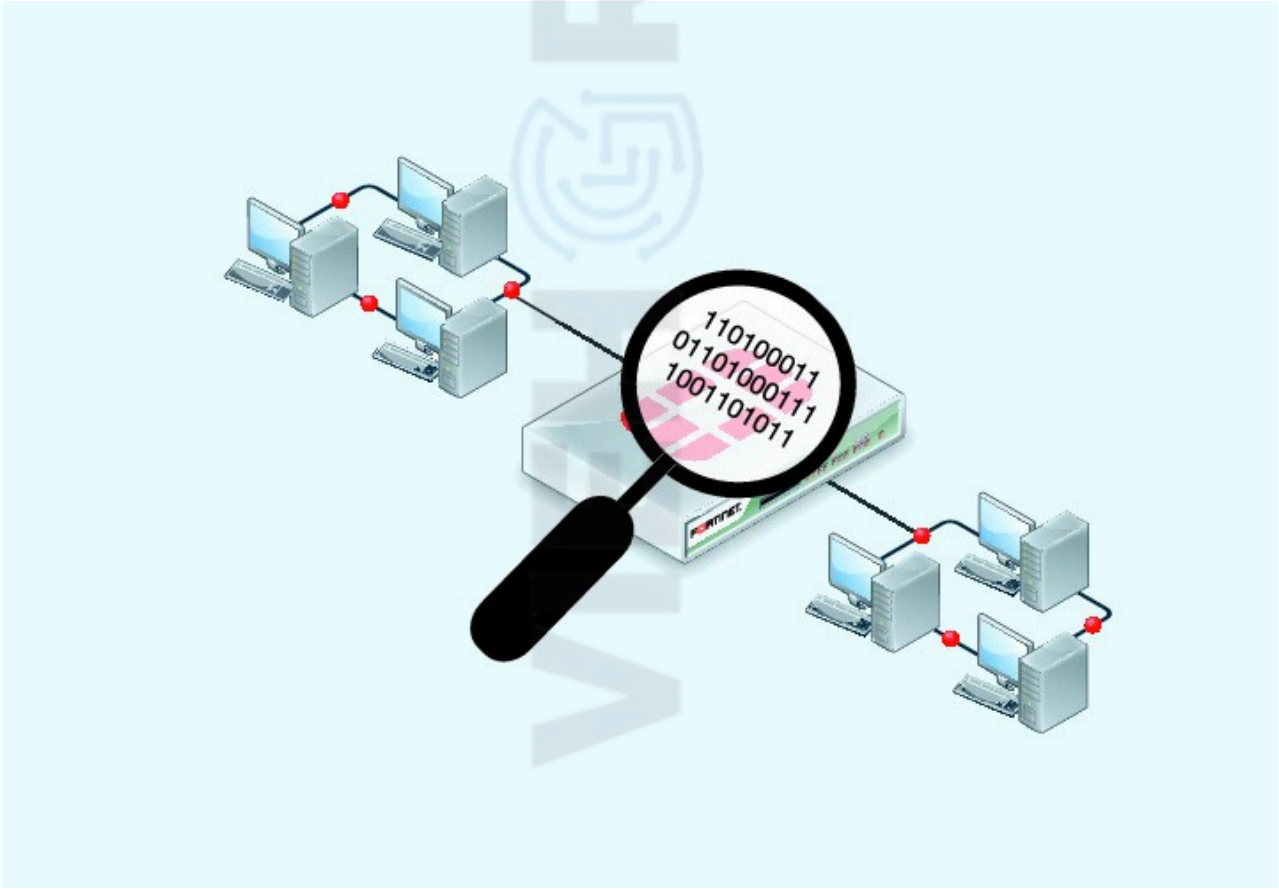
29) What is Hacking?

Hacking is a technique used to find out weaknesses in the private network or computer to exploit its weaknesses and gain access. In simple words, it is the name of using password cracking techniques to gain access to the system.

30) Who are The Hackers?

Hackers are those people who find and exploit the weakness in any network or computing device to gain access. They are experienced programmers with a great knowledge of computer security.

