Level 1 Questions

This group of questions will cover the basics of penetration testing, focused on the following areas:

- A definition of pentesting
- The purpose and goals of pentesting
- The difference between vulnerability testing and pentesting
- The types of pentesting methodologies
- The teams that are required to conduct a pentesting exercise
- The certs that are required in order to demonstrate deep skills and knowledge in pentesting
- How a pentester should explain the results of a pentest to a C-level executive

1.What is a specific definition of pentesting?

Let's ask the people in the know. Cloudflare.com says the following: "Penetration testing (or pentesting) is a security exercise where a cybersecurity expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of."

2.What is the primary purpose of pentesting?

The main purpose of a pentest is to conduct a "deep dive" into the IT Infrastructure of a business or a corporation with the primary intention of gaining access to any (and if possible, all) of the electronic based assets that exist. It is important to note that the goal of the pentester is not to attempt to strike a hard blow right at the very beginning; rather, they escalate the intensity of the cyber-attack over a period of time.

3.What are the goals of conducting a pentesting exercise?

The goals are as follows:

- To test adherence to the security policies that have been crafted and implemented by the organization
- To test for employee proactiveness and awareness of the security environment that they are in
- To fully ascertain how a business entity can face a massive security breach, and how quickly they react to it and restore normal business operations after being hit.

4.There is very often confusion between vulnerability testing and pentesting. What is the primary difference between the two?

With vulnerability testing, one is simply scanning for any weaknesses that may reside in any component of the IT Infrastructure. In a pentest, a full-scale cyber-attack or series of cyberattacks is launched with explicit permission from the client (or whoever is requesting it) in order to specifically find any types or kinds of gaps that have not yet been discovered by the IT security staff.

5.What are the three types of pentesting methodologies?

The three types are as follows:

- Black-Box Testing
- White-Box Testing
- Gray-Box Testing

6.Describe these tests in much more detail.

Black-Box Testing

In some instances, the cyber-attacker may know nothing about their intended target. So in an effort to try to break through the lines of defense, the cyber-attacker will carry an all-out attack, also known as a brute-force Attack. In a black-box scenario, the pentester will not have any knowledge whatsoever about the target(s) they are going to hit. As a result, this kind of pentest can take a very long time to conduct, and automated tools are heavily relied upon. This kind of exercise is also known as a trial-and-error approach.

White-Box Testing

This kind of pentest is also known as clear-box testing. In these instances, the pentester has advanced knowledge to some degree about the Web application that they are about to hit and its underlying source code. This kind of attack takes a shorter amount of time to launch when compared to the black-box test.

Gray-Box Testing

This kind of pentesting is a combination of both of black-box and white-box testing. This simply means that the pentester has some advanced knowledge on the targets they plan to attack. This kind of exercise requires both the use of automated and manual tools. When compared to the other two tests, this one offers the highest chances of discovering unknown security holes and weaknesses.

7.What are the teams that can carry out a pentest?

The teams are as follows:

- The Red Team
- The Blue Team
- The Purple Team

8.Can you describe these teams in more detail?

The functionalities of these three teams can be described as follows:

The Red Team

This group of pentesters acts like the actual cyber-attack. That means this team is the one that launches the actual threat, in order to break down the lines of defense of the business or corporation and attempt to further exploit any weaknesses that are discovered.

The Blue Team

These are the pentesters that act like the actual IT staff in an organization. Their main objective is to thwart any cyber-attacks that are launched by the Red Team. They assume a mindset of being proactive as well as maintaining a strong sense of security consciousness.

The Purple Team

This is a combination of both the Red Team and the Blue Team. For example, they have the security arsenal that is used by the Blue Team and possess a working knowledge of what the Red Team is planning to attack. It is the primary job of the Purple Team to help out both these teams out. Because of that, the pentesters of the Purple team cannot be biased in any regard and have to maintain a neutral point of view.

9.What kinds of certifications in the most demand for penetration testing?

There is no doubt that in the cybersecurity field, there an endless number of certs one can pursue. But if a pentester is to be recognized as the top in their field, the following certs are a must-have:

- The Certified Ethical Hacker (aka CEH – this is administered by the EC Council)
- The Offensive Security Certified Professional (aka OSCP – this is administered by Offensive Security)

10.The results of a pentesting exercise have to be made available not only to the IT staff, but also to the C-level executives. The latter may not possess a strong technical knowledge like their IT staff does. How would you explain the results to them?

The C-suite can understand results when they are explained to them in terms of financial impact. Thus, a pentesting report should also include a risk analysis which demonstrates the benefit versus the cost of any of the vulnerabilities that are discovered and not fixed. It should also have financial calculations demonstrating the impacts of a security breach.

Level 2 Questions

In this section, we’ll look at some intermediate-level questions about penetration testing concepts. These will focus on the following:

- Cross-site scripting
- Data packet sniffing
- Various abbreviations that are used in pentesting
- Common network security vulnerabilities
- Pentesting techniques
- The various network ports
- SQL injection attacks
- Asymmetric/symmetric cryptography
- SSL/TLS

11.Explain what cross-site scripting (XSS) is all about.

This is a type of cyber-attack where malicious pieces of code, or even scripts, can be covertly injected into trusted websites. These kinds of attacks typically occur when the attacker uses a vulnerable Web-based application to insert the malicious lines of code. This can occur on the client side or the browser side of the application. As a result, when an unsuspecting victim runs this particular application, their computer is infected and can be used to access sensitive information and data. A perfect example of this is the contact form, which is used on many websites. The output that is created when the end user submits their information is often not encoded, nor is it encrypted.

12.What exactly is data packet sniffing, and what are some of the most widely used tools?

Data packet sniffing is a specific process in which network traffic can be captured ether across the entire IT Infrastructure, or just certain parts of it. Once this has been accomplished, then a deep analysis of the data packets in question can then be made.

For example, if a business or a corporation is hit by a cyber-attack, examining the network traffic and the data packets that were associated with it at the time of the security breach occurred becomes extremely crucial, especially from the standpoint of forensics. Even if no attack is imminent, it is still very crucial for the IT staff to conduct a check on their network traffic in order to determine if there is any sort of anomaly that is present. There are many data packet sniffing tools that are available today, but probably the most widely-used one is Wireshark.

13.Please provide the exact names of the following abbreviations that are commonly used in pentesting: 2FA, 2S2D, 2VPCP, 3DES, 3DESE, 3DESEP.

The acronyms stand for the following:

- 2FA means “Two-Factor Authentication”
- 2SD2D means “Double-Sided, Double Density”
- 2VPCP means “Two-Version Priority Ceiling Protocol”

- 3DES means “Triple Data Encryption Standard”
- 3DESE means “Triple Data Encryption Standard Encryption”
- 3DESEP means “Triple Data Encryption Standard Encryption Protocol”

14.What are some of the most common network security vulnerabilities that a pentester comes across?

Of course, there are countless numbers of issues that can impact the network infrastructure of an organization, and you probably have your own stories about what you’ve encountered. The following vulnerabilities are some of the most prevalent:

- The usage of extremely weak passwords in the network security tools themselves, which include the routers, firewalls, network intrusion devices and so on. Very often, business entities are in a rush to deploy these kinds of technologies, and they forget to create a robust and secure password. This leads to them using the insecure default one set up by the vendor
- Implementing security patches on the wrong servers and related network components. There are also times when a security patch is installed on the right machine but not configured properly, thus leaving it wide open to a cyber-attack
- The misconfiguration of network devices, as described previously
- The use of infected portable media devices (primarily USB drives) and inserting them into a server and other related network components
- The lack of a coherent network security policy; even if one was implemented, compliance is still a huge issue

15.What are the different pentesting techniques?

Pentesting techniques fall into these following categories:

- Web Application Testing
- Wireless Network/Wireless Device Testing
- Network Infrastructure Services
- Social Engineering Testing
- Client-Side Application Testing

1.6What network ports are commonly examined in a pentesting exercise, and what tool can be used for this?

They are as follows:

- HTTPS (Port #443)
- FTP (Port #’s 20 & 21)
- NTP (Port #123)
- SSH (Port #22)
- HTTP (Port #80)
- Telnet (Port #23)

- SMTP (Port #25)

In these particular instances, “Nmap” is the most commonly used tool.

17.Describe in detail what SQL injection is.

This is a method in which malicious SQL code is inserted into the database or the back end of the Web-based application. These are typically deployed into an entry-level field so that the malicious code can be executed. This kind of attack is used primarily for heavy data-driven applications in which multiple security vulnerabilities can be found and exploited. It should be noted that although SQL injection attacks are primarily used to hit Web-based applications, the attacker can also target the SQL database just by itself as well.

18.What is the primary difference between asymmetric and symmetric cryptography? Give an example of the former.

Only one type of key is used in symmetric cryptography, and this key is known as the Private Key. Although the main advantage of this is that this type of system is relatively easy to deploy, the primary disadvantage of it is that if the Private Key falls outside the reach of the sending and receiving parties, the cyber-attacker can easily capture the ciphertext and decrypt it very easily.

With asymmetric cryptography, two keys are used: the Public Key and the Private Key. The advantage of this system is that it offers far greater levels of security as opposed to just using a Private Key, but it requires considerably more processing power resources. An example of an asymmetric cryptography system is Public Key Infrastructure, also known as PKI.

19.What are the permutations required for a robust SSL connection to take place?

The following characteristics are required:

- The session identifier
- A peer certificate
- An established compression method
- Any associated cipher specs

20.What are SSL and TSL?

SSL stands for “Secure Sockets Layer.” This is the de facto standard to keep all Internet connections safe and secure. You will know that a particular website can be safely accessed when it has “HTTPS” in its URL address. SSLs are used most in e-commerce-based applications, in which credit card and other personal information and data is transmitted to the online merchant.

TSL stands for “Transport Layer Security” and is actually a much more updated and advanced version of SSL. It is important to note that with TSL, it can come with three types of encryption:

- Elliptical Curve Cryptography (ECC)
- Rivest–Shamir–Adleman (RSA)
- Digital Signature Algorithm (DSA)

Level 3 Questions

This section covers advanced-level questions about penetration testing, focusing on the following:

- The SSL/TSL handshake
- The phases of a network intrusion attack
- Diffie-Hellman public key exchanges
- The establishment of network controls
- Traceout/Tracert
- Omniquad BorderSecure
- The various pentesting models
- The types of cross-site scripting (XSS)
- Cross-site request forgery

21.How exactly does SSL/TSL work?

Establishing an SSL/TSL connection works in this fashion:

- On the client side, the end user enters a URL address into their Web browser. This then initiates the SSL/TLS connection by transmitting a particular message to the server on which the website resides
- This server then returns a Public Key (or even a certificate) back to the end user’s Web browser
- The browser then closely inspects this Public Key, and if all looks good, a Symmetric Key is transmitted back to the server. If there are anomalies detected from within the Public Key, the communications are instantly cut off
- Once the server gets the Symmetric Key, it then sends the encrypted webpage that is being requested back to the end user’s Web browser
- The browser then decrypts the content into a form that can be easily understood by the end user

It is important to note that this entire process can also be referred to as the SSL/TSL Handshake.

22.Describe the different phases of a network intrusion attack.

The phases are as follows:

- Reconnaissance: This is where the pentester learns more about the target they are about to hit. This can either be done on an active or passive basis. In this step, you learn more about the following:
    - The IP address range that the target is in
    - Finding out its domain name
    - DNS records
    - Scanning: This is the step where the pentester learns about the vulnerabilities of the particular target. Weaknesses are found in the network infrastructure and the associated software applications. For example, this include the following:
        - Ascertaining the services that are currently being run
        - Any open ports
        - The detection of any firewalls
        - Weaknesses of the operating system in question
- **Gaining the needed access:** This is the part where the pentester starts to actually initiate the launch of the cyber-attack, based on the weaknesses and the vulnerabilities that they have discovered in the last step
- **Maintaining the access:** The pentester has entered the target itself and tries to keep that access point open so that they can extract as much private information and data as possible
- **Covering their tracks:** In this last step, the pentester ensures that any "footprints" left behind in the course of their attack are covered up so that they can't be detected. For instance, this involves the following:
    - The deletion of any log-related files
    - Closing off any backdoors
    - Hiding all controls that may have been used

23.What is a specific pentesting exercise that can be done with a Diffie-Hellman exchange?

This was actually one of the first Public Key protocols to be put into place, and it is a methodology that can be utilized to securely exchange Public Keys over an open network line of communications. A pentest can be done here in order to determine and ascertain any kind of weak/TLS services that are associated with this exchange process.

24.After a pentest is conducted, what are some of the top network controls you would advise your client to implement?

The following types of controls should be implemented:

- Only use those applications and software tools that are deemed "whitelisted"
- Always implement a regular firmware upgrade and software patching schedule, and make sure that your IT staff sticks with the prescribed timetable
- With regards to the last point, it is absolutely imperative that the operating systems(s) you utilize are thoroughly patched and upgraded
- Establish a protocol for giving out administrative privileges only on an as-needed basis, and only to those individuals that absolutely require them

25.How does traceout/tracert exactly work?

This is used to determine exactly the route of where the data packets are exactly going. For example, this method can be used to ascertain if data packets are being maliciously redirected, they take too long to reach their destination, as well as the number of hops it takes for the data packets to go from the point of origination to the point of destination.

26.What is Omniquad BorderSecure?

This is a type of specific service that can help to perform network-based audits or even automated pentesting of an entire network infrastructure. It can give the pentesting team detailed information and data as to how the cyber-attacker can gain access to your network-based digital assets. It can also be used to help mitigate any form of threat that is launched by a malicious third party.

27.What number of vulnerabilities can the abovementioned service actually detect?

All types of network infrastructures can be pentested, and up to a thousand total vulnerabilities can be detected with this particular service.

28.Describe the theoretical constructs of a threat model that can be used in a pentesting exercise.

The constructs behind a threat model include the following:

- Gathering the required documentation
- Correctly identifying and categorizing the digital assets that are found within the IT infrastructure of a corporation or business
- Correctly identifying and categorizing any type of kind of cyber-threat that can be targeted towards the digital assets
- Properly correlating the digital assets with the cyber-threat that they are prone to (this is can also be considered as a mapping exercise where a digital asset is associated with its specific cyber-threat)

It is also important to note that there are three types of threat models that a pentesting team can use, and they are as follows:

- Digital Asset-Centric
- Cyber-Attacker-Centric
- Software Application-Centric.

The above is an example of a Digital Asset-Centric Threat Model.

29.What are the three types of cross-site scripting (XSS)?

The three types are as follows:

- **Persistent/Stored XSS:** This is where the malicious input is stored onto the target server, such as a database, and is reflected at the page where the end user entered in their information (such as a "Contact Us" form)
- **Reflected XSS:** Any form of malicious user input is instantaneously returned by the Web-based application as an "Error Message." As a result, this data is deemed to be unsafe by the Web browser, and it is not stored in any fashion
- **DOM-based XSS:** This will actually for any type or kind of client scripting language (such as Java) to access and maliciously modify the end user input. It can also covertly alter the content, structure and even the particular style of a webpage. The types of objects that can be manipulated include the following:
  - Document.URL
  - Document.location
  - Document.referrer

30.What exactly is CSRF and how can it be prevented when executing a pentest exercise?

This stands for cross-site request forgery, and it takes advantage of the trust levels that are established in an authenticated user session. For example, in these scenarios, Web-based applications typically do not conduct any form of verification tests that a specific request actually came from an authenticated user; rather, the only form of verification is sent by the particular Web browser that the end user is utilizing. There are two ways to avoid this scenario:

- Double-check the specific CSRF token that is being used
- Confirm that the specific requests are coming from within the same origin

Conclusion

Overall, we've looked at some of the interviews that you could be asked if you are applying for a pentesting job. These questions can also be asked of a pentester if they are currently employed in this field.

It is important to keep in mind that although answering these questions will demonstrate to the interviewer your in-depth knowledge of pentesting, it takes other qualitative skills as well in order to become a successful pentester. For instance, you must have the ability to work well with others in a team-oriented fashion and work long hours.

Pentesting also requires you to have a great deal of patience on your part, as it these kinds of exercises do not happen in just one day. A successful pentest can take weeks or even months to accomplish.

