Top 50 Cybersecurity Interview Questions

Part A - 40 Theoretical Questions

1. 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.

2. What is the difference between Symmetric and Asymmetric encryption?

Basis of Comparison	Symmetric Encryption	Asymmetric Encryption
Encryption key	Same key for encryption & decryption	Different keys for encryption & decryption
Performance	Encryption is fast but more vulnerable	Encryption is slow due to high computation
Algorithms	DES, 3DES, AES and RC4	Diffie-Hellman, RSA
Purpose	Used for bulk data transmission	Often used for securely exchanging secret keys

3. 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.

4. 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.

5. 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.

6. 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.

7. What is the difference between VA(Vulnerability Assessment) and PT(Penetration Testing)?

Vulnerability Assessment is the process of finding flaws on the target. Here, the organization knows that their system/network has flaws or weaknesses and want to find these flaws and prioritize the flaws for fixing.

Penetration Testing is the process of finding vulnerabilities on the target. In this case, the organization would have set up all the security measures they could think of and would want to test if there is any other way that their system/network can be hacked.

8. 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

9. What are the response codes that can be received from a Web Application?

Ixx	Informational responses
2xx	Success
3xx	Redirection
4xx	Client-side error
5xx	Server-side error

10. What is traceroute? Why is it used?

Traceroute is a tool that shows the path of a packet. It lists all the points (mainly routers) that the packet passes through. This is used mostly when the packet is not reaching its destination. Traceroute is used to check where the connection stops or breaks to identify the point of failure.

11. What is the difference between HIDS and NIDS?

HIDS(Host IDS) and NIDS(Network IDS) are both Intrusion Detection System and work for the same purpose i.e., to detect the intrusions. The only difference is that the HIDS is set up on a particular host/device. It monitors the traffic of a particular device and suspicious system activities. On the other hand, NIDS is set up on a network. It monitors traffic of all device of the network.

12. 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 fotwarding: 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.

13. Explain SSL Encryption

SSL(Secure Sockets Layer) is the industry-standard security technology creating encrypted connections between Web Server and a Browser. This is used to maintain data privacy and to protect the information in online transactions. The steps for establishing an SSL connection is as follows:

1. . A browser tries to connect to the webserver secured with SSL
2. The browser sends a copy of its SSL certificate to the browser
3. The browser checks if the SSL certificate is trustworthy or not. If it is trustworthy, then the browser sends a message to the web server requesting to establish an encrypted connection
4. The web server sends an acknowledgment to start an SSL encrypted connection
5. SSL encrypted communication takes place between the browser and the web server

14. What steps will you take to secure a server?

Secure servers use the Secure Sockets Layer (SSL) protocol for data encryption and decryption to protect data from unauthorized interception.

Here are four simple ways to secure server:

Step 1: Make sure you have a secure password for your root and administrator users

Step 2: The next thing you need to do is make new users on your system. These will be the users you use to manage the system

Step 3: Remove remote access from the default root/administrator accounts

Step 4: The next step is to configure your firewall rules for remote access

15. Explain Data Leakage/Loss

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 Breach: The authorized entity sends data to an unauthorized entity on purpose
3. System Hack: Hacking techniques are used to cause data leakage

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

16. What are some of the common Cyberattacks?

Following are some common cyber attacks that could adversely affect your system.

1. Malware
2. Phishing
3. Password Attacks
4. DD0S
5. Man in the Middle
6. Drive-By Downloads
7. Malvertising
8. Rogue Software

17. 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.

18. 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

19. 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:

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.

20. 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.

21. 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

22. 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)

23. 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. Look out for our Ethical Hacking Course to learn more about the Ethical Hacking. 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.

24. 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.

25. 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.

26. 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

27. 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

28. Explain XSS attack and how to prevent it?

XSS(Cross-Site Scripting) is a cyberattack that enables hackers to inject malicious client-side scripts into web pages. XSS can be used to hijack sessions and steal cookies, modify DOM, remote code execution, crash the server etc.

You can prevent XSS attacks by using the following practices:

- Validate user inputs
- Sanitize user inputs
- Encode special characters
- Use Anti-XSS services/tools
- Use XSS HTML Filter

29. 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.

30. 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.