31) What is Network Sniffing?



It is a tool used to analyze data packets sent over a network using specialized software and hardware equipment. Sniffing can be used for:

- Capturing sensitive and confidential data such as password
- Eavesdropping on chat messages
- Monitoring data package over a network

32) Why DNS Monitoring Is Important?

Newly registered domains are easily infected with malicious software, so the DNS monitoring tools are used to identify malware.

33) What Is The Process Of Salting And Why It Is Used?

Salting is a process in which passwords length is extended using special characters. In order to use it more efficiently, you need to understand the entire mechanism of salting. It is an efficient way to safeguard your passwords because it also prevents attackers from testing known words across the system. For example, ("QxLUF1bgIAdeQX") is added to each password for the protection of passwords.

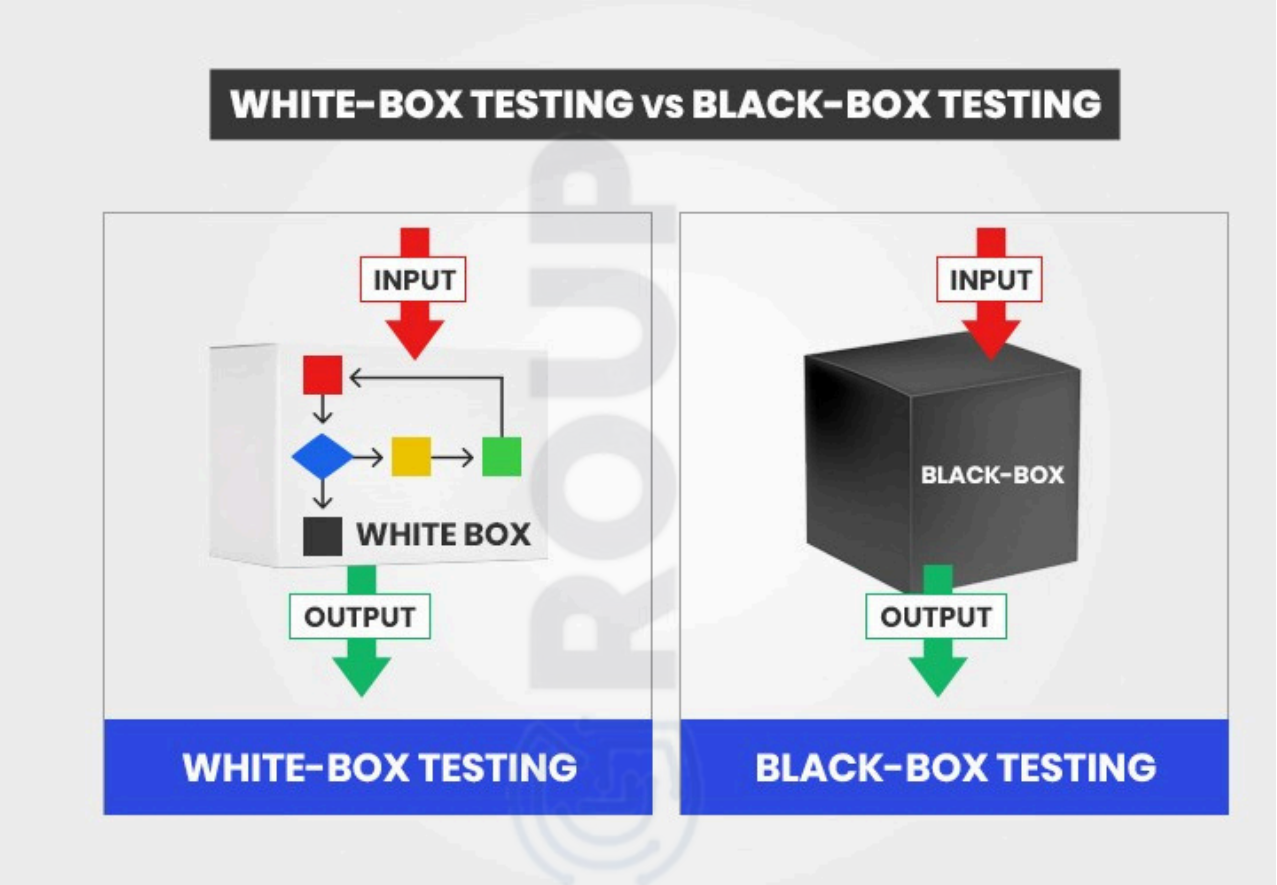
34) What is SSH?