Finally, you must also have the ability to take all of the techno-jargon that is associated with the results you have obtained and bring it down to a level that your client can understand and implement. You will be gauged on these qualitative factors as well in your interview.

Why would you want to use SSH from a Windows PC?

SSH (TCP port 22) is a secure connection used on many different systems and dedicated appliances. Routers, switches, SFTP servers and unsecure programs being tunneled through this port all can be used to help harden a connection against eavesdropping. Despite the fact that most times when you hear about somebody "SSHing" into a box it involves Linux, the SSH protocol itself is actually implemented on a wide variety of systems — though not by default on most Windows systems. Programs like PuTTY, Filezilla and others have Windows ports available, which allow Windows users the same ease-of-use connectivity to these devices as do Linux users.

7. What's the difference between symmetric and asymmetric encryption?

To boil down an extremely complicated topic into a few short words, symmetric encryption uses the same key to encrypt and decrypt, while asymmetric uses different keys for encryption and decryption. Symmetric is usually much faster, but is difficult to implement most times due to the fact that you would have to transfer the key over an unencrypted channel. Therefore many times an asymmetric connection will be established first, then create the symmetric connection. This leads us into the next topic …

8. What is SSL and why is it not enough when it comes to encryption?

SSL is identity verification, not hard data encryption. It is designed to be able to prove that the person you are talking to on the other end is who they say they are. SSL and its big brother TLS are both used almost everyone online, but the problem is because of this it is a huge target and is mainly attacked via its implementation (the Heartbleed bug for example) and its known methodology. As a result, SSL can be stripped in certain circumstances, so additional protections for data-in-transit and data-at-rest are very good ideas.

9. How would you find out what a POST code means?

POST is one of the best tools available when a system will not boot. Normally, through the use of either display LEDs in more modern systems, or traditionally through audio tones, these specific codes can tell you what the system doesn't like about its current setup. Because of how rare these events can be, unless you are on a tech bench day in and day out, reference materials such as the motherboard manual and your search engine of choice can be tremendous assets. Just remember to make sure that everything is seated correctly, you have at least the minimum required components to boot, and most importantly, that you have all of your connections on the correct pins.

10. What is the difference between a black hat and a white hat?

This particular question can lead into a major philosophical debate about freedom of information, and if something is implemented in a deliberately broken way it isn't actually breaking into it, etc. The one I've heard the most is the classic Jedi example — same tools, different ideologies. Personally, the people I know that have worked on both sides of the line it comes down to this — the difference between a black hat and a white hat is who is signing the check.

Level 2 interview questions: The breaker/fixer

Secondary positions usually require a bit more experience — a bit more legwork, a bit more time to think outside the box and discover things that make you go, "Huh. That's funny." You've had situations where you've had to break into different systems and wonder if you did the right thing and know that you could get into quite a bit of trouble if you did the same thing to say the accountant's PC on the 4th floor. You've seen a few breakouts and know enough not to panic when you see a virus alert. Finally, when you are performing a cleanup on a box you know you want to gather information about how it got on there as well as save as much data as possible before either removing the offending infection or nuking the box. Not full blown digital forensics necessarily, but knowing the basics of the art will help you a great deal. Maxim #1: "Pillage, THEN burn."

11. You need to reset a password-protected BIOS configuration. What do you do?

While BIOS itself has been superseded by UEFI, most systems still follow the same configuration for how they keep the settings in storage. Since BIOS itself is a pre-boot system, it has its own storage mechanism for its settings and preferences. In the classic scenario, simply popping out the CMOS (complementary metal-oxide-semiconductor) battery will be enough to have the memory storing these settings lose its power supply, and as a result it will lose its settings. Other times, you need to use a jumper or a physical switch on the motherboard. Still other times, you need to actually remove the memory itself from the device and reprogram it in order to wipe it out. The simplest way by far however is this: if the BIOS has come from the factory with a default password enabled, try "password".

12. What is XSS?

Cross-site scripting is the nightmare of Javascript. Because Javascript can run pages locally on the client system as opposed to running everything on the server side, this can cause headaches for a programmer if variables can be changed directly on the client's webpage. There are a number of ways to protect against this, the easiest of which is input validation.

13. How would you login to Active Directory from a Linux or Mac box?

While it may sound odd, it is possible to access Active Directory from a non-Windows system. Active Directory uses an implementation of the SMB protocol, which can be accessed from a Linux or Mac system by using the Samba program. Depending on the version, this can allow for share access, printing and even Active Directory membership.

14. What are salted hashes?

Salt at its most fundamental level is random data. When a properly protected password system receives a new password, it will create a hashed value for that password, create a new random salt value and then store that combined value in its database. This helps defend against dictionary attacks and known hash attacks. For example, if a user uses the same password on two different systems, if they used the same hashing algorithm, they could end up with the same hash value. However, if even one of the systems uses salt with its hashes, the values will be different.

15. What do you think of social networking sites such as Facebook and LinkedIn?

This is a doozy, and there are an enormous number of opinions for this question. Many think they are the worst thing that ever happened to the world, while others praise their existence. In the realm of security, they can be the source of extreme data leaks if handled in their default configurations. It is possible to lock down permissions on social networking sites, but in some cases this isn’t enough due to the fact that the backend is not sufficiently secured. This also doesn’t help if somebody else’s profile you have on your list gets compromised. Keeping important data away from these kinds of sites is a top priority, and only connecting with those you trust is also extremely helpful.

16. What are the three ways to authenticate a person?

Something they know (password), something they have (token), and something they are (biometrics). Two-factor authentication often uses a password and token setup, although in some cases this can be a PIN and thumbprint.

17. How would you judge if a remote server is running IIS or Apache?

Error messages oftentimes give away what the server is running, and many times if the website administrator has not set up custom error pages for every site, it can give it away as simply as just entering a known bad address. Other times, just using telnet can be enough to see how it responds. Never underestimate the amount of information that can be gained by not getting the right answer but by asking the right questions.

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

When data is protected while it is just sitting there in its database or on its hard drive — it can be considered at rest. On the other hand, while it is going from server to client, it is in-transit. Many servers do one or the other — protected SQL databases, VPN connections, etc. However, there are not many that do both, primarily because of the extra drain on resources. It is still a good practice to do both. Even if it does take a bit longer.

19. You see a user logging in as root to perform basic functions. Is this a problem?

A Linux admin account (root) has many powers that are not permitted for standard users. That being said, it is not always necessary to log all the way off and log back in as root in order to do these tasks. For example, if you have ever used the “run as admin” command in Windows, then you will know the basic concept behind “sudo” or “superuser (root) do” for whatever it is you want it to do. It’s a very simple and elegant method for reducing the amount of time you need to be logged in as a privileged user. The more time a user spends with enhanced permissions, the more likely it is that something is going to go wrong — whether accidentally or intentionally.

20. How do you protect your home wireless access point?

This is another opinion question. There are a lot of different ways to protect a wireless access point: using WPA2, not broadcasting the SSID and using MAC address filtering are the most popular among them. There are many other options, but in a typical home environment, those three are the biggest.

Level 3 interview questions: The savvy

By now you’ve seen more than a fair amount of troubles. You’ve got a toolkit of regularly used programs and a standard suite of protection utilities. You’re comfortable with cleanups, and you’ve spent quite a bit of time discovering there are a lot of ways to make things go boom. You’ve also seen that it doesn’t take much to have data disappear forever — and that you need help to protect and manage it. By this stage you are more than likely a member of a team rather than a lone figure trying to work out everything, and as a result you are now on the specialization track. You may or may not, however, have a pointed hat and a predisposition to rum.

21. What is an easy way to configure a network to allow only a single computer to login on a particular jack?

Sticky ports are one of the network admin’s best friends and worst headaches. They allow you to set up your network so that each port on a switch only permits one (or a number that you specify) computer to connect on that port by locking it to a particular MAC address. If any other computer plugs into that port, the port shuts down and you receive a call that they can’t connect anymore. If you were the one that originally ran all the network connections then this isn’t a big issue, and likewise, if it is a predictable pattern, then it also isn’t an issue. However, if you’re working in a hand-me-down network where chaos is the norm, then you might end up spending a while toning out exactly what they are connecting to.

22. You are remoted in to a headless system in a remote area. You have no physical access to the hardware and you need to perform an OS installation. What do you do?

There are a couple of different ways to do this, but the most like scenario you will run into is this: What you would want to do is setup a network-based installer capable of network-booting via PXE (if you've ever seen this during your system boot and wondering what it was for, tada). Environments that have very large numbers of systems more often than not have the capability of pushing out images via the network. This reduces the amount of hands-on time that is required on each system, and keeps the installs more consistent.

23. On a Windows network, why is it easier to break into a local account than an AD account?

Windows local accounts have a great deal of baggage tied to them, running back a long long way to keep compatibility for user accounts. If you are a user of passwords longer than 13 characters, you may have seen the message referring to this fact. However, Active Directory accounts have a great deal of security tied onto them, not the least of which is that the system actually doing the authenticating is not the one you are usually sitting at when you are a regular user. Breaking into a Windows system if you have physical access is actually not that difficult at all, as there are quite a few dedicated utilities for just such a purpose. However, that is beyond the scope of what we'll be getting into here.

24. What is the CIA triangle?

Confidentiality, integrity, availability. As close to a "code" for information security as it is possible to get, it is the boiled down essence of InfoSec. Confidentiality is keeping data secure. Integrity is keeping data intact. Availability is keeping data accessible.

25. What is the difference between an HIDS and a NIDS?

Both acronyms are intrusion detection systems. However, the first is a host intrusion detection system whereas the second is a network intrusion detection system. An HIDS runs as a background utility the same as an antivirus program, for instance, while a NIDS sniffs packets as they go across the network looking for things that aren't quite ordinary. Both systems have two basic variants: signature based and anomaly based. Signature based is very much like an antivirus system, looking for known values of known "bad things," while anomaly looks more for network traffic that doesn't fit the usual pattern of the network. This requires a bit more time to get a good baseline, but in the long term can be better on the uptake for custom attacks.

26. You find out that there is an active problem on your network. You can fix it, but it is out of your jurisdiction. What do you do?

This question is a biggie. The true answer is that you contact the person in charge of that department via email — make sure to keep that for your records — along with CCing your manager. There may be a very important reason why a system is configured in a particular way, and locking it out could mean big trouble. Bringing up your concerns to the responsible party is the best way to let them know that you saw a potential problem, are letting them know about it, and covering yourself at the same time by having a timestamp on it.

27. You are an employee for a tech department in a non-management position. A high-level executive demands that you break protocol and allow him to use his home laptop at work. What do you do?

You would be amazed how often this happens, even more so in the current BYOD environment. Still, the easiest way out of this one is to contact your manager again and have them give a yay or nay. This puts the authority and decision where it needs to be and gives you assistance if the department needs to push back. Stress can be a real killer in position where you have to say “no” to people that don’t like hearing it, so passing the buck can be a friend.

28. What is the difference between a vulnerability and an exploit?

A lot of people would say that they are the same thing, and in a sense they would be right. However, one is a potential problem while the other is an active problem. Think of it like this: You have a shed with a broken lock where it won’t latch properly. In some areas such as major cities, that would be a major problem that needs to be resolved immediately, while in others like rural areas its more of a nuisance that can be fixed when you get around to it. In both scenarios it would be a vulnerability, while the major cities shed would be an example of an exploit — there are people in the area, actively exploiting a known problem.

29. How would you compromise an “office workstation” at a hotel?

Considering how infected these typically are, I wouldn’t touch one with a ten-foot pole. That being said, a USB keylogger is easy to fit into the back of these systems without much notice. An autorun program would be able to run quickly and quietly leaving behind software to do the dirty work. In essence, it’s open season on exploits in this type of environment.

Level 4 interview questions: The keymaster

At this stage, if you have physical access to the box, you own it. You also have enough ethics to not break into every single thing you touch, and here is where personal ethics start to become a tremendous asset — provided you know where to draw the line. You’ve seen a lot of the dirty side of InfoSec, know that it can be used for good and bad just as much as anything else, and you very likely have done some things on both sides of the fence. By the same token, you know the truth of the saying, “It takes a thief to catch a thief,” and so you have gone through penetration testing events and may be a part of a regular team performing exercises against your network and its sites. Unfortunately, Gozer will not be stopping by for s’mores. Sorry about that.

31. What is worse in firewall detection, a false negative or a false positive? And why?

Far and away is a false negative. A false positive is annoying, but easily dealt with — calling a legitimate piece of traffic bad. A false negative is a piece of malicious traffic being let through without incident — definitely bad.

32. What’s better, a red team or a blue team?

Another opinion question, more along the lines of where your interests lie. In penetration testing scenarios, a red team is trying to break in while a blue team is defending. Red teams typically are considered the “cooler” of the two, while the blue team is usually the more difficult. The usual rules apply like in any defense game: the blue team has to be good every time, while the red team only has to be good once. That’s not entirely accurate given the complexities at work in most scenarios, but it’s close enough to explain the idea.

33. What’s the difference between a white box test and a black box test?

The difference is information given by the person commissioning the test. A white box test is one where the pentesting team is given as much information as possible regarding the environment, while a black box test is … well … a black box. They don’t know what’s inside.

34. What is the difference between information protection and information assurance?

Information protection is just what it sounds like — protecting information through the use of encryption, security software and other methods designed to keep it safe. Information assurance on the other hand deals more with keeping the data reliable — RAID configurations, backups, non-repudiation techniques, etc.

35. How would you lock down a mobile device?

Another opinion question, and as usual a lot of different potential answers. The baseline for these though would be three key elements: an anti-malware application, a remote wipe utility and full-disk encryption. Almost all modern mobile devices regardless of manufacturer have anti-malware and remote wipe available for them, and very few systems now do not come with full-disk encryption available as an option directly within the OS.

36. What is the difference between closed-source and open-source? Which is better?

Yet another opinion question. Closed-source is a typical commercially developed program. You receive an executable file which runs and does its job without the ability to look far under the hood. Open-source, however, provides the source code to be able to inspect everything it does, as well as be able to make changes yourself and recompile the code. Both have arguments for and against them, most have to do with audits and accountability. Closed-source advocates claim that open-source causes issues because everybody can see exactly how it works and exploit weaknesses in the program. Open-source counter saying that because closed-source programs don’t provide ways to fully check them out, its difficult to find and troubleshoot issues in the programs beyond a certain level.

37. What is your opinion on hacktivist groups such as Anonymous?

You might have guessed that this level is very much about forming opinions and drawing conclusions, and you'd be right. This one is an especially loaded question. Like any major group without a central leader, they seem to be mostly chaotic, at times seeming like a force for good, while at others causing havoc for innocents. Choose your words very carefully here, as it could be a deal breaker.

38. What is the three-way handshake? How can it be used to create a DOS attack?

The three-way handshake is a cornerstone of the TCP suite: SYN, SYN/ACK, ACK. SYN is the outgoing connection request from client to server. SYN/ACK is the acknowledgement of the server back to the client, saying that yes I hear you, let's open a connection. ACK is the final connection, and allows the two to speak. The problem is that this can be used as a very basic type of denial-of-service attack. The client opens up the SYN connection, the server responds with the SYN/ACK, but then the client sends another SYN. The server treats this as a new connection request and keeps the previous connection open. As this is repeated over and over many times very quickly, the server quickly becomes saturated with a huge number of connection requests, eventually overloading its ability to connect to legitimate users.

39. Why would you bring in an outside contractor to perform a penetration test?

Much like getting a fresh set of eyes on a problem, sometimes you have people that don't want to see or don't want to admit to an issue. Bringing in extra help as an audit can really help eliminate problems your team isn't able to resolve on their own. Granted they may cost a small fortune, but they are extremely good at what they do.

40. If you were going to break into a database-based website, how would you do it?

And here's other side of the coin: learning to break into your own systems so that you can pentest them yourself. While the exact methods are different for each type of database server and programming language, the easiest attack vector to test for first is an SQL injection technique. For example, if the input fields are not sterilized, just entering a specific set of symbols into a form field may be enough to get back data. Alternatively, depending again on how the site is written, using a specially crafted URL may be enough to get back data as well. Footprinting the server ahead of time can help in this task if it isn't one you built yourself.