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

TCP/IP	TCP/IP Protocol Examples
Application	NFS, NIS+, DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP and others
Transport	TCP, UDP
Internet	IP, ARP, ICMP
Data Link	PPP, IEEE 802.2
Physical Network	Ethernet (IEEE 802.3) Token ring, RS-232, others

32. What is a Botnet?

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.

33. 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

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.

34. Explain SSL and TLS

SSL is meant to verify the sender's identity but it doesn't search for anything more than that. SSL can help you track the person you are talking to but that can also be tricked at times.

TLS is also an identification tool just like SSL, but it offers better security features. It provides additional protection to the data and hence SSL and TLS are often used together for better protection.

35. What is data protection in transit vs data protection at rest?

Data Protection in transit	Data protection at rest
When data is going from server to client	When data just exists in its database or on its hard drive
Effective Data protection measures for in-transit data are critical as data is less secure when in motion	Data at rest is sometimes considered to be less vulnerable than data in transit

36. What is 2FA and how can it be implemented for public websites?

An extra layer of security that is known as "multi-factor authentication".

Requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand — such as a physical token.

Authenticator apps replace the need to obtain a verification code via text, voice call or email.

37. What is Cognitive Cybersecurity?

Cognitive Cybersecurity is an application of Al technologies patterned on human thought processes to detect threats and protect physical and digital systems.

Self-learning security systems use data mining, pattern recognition, and natural language processing to simulate the human brain, albeit in a high-powered computer model.

38. What is the difference between VPN and VLAN?

VPN	VLAN
Helps to group workstations that are not within the same locations into the same broadcast domain	Related to remote access to the network of a company
Means to logically segregate networks without physically segregating them with various switches	Used to connect two points in a secured and encrypted tunnel
Saves the data from prying eyes while in transit and no one on the net can capture the packets and read the data	Does not involve any encryption technique but it is only used to slice up your logical network into different sections for the purpose of management and security

39. Explain Phishing and how to prevent it?

Phishing is a Cyberattack in which a hacker disguises as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant message.

You can prevent Phishing attacks by using the following practices:

- Don't enter sensitive information in the webpages that you don't trust
- Verify the site's security
- Use Firewalls
- Use AntiVirus Software that has Internet Security
- Use Anti-Phishing Toolbar

40. Explain SQL Injection and how to prevent it?

SQL Injection (SQLi) is a code injection attack where an attacker manipulates the data being sent to the server to execute malicious SQL statements to control a web application's database server, thereby accessing, modifying and deleting unauthorized data. This attack is mainly used to take over database servers.

You can prevent SQL Injection attacks by using the following practices:

- Use prepared statements
- Use Stored Procedures
- Validate user input

Part B - 10 Scenario Based Questions

1. Here's a situation- You receive the following email from the help desk:

Dear XYZ Email user,

To create space for more users we're deleting all inactive email accounts. Here's what you have to send to save your account from getting deleted:

- Name (first and last):
- Email Login:
- Password:
- Date of birth:
- Alternate email

If we don't receive the above information from you by the end of the week, your email account will be terminated.

If you're a user what do you do? Justify your answer.

This email is a classic example of "phishing" — trying to trick you into "biting". The justification is the generalized way of addressing the receiver which is used in mass spam emails.

Above that, a corporate company will never ask for personal details on mail.

They want your information. Don't respond to email, instant messages (1M), texts, phone calls, etc., asking you for your password or other private information.

You should never disclose your password to anyone, even if they say they work for UCSC, ITS, or other campus organizations.

2. A friend of yours sends an e-card to your mail. You have to click on the attachment to get the card.

What do you do? Justify your answer

There are four risks here:

- Some attachments contain viruses or other malicious programs, so just in general, it's risky to open unknown or unsolicited attachments.
- Also, in some cases just clicking on a malicious link can infect a computer, so unless you are sure a link is safe, don't click on it.
- Email addresses can be faked, so just because the email says it is from someone you know, you can't be certain of this without checking with the person.
- Finally, some websites and links look legitimate, but they're really hoaxes designed to steal your information.

3. One of the staff members in XYZ subscribes to many free magazines. Now, to activate her subscriptions one of the magazines asked for her month of birth, second asked for her year of birth, the other one asked for her maiden name.