Secure Socket Shell (also known as Secure Shell) is a utility suite which is used by the system administrators to get a secure way to access the data on a network.

35) Is SSL Protocol enough For Network Security?

SSL is not an all-in-one security solution because it does not provide security once the data is transferred to the server. So, it is a proactive approach to use server-side encryption and hashing to protect against any data breach.

36) Define Black Box Testing And White Box Testing?



- Black box testing: It is a software testing technique in which the internal structure or program code of any application is hidden.
- White box testing: It is a software testing way in which internal structure or program of an application is known by the tester.

37) Explain Vulnerabilities In Network Security?

Vulnerabilities refer to any weak point in the applications or software code that can be exploited by an attacker. It is commonly found in SaaS (Software as a Service) applications.

38) What Is TCP Three-way handshake?

The three-way handshake is the process to make a connection between localhost and sever in the network. This process requires the client and server to exchange the synchronization and acknowledgement packets before the actual communication of data.

39) What Is Residual Risk and How To Deal With It?

Residual risk is a threat that balances the risk exposure after eliminating threats, so we can deal with the risk by choosing the following ways:

1.Reduce it
2.Avoid it

3.Accept it

40) Can You Define Exfiltration?

It is the name of unauthorized data transfer from a computer system. This transmission may be carried out by anyone having physical access to computing devices.

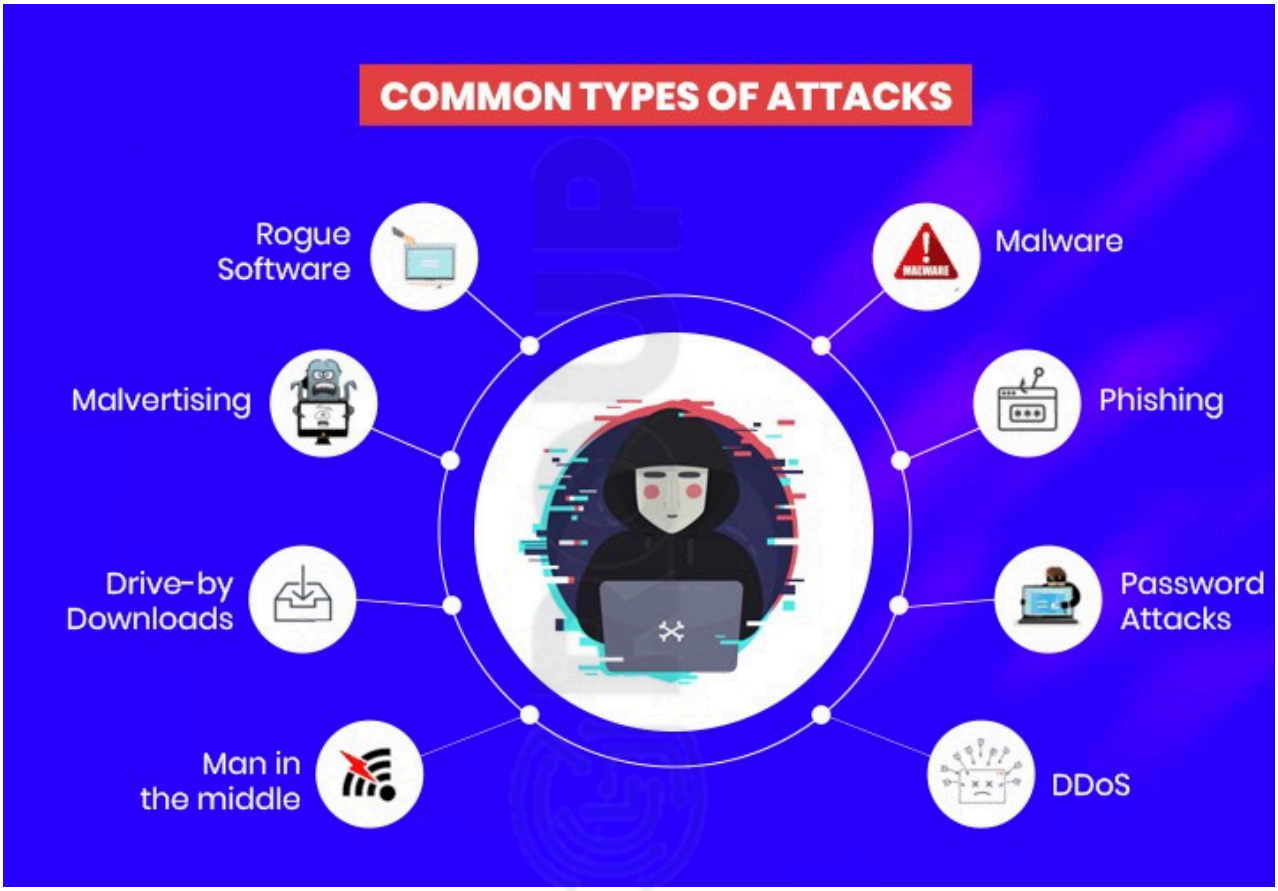
41) Do You Know About Exploit in Network Security?