Level 5 interview questions: The mastermind

By this stage, you are likely in charge of your own department and have a chosen team to work with you. You spend more of your time working on policy changes and directing where your people will be 12-36 months down the road than you do writing code, but you've more than made up for it in legal-jitsu. Protecting the organization at its highest levels is now your job, and the buck stops with you for better or worse. As a result, you need to be on your game all the time and have as much of an edge as possible over outsiders and disgruntled employees wanting to make a statement.

41. Why are internal threats oftentimes more successful than external threats?

When you see something day in and day out, even if it shocks you at first, you tend to get used to it. This means that if you see somebody that pokes around day after day, month after month, you might get used to the fact that he’s just curious. You let your guard down, and don’t react as quickly to possible threats. On the other hand, say you have an annoyed employee that is soon to be fired and wants to show his soon to be former employer that he can bring them down. So he sells his still active credentials and key card to a local group that specializes in white-collar crime. Still other infiltrators dress up as delivery people and wander around aimlessly in office buildings, getting information off of post-it notes and papers lying around. External threats do not have access to near this level of information about the company, and more often than not do not get in as far as somebody that spent 20 bucks on a knock-off UPS uniform.

42. What is residual risk?

I’m going to let Ed Norton answer this one: “A new car built by my company leaves somewhere traveling at 60 mph. The rear differential locks up. The car crashes and burns with everyone trapped inside. Now, should we initiate a recall? Take the number of vehicles in the field, *A*, multiply by the probable rate of failure, *B,* multiply by the average out-of-court settlement, *C*. *A* times *B* times *C* equals *X*. If *X* is less than the cost of a recall, we don’t do one.” Residual risk is what is left over after you perform everything that is cost effective to increase security, but to go further than that is a waste of resources. Residual risk is what the company is willing to live with as a gamble in the hopes that it won’t happen.

43. Why is deleted data not truly gone when you delete it?

When you press delete on a file, it doesn’t actually go anywhere. A bit on the file is flipped telling the operating system that that file is no longer needed and it can be overwritten as is required. Until that happens, the file can still be restored no matter if it’s in a Recycling Bin or not. There are ways around this, such as using file shredders and disk wipers, but both of these take quite a bit of time to finish their jobs to a reasonable degree.

44. What is the chain of custody?

When keeping track of data or equipment for use in legal proceedings, it needs to remain in a pristine state. Therefore, documenting exactly who has had access to what for how long is vital when dealing with this situation. Any compromise in the data can lead to legal issues for the parties involved and can lead to a mistrial or contempt depending on the scenario.

45. How would you permanently remove the threat of data falling into the wrong hands?

If data is on physical media such as a diskette, CD or even paper, there are shredders, pulverizers and destroyers that can turn plastic and paper into confetti. For hard disks however, that becomes a bit more tricky. Most locations will turn to a two-fold method for ensuring a disk's destruction. First, they'll use a specially made disc-wiping program and take apart the hard drive, remove the platters and scratch them up beyond recognition. Then they'll degauss them with a high-powered magnet. This ensures that the data cannot be recovered through conventional means.

46. What is exfiltration?

Infiltration is the method by which you enter or smuggle elements into a location. Exfiltration is just the opposite: getting sensitive information or objects out of a location without being discovered. In an environment with high security, this can be extremely difficult but not impossible. Again we turn to our friends in the fake delivery uniforms wandering around the building, and see that, yes, there are ways to get in and out without a lot of issues.

47. I run an SMB. I have four people in my entire company and a web-based store. I don't have the time, patience or manpower to have a computer guy. Why should I care about exploits and computer jibberish?

This is a classic catch-22 situation: a company doesn't have enough money to secure their networks, but by the same token they can't afford a payout if they get compromised. At the same time, they really can't afford to have a dedicated computer technician, let alone a security consultant. If you are able to explain (in words that don't make it sound like you're just fearmongering), an SMB will acknowledge what they need to do to keep their store secure and keep receiving payments, since following the money will tend to help move things along.

48. I'm the CEO of a Fortune 500 company. I make more in an afternoon than you make in a year. I don't care about this stupid security stuff. It just costs time and money and slows everything down. Why should I care about this junk?

This one is significantly harder — they are used to having people lie, cheat and steal from them on a regular basis, and when somebody comes in saying that the company is going to lose all this money unless you pay for this, they're probably going to say no. Therefore, having done your homework and having the support of the local IT team instead of alienating them is vital. Performing site assessments, creating executive summaries and line-by-line breakdowns of what goes where can help them to better understand what is going to be done and keep the project going.

49. I'm the legal council for a large corporation. We have requirements to document assets and code changes. We have a very limited budget for this task. How would you resolve this?

This is actually one of the easier ones. You have an informed party, asking for assistance to something that is important. They have money for the project (albeit not much), but it is better than nothing. At the very bottom of the spectrum, this could be accomplished in nothing more than Excel with a lot of time and data entry, moving all the way up the chain to automated network scanners documenting everything they find to a database and programs that check-in and out programs with versioning and delta files. It all depends on how big the project is, and how big the company is.

50. I'm the new guy. I used to be a coder at my old job and my manager wants me to create some custom programs. I need domain administrator rights for this task. My boss said it's alright, and you either give me what I need or you're fired and I'll find somebody that will. How do you respond?

Unfortunately, you will run into the hardball guy at least once in your career. In this case though, like others we have run into, it's time to move it up the chain to the manager. They will be able to give the yay or nay depending on exactly what the project is and be able to take the brunt of an attack if it comes.

1. What are the hacking stages? Explain each stage

Hacking, or targeting a specific machine, should follow and go through the following five phases:

- **Reconnaissance:** This is the first phase where the hacker attempts to collect as much information as possible about the target.
- **Scanning:** This stage involves exploiting the information gathered during reconnaissance phase and using it to examine the victim. The hacker can use automated tools during the scanning phase which can include port scanners, mappers and vulnerability scanners.
- **Gaining access:** This is the phase where the real hacking takes place. The hacker now attempts to exploit vulnerabilities discovered during the reconnaissance and scanning phase to gain access.
- **Maintaining access:** Once access is gained, hackers want to keep that access for future exploitation and attacks by securing their exclusive access with backdoors, rootkits and trojans.
- **Covering tracks:** Once hackers have been able to gain and maintain access, they cover their tracks and traces to avoid detection. This also allows them to continue the use of the hacked system and avoid legal actions.

2. What is scanning and what are some examples of the types of scanning used?

Scanning may be referred to as a set of procedures for identifying hosts, ports and the services attached to a network. Scanning is a critical component for information gathering. It allows the hacker to create a profile on the site of the organization to be hacked. Types of scanning include:

- Port scanning
- Vulnerability scanning

- Network scanning

3. What is footprinting? What are the techniques used for footprinting?

Footprinting refers to accumulating and uncovering information about the target network before attempting to gain access. Hacking techniques include:

- **Open source footprinting:** This technique will search for administrator contact information, which can be later used for guessing the correct password in social engineering.
- **Network enumeration:** This is when the hacker attempts to identify the domain names and network blocks of the targeted
- **Scanning:** Once the network is known, the second step is to pry on the active IP addresses on the network.
- **Stack fingerprinting:** This techinique should be the final footprinting step that takes place once the port and host are mapped.

4. What are some of the standard tools used by ethical hackers?

To facilitate some manual tasks and speed up the hacking process, hackers can use a set of tools such as:

- Metasploit
- Wireshark
- NMAP
- Burp Suite
- OWASP ZAP
- Nikto
- SQLmap

5. What is Burp Suite? What tools does it contain?

Burp Suite is an integrated platform used for attacking web applications. It contains all the possible tools a hacker would require for attacking an application. Some of these functionalities include, but are not limited to:

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Decoder

- Comparer
- Sequencer

6. What is network sniffing?

Network sniffing involves using sniffer tools that enable real-time monitoring and analysis of data packets flowing over computer networks. Sniffers can be used for different purposes, whether it’s to steal information or manage networks.

Network sniffing is used for ethical as well as unethical purposes. Network administrators use these as network monitoring and analysis tools to diagnose and prevent network-related problems such as traffic bottlenecks. Cybercriminals use these tools for dishonest purposes such as identity usurpation, email, sensitive data hijacking and more.

7. What is SQL injection and its types?

A SQL injection occurs when the application does not sanitize the user input. Thus a malicious hacker would inject SQL query to gain unauthorized access and execute administration operations on the database. SQL injections can be classified as follows:

- Error-based SQL injection
- Blind SQL injection
- Time-based SQL injection

8. What is cross-site scripting and its different variations?

Cross-site scripting (XSS) attacks are a type of injection where malicious scripts are injected into otherwise benign and trusted websites. XSS takes place when an attacker inserts a malicious payload, usually in the form of JavaScript code in a web form. XSS vulnerabilities are categorized as follows:

- Reflected cross-site scripting
- Stored cross-site scripting
- DOM-based cross-site scripting

9. What is a denial of service (DOS) attack and what are the common forms?

DOS attacks involve flooding servers, systems or networks with traffic to cause over-consumption of victim resources. This makes it difficult or impossible for legitimate users to access or use targeted sites.

Common DOS attacks include:

- Buffer overflow attacks
- ICMP flood
- SYN flood
- Teardrop attack
- Smurf attack

10. How can you avoid or prevent ARP poisoning?

ARP poisoning is a form of network attack that can be mitigated through the following methods:

- Use packet filtering: Packet filters can filter out and block packets with conflicting source address information.
- Avoid trust relationship: Organizations should develop a protocol that relies on trust relationship as little as possible.
- Use ARP spoofing detection software: Some programs inspect and certify data before it is transmitted and blocks data that is spoofed.
- Use cryptographic network protocols: ARP spoofing attacks can be mitigated by the use of secure protocols such as SSH, TLS and HTTPS which send data encrypted before transmission and after reception.

1. What is the difference between a public key cryptography and a private key for encrypting and signing content?

A sender or recipient publishes his public key. You use the public key to encrypt content and your private key to sign the content. This is the standard form of communication with encryption and signing.

2. What port is for ICMP or pinging?

Ping uses the ICMP protocol, which is a layer 3 protocol. Ping doesn’t use a port, so you will want to note this is a trick question if asked.

3. Do you prefer Windows or Linux?

This question is more of a preference, but many network security professionals know Linux works well with security. For instance, Linux is better to know when working with routers. Be honest with your answer and give pros and cons that relate to which one you prefer.

4. What should be implemented on a login page?

Whenever you transfer sensitive data, you need to use HTTPS. Ensure you answer this question with HTTPS and possibly how you would implement a conversion of HTTP to HTTPS.

5. How would an HTTP program handle state?

HTTP does not handle state natively. HTTP applications use cookies to handle the state of an application. The developer can also store data in the web server's session.

6. What is Cross Site Scripting (XSS)?

Cross-site scripting occurs when an attacker is able to inject executable code within JavaScript. This is done through a hacked database or poorly scrubbed querystring variables.

7. What are the two types of XSS?

Cross-site scripting has two types of attacks: reflected and stored. A stored XSS hack allows the attacker to store malicious code within the database. The database content is served to the user from the database and can be used in private pages behind a secure login to gain access to site private data. The next is reflected, and this comes from the hacker sending the user a link that runs JavaScript code within the pages directly from the querystring.

8. What are some ways that the company can defend against XSS?

First, programmers should defend against JavaScript added to a querystring. Also, remove JavaScript from any input variables sent through online forms and stored in a database.

9. What can you use to defend against multiple login attempts?

You can create a lockout policy that locks accounts when a user has too many login attempts.

10. How can you defend against phishing attempts?

Phishing is usually done through email, so you can block some SMTP servers and senders, and educate users on phishing attempts.

11. What is an ACL?

An access control list. It is a list used to grant users and processes access to system resources.

12. What is the purpose of a firewall?

It is used to control network traffic by determining what type of packets are allowed to pass through.

13. Describe a proxy.

A network service that allows clients to make indirect network connections to other network services.

14. What is a HIDS?

A host based IDS (intrusion detection system) is used to monitor malicious activity. It is placed on an individual host computer instead of a server.

15. What is a good practice for securing network devices?

Disabling unused ports.

16. Describe an IDS (intrusion detection system).

A network- or host-based monitoring system that is used to alert system administrators of suspected intrusions or other unauthorized activity.

17. What are MAC, DAC and RBAC?

Mandatory access control, discretionary access control and role-based access control. MAC uses the operating system to prevent a user from accessing a particular target. DAC restricts access to an object based on a user’s identity or group. RBAC denies or grants access based on a user’s role.

18. How can you ensure the privacy of a VPN connection?

Tunneling.

19. What is a packet sniffer or protocol analyzer?

A software tool used for monitoring and examining contents of the network traffic.

20. What are the layers in the OSI model?

Physical, data link, network, transport, session, presentation and application.

21. What is port 443?

HTTPS (hypertext transfer protocol secure).

22. What is Wireshark?

A network protocol analyzer used to examine packets sent across a network.

23. What is UTM?

Unified threat management. A network security solution that provides URL filtering, malware or content inspection. It combines the functionality of a firewall with these additional safeguards.

24. Describe a signature-based IDS.

It uses known attack patterns to detect an intrusion.

25. Describe rule-based access control.

A type of access control model which grants or denies access to resources based on ACL entries.

Get live, expert ins

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
- Network security
- Operational security
- Application security
- End-user education
- 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 prevent 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:

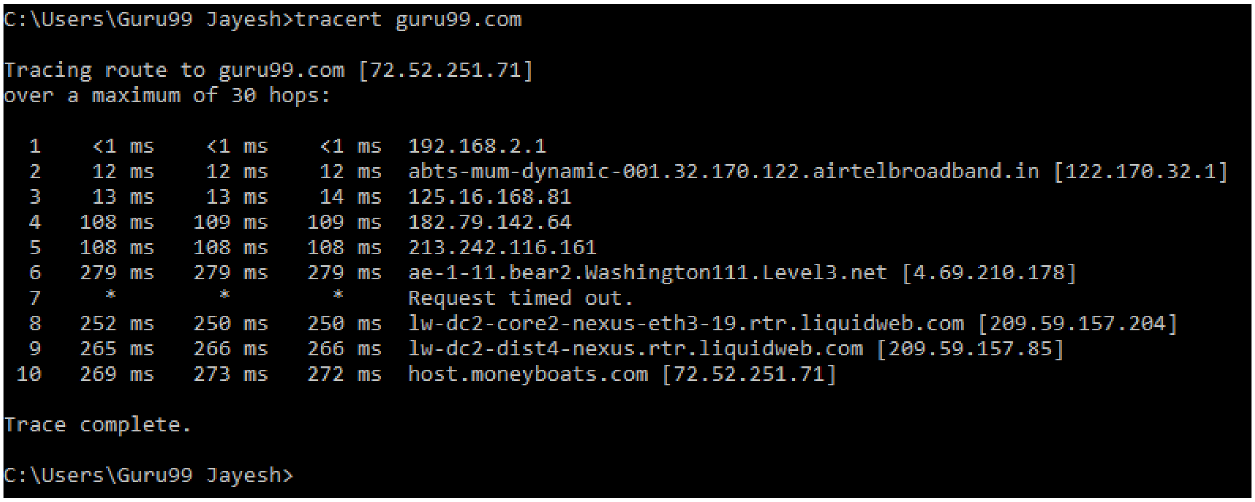
- Confidentiality: Ensure the sensitive data is accessed only by an authorized user.
- Integrity: Integrity means the information is in the right format.
- Availability: Ensure the data and resources are available for users who need them.

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 device 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:

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, 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 address associated with IPv4 address. This protocol work 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 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 server.

52) Define Forward Secrecy.

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

Following are some examples of symmetric encryption algorithm.

- RCx
- Blowfish
- Rijndael (AES)
- DES

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 object.

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 email.
- 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 is 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 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 faster compared to a virus.

71) Name some tools used for packet sniffing.

Following are some tools used for packet sniffing.

- Tcpdump
- Kismet
- Wireshark

- NetworkMiner
- Dsniff

72) Explain anti-virus sensor systems

Antivirus is 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

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 application 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 share confidential data with outsiders or a business partner going beyond the policy of the company.

