Cybersecurity Interview Questions and Answers

1. What are the key differences 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

2. What do you mean by Cybersecurity?

Cybersecurity is the combination of best processes and practices to ensure the security of networks, computers, programs, data and information from attack, damage or unauthorized access.

3. What is the least that you should have on your home network?

A home network is a testing environment for experimentation. You can have an Active Directory Domain Controller, a dedicated firewall appliance, and net-attached toaster. This is the least that you can have on your computer.

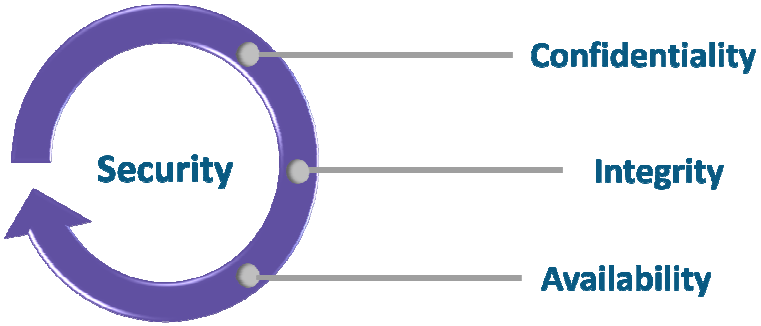
4. What is Encryption? Why is it important?

Encryption is a process of converting data into an unreadable form to prevent unauthorized access and thus ensuring data protection.

Encryption is important because it is the most effective way to ensure data security. Businesses, corporates, and governments use it to guard against identity theft.

5. What is a CIA triad?

CIA provides a standard for evaluating and implementing information security – irrespective of the system and/or organization in question.



Confidentiality: Data is accessible only to its concerned audience

Integrity: Ensuring that data is kept intact without meddling in the middle

Availability: Data and computers are available to authorized parties, as needed

6. 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

7. How do you report a risk?

Risk needs to be assessed before it can actually be reported. There are two ways to analyze risk: it can either be qualitative or quantitative. This approach goes well for both technical and business people. The business guys would check for the probable loss in numbers while the technical people will monitor and assess the impact and frequency. Depending on the audience, the risk can be reported.

8. How do you differentiate between IPS and IDS system?

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IDS just detect the intrusion and leaves the rest to the administrator for assessment and evaluation. Whereas, IPS detects the intrusion and takes necessary action to further prevent intrusion.

Also, there is a difference in the positioning of these devices in the network. Although they work on the same concept, the placement is different.

9. What do you know about Cybersecurity Frameworks?

Frameworks are voluntary guidance, based on existing guidelines and practices for organizations to better manage and reduce cybersecurity risk.

10. What is weak information security?

Information security policy is considered to be weak if it does not meet the criteria of an effective one. The criteria include *distribution, review, comprehension, compliance, and uniform*.

Information security is weak if:

- The policy has not been made readily available for review by every employee within the organization
- The organization is unable to demonstrate that employees can review the policy document
- The organization is unable to demonstrate that employees understand the content of the policy document

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

Following are the steps to set up a firewall

1. *Username/password:* modify the default password for a firewall device
2. *Remote administration:* Disable the feature of the remote administration

3. *Port forwarding:* Configure appropriate port forwarding for certain applications to work properly, such as 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.

12. Can you explain SSL encryption?

SSL (Secure Socket Layer) enables safe conversation between two or more parties. It is designed to identify and verify the person you are talking to on the other end.

HTTP combined with SSL provides you with a safer browsing experience with encryption. So, you can say it is a tricky question, but SSL wins in terms of security.

13. 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.

14. What are salted hashes?

Salt is a random data. When a properly protected password system receives a new password, it creates a hash value of that password, a random salt value, and then the combined value is stored in its database. This helps to defend against dictionary attacks and known hash attacks.

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

15. How could 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)

16. How can you prevent man in the middle(M.I.T.M) attack?

Now to answer that question, allow me to first tell you *what is MITM attack?*

A **MITM** attack happens when a communication between two parties (systems) is intruded or intercepted by an outside entity. This can happen in any form of online communication such as email, social media web surfing etc. Not only they are trying to eavesdrop on your private conversations, then they can also target all the information inside your devices and the outcome could be catastrophic.

Now here are some methods to prevent such attack,

- The first method to prevent this attack would be an encryption (preferably public key encryption) between both the parties. This way, they both will have an idea with whom they are talking because of the digital verification.
- The second method is to avoid open Wi-Fi networks and if it is necessary then use plugins like HTTPS, Forced TLS etc.

17. Explain encoding, hashing, and encryption?

Encoding: Converts the data in the desired format required for exchange between different systems.

Hashing: Maintains the integrity of a message or data. Any change done could be noticed.

Encryption: Ensures that the data is secured and one needs a digital verification code or image to open or access it.

18. 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

19. What is a DDoS attack? How is it mitigated?

DDoS stands for distributed denial of service. So, when a network is flooded with a large number of requests which is not recognized to handle, making the server unavailable to the legitimate requests.