It is a method used by hackers to access data in an unauthorized way. Exploit is incorporated into malware.

42) What is Penetration Testing?

Penetration testing is the name of checking exploitable vulnerabilities on the target. It is used to augment the web application firewall in web security.

43) Enlist The Most Common Cyber-Attacks?



When you are preparing cyber security interview questions and answers, then be prepared about the commonly used cyber-attacks. Following are the popular types of cyber-attacks:

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

- Malvertising (malicious advertising)

44) What is The Name Of Protocol That Broadcast The Information Across All The Devices?

IGMP (Internet Group Management Protocol) is a communication protocol that is used in gaming or video streaming and facilitates communication devices, including routers, to send packets.

45) How Can We Protect Email Messages?

Cipher algorithm is highly recommended to protect email, credit card information and confidential data.

46) What is Data Encryption and Why It Is Important In Network Security?

Data encryption is a technique that is used to secure the data by converting it into a code. So, the only authorized users can access this code or converted form of data. It is important for network security because your data can be breached at any stage in the network if it is not encrypted. In the cyber security interview questions and answers, your most questions should be on the encryption and decryption techniques and how you can secure the network.

47) What is The Main Difference Between Diffie-Hellman and RSA?

Diffie-Helman is a protocol that is used whenever the key is exchanged between two parties and RSA is an encryption algorithm that takes the keys (public and private) to do the encryption and decryption.

48) What is The Remote Desktop Protocol?

RDP is developed by Microsoft and provides GUI (graphical user interface) to connect two devices over a network. In order to get successful communication, the user will use RDP client software and other devices must run RDP server software. RDP (Remote Desktop Protocol) is dedicatedly designed for remote management and to access virtual applications, computers or terminal servers.