What is Security Testing?

Security testing is a process intended to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended.

Security testing is the most important type of testing for any application. In this type of testing, tester plays an important role as an attacker and play around the system to find security-related bugs.

Top 30 Security Testing Interview Questions

Q #1) What is Security Testing?

Answer: Security testing can be considered as the most important in all types of software testing. Its main objective is to find vulnerabilities in any software (web or networking) based application and protect their data from possible attacks or intruders.

As many applications contain confidential data and need to be protected from being leaked. Software testing needs to be done periodically on such applications to identify threats and to take immediate action on them.

Q #2) What is "Vulnerability"?

Answer: Vulnerability can be defined as the weakness of any system through which intruders or bugs can attack the system.
If security testing has not been performed rigorously on the system then chances of vulnerabilities get increased. Time to time patches or fixes is required to prevent a system from the vulnerabilities.

Q #3) What is Intrusion Detection?

Answer: Intrusion detection is a system which helps in determining possible attacks and deal with it. Intrusion detection includes collecting information from many systems and sources, analysis of the information and finding the possible ways of the attack on the system.

Intrusion detection checks the following:

- Possible attacks
- Any abnormal activity
- Auditing the system data
- Analysis of different collected data, etc.

Q #4) What is "SQL Injection"?

Answer: SQL Injection is one of the common attacking techniques used by hackers to get critical data.

Hackers check for any loophole in the system through which they can pass SQL queries, bypass the security checks, and return back the critical data. This is known as SQL injection. It can allow hackers to steal critical data or even crash a system.

SQL injections are very critical and need to be avoided. Periodic security testing can prevent this kind of attack. SQL database security needs to be defined correctly and input boxes and special characters should be handled properly.

Q #5) List the attributes of Security Testing?

Answer: There are following seven attributes of Security Testing:

1. Authentication
2. Authorization
3. Confidentiality
4. Availability
5. Integrity
6. Non-repudiation
7. Resilience

Q #6) What is XSS or Cross-Site Scripting?

Answer: XSS or cross-site scripting is a type of vulnerability that hackers used to attack web applications.

It allows hackers to inject HTML or JAVASCRIPT code into a web page that can steal the confidential information from the cookies and returns to the hackers. It is one of the most critical and common techniques which needs to be prevented.

Q #7) What are the SSL connections and an SSL session?

Answer: SSL or Secured Socket Layer connection is a transient peer-to-peer communications link where each connection is associated with one SSL Session.

SSL session can be defined as an association between client and server generally created by the handshake protocol. There are a set of parameters defined and it may be shared by multiple SSL connections.

Q #8) What is “Penetration Testing”?

Answer: Penetration testing is on security testing which helps in identifying vulnerabilities in a system. A penetration test is an attempt to evaluate the security of a system by manual or automated techniques and if any vulnerability found, testers use that vulnerability to get deeper access to the system and find more vulnerabilities.

The main purpose of this testing is to prevent a system from any possible attacks. Penetration testing can be done in two ways –White Box testing and Black box testing.

In white-box testing, all the information is available with the testers whereas in black box testing, testers don't have any information and they test the system in real-world scenarios to find out the vulnerabilities.

Q #9) Why "Penetration Testing" is important?

Answer: Penetration testing is important because-

- Security breaches and loopholes in the systems can be very costly as the threat of attack is always possible and hackers can steal important data or even crash the system.
- It is impossible to protect all the information all the time. Hackers always come with new techniques to steal important data and it is necessary for testers as well to perform periodical testing to detect the possible attacks.
- Penetration testing identifies and protects a system by the above-mentioned attacks and helps organizations to keep their data safe.

Q #10) Name the two common techniques used to protect a password file?

Answer: Two common techniques to protect a password file is- hashed passwords and a salt value or password file access control.

Q #11) List the full names of abbreviations related to Software security?

Answer: Abbreviations related to software security include:

1. **IPsec** – Internet Protocol Security is a suite of protocols for securing Internet
2. **OSI** – Open Systems Interconnection
3. **ISDN** Integrated Services Digital Network
4. **GOSIP-** Government Open Systems Interconnection Profile
5. **FTP** – File Transfer Protocol
6. **DBA** – Dynamic Bandwidth Allocation
7. **DDS** – Digital Data System
8. **DES** – Data -Encryption Standard
9. **CHAP** – Challenge Handshake Authentication Protocol
10. **BONDING** – Bandwidth On Demand Interoperability Group
11. **SSH** – The Secure Shell
12. **COPS** Common Open Policy Service
13. **ISAKMP** – Internet Security Association and Key Management Protocol
14. **USM** – User-based Security Model
15. **TLS** – The Transport Layer Security

Q #12) What is ISO 17799?

Answer: ISO/IEC 17799 is originally published in the UK and defines best practices for Information Security Management. It has guidelines for all organizations small or big for Information security.

Q #13) List down some factors that can cause vulnerabilities?

Answer: Factors causing vulnerabilities are:

1. **Design flaws:** If there are loopholes in the system that can allow hackers to attack the system easily.
2. **Passwords:** If passwords are known to hackers they can get the information very easily. Password policy should be followed rigorously to minimize the risk of password steal.
3. **Complexity:** Complex software can open doors on vulnerabilities.
4. **Human Error:** Human error is a significant source of security vulnerabilities.
5. **Management:** Poor management of the data can lead to the vulnerabilities in the system.

Q #14) List the various methodologies in Security testing?

Answer: Methodologies in Security testing are:

1. **White Box-** All the information are provided to the testers.
2. **Black Box-** No information is provided to the testers and they can test the system in a real-world scenario.
3. **Grey Box-** Partial information is with the testers and rest they have to test on their own.

Q #15) List down the seven main types of security testing as per Open Source Security Testing methodology manual?

Answer: The seven main types of security testing as per the Open Source Security Testing methodology manual are:

- **Vulnerability Scanning:** Automated software scans a system against known vulnerabilities.
- **Security Scanning:** Manual or automated technique to identify network and system weaknesses.
- **Penetration testing:** Penetration testing is on the security testing which helps in identifying vulnerabilities in a system.
- **Risk Assessment:** It involves the analysis of possible risks in the system. Risks are classified as Low, Medium and High.
- **Security Auditing:** Complete inspection of systems and applications to detect vulnerabilities.
- **Ethical hacking:** Hacking is done on a system to detect flaws in it rather than personal benefits.
- **Posture Assessment:** This combines Security Scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.

Q #16) What is SOAP and WSDL?

Answer: SOAP or **Simple Object Access Protocol** is an XML-based protocol through which applications exchange information over HTTP. XML requests are sent by web services in SOAP format then a SOAP client sends a SOAP message to the server. The server responds back again with a SOAP message along with the requested service.

Web Services Description Language (WSDL) is an XML formatted language used by UDDI. “Web Services Description Language describes Web services and how to access them”.

Q #17) List the parameters that define an SSL session connection?

Answer: The parameters that define an SSL session connection are:

1. Server and client random
2. Server write MACsecret
3. Client write MACsecret
4. Server write key
5. Client write key
6. Initialization vectors
7. Sequence numbers

Q #18) What is file enumeration?

Answer: This kind of attack uses forceful browsing with the URL manipulation attack. Hackers can manipulate the parameters in URL string and can get the critical data which generally does not open for the public such as achieved data, old version or data which is under development.

Q #19) List the benefits that can be provided by an intrusion detection system?

Answer: There are three benefits of an intrusion detection system.

1. NIDS or Network Intrusion Detection
2. NNIDS or Network Node Intrusion Detection System
3. HIDS or Host Intrusion Detection System

Q #20) What is HIDS?

Answer: HIDS or Host Intrusion Detection system is a system in which a snapshot of the existing system is taken and compared with the previous snapshot. It checks if critical files were modified or deleted then an alert is generated and sent to the administrator.

Q #21) List down the principal categories of SET participants?

Answer: Following are the participants:

1. Cardholder
2. Merchant
3. Issuer
4. Acquirer

5. Payment gateway
6. Certification authority

Q #22) Explain “URL manipulation”?

Answer: URL manipulation is a type of attack in which hackers manipulate the website URL to get the critical information. The information is passed in the parameters in the query string via HTTP GET method between client and server. Hackers can alter the information between these parameters and get the authentication on the servers and steal the critical data.

In order to avoid this kind of attack security testing of URL manipulation should be done. Testers themselves can try to manipulate the URL and check for possible attacks and if found they can prevent these kinds of attacks.

Q #23) What are the three classes of intruders?

Answer: The three classes of intruders are:

1. **Masquerader:** It can be defined as an individual who is not authorized on the computer but hacks the system’s access control and get access of authenticated user’s accounts.
2. **Misfeasor:** In this case, user is authenticated to use the system resources but he misuses his access to the system.
3. **Clandestine user,** It can be defined as an individual who hacks the control system of the system and bypasses the system security system.

Q #24) List the component used in SSL?

Answer: Secure Sockets Layer protocol or SSL is used to make secure connections between clients and computers.

Below are the component used in SSL:

1. SSL Recorded protocol
2. Handshake protocol
3. Change Cipher Spec
4. Encryption algorithms

Q #25) What is port scanning?

Answer: Ports are the point where information goes in and out of any system. Scanning of the ports to find out any loopholes in the system is known as Port Scanning. There can be some weak points in the system to which hackers can attack and get the critical information. These points should be identified and prevented from any misuse.

Following are the types of port scans:

- **Strobe:** Scanning of known services.
- **UDP:** Scanning of open UDP ports
- **Vanilla:** In this scanning, the scanner attempts to connect to all 65,535 ports.
- **Sweep:** The scanner connects to the same port on more than one machine.
- **Fragmented packets:** The scanner sends packet fragments that get through simple packet filters in a firewall
- **Stealth scan:** The scanner blocks the scanned computer from recording the port scan activities.
- **FTP bounce:** The scanner goes through an FTP server in order to disguise the source of the scan.

Q #26) What is a Cookie?

Answer: A cookie is a piece of information received from a web server and stored in a web browser which can be read anytime later. A cookie can contain password information, some auto-fill information and if any hackers get these details it can be dangerous

Q #27) What are the types of Cookies?

Answer: Types of Cookies are:

- **Session Cookies** – These cookies are temporary and last in that session only.
- **Persistent cookies** – These cookies stored on the hard disk drive and last till its expiry or manual removal of it.

Q #28) What is a honeypot?

Answer: Honeypot is a fake computer system that behaves like a real system and attracts hackers to attack it. Honeypot is used to find out loopholes in the system and to provide a solution for these kinds of attacks.

Q #29) List the parameters that define an SSL session state?

Answer: The parameters that define an SSL session state are:

1. Session identifier
2. Peer certificate
3. Compression method
4. Cipher spec
5. Master secret
6. Is resumable

Q #30) Describe the Network Intrusion Detection system?

Answer: Network Intrusion Detection system generally is known as NIDS. It is used for the analysis of the passing traffic on the entire subnet and to match with the known attacks. If any loophole identified then the administrator receives an alert.

Q1. What is Information Security?

Ans: In simple words, Information Security is a practice to secure information from any unauthorized access. ISO/IEC 27000:2009 defined this term as "Preservation of confidentiality, integrity, and availability of information. Note: Also, other properties, such as authenticity, accountability, non-repudiation, and reliability, can also be involved."

Q2. What is the importance of A Penetration Test?

Ans: Penetration Testing is important for identifying vulnerabilities in an IT system from outside the network. Generally, It is an activity done after vulnerability assessment. In simple words, you can say, by doing Penetration testing, security analysts are attempting to gain access to resources without knowledge of usernames, passwords, and other normal means of access. You can only differentiate hackers from security experts is the permission given by the organization.

Q3. What are the phases of Network Penetration?

Ans: Penetration testing dividing into 5 phases:
Phase 1 – Reconnaissance It is a process of collecting data about the target. It can be performed actively or passively. In this phase, you learn more and more about the target business and its operation. Activities include identifying the target, finding out the target IP address range, network, domain name, mail server, DNS records, etc.
Phase 2 – Scanning This is another crucial phase of penetration testing. In this phase, scanning has been done to identify vulnerabilities in the network and software and OS used by devices. After this activity, the pen tester learns about services running, open ports, firewall detection, vulnerabilities, OS, etc. There are a lot of tools available, both open-source and paid.
Phase 3 – Gaining Access In this phase, the pen tester started executing the attack by gaining access to vulnerable devices and servers. This can be done by using tools.
Phase 4 – Maintaining Access As a pen tester already gained access to a vulnerable system, in this phase, he/she tries to extract as much data and also remain stealthy.
Phase 5 – Covering Tracks In this phase, the pen tester takes all the necessary steps to hide the intrusion and possible controls left behind for future visits. He/she also remove all kinds of logs, uploaded backdoor(s), and anything related to the attack.

Q4. What is XSS or Cross-Site Scripting?

Ans: As explained by OWASP, "Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in a browser-side script, to a different end-user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it."

Q5. What is the difference between asymmetric and symmetric encryption?

Ans: The major difference between symmetric and asymmetric cryptography is using the single key for encryption and decryption in case of symmetric cryptography during the use of the public and private key for encryption and decryption in case of asymmetric cryptography.

Q6. What is "Vulnerability"?

Ans: Vulnerability is a term that every information security expert wants to eradicate from the IT system. If someone exploited those vulnerabilities, it might result in an intentional or unintentional compromise of a system.

Q7. Discuss a recent project of pen test which you have done?

Ans: To answer this question, you can start with the last project you have done in a pen test field. Also, mention your approach, which tools you have used, which vulnerabilities you have found, and how you help the developer to fix those issues.

Q8. What are the strengths and differences between Windows and Linux?

Ans:

	Linux	**Windows**
Price	Available Free	Paid
Ease Of Use	Little difficult for beginners	User-friendly
Reliability	more reliable and secure	less reliable and secure
less reliable and secure	available for install both paid and free	software available for install both paid and free
Software Cost	most software available for free	mostly commercial software available
Hardware	In beginning, hardware compatibility was an issue. But now, the majority of physical appliance support Linux	Hardware compatibility never an issue for Windows
Security	Highly secure Operating System	As this OS used by the novice user, it is vulnerable to hackers
Support	Community support available online for rectifying any issue	Microsoft support available online and also many books published to diagnosed any issue.
Use Cases	Used mainly by corporate, scientific and educational institute	Used mainly by novice users, gamers, corporates etc. where more skills are not required

Showing 1 to 9 of 9 entries
PreviousNext

Q9. What kind of penetration can be done with the Diffie Hellman exchange?

Ans: Diffie–Hellman key exchange (DH) is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols.
Weak ephemeral Diffie-Hellman parameter detection for SSL/TLS services is a kind of PT that can be done with this method.

Q10. What type of tools are there out there for packet sniffing?

Ans: Packet Sniffing is a process of capture network traffic and able to see traffic on an entire network or only a certain segment of it with the help of packet sniffing tool, depending on how the network switches are configured, placed, etc. The most popular packet sniffing tool available free is Wireshark.

Q11. How will you protect the data during and after Penetration Testing?

Ans: Pen Tester clearly specified policy regarding the finding of user data while testing. The policy tells what to do if any data encountered during and after testing. However, Backup is a must to avoid any loss of data.

Q12. What is Intrusion Detection?

Ans: Intrusion Detection, as the name suggests, it protects IT infrastructure from any cyber attack. It identifies security breaches from both outsides and within a network. Intrusion Detection performs a wide variety of functions, including monitoring and analyzing traffic, recognizing the pattern of attack, checking the integrity of files in servers, checking if any policy violation happens, etc.

Q13. What are the full names of abbreviations related to Software security: 2FA, 2S2D, 2VPCP, 3DES, 3DESE, and 3DESEP?

Ans: Full names of abbreviations:

- **2FA** Two Factor Authentication
- **2S2D** Double-Sided Double-Density
- **2VPCP** Two-Version Priority Ceiling Protocol
- **3DES** Triple Data Encryption Standard
- **3DESE** Triple Data Encryption Standard Encryption
- **3DESEP** Triple Data Encryption Standard Encryption Protocol

Q14. List down some factors that can cause security vulnerabilities.