What do you Infer from this situation? Justify.

All three newsletters probably have the same parent company or are distributed through the same service. The parent company or service can combine individual pieces of seemingly-harmless information and use or sell it for identity theft

It is even possible that there is a fourth newsletter that asks for a day of birth as one of the activation questions

Often questions about personal information are optional. In addition to being suspicious about situations like the one described here, never provide personal information when it is not legitimately necessary, or to people or companies, you don't personally know.

4. In our computing labs, print billing is often tied to the user's login. Sometimes people call to complain about bills for printing they never did only to find out that the bills are, indeed, correct.

What do you Infer from this situation? Justify.

Sometimes they realize they loaned their account to a friend who couldn't remember his/her password, and the friend did the printing. Thus the charges. It's also possible that somebody came in behind them and used their account

This is an issue with shared or public computers in general. If you don't log out of the computer properly when you leave, someone else can come in behind you and retrieve what you were doing, use your accounts, etc. Always log out of all accounts, quit programs, and close browser windows before you walk away.

5. There is this case that happened in my computer lab. A friend of mine used their yahoo account at a computer lab on campus. She ensured that her account was not left open before she left the lab. Someone came after her and used the same browser to re-access her account. and they started sending emails from it.

What do you think might be going on here?

The first person probably didn't log out of her account, so the new person could just go to history and access her account.

Another possibility is that she did log out, but didn't clear her web cache. (This is done through the browser menu to clear pages that the browser has saved for future use.)

6. Two different offices on campus are working to straighten out an error in an employee's bank account due to a direct deposit mistake.

Office #1 emails the correct account and deposit information to office #2, which promptly fixes the problem.

The employee confirms with the bank that everything has, indeed, been straightened out.

What is wrong here?

Account and deposit information is sensitive data that could be used for identity theft. Sending this or any kind of sensitive information by email is very risky because email is typically not private or secure. Anyone who knows how can access it anywhere along its route.

As an alternative, the two offices could have called each other or worked with ITS to send the information a more secure way.

7. The mouse on your computer screen starts to move around on its own and click on things on your desktop. What do you do?

a) Call your co-workers over so they can see

b) Disconnect your computer from the network

c) Unplug your mouse

d) Tell your supervisor

e) Turn your computer off

f) Run anti-virus

g) All of the above

Select all the options that apply.

Right answer is B & D.

This is definitely suspicious. Immediately report the problem to your supervisor and the ITS Support Center: itrequest.ucsc.edu, 459-HELP (4357), help@ucsc.edu or Kerr Hall room 54, M-F 8AM-5PM

Also, since it seems possible that someone is controlling the computer remotely, it is best if you can disconnect the computer from the network (and turn off wireless if you have it) until help arrives. If possible, don't turn off the computer.

8. Below is a list of passwords pulled out a database.

A. @#$)*&^%

B. akHGksmLN

C. UcSc4Evr!

D.Password1

Which of the following passwords meets UCSC's password requirements?

Answer is UcSc4Evr!

This is the only choice that meets all of the following UCSC requirements:

- At least 8 characters in length
- Contains at least 3 of the following 4 types of characters: lower case letters, upper case letters, numbers, special characters.

9. You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log into your account and fix the problem.

What should you do?

Delete the email. Better yet, use the web client (e.g. Gmail, Yahoo mail, etc.) and report it as spam or phishing, then delete it.

Any unsolicited email or phone call asking you to enter your account information, disclose your password, financial account information, social security number, or other personal or private information is suspicious — even if it appears to be from a company you are familiar with. Always contact the sender using a method you know is legitimate to verify that the message is from them.

10. A while back, the IT folks got several complaints that one of our campus computers was sending out Viagra spam. They checked it out, and the reports were true: a hacker had installed a program on the computer that made it automatically send out tons of spam email without the computer owner's knowledge.

How do you think the hacker got into the computer to set this up?

This was the result of a hacked password. Using passwords that can't be easily guessed, and protecting your passwords by not sharing them or writing them down can help to prevent this. Passwords should be at least 8 characters in length and use a mixture of upper- and lower-case letters, numbers, and symbols.

Even though in this case it was a hacked password, other things that could possibly lead to this are:

- Out of date patches/updates
- No anti-virus software or out of date anti-virus software