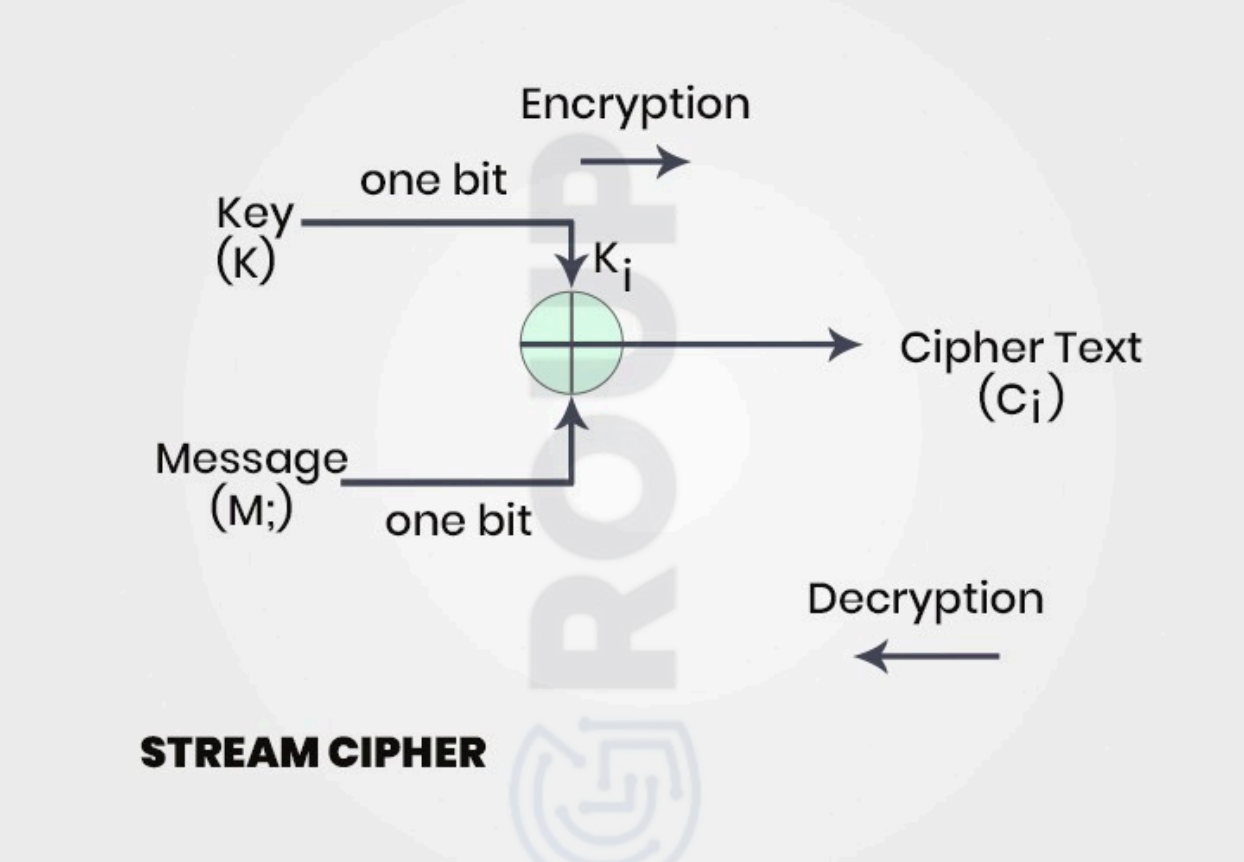
49) Do You Know About Forward Secrecy?

Forward secrecy is a security measure which is used to confirm the integrity of the unique session key in event that long term key is compromised.