Ans: There are many factors involved in security vulnerabilities. Some of them are listed below:

- The web application is not doing input validation
- Weak passwords
- The session id is not changing after login
- Sensitive data stored in clear text
- Errors reveal sensitive information about infrastructure
- Software installed not updated

Q15. List down parameters that define an SSL session connection.

Ans: The session identifier, peer certificate, compression method, cipher spec, master secret, and Is resumable are the parameters that define SSL session connection.

Q16. List the benefits that can be provided by an intrusion detection system.

Ans: Here are some benefits of using IDS:

- Helps in identifying security incidents and Denial of Service attack.
- Check for the unexpected and abstract behavior of traffic.
- Stops cross-site scripting, SQL injection etc. attacks
- Protect vulnerable assets by providing temporary patches for known vulnerabilities.

Q17. What is SQL injection?

Ans: It is an attack in which an attacker inserts untrusted data in the application that results in revealing sensitive information of the database.

Q18. How SSL/TLS works?

Ans: SSL/TLS layer provides confidentiality and integrity while data is transmitting from source to destination.

Steps involved:

1. The user initiates the connection by typing the website address. The browser initiates SSL/TLS communication by sending a message to the website's server.
2. The website's server sends back the public key or certificate to the user's browser.
3. User's browser checks for public key or certificate. If it is ok, it creates a symmetric key and sends it back to the website's server. If the certificate is not ok, the communication fails.
4. On receiving the symmetric key, the website's server sent the key and encrypted the requested data.
5. The user's browser decrypts the content using a symmetric key, which completes the SSL/TLS handshake. The user can see content as now connection is established.

Q19. What is the difference between Vulnerability Scan, Risk Analysis, and Penetration Test?

Ans:

Show
entries

Parameter	Vulnerability Scan	Penetration Testing	Risk Analysis
Activity	Check for known vulnerabilities in configuration	Test for exploitability of vulnerabilities and test for how much data leak if an attacker successfully exploits the vulnerability.	Analysis of cost/benefit if the vulnerability is not fixed. It also involves calculation of loss incurred on any security breach.
Skill	Minimal as many tools available	Difficult to find all possible vulnerabilities and exploit them	It requires a skilled person who knows IT, statistics, finance, and probabilities.
Major tools	Nikto, Nessus, OpenVAS	Metaspoilt, Qualys	Difficult to automate

PreviousNext

Q20. What network controls would you recommend to strengthen the network security of an organization?

Ans: These top network controls help in strengthing network security of an organization:

- Always install and run whitelisted applications and software.
- Regular patch all the running applications and software.
- Update OS with the latest security patches.
- Minimize administrative privileges.

Q21. What tools/infrastructure do you have in your penetration testing lab?

Ans: As a penetration tester, you need to use the high processing computer system and many penetration testing tools. Use virtual machines on your desktop and install operating systems such as Windows XP, Windows Server 2008, Windows Server 2012, Ubuntu, etc. to test the configurations. I am listing some tools below, which we can use for penetration testing.

- Burpsuite (both free and commercial version available)
- Wireshark (open source)
- OWASP ZAP (open source)
- Nessus (both free and commercial version available)
- Metasploit (open source)
- NMap (open source)
- Nikto (open source)
- OpenVAS (open source)

You can also install Kali Linux (open-source operating system) on one of your virtual machines, which come with many preinstalled software. This is not an exhaustive list, but you have enough confidence to execute penetration testing jobs after learning these tools.

Q22. List out common network security vulnerabilities.

Ans: Some common network security vulnerabilities are listed below:

- Usage of default or weak passwords in network components such as the router, firewall, etc., and different servers.
- Missing security patches in software running on different network components and different servers.
- Misconfigured network firewall.
- Use of infected USB drives by network professionals in data centers.
- The data backup policy is not implemented properly.

Q23. What are the common ports to focus on during penetration testing?

Ans: You can use the Nmap tool for the port scan. Here is a list of common ports to focus on during penetration testing:

- FTP (port 20, 21)
- SSH (port 22)
- Telnet (port 23)
- SMTP (port 25)
- HTTP (port 80)
- NTP (port 123)
- HTTPS (port 443)

Q24. Do you hire criminals for a pen test? Aren't former "black hats" the best penetration testers?

Ans: This interview question is related to ethics. You can definitely hire a former "black hats" for penetration testing by doing proper verification checks. An organization can decide regarding the hiring of individuals based on company policies.

Q25. If we're already performing vulnerability scanning, why should we perform a penetration test?

Ans: Vulnerability scan generally identifies weaknesses based on vulnerability signatures available in the scanning tool. While penetration testing helps in identifying the extent of data loss and exposure on occurring of cyber attack.

Q26. We received a Penetration Test proposal that was quoted significantly lower than other proposals we received – why is that?

Ans: Charges of penetration testing varies from company to company. Generally, quotation of penetration testing charges based on the salary of security tester, charges of tools used, size of the project, etc. Also, some infosec organization charges less than others based on competition in the market.

Q27. How do you schedule a penetration test?

Ans: It is advisable to conduct penetration testing regularly or on changing in any hosting infrastructure.

Q28. What is an example of a large pen test engagement you've performed?

Ans: Here, give information regarding your penetration testing projects which you have performed in your previous organization. You can also mention the major vulnerabilities and tools used which you have found.

Q29. How long does it take to perform a penetration test?

Ans: It depends on many factors such as the size of the project, skill of penetration tester, the technology used, etc.

Q30. How much experience do you have performing penetration testing?

Ans: Here, you can mention your experience in performing penetration testing jobs.

Q31. Can a penetration test break any system?

Ans: Every system has some security vulnerability- it may be known or unknown by researchers. No system is full proof so if proper penetration testing performs, any system can be break by the security analyst. If the system is more secure, the security analyst will take more time to break and vice-versa. Time may vary from some days to months.

Q32. What certifications do you have to perform penetration testing?

Ans: Certifications are just additional qualifications of a penetration tester. But certifications are not proof of skills of the tester. Some professionals don't have any certification, but still, they are best in their job. Certifications which are beneficial for penetration tester are EC-Council Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP) and GIAC Exploit Researcher & Advanced Penetration Tester (GXPN).

Q33. My data is stored in the cloud. Why do I need a Penetration test?

Ans: Even data is stored in the cloud, penetration testing is still essential to see whether your data is secure or not.

Q34. What types of systems have you performed penetration testing on?

Ans: Penetration testing performed on servers, endpoints, web applications, mobile devices, wireless networks, network devices, cloud services and other potential targets of exposure.

Q35. How often should an organization have a penetration test performed by a third-party?

Ans: It depends on the criticality of the organization's data hosted on the system. If data is more sensitive, the frequency of penetration testing should be more and vice-versa.

Q36. Do penetration tests cause any disruption to an organization's network?

Ans: It may cause disruption of services if penetration tester successfully exploits the vulnerabilities. To minimize disruption, keep your client informed and also stop the testing if required.

Q37. Why is penetration testing important to an organization's risk management strategy?

Ans: Risk management strategy is a process of identifying, accessing, and managing the risk in the system. Penetration testing is an assessment of the IT system from the perspective of a hacker. This activity gives confidence to management that the company's IT assets are secure.

Q38. Can you target any IP Address for penetration testing?

Ans: Penetration testing started only after detailed discussion regarding targets with the management of the company. The legal agreement also signed between pen-testing agency and company and mention all IP address which are in the scope of the test.

Q39. We have a firewall in place. Do we still need network penetration testing if we have a Firewall?

Ans: Firewall is used for analyzing traffic and blocks it based on predetermined configuration. While penetration testing checks for exploitability of IT assets including the firewall. Penetration testing is a necessary activity even with all the network components in place.

Q40. Why should a third party assess your system?

Ans: Generally organizations have their own security teams to manage the cybersecurity-related operations. But still, third-party penetration testing is recommended to build confidence in management and takes advantage of the experience of other organizations in identifying new vulnerabilities in the system.

Q41. Does Pentesting do social engineering?

Ans: Generally, social engineering is not in the scope of penetration testing. But nowadays some organizations do consider the social engineering aspect while doing pen-testing.

Q42. Are Denial-of-service attacks also tested?

Ans: Denial-0f-service (DoS) attacks are also within the scope of penetration testing. Many tools are available to see whether the system is vulnerable to DoS attacks or not.

Q43. Why should not only the network perimeter be tested, but also the internal network?

Ans: Internal network also vulnerable to some type of attack. It is advisable that the scope is not just internet-facing servers, other internal servers also should be in scope.

Q44. What time investment do you estimate for a Penetration Test?

Ans: Time estimate depends on the number of IT devices, and experience of the tester, the time required for fixing of security issues by developers, etc**.**

Q45. Are there legal requirements for Penetration Tests?

Ans: Penetration testing started only when there is an agreement signed by the organization and pen testing agency. In an agreement, the list of targets explicitly mentioned which are the scope of pen-testing. Testers advised not to test any other target outside the scope.

Q46. How can you encrypt email messages?

Ans: OpenPGP is the most popularly used email encryption standard. Both open source such as Gpg4win, and many commercial tools available that support the OpenPGP type of encryption.

Q47. Do You Automate Using Scripting?

Ans: Good pen tester generally do a lot of scripting in Python, Perl, shell, etc. to automate tasks.

Q48. What is a 'Threat Model'?

Ans: Threat model is a process of analyzing the application or IT system in terms of security. In simple terms, it helps in identify, quantify, and address the security risk available in the system.

Q49. What is STRIDE?

Ans: STRIDE is an acronym for the threat modeling system. It helps in categorizing all cyberattacks into the below techniques:

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service (DoS)
- **E**levation of privilege

Q50. What is file enumeration?

Ans: File enumeration, also called forced browsing, is a directory traversal technique when a security analyst access those files and folders which are not linked by an application.

Q1. What is Penetration Testing and how is it useful?

Answer:
Penetration Testing is also called Pen Testing and is a kind of cyber attack on a web application or a system which can be of good or bad intent. In terms of bad intent, it is a kind of cyber attack on a system to steal some kind of secure, confidential and sensitive information. In terms of good intent, it is a kind of checking the strengths and weaknesses of a system to vulnerabilities and external attacks and the strength of security levels it can handle.

Q2. What are the advantages of Penetration Testing?

Answer:
This is the common Penetration Testing Interview Questions asked in an interview. The advantages of performing Penetration Testing on a System are –

1. It will help in detecting the security threats and vulnerabilities of a system or web application.
2. It will help in monitoring the necessary standards to evade some.
3. It is helpful in reducing the downtime of the application in case of diverting large amounts of traffic to the network by penetrating into the application.
4. It protects the organizations confidential and secured information and maintains the brand image or value.
5. It is important in securing the application to avoid huge financial losses.
6. Focuses more on business continuity.
7. Maintains trust among the customers.

Q3. What are the different stages of Penetration Testing?

Answer:
There are different stages of performing penetration testing on a target system or web application such as Planning and reconnaissance, Scanning, Gaining access, Maintaining access, Analysis and configuration:

1. **Planning and Reconnaissance**: In this stage analysis and testing the goals to carry out are performed and the information is gathered.
2. **Scanning:** In this stage, any kind of scanning tool is used to test the responsiveness of a target system in the case of intruder penetration.
3. **Gaining Access:** In this stage, penetration or intruder attack will be executed and web applications are attacked to disclose the possible vulnerabilities of the system.
4. **Maintaining Access:** In this, stage the gained access will be maintained carefully to identify the vulnerabilities and weakness of the system.
5. **Analysis and Configuration:** In this stage, the results obtained from the maintained access will be used to configure Web Application Firewall settings also.

Let us move to the next Penetration Testing Interview Questions.

Q4. What are the needs of Scrum?

Answer:
The below is the list of few requirements of Scrum but are not exhausted :

1. It requires User Stories to describe the requirement and track the completion status of the assigned user story to the team member whereas Use Case is the older concept.
2. A name is required is it describes a sentence as a single line overview to give the simple explanation of the User Story.
3. A description is required as it gives a high-level explanation of the requirement to be met by the assignee.
4. Documents or attachments are also required to know about the story. For eg. In the case of any change in User Interface Screen Layout, that can be easily known only by having a look at the Wire Frame or Prototype of the Screen model. This can be attached to the board using the attachment option.

Q5. What are the different Penetration Testing methods?

Answer:
The different penetration testing methods are External Testing, Internal Testing, Blind Testing, Double-Blind Testing, and Targeted Testing. External Testing is a form of testing on the internet sites those are publicly visible and email applications and DNS servers etc., Internal Testing is a kind of testing which will penetrate into the internal applications of the system through a form of phishing or internal attacks. Blind Testing is a form of penetrating into the application based on its name in the form of a real-time possibility. Double Blind Testing is a form of testing where even the name of the application is also unknown and even the security professional will be having any idea in executing on a particular target and Targeted Testing is a form of performing testing from both the security professional and tester together in the form of targeting on each other.

Part 2 – Penetration Testing Interview Questions (Advanced)

Let us now have a look at the advanced Penetration Testing Interview Questions.

Q6. What is Cross Site Scripting (XSS)?

Answer:
Cross Site Scripting is a type of attack in the form of injections into a web application or system. In this case, different types of malicious scripts are injected into a weak system to acquire confidential information or hack the system without the knowledge of the administrator of the system.

Q7. What is Intruder Detection?

Answer:
Intruder Detection mechanism will help in detecting the possible attacks those happened by scanning the existing files in the form of records in the file system of the application. This will help the organization to detect the attacks early on their system applications.

Let us move to the next Penetration Testing Interview Questions.

Q8. What is SQL injection?

Answer:

SQL injection is a form of attack in which the attacker injects data into an application which will result in executing the queries to retrieve the sensitive information from the database that results in the data breach.

Q9. What is SSL/TLS?

Answer:
This is the popular Penetration Testing Interview Questions asked in an interview. It is Secure Socket Layer / Transport Layer Security which are standard security protocols to establish encryption between a web server and a web browser.

Q10. What are different open source penetration testing tools?

Answer:
Following are the different open source penetration testing tools:

1. Wireshark
2. Metasploit.
3. Nikto.
4. NMap.
5. OpenVAS.

Describe What Information Security Is All about

Information Security can be described as the protection of all the data associated with the software. It is the process of putting measures in place to ensure that all the data related to software does not get into the wrong hands or does not get leaked to the general public. An unsecured software is a considerable risk to both the development company and the end-users.

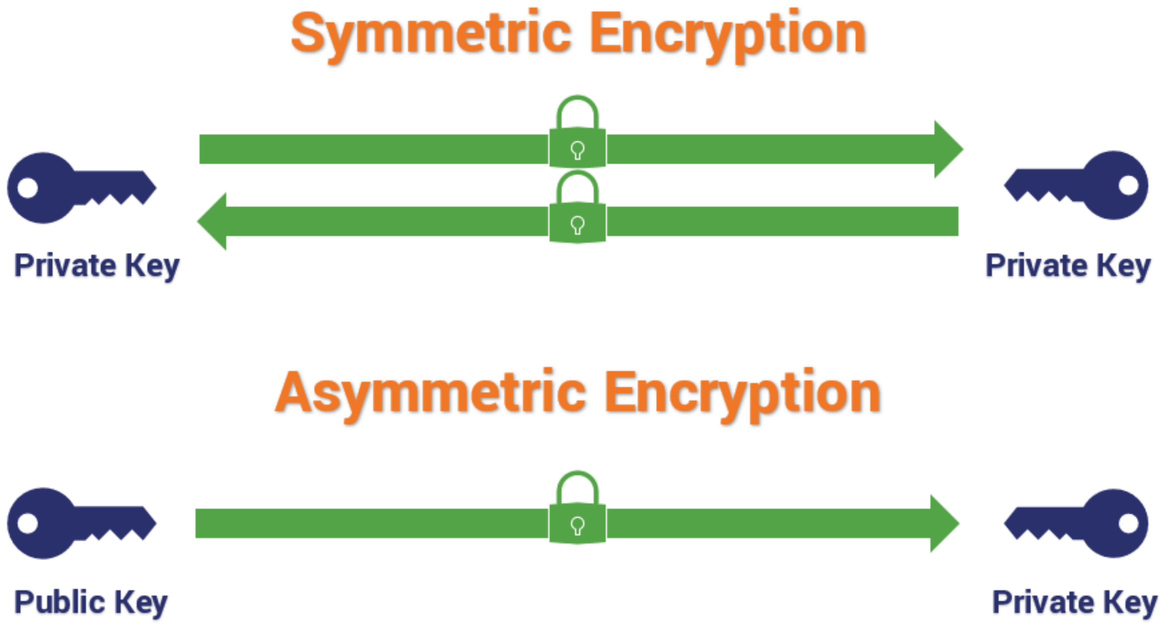
Conducting tests such as penetration testing can help a company understand how secure their information is and fortify loopholes. The security of every info coming in and going out of your software must be guaranteed before launching it to the general public.