For mitigating a DDoS attack you need to identify normal conditions for network traffics which is necessary for threat detection. DDoS mitigation also requires identifying incoming traffic to separate human traffic from human-like bots and hijacked web browsers.

20. Why do you need DNS monitoring?

The DNS allows your website under a certain domain that is easily recognizable and also keeps the information about other domain names. It works like a directory for everything on the internet. Thus, DNS monitoring is very important since you can easily visit a website without actually having to memorize their IP address.

21. What is a three-way handshake?

The three-way handshake is used by TCP to set up a TCP/IP connection over an internet protocol based network. It is also referred to as “SYN, SYN-ACK, ACK” because there are three messages transmitted by TCP to negotiate and start a TCP session between two computers.

22. 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.

White hat hackers use their powers for good deeds and so they are also called ethical hackers. These are mostly hired by companies as a security specialist that attempts to find and fix vulnerabilities and security holes in the systems.

Grey hat hackers are an amalgamation of a white hat and black hat hacker. They look for system vulnerabilities without the owner’s permission.

23. 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.

24. Can you explain what is application security?

Application security is the practice of improving the security of applications using software, hardware, and other methods.

Countermeasures are taken to ensure application security, the most common being an application firewall, that limits the execution of files or the handling of data by specific installed programs.

25. Differentiate between Vulnerability Assessment & Penetration testing.

Vulnerability Assessment	Penetration Testing
Focusses on uncovering as many security weaknesses as possible (It takes breadth over depth approach)	Focuses on the functionality of the software and not the security aspect. It checks if the network security defenses are strong (depth over breadth approach)
Vulnerability assessment is usually automated which allows better vulnerability coverage	Penetration testing is a combination of automated and manual techniques, which allows digging deeper into the weakness

26. When to use tracert/traceroute?

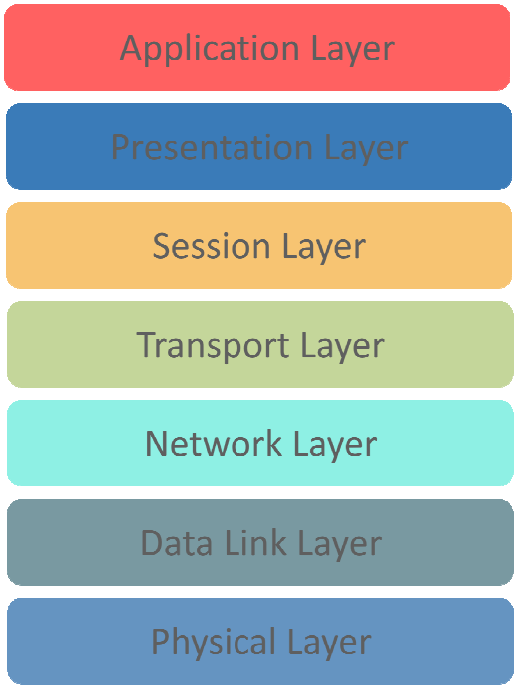
Traceroute shows you the path, a packet of information has gone through from your computer. It lists out all the routers that the packet passes through until reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each ‘hop’ from a router to router takes.

27. Tell me some common cyber attacks.

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

28. What are the different OSI layers? What is the job of Network layer?

Let me first tell you what is an 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: 

Here, focusing on the network layer: The Network layer controls the operation of the subnet. The main job of this layer is to deliver packets from source to destination across multiple links.

Q 29. 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.

The simplest way is to use the password ‘password’, this will work for the BIOS that has come from the factory.

Q 30. What is Cross Site Scripting?

Cross-Site Scripting (or XSS) refers to client-side code injection attack wherein an attacker can execute malicious into a legitimate website or web application.

XSS is amongst the most rampant of web application vulnerabilities and occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Q 31. 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

Q 32. Tell me the difference between Cybersecurity and Network Security?

Cybersecurity	Network Security
Describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources	designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.

Q 33. How will you prevent data leakage?

Data leakage is when data gets out of the organization in an unauthorized way.

Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorized upload of data to public portals, removable drives, photographs etc.

A few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the emails to the internal network, restriction on printing confidential data etc.

Q 34. 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.

Now let me tell you how it works.

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.

Q 35. What is 2FA and how can it be implemented for the 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.

Q 36. What technique can be used to prevent brute force login attack?

For Brute force login, the attacker tries to determine the password for a target (service/system/device) through a permutation or fuzzing process
As it is a lengthy task, attackers usually employ a software such as fuzzer, to automate the process of creating numerous passwords to be tested against a target.
In order to avoid such attacks – password best practices should be followed, mainly on critical resources like servers, routers, exposed services and so on.

Q 37. What is Cognitive Cybersecurity?

Cognitive Cybersecurity is an application of AI 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

Q 38. 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.

Q 39. 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

Q 40. 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

Scenerio 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 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 (IM), 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
Not a word preceded or followed by a digit

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 a number of 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 actually 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