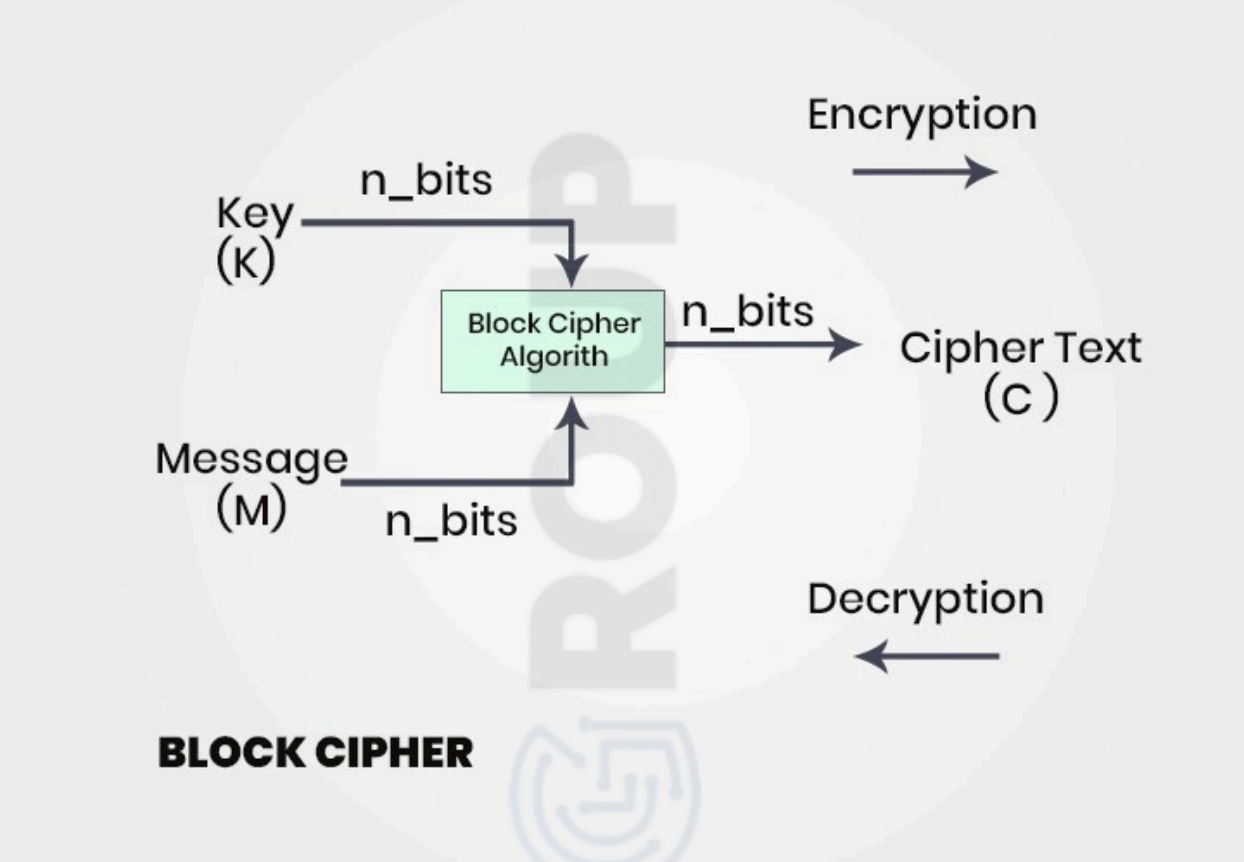
50) Explain The Concept of IV in Encryption?

IV (Initial Vector) is an arbitrary number which is used to ensure that identical text encrypted to different cipher texts. IV program is used by the encryption program only once per session.

51) What is The Difference Between Stream Cipher and Block Cipher?



STREAM CIPHER



Parameter	Stream Cipher	Block
Working	Operates on small plaintext	Works on large data bloc
Code requirements	Less code required	More code required
Usage of keys	Only once	Reuse of key is possible
Application	Secure Socket layer	File encryption and datab
Usage	Used to implement hardware	Used to implement softw

52) Enlist Some Examples of A Symmetric Encryption Algorithm?

Following are the examples of symmetric encryption algorithm:

- RCx
- Rijndael (AES)
- DES
- Blowfish

53) What is The Abbreviation of ECB and CBC?

ECB stands for Electronic Codebook and CBC stands for Cipher Block Chaining.

54) Can You Define Spyware?

It is a type of malware that is used to steal data about the company or person. Spyware can damage the computer system of the companies or organizations.

55) Do You Know About Impersonation?

Yes, it is a mechanism that is used to assign the user account to an unknown user.

56) What is SRM?

SRM (Security Reference Monitor) is a Microsoft Windows system that is used to implement security in the windows. It determines whether access to a resource is allowed or not. MSFT Access Token is used for the verification of all user actions.

57) What is The Computer Virus?

It is malicious software that is executed on the system without users' consent and consumes computing resources such as CPU time and memory. In some special cases, this malicious software makes changes in other computer programs and insert its own code to harmthe computer system. Different computer viruses may be used to:

- Access user ID and passwords
- Corrupt data in the computer
- Log the users' keystrokes
- Show annoying messages

58) What Do You mean By Authenticode?