2. Explain the Advantages of Penetration Testing

As briefly explained earlier, penetration testing helps a company stay prepared against hackers and security breaches by exposing security loopholes and unforeseen errors that were not identified during the development process. It gives a company extra protection against possible future attacks.

Penetration testing guarantees all the information within the software by ensuring that the data bank is secured. Apart from protection against hackers' attacks, penetration testing helps a company quickly identify other errors such as bugs, viruses, glitches, etc.

3. Explain Symmetric and Asymmetric Encryption



Firstly, encryption is changing the order of data's appearance from its original format to keep out intrusion from those who do not have the clearance to access the data. Symmetric encryption involves the use of a single encryption and decryption pass key. One password can both encrypt and decrypt the data in such cases, and both the owner and end-user share the same key.

In asymmetric encryption, the software owners have a private passkey while the end-users have a public pass key. This is to segregate high-level data that the public cannot access from available data.

4. Explain the Term "Vulnerability"

The vulnerability of software is the condition of being prone to attacks from hackers or the state of not staying completely secure. Vulnerable software has some security defects that can be exploited by fraudulent people to gain access to the software and cause havoc.

In some cases, individuals without ulterior motives may stumble upon such vulnerabilities, and they may mistakenly expose intellectual properties, private information, or merely the data bank. A vulnerable software must undergo penetration testing to ascertain all the vulnerabilities.

5. Talk about Your Penetration Testing Experience

The candidate should be able to explain the previous penetration tests he/ she carried out. Every detail is essential, such as the type of software that was tested, the penetration testing technique used, how difficult or easy the test was, the time it took to complete the test, the discovered vulnerabilities, how the vulnerabilities were corrected, etc.

It is important not to push the candidate to reveal any non-disclosure agreement signed with a previous employer. The candidate's experience level should give you an idea of what he/ she will bring to your company if hired.

6. Explain How Data Is Protected During and after Penetration Testing

Before commencing a penetration test, all the data associated with the software must be carefully backed up because the test can affect the data to prove the software's vulnerability. Protecting data is a priority before, during, and also after penetration testing. Data can be backed up by either storing copies in the cloud or directly into an external secure hard drive or setting up private encryption. The whole idea is to have a replacement for your data in case of any damage.

7. Explain the Term "Intrusion Detection"

Intrusion Detection is the process of finding out an external influence trying to gain illegal access into a software. As its name implies, any form of unlawful access is discovered and reported for necessary action to be taken against the intrusion. It's like the technology that detects burglary and sounds the alarm. During penetration testing, the company will automatically determine whether the intrusion detection technology in its software is functioning correctly.

8. What Are the Possible Causes of Security Vulnerabilities?

TOP 5 FLAWS
1
Missing patches and out of date software
2
Default or poor passwords
3
Cross-site scripting (XSS)
4
SQL injections
5
Brute force protection

The software may be classified as vulnerable for various reasons. Most of the time, it is the penetration testers' role to determine the vulnerability level of the software. Erroneous programming can make software vulnerable. Lack of proper private and public encryption can make software vulnerable. Lack of adequate intrusion detection systems. Lack of appropriate surveillance systems. When the software's data are not adequately backed up or protected, the software can be classified as vulnerable.

9. Advantages of Intrusion Detection Systems

An intrusion detection system helps a company to know when hackers try to gain access to their software. It keeps the company ready at all times to swing into action as soon as there is an attempted breach. Hackers are discouraged from gaining access to the software when they find out that intrusion detection systems are in place. It gives software extra protection from intrusion, and some high-level intrusion detection systems can point out the exact location and device from where the intrusion took place. This ensures quick identification and arrest of the culprits.

10. Explain SSL/TLS

TLS stands for Transport Layer Security while SSL stands for Secure Sockets Layer. It is important to note that TLS is an upgraded version of SSL, which is meant to carry out similar functions. They are supposed to protect the transmission of data of any kind between web browsers and web application owners. SSL/TLS ensures the security of communication, images, videos, text, encrypted files, etc. by creating a confidential route between those providing the data and those receiving it.

11. Explain How Risk Analysis and Penetration Testing Are Different from Each Other

Risk analysis is merely studying all the possible errors that may cause problems in the software, while penetration testing is the process of legally attacking the system to discover the vulnerabilities of the software. Risk analysis is a more economical approach to solving problems, while penetration testing takes a more technical approach. Risk analysis can be carried out by a finance expert who has some probability skills, while penetration testing requires a skilled information technology expert in computer programming and preferably hacking. Risk analysis is more speculative, while penetration testing involves actual work.

12. Explain the Tools You Will Use for Penetration Testing

Penetration testing requires high-level computer systems, operating systems, graphic cards, and certain software that can be used for high-level hacking. Some of the effective tools every penetration tester should have include:

- Burp suite (both the free and commercial versions are available);
- Nessus (both free and commercial versions are available); Wireshark (open source);
- Metasploit (open source);
- NMap (open source);
- OpenVAS (open source);
- Nikto (open source);
- OWASP ZAP (open source).

Some of these tools require extensive training, and some come with certifications.

13. A Penetration Test Takes How Long to Be Completed?

The length of time it would take to complete a penetration test depends on some factors such as the nature of the software being tested, the size of the software, its vulnerability level, the level of security of the software, the experience level of the penetration tester, the software being used for the test, the technique of the test (either automated or manual), etc. These factors will determine how fast or how slow the test will go. For instance, if the software is enormous, expect the penetration test to take more time than when a smaller software is being tested.

14. Does Penetration Testing Break a System?

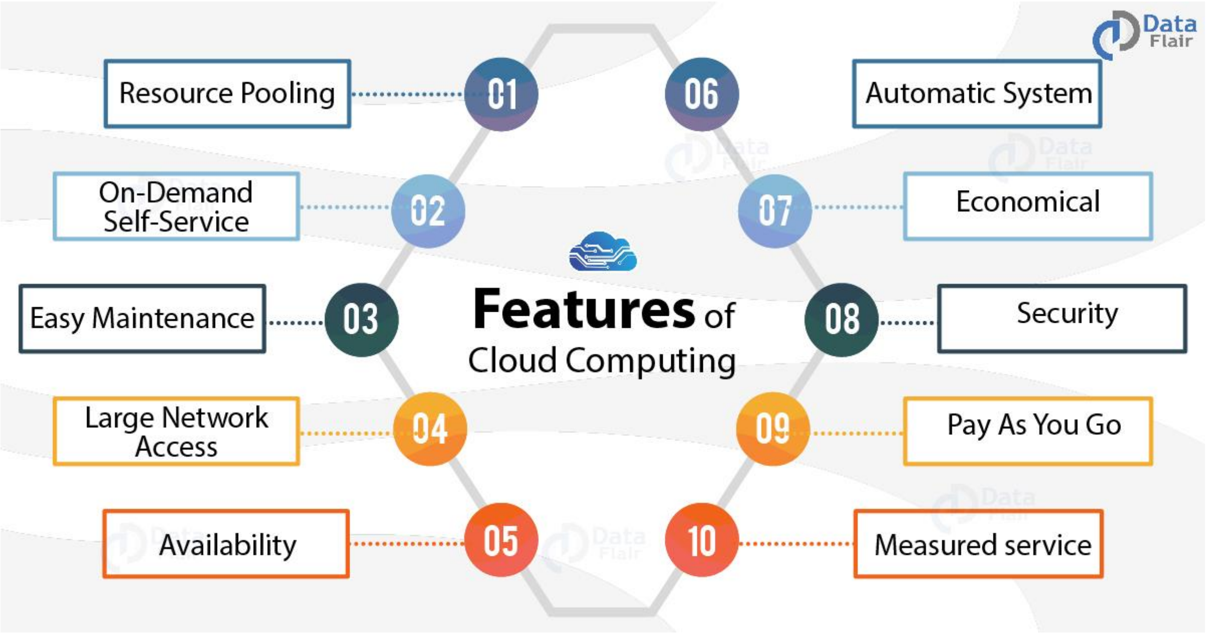
The primary purpose of Penetration Testing is to break software in some way or another. By the break, we mean breaking it up for unauthorized accessibility, which may lead to damages. That is why it is highly advisable to backup the data associated with the software before starting a penetration test because the test might damage some of the software’s data. Therefore to answer the question, Yes! Penetration testing can break a system.

15. Do You Have Any Penetration Testing Certification?

Some notable certificates that may demonstrate a candidate's level of knowledge concerning penetration testing include EC-Council Certified Ethical Hacker (CEH); GIAC Exploit Researcher & Advanced Penetration Tester (GXPN); and Offensive Security Certified Professional (OSCP).

Although, in some cases, certifications can be an added advantage; however, further inquiries have proved that many candidates without any certification can be better than those with certificates. It is better to dwell on asking a candidate for more details concerning carrying out actual tests. If the candidate has some certifications, you can then probe deeper by asking him/her more questions concerning the certificate to know if it will add value to your intended penetration test.

16. Do I Still Need Penetration Testing Although My Data Is in the Cloud?



Source: DataFlair

Of course! The fact that all your data is in the cloud does not mean that they cannot be hacked into. No matter how secure you feel that your software is, you have to put it through rigorous penetration testing. Ethical hackers have to mimic the fraudulent hackers out there to prepare and fortify your software against the worst possible attack. The most recent hacks are taking place via the cloud. Thus, online storage can also be vulnerable.

17. Outline the Systems on Which Penetration Testing Can Be Performed

Although we have been entirely focused on using the term software to generalize, penetration testing can be carried out on various systems such as web applications, servers, mobile devices, endpoints, computers, wireless networks, cloud services, network devices, hardware systems, programmable controllers, complex systems, databases, mobile applications, websites, internet services, browsers, virtual private networks (VPN), public networks, transmission technologies, transmission towers, satellite communication systems, network receivers, storage systems, etc.

Anything that can be hacked can and should go through penetration testing to attain a higher level of security. In the course of this article, we may use the term system, software, or product when describing platforms on which penetration testing can be carried out.

18. Should Penetration Testing Be a Routine Test?

The simple answer to this question is Yes! Penetration testing should be a routine test that can be done just before the product is launched, after a minor or major update, after the intrusion detection system detects an intrusion, when developing a different version, etc. Some companies also conduct penetration tests periodically, like 3 to 4 times annually to stay ahead of potential threats.

Change is constant, and therefore the dangers posed today might not be the dangers faced tomorrow, this is why penetration testing should be carried out routinely. It’s a continuous process that never ends as long as the product remains active.

19. Can Penetration Testing Disrupt a Company’s Network of Operations?

Just like in the case of whether penetration testing can break a system, in this case, it is crucial to understand that penetration testing can disrupt an organization’s network of operation. Look at it this way, just like a hack into the organization’s software can disrupt its operations, so also can penetration testing cause disruption. Penetration testing is simply legalized hacking, so those who carry out penetration tests are sometimes referred to as Ethical Hackers.

20. What’s Different between Penetration Testing and Security Testing?

Security testing is a broader term. While penetration testing only involves using external experts to attack the system or software to ascertain how secure it is, security testing consists of guarding the system or software by developing and testing various security measures.

Penetration Testing	Security Testing
Intrusive form of testing	Non-intrusive form of testing
Narrow focus	Wide focus
Heavy use of security tools	Combined interviews and tools

21. Is Penetration Testing Still Important If the Company Has a Firewall?

Simply put, penetration testing is still necessary whether the company has a firewall or not because hackers do not care if a company has a firewall or not before trying to gain unauthorized access. Hackers can bypass a firewall, or sometimes the firewall may just be damaged, so it is vital to ascertain the firewall's condition through penetration testing.

22. Why Should Penetration Testing Be Carried out by a Third Party?

Penetration testing should be carried out by a third party with little or no knowledge of how the software was developed. He/ she should not be someone involved in the development process of the software. This ensures that the ethical hacker mimics the exact approach a fraudulent hacker will take in trying to gain unauthorized access into the system. Simply put, a fraudulent hacker is most likely someone who wasn't involved in developing the system; therefore, the ethical hacker shouldn't be either.

23. What Are the Legal Steps Involved in Penetration Testing?

Before penetration testing commences, the ethical hacker must sign a non-disclosure agreement with the company to ensure the confidentiality of all the data associated with the company.

24. Can Penetration Testing Be Automated?

Some systems can be programmed to try to automatically study the architecture of a system and try to break into it. Such systems can either be used in place of human ethical hackers or utilized together with ethical hackers.

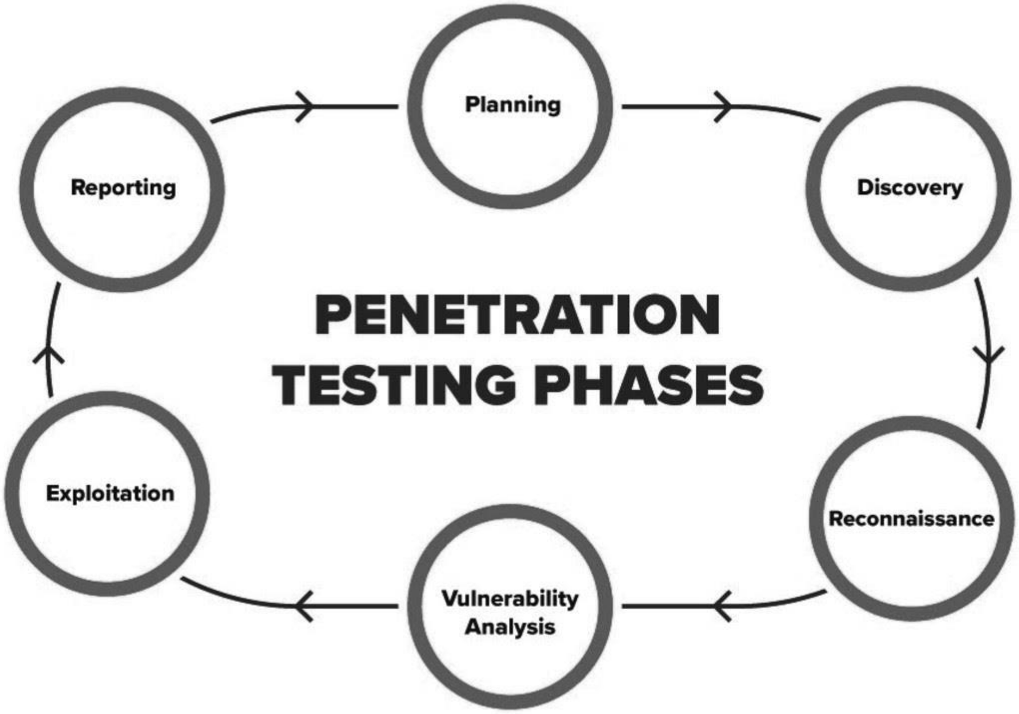
25. Explain the Term "Threat Modelling"

Threat modeling is simply the process of analyzing the possible threats and vulnerabilities within a system. It involves identifying the hazards, carefully studying them, and correcting them accordingly.

26. Explain the Term "File Enumeration"

File enumeration, as its name implies, is the process of shedding more light on the files within a database. It gives the organization and the ethical hacker a complete description, function, location, and the type of data within a system.

27. Explain the Phases of Penetration Testing



Penetration testing involves various effective techniques. One of the most effective tactics involves the following phases:

- *Analysing the system that is to be tested.
- *Backing up all the data associated with the system.
- *Carrying out threat modeling.
- *Trying to hack the system.
- *Analysing the vulnerability and loopholes that were identified
- *Correcting all the issues encountered and setting up an intrusion detector.
- *Documenting the whole process from top to bottom
- *Scheduling a standard penetration testing package.

28. Explain the Most Difficult Penetration Test You Have Experienced

The candidate should be able to explain the toughest penetration test he/ she had to carry out. This will help you understand their breaking points and help you know whether they could improve their skills based on the difficulty encountered. You will be able to discover their strengths, weaknesses, and personal upgrades.

29. Outline the Full Meanings of 2FA, 2S2D, 2VPCP, 3DES, 3DESE, And 3DESEP

- 2FA: Two Factor Authentication
- 2S2D: Double-Sided Double-Density
- 2VPCP: Two-Version Priority Ceiling Protocol
- 3DES: Triple Data Encryption Standard
- 3DESE: Triple Data Encryption Standard Encryption
- 3DESEP: Triple Data Encryption Standard Encryption Protocol

30. Explain the Term “STRIDE”

STRIDE is an abbreviation used to identify a thread modeling technique.

- The S stands for Spoofing.
- The T stands for Tampering.
- The R stands for Repudiation.
- The I stands for Information disclosure.
- The D stands for Denial of Service (DoS).
- The E stands for: Elevation of privilege.
- To correctly identify, analyze, and correct the threats to a system, a company must adopt the above threat modeling technique.

1. Explain risk, vulnerability and threat?
TIP: A good way to start this answer is by explaining vulnerability, and threat and then risk. Back this up with an easy to understand example.

Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when that the vulnerability is exploited by the threat e.g. Default username and password for a server – An attacker can easily crack into this server and compromise it (Here's a resource that will navigate you through cyber security attacks).

2. What is the difference between Asymmetric and Symmetric encryption and which one is better?
TIP: Keep the answer simple as this is a vast topic.

Symmetric encryption uses the same key for both encryption and decryption, while Asymmetric encryption uses different keys for encryption and decryption.

Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel.

Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using symmetric process.

3. What is an IPS and how does it differs from IDS?

IDS is an intrusion detection system whereas an IPS is an intrusion prevention system. IDS will just detect the intrusion and will leave the rest to the administrator for further action whereas an IPS will detect the intrusion and will take further action to prevent the intrusion. Another difference is the positioning of the devices in the network. Although they work on the same basic concept but the placement is different.

4. What is XSS, how will you mitigate it?

Cross site scripting is a JavaScript vulnerability in the web applications. The easiest way to explain this is a case when a user enters a script in the client side input fields and that input gets processed without getting validated. This leads to untrusted data getting saved and executed on the client side.

Countermeasures of XSS are input validation, implementing a CSP (Content security policy) etc (Also consider checking out this career guide for cissp certification).

TIP: Know the different types of XSS and how the countermeasures work.

5. What is the difference between encryption and hashing?
TIP: Keep the answer short and straight.

Point 1: Encryption is reversible whereas hashing is irreversible. Hashing can be cracked using rainbow tables and collision attacks but is not reversible.

Point 2: Encryption ensures confidentiality whereas hashing ensures Integrity.

6. Are you a coder/developer or know any coding languages?
TIP: You are not expected to be a PRO; understanding of the language will do the job.

Although this is not something an information security guy is expected to know but the knowledge of HTML, JavaScript and Python can be of great advantage. HTML and JavaScript can be used in web application attacks whereas python can be used to automate tasks, exploit development etc. A little knowledge of the three can be of great advantage - both in the interview and on the floor.

7. What is CSRF?

Cross Site Request Forgery is a web application vulnerability in which the server does not check whether the request came from a trusted client or not. The request is just processed directly. It can be further followed by the ways to detect this, examples and countermeasures.

8. What is a Security Misconfiguration?

Security misconfiguration is a vulnerability when a device/application/network is configured in a way which can be exploited by an attacker to take advantage of it. This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

9. What is a Black hat, white hat and Grey hat hacker?
TIP: Keep the answer simple.

Black hat hackers are those who hack without authority. White hat hackers are authorised to perform a hacking attempt under signed NDA. Grey hat hackers are white hat hackers which sometimes perform unauthorised activities.

10. What is a firewall?
TIP: Be simple with the answer, as this can get complex and lead to looped questions.

A firewall is a device that allows/blocks traffic as per defined set of rules. These are placed on the boundary of trusted and untrusted networks.

11. How do you keep yourself updated with the information security news?
TIP: Just in case you haven't followed any: the hacker news, ThreatPost, Pentest mag etc.

Be sure to check and follow a few security forums so that you get regular updates on what is happening in the market and about the latest trends and incidents.

12. The world has recently been hit by ……. Attack/virus etc. What have you done to protect your organisation as a security professional?

Different organisations work in different ways, the ways to handle incident is different for all. Some take this seriously and some not. The answer to this should be the process to handle an incident. Align this with one you had and go on… just don’t exaggerate.

13. CIA triangle?

- Confidentiality: Keeping the information secret.
- Integrity: Keeping the information unaltered.
- Availability: Information is available to the authorised parties at all times.

14. HIDS vs NIDS and which one is better and why?

HIDS is host intrusion detection system and NIDS is network intrusion detection system. Both the systems work on the similar lines. It’s just that the placement in different. HIDS is placed on each host whereas NIDS is placed in the network. For an enterprise, NIDS is preferred as HIDS is difficult to manage, plus it consumes processing power of the host as well.

Level 02 - Learners (Experienced but still learning)

15. What is port scanning?

Port scanning is process of sending messages in order to gather information about network, system etc. by analysing the response received.

16. What is the difference between VA and PT?

Vulnerability Assessment is an approach used to find flaws in an application/network whereas Penetration testing is the practice of finding exploitable vulnerabilities like a real attacker will do. VA is like travelling on the surface whereas PT is digging it for gold.

17. What are the objects that should be included in a good penetration testing report?

A VAPT report should have an executive summary explaining the observations on a high level along with the scope, period of testing etc. This can be followed by no of observations, category wise split into high, medium and low. Also include detailed observation along with replication steps, screenshots of proof of concept along with the remediation.

18. What is compliance?

Abiding by a set of standards set by a government/Independent party/organisation. E.g. An industry which stores, processes or transmits Payment related information needs to be complied with PCI DSS (Payment card Industry Data Security Standard). Other compliance examples can be an organisation complying with its own policies.

19. Tell us about your Personal achievements or certifications?

Keep this simple and relevant, getting a security certification can be one personal achievement. Explain how it started and what kept you motivated. How you feel now and what are your next steps.

20. Various response codes from a web application?

1xx - Informational responses
2xx - Success
3xx - Redirection
4xx - Client side error
5xx - Server side error

21. When do you use tracert/traceroute?

In case you can’t ping the final destination, tracert will help to identify where the connection stops or gets broken, whether it is firewall, ISP, router etc.

22. DDoS and its mitigation?

DDoS stands for distributed denial of service. When a network/server/application is flooded with large number of requests which it is not designed to handle making the server unavailable to the legitimate requests. The requests can come from different not related sources hence it is a distributed denial of service attack. It can be mitigated by analysing and filtering the traffic in the scrubbing centres. The scrubbing centres are centralized data cleansing station wherein the traffic to a website is analysed and the malicious traffic is removed.

23. What is a WAF and what are its types?
TIP: This topic is usually not asked in detail.

WAF stands for web application firewall. It is used to protect the application by filtering legitimate traffic from malicious traffic. WAF can be either a box type or cloud based.

24. Explain the objects of Basic web architecture?
TIP: Different organisations follow different models and networks. BE GENERIC.

A basic web architecture should contain a front ending server, a web application server, a database server.

Level 03 - Master (Entered into a managerial position or sitting for one)

25. How often should Patch management be performed?

Patch should be managed as soon as it gets released. For windows – patches released every second Tuesday of the month by Microsoft. It should be applied to all machines not later than 1 month. Same is for network devices, patch as soon as it gets released. Follow a proper patch management process.

26. How do you govern various security objects?

Various security objects are governed with the help of KPI (Key Performance Indicators). Let us take the example of windows patch, agreed KPI can be 99%. It means that 99% of the PCs will have the latest or last month’s patch. On similar lines various security objects can be managed.

27. How does a Process Audit go?

The first thing to do is to identify the scope of the audit followed by a document of the process. Study the document carefully and then identify the areas which you consider are weak. The company might have compensatory controls in place. Verify they are enough.

28. What is the difference between policies, processes and guidelines?

As security policy defines the security objectives and the security framework of an organisation. A process is a detailed step by step how to document that specifies the exact action which will be necessary to implement important security mechanism. Guidelines are recommendations which can be customised and used in the creation of procedures.

29. How do you handle AntiVirus alerts?

Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virustotal, malwares.com etc. AV needs to be fine-tuned so that the alerts can be reduced.

30. What is a false positive and false negative in case of IDS?

When the device generated an alert for an intrusion which has actually not happened: this is false positive and if the device has not generated any alert and the intrusion has actually happened, this is the case of a false negative.

31. Which one is more acceptable?

False positives are more acceptable. False negatives will lead to intrusions happening without getting noticed.

32. Software testing vs. penetration testing?

Software testing just focuses on the functionality of the software and not the security aspect. A penetration testing will help identify and address the security vulnerabilities.

33. What are your thoughts about Blue team and red team?

Red team is the attacker and blue team the defender. Being on the red team seems fun but being in the blue team is difficult as you need to understand the attacks and methodologies the red team may follow.

34. What is you preferred - Bug bounty or security testing?

Both are fine, just support your answer like Bug Bounty is decentralised, can identify rare bugs, large pool of testers etc.

35. Tell us about your Professional achievements/major projects?

This can be anything like setting up your own team and processes or a security practice you have implemented. Even if the achievement is not from a security domain just express it well.

36. 2 quick points on Web server hardening?
TIP: This is a strong topic, get over with the exact answer and carry on the conversation over the lines.

Web server hardening is filtering of unnecessary services running on various ports and removal of default test scripts from the servers. Although web server hardening is a lot more than this and usually organisations have a customised checklist for hardening the servers. Any server getting created has to be hardened and hardening has to be re-confirmed on a yearly basis. Even the hardening checklist has to be reviewed on a yearly basis for new add-ons.

37. What is data leakage? How will you detect and prevent it?

Data leak is when data gets out of the organisation in an unauthorised way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorised upload of data to public portals, removable drives, photographs etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to internal network, restriction on printing confidential data etc.

Level 04 - Grandmaster (Senior management roles)

38. What are the different levels of data classification and why are they required?

Data needs to be segregated into various categories so that its severity can be defined, without this segregation a piece of information can be critical for one but not so critical for others. There can be various levels of data classification depending on organisation to organisation, in broader terms data can be classified into:

- Top secret – Its leakage can cause drastic effect to the organisation, e.g. trade secrets etc.
- Confidential – Internal to the company e.g. policy and processes.
- Public – Publically available, like newsletters etc.

39. In a situation where a user needs admin rights on his system to do daily tasks, what should be done – should admin access be granted or restricted?

Users are usually not provided with admin access to reduce the risk, but in certain cases the users can be granted admin access. Just ensure that the users understand their responsibility. In case any incident happens, the access should be provided for only limited time post senior management approval and a valid business justification.

40. What are your views on usage of social media in office?

Social media is acceptable, just ensure content filtering is enabled and uploading features are res

41. What are the various ways by which the employees are made aware about information security policies and procedures?

There can be various ways in which this can be done:

- Employees should undergo mandatory information security training post joining the organisation. This should also be done on yearly basis, and this can be either a classroom session followed by a quiz or an online training.
- Sending out notifications on regular basis in the form of slides, one pagers etc. to ensure that the employees are kept aware.

42. In a situation where both Open source software and licensed software are available to get the job done. What should be preferred and why?
TIP: Think from a security perspective and not from the functionality point.

For an enterprise, it is better to go for the licensed version of the software as most of the software have an agreement clause that the software should be used for individual usage and not for commercial purpose. Plus, the licensed version is updated and easy to track in an organisation. It also helps the clients develop a confidence on the organisations' software and practices.

43. When should a security policy be revised?

There is no fixed time for reviewing the security policy but all this should be done at least once a year. Any changes made should be documented in the revision history of the document and versioning. In case there are any major changes the changes need to be notified to the users as well.

44. What all should be included in a CEO level report from a security standpoint?

A CEO level report should have not more than 2 pages:

1. A summarised picture of the state of security structure of the organisation.
2. Quantified risk and ALE (Annual Loss Expectancy) results along with countermeasures.

45. How do you report risks?

Risk can be reported but it needs to be assessed first. Risk assessment can be done in 2 ways: Quantitative analysis and qualitative analysis. This approach will cater to both technical and business guys. The business guy can see probable loss in numbers whereas the technical guys will see the impact and frequency. Depending on the audience, the risk can be assessed and reported.

46. What is an incident and how do you manage it?

Any event which leads to compromise of the security of an organisation is an incident. The incident process goes like this:

- Identification of the Incident
- Logging it (Details)
- Investigation and root cause analysis (RCA)
- Escalation or keeping the senior management/parties informed
- Remediation steps
- Closure report.

47. Is social media secure?
TIP: This is another debatable question but be generic.

Not sure if the data is secure or not but users can take steps from their end to ensure safety.

- Connect with trusted people
- Do not post/upload confidential information
- Never use the same username password for all accounts

48. Chain of custody?

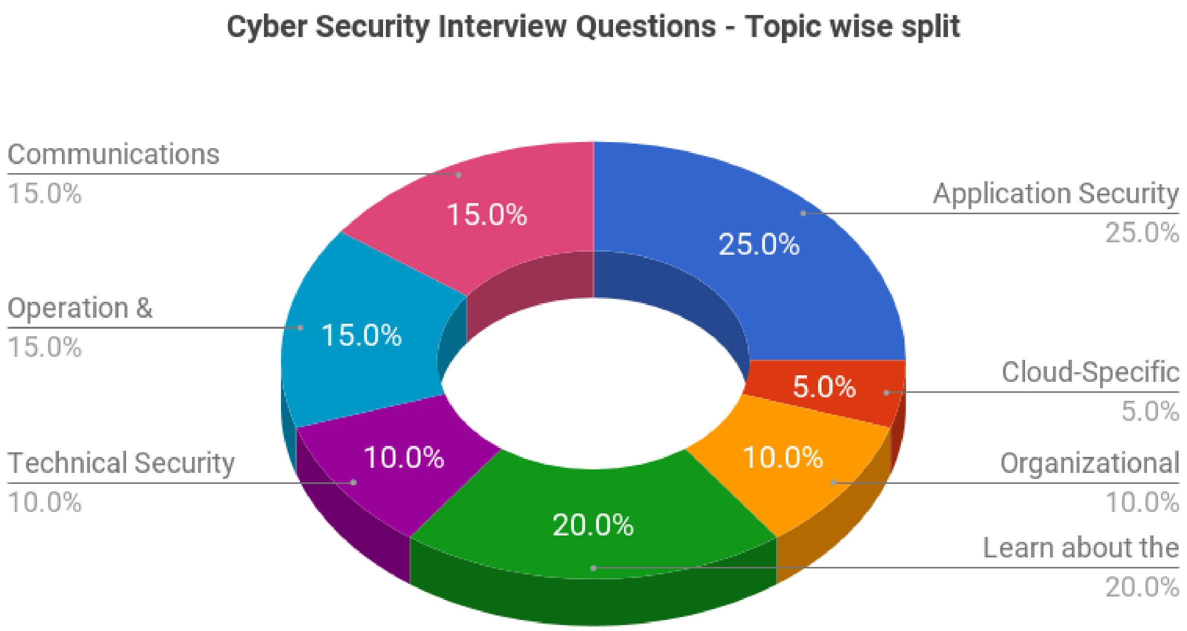
For legal cases the data/device (evidence) needs to be integrated, hence any access needs to be documented – who, what when and why. Compromise in this process can cause legal issues for the parties involved.

49. How should data archives be maintained?

Gone are the times when there used to be files and cabinets which held data over the years. This phase was long followed by archiving data over magnetic tapes and storing the tapes. There is another overhead for the maintenance and safety of the tapes. These are few conventional approaches, but the world is slightly moving to the cloud storage architecture. The only hurdle is the data privacy. Companies are not very sure about handing the critical data. This will actually take time but securely configured and managed cloud can be one of the best options.