It is a technology used to identify the publisher of Authenticode sign software. With the help of Authenticode, every user can verify that software is genuine or contains any malicious program.

59) Define CryptoAPI?

As the name indicates, CryptoAPI is the collection of encryption APIs that allows the developers to create a project on a protected and secure network.

60) What are The Steps To Secure Web Server?

Following are the simple steps to secure your web server:

- Update the ownership of the file
- Keep your webserver up-to-date
- Disable all extra modules
- Delete default scripts

61) What is MBSA?

Microsoft Baseline Security Analyzer (MBSA) is a graphical and command-line interface used to find missing security updates and misconfigurations.

62) What is Ethical Hacking?

It is a type of hacking in which attackers understand the weak points and try to improve the overall security of a network. Ethical hackers get the help of different tools and fix vulnerabilities of computer or network.

63) Explain Social Engineering and Enlist its Attacks?

The term social engineering is used to convince people to reveal the confidential information and it has three types: Human-based, mobile-based and computer-based.

- Human-based attack: Attackers may pretend like a genuine user who is making a request higher authority to reveal confidential information of the organization.
- Computer-based attack: In this type of attacks, attackers send fake emails to harm the computer and ask them to forward such email.
- Mobile-based attack: They may send SMS to others and collect private information. If any user downloads a malicious application, then it can be misused to grant access to confidential information.

64) What is IP and MAC Addresses?

IP address stands for Internet Protocol address and used to uniquely identify any computer or other devices such as printers, storage disks on a computer network.

MAC address stands for Media Access Control address that is used to uniquely identify network interfaces for proper communication at the physical layer.

65) What Do You mean By A Worm?

The worm is a type of malware which replicates from one computer to another.

66) What is The Difference Between Virus and Worm?

Parameter `	Virus
How they infect?	The virus inserts malicious code into a particular program or file
Worm is attached in Instant	
Dependency	It needs a host program to work
There is no need for any ho	
Linked with	Virus is linked with .com, .xls, .exe, .doc, and others
The worm is linked with an	
Affecting speed	It is slower than worm
It is faster as compared to v	

67) Enlist Some Tools Used For Packet Sniffing?

Following tools are used for packet sniffing:

- Tcpdump
- Kismet
- Wireshark
- NetworkMiner
- Dsniff

68) Do You Know About Anti-Virus Sensor Systems?

Yes, it is a tool used for the identification, prevention or removal of viruses presented in the computing devices. Anti-virus sensor systems perform system checks and increase the security of the computer on a regular basis.

69) What are The Types of Sniffing Attacks?

Following are the types of sniffing attacks:

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

70) Explain Distributed Denial-Of-Service Attack (DDoS)?

It is a type of attack in which a malicious actor aims to render a computer, server or any network resource to its intended users. In other words, it is a process of disrupting the normal traffic of a targeted server by overwhelming the target.

71) What is The Concept Of Session Hijacking?

TCP session hijacking is the name of misusing a valid compute session. The most common method of hijacking is IP spoofing and attackers use IP packets to insert a command between two nodes of the network.

72) What are The Different Methods Of Session Hijacking?

Following are the common methods of session hijacking:

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

73) Define Hacking Tools?

Hacking tools are programming scripts and computer programs that are useful for finding and exploiting the weaknesses in computer systems, server, networks or web applications. A lot of tools are available in the market both free and paid solutions for commercial use.

74) What are The Common Encryption Tools?

Following are the most common encryption tools:

- RSA
- AES
- Twofish
- Triple DES

75) Define Backdoor?

Backdoor term is used when a security mechanism is bypassed to access a system by adopting malware technique.

76) Is it a Good Way To Send Login Credentials Through Email?

No, it is not recommended to send your login credential through email because there are solid chances of email attacks.

77) What is The 80/20 Rule of Networking?

This networking rule is defined on the basis of network traffic, in which 80% of all network traffic should remain local while 20% of traffic should be routed towards a permanent VPN.

78) What is WEP Cracking?

WEP cracking is a method that is used for a security breach in wireless networks. Mainly, it is categorized into two types: Active cracking and Passive cracking.

79) What are The WEP cracking tools?

Following tools are commonly used in WEP cracking:

- Aircrack
- Kismet
- WEPCrack
- WebDecrypt

80) Define Security Auditing?

It is the name of internal inspection of operating systems and software applications for security flaws.

The audit can be done through line by line code inspection.

81) What is Phishing?

Phishing is a technique used to obtain the confidential information such as username, password or credit card information of users.

82) Can You Define Nano-Scale Encryption?

Nano-scale encryption is a research area that provides robust security to computers and prevents them from attacks.

83) What is Security Testing?

It is a type of software testing that ensures the applications and systems are free from any vulnerabilities, risks or threats that may cause a big loss.

84) What is Security Scanning?

Security scanning is the name of identification of network and system weaknesses to provide solutions for reducing these risks. It can be done for both manual as well as automated scanning.

85) What are The Available Hacking Tools?

Here is a list of useful hacking tools:

- Acunetix
- Burp Suite
- Savvius
- Probably
- Netsparker

- WebInspect
- Angry IP scanner

86) What are The Disadvantages of Penetration Testing?

Following are the main disadvantages of testing:

- Corruption and data loss
- Higher downtime which increases costs
- It cannot find all vulnerabilities available in the system
- There are many limitations such as budget, time, scope and skills of testers

87) What is Security Threat?

It is a risk which can steal confidential data and harm computer systems or networks as well as organization.

88) What are Physical Threats?

It is known as potential cause of any incident that may result in physical damage to your network or compute systems.

89) What are The Examples Of Non-Physical Threats?

Following are the common examples of non-physical threat:

- Loss of confidential information
- Corruption or loss of system data
- Cyber security Breaches
- Disrupt business operations
- Illegal monitoring of activities on computing devices

90) Do You Know About Trojan Virus?

It is a type of malware that is used to gain access to any computer using social engineering techniques to execute the trojan virus on the system.

91) What is SQL Injection?

SQL injection is an attack that poisons malicious SQL statements to the database by taking advantage of poorly designed web applications.

92) Enlist Security Vulnerabilities As Per Open Web Application Security Project (OWASP)

Following are the security vulnerabilities as per OWASP:

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

93) What is an Access Token?

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

94) What is ARP Poisoning?

Address Resolution Protocol poisoning is a type of attack in which the IP address is converted to the physical address on a network device. The host will send an

ARP broadcast and all receivers respond back with their physical addresses. In other words, ARP poisoning is the name of sending fake addresses to the switch so that it can associate the fake addresses with the IP address of a computer connected to the network and hijack the traffic.

95) Enlist The Common Types of Non-Physical Threats:

Following are the common types of non-physical threats:

- Trojans
- Adware
- Worms
- Spyware
- DoS Attack
- Distributed DoS Attacks
- Virus
- Key loggers
- Phishing
- Unauthorized access to computer systems resources

96) What is The Sequence of a TCP Connection?

The sequence of a TCP connection (also known as a 3-way handshake) is SYN SYN-ACK ACK.

97) What is Nmap?

Nmap is a network scanning tools that use the IP packets and used to identify all the devices connected to a network and to deliver information on the operating systems they are running.

98) What is The Use Of EtterPeak Tool?

It is a network analysis tools which is used for sniffing packets of network traffic.

99) What are The Types of Cyber-Attacks?

Mainly, there are two types of cyber-attacks: web-based and system-based attacks.

100) List Out Web-based Attacks

Common web-based attacks are SQL injection, Brute Force attack, Phishing, DNS Spoofing, DoS and Dictionary attacks.

101) Some examples of System-based Attacks

Following are the examples of system-based attacks:

- Virus
- Backdoors
- Bots
- Worm

102) List Out The Types of Cyber Attackers

Mainly, there are four types of cyber attackers: Cybercriminals, Hacktivists, Insider threats, and State-sponsored attackers.

0

Thanks for checking out, A lot of love from VIEH Group

Jai hind