50. What are your thoughts on BYOD?

There is no correct answer for this but just ensure that whatever side you are on, justify it with examples, scenarios and logic.



Although there is no defined scope and end to the questions, but having a strong foundation of the basic concepts and awareness about the latest trends will give you an upper hand in the interview.

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.

Cybersecurity Interview Questions

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?

1xx – Informational responses
2xx – Success
3xx – Redirection
4xx – Client-side error
5xx – Server-side error

Let us now go ahead and take a look at some of the other Cybersecurity Interview Questions

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

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

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 can be prevented by using tools, software, and strategies known as **DLP(Data Leakage 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. DDoS
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?

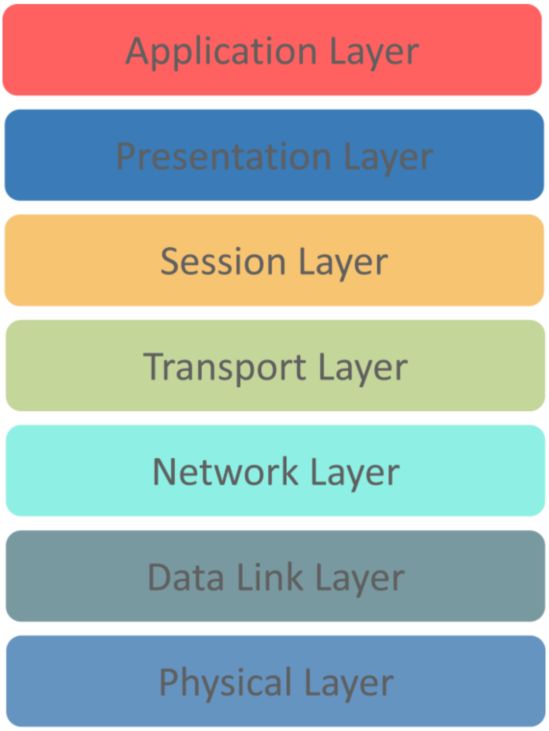
Port Scanning is the technique used to identify open ports and service available on a host. Hackers use port scanning to find information that can be helpful to exploit vulnerabilities. Administrators use Port Scanning to verify the security policies of the network. Some of the common Port Scanning Techniques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

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

Cybersecurity Interview Questions

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**. 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

Cybersecurity Interview Questions

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 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.

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 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.

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

This brings us to the end of Theory Based Cybersecurity Interview Questions

Part B – Scenario Based Cybersecurity Interview 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.

Cyber Security Training

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

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.

Cybersecurity Interview Questions

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

Q1) Define Cybersecurity?

Ans. Cybersecurity refers to the protection of internet-connected systems such as software, hardware, electronic data, etc., from cyber attacks. In a computing text, it is referred to as protection against unauthorized access.

Q2) What is Cryptography?

Ans. Cryptography is a method to transform and transmit confidential data in an encoded way to protect the information from third parties for whom data is not authorized.

Q3) What is the difference between Threat, Vulnerability, and Risk?

Ans.

- **Threat:** Someone with the potential to cause harm by damaging or destroying the official data to a system or organization.

Ex: Phishing attack

- **Vulnerability:** It refers to weaknesses in a system that makes threat outcomes more possible and even more dangerous.

Ex: SQL injections, cross-site scripting

- **Risk:** It refers to a combination of threat probability and impact/loss. In simple terms, it is related to potential damage or loss when threat exploits the vulnerability.

Threat probability * Potential loss = Risk

Q4) What is Cross-Site Scripting and how it can be prevented?

Ans. Cross-Site Scripting is also known as a client-side injection attack, which aims at executing malicious scripts on a victim's web browser by injecting malicious code.

The following practices can prevent Cross-Site Scripting:

- Encoding special characters
- Using XSS HTML Filter
- Validating user inputs
- Using Anti-XSS services/tools

Q5) What is the difference between IDS and IPS?

Ans.

Intrusion Detection Systems (IDS)	Intrusion Prevention Systems (IPS)
It only detects intrusions but unable to prevent intrusions.	It detects and prevents intrusions.
It's a monitoring system.	It's a control system.
It needs a human or another system to look at the results.	It needs a regularly updated database with the latest threat data.

Q6) What is a Botnet?

Ans.

A Botnet is a group of internet-connected devices such as servers, PCs, mobile devices, etc., that are affected and controlled by malware.

It is used for stealing data, sending spam, performing distributed denial-of-service attack (DDoS attack), and more, and also to enable the user to access the device and its connection.

Q7) What is a CIA triad?

Ans. CIA (confidentiality, integrity, and availability) triad is a model designed to handle policies for information security within an organization.

- **Confidentiality -** A collection of rules that limits access to information.
- **Integrity -** It assures the information is trustworthy and reliable.
- **Availability -** It provides reliable access to data for authorized people.

Q8) Symmetric Vs Asymmetric encryption.

Ans.

Purpose	Symmetric Encryption	Asymmetric Encryption
Encryption	Uses a single key to encrypt and decrypt information.	Uses a pair of public and private keys to encrypt and decrypt information.
Speed	Symmetric encryption performs faster	Asymmetric encryption performs slower compared to symmetric encryption.
Algorithms	AES, RC4, DES, QUAD, 3DES, Blowfish etc.	Diffie-Hellman and RSA
Purpose	Preferred for transferring huge data	Mostly used for exchanging secret keys safely.

Q9) What is the difference between hashing and encryption?

Ans. Both hashing and encryption are used to convert readable data into an unreadable format. The significant difference is that encrypted data can be transformed into original data by decryption, whereas hashed data cannot be processed back to the original data.

Q10) What is two-factor authentication and how it can be implemented for public websites?

Ans.

- Tw0-factor authentication is also referred to as dual-factor authentication or two-step verification where the user provides two authentication factors for protecting both user credentials and resources while accessing.
- The two-factor authentication can be implemented on public websites such as Twitter, Microsoft, LinkedIn, and more for enabling another protection on your already protected account with a password.
- For enabling this double factor authentication, you can easily go to settings and then manage security settings.

Q11) What is the use of a firewall and how it can be implemented?

Ans. A firewall is a security system used to control and monitor network traffic. It is used for protecting the system/network from malware, viruses, worms, etc., and secures unauthorized access from a private network.

The steps required to set up and configure the firewall are listed below:

- Change the default password for a firewall device.
- Disable the remote administration feature.
- Configure port forwarding for specific applications to function correctly, such as an FTP server or a web server.
- Firewall installation on a network with an existing DHCP server can cause errors unless its firewall's DHCP is disabled.
- Make sure the firewall is configured to robust security policies.

Q12) What is the difference between vulnerability assessment and penetration testing?

Ans.

- The terms Vulnerability assessment and penetration testing are both different, but serve an essential function of protecting network environment.
- Vulnerability Assessment: It's a process to define, detect, and prioritize the vulnerabilities in computer systems, network infrastructure, applications, etc., and gives the organization with the required information to fix the flaws.
- Penetration Testing: It is also called as pen testing or ethical hacking. It's a process of testing a network, system, application, etc.to identify vulnerabilities that attackers could exploit. In the context of web application security, it is most widely used to augment a web application firewall (WAF).

Q13) What is the difference between stored and reflected XSS?

Ans.

- **Stored XSS Attacks -** The attacks where the injected scripts are stored on the target servers permanently. In this, the victim retrieves the malicious script from the server when requests the stored information.
- **Reflected XSS Attacks -** In this, the user has to send the request first, then it will start running on the victim's browser and reflects results from the browser to the user who sent the request.

Q14) What is a three-way handshake process?

Ans. A three-way handshake process is used in TCP (Transmission Control Protocol) network for transmission of data in a reliable way between the host and the client.

It's called a three-way handshake because three segments are exchanged between the server and the client.

- **SYN:** The client wants to establish a connection with the server, and sends a segment with SYN(Synchronize Sequence Number) to the server if the server is up and has open ports.
- **SYN + ACK:** The server responds to the client request with SYN-ACK signal bits set if it has open ports.
- **ACK:** The client acknowledges the response of a server and sends an ACK(Acknowledgment) packet back to the server.

Q15) What are HTTP response codes?

Ans. HTTP response codes display whether a particular HTTP request has been completed.

- **1xx (Informational) -** The request has been received, and the process is continuing.
- **2xx (Success) -** The request was successfully received and accepted.
- **3xx (Redirection) -** Further action must be taken to complete it.
- **4xx (Client Error) -** Request cannot be fulfilled or has incorrect syntax.
- **5xx (Server Error) -** The server fails to fulfil the request.

Q16) What are the techniques used in preventing a Brute Force Attack?

Ans. **Brute Force Attack** is a trial and error method that is employed for application programs to decode encrypted data such as data encryption keys or passwords using brute force rather than using intellectual strategies. It's a way to identify the right credentials by repetitively attempting all the possible methods.

Brute Force attacks can be avoided by the following practices:

- **Adding password complexity:** Include different formats of characters to make passwords stronger.
- **Limit login attempts:** set a limit on login failures.
- **Two-factor authentication:** Add this layer of security to avoid brute force attacks.

Q17) List the common types of cybersecurity attacks.

Ans. The following are the most common types of cybersecurity attacks:

- Malware
- SQL Injection Attack
- Cross-Site Scripting (XSS)
- Denial-of-Service (DoS)
- Man-in-the-Middle Attacks
- Credential Reuse
- Phishing
- Session Hijacking

Q18) Define data leakage and its types?

Ans. Data Leakage refers to the illegal transmission of data to an external destination or unauthorized entity within an organization. It can transfer data either physically or electronically. It usually occurs via the web, emails, and mobile data storage devices.

Types of data leakage:

1. The Accidental Breach - Majority of data leakage incidents are accidental.

Ex: An entity may choose the wrong recipient while sending confidential data.

2. The Disgruntled or ill-intentioned Employee - The authorized entity sends confidential data to an unauthorized body.

3. Electronic Communications with Malicious Intent - The problem is all the electronic mediums are capable of file transferring and external access sources over the internet.

Q19) What is the use of Traceroute?

Ans. A Traceroute is a network diagnostic tool, used for tracking the pathway of an IP network from source to destination. It records the period of each hop the packet makes while its route to its destination.

Q20) How to prevent CSRF attacks?

Ans. CSRF is referred to as Cross-site Request Forgery, where an attacker tricks a victim into performing actions on their behalf.

CSRF attacks can be prevented by using the following ways:

- Employing the latest antivirus software which helps in blocking malicious scripts.
- While authenticating to your banking site or performing any financial transactions on any other website do not browse other sites or open any emails, which helps in executing malicious scripts while being authenticated to a financial site.

- Never save your login/password within your browser for financial transactions.
- Disable scripting in your browser.

Q21) What is port scanning?

Ans. A port scanning is an application designed for identifying open ports and services accessible on a host network. Security administrators mostly utilize it for exploiting vulnerabilities, and also by hackers for targeting victims.

Some of the most popular port scanning techniques are listed below:

- Ping scan
- TCP connect
- TCP half-open
- Stealth scanning – NULL, FIN, X-MAS
- UDP

Q22) What is the need for DNS monitoring?

Ans.

- DNS (Domain Name System) is a service that is used for converting user-friendly domain names into a computer-friendly IP address. It allows websites under a particular domain name which is easy to remember.
- DNS monitoring is nothing but monitoring DNS records to ensure does it route traffic properly to your website, electronic communication, services, and more.

Q23) What is the difference between hashing and salting?

Ans.

- Hashing is majorly used for authentication and is a one-way function where data is planned to a fixed-length value.
- Salting is an extra step for hashing, where it adds additional value to passwords that change the hash value created.

Q24) How to prevent 'Man-in-the-Middle Attack'?

Ans. The following practices prevent the 'Man-in-the-Middle Attacks':

- Have a stronger WAP/WEP Encryption on wireless access points avoids unauthorized users.
- Use a VPN for a secure environment to protect sensitive information. It uses key-based encryption.
- Public key pair based authentication must be used in various layers of a stack for ensuring whether you are communicating the right things are not.

- HTTPS must be employed for securely communicating over HTTP through the public-private key exchange.

Q25) What are the common methods of authentication for network security?

Ans.

- **Biometrics -** It is a known and registered physical attributes of a user specifically used for verifying their identity.
- **Token -** A token is used for accessing systems. It makes more difficult for hackers to access accounts as they have long credentials.
- **Transaction Authentication -** A one time pin or password is used in processing online transactions through which they verify their identity.
- **Multi-Factor Authentication -** It's a security system that needs more than one method of authentication.
- **Out-of-Band Authentication -** This authentication needs two different signals from two different channels or networks. It prevents most of the attacks from hacking and identity thefts in online banking.
-
- Q26) Which is more secure SSL or HTTPS?

Ans.

- SSL (Secure Sockets Layer) is a secure protocol which provides safer conversations between two or more parties across the internet. It works on top of the HTTP to provide security.
- HTTPS (Hypertext Transfer Protocol Secure) is a combination of HTTP and SSL to provide a safer browsing experience with encryption.
- In terms of security, SSL is more secure than HTTPS.

Q27) What is the difference between black hat, white hat, and grey hat hackers?

Ans.

- Black-hat hacker is a person who tries to obtain unauthorized access into a system or a network to steal information for malicious purposes.
- White-hat hackers are also known as ethical hackers; they are well-versed with ethical hacking tools, methodologies, and tactics for securing organization data. They try to detect and fix vulnerabilities and security holes in the systems. Many top companies recruit white hat hackers.
- Grey hat hacker is a computer security expert who may violate ethical standards or rules sometimes, but do not have malicious intent of black hat hacker.

Q28) What is cognitive security?

Ans. Cognitive security is one of the applications of AI technologies that is used explicitly for identifying threats and protecting physical and digital systems based on human understanding processes.

Self-learning security systems use pattern recognition, natural language processing, and data mining to mimic the human brain.

Q29) What is phishing and how it can be prevented?

Ans. Phishing is a malicious attempt of pretending oneself as an authorized entity in electronic communication for obtaining sensitive information such as usernames, passwords, etc. through fraudulent messages and emails.

The following practices can prevent phishing:

- Use firewalls on your networks and systems.
- Enable robust antivirus protection that has internet security.
- Use two-factor authentication wherever possible
- Maintain adequate security.
- Don't enter sensitive information such as financial or digital transaction details on the web pages that you don't trust.
- Keep yourself updated with the latest phishing attempts.

Q30) What is SQL injection and how it can be prevented?

Ans. SQL Injection (SQLi) is a type of code injection attack where it manages to execute malicious SQL statements to control a database server behind a web application. Attackers mostly use this to avoid application security measures and thereby access, modify, and delete unauthorized data.

The following ways will help you to mitigate or prevent SQL injection attacks:

- Include Prepared Statements (with Parameterized Queries)
- Use Stored Procedures
- Validate user input
- Hide data from the error message
- Update your system
- Store database credentials separate and encrypted
- Disable shell and any other functionalities you don’t need

Q31) How will you keep yourself updated with the latest cybersecurity news?

Ans. The following ways will help you to keep up with the latest cybersecurity updates:

- Follow news websites and blogs from security experts.
- Browse security-related social media topics.

- Check vulnerability alert feeds and advisory sites.
- Attend cybersecurity live events.

Q32) What is a DDOS attack and how to stop and prevent them?

Ans. A DDOS (distributed denial-of-service) is a malicious attempt of disrupting regular traffic of a network by flooding with a large number of requests and making the server unavailable to the appropriate requests. The requests come from several unauthorized sources and hence called distributed denial of service attack.

The following methods will help you to stop and prevent DDOS attacks:

- Build a denial of service response plan
- Protect your network infrastructure
- Employ basic network security
- Maintain strong network architecture
- Understand the Warning Signs
- Consider DDoS as a service

Q33) What do you understand by compliance in Cybersecurity?

Ans.

- Compliance means living by a set of standards set by organization/government/independent party.
- It helps in defining and achieving IT targets and also in mitigating threats through processes like vulnerability management.

Q34) What is the use of Patch Management?

Ans.

- The purpose of patch management is to keep updating various systems in a network and protect them against malware and hacking attacks.
- Many enterprise patch management tools manage the patching process by installing or deploying agents on a target computer, and they provide a link between centralized patch servers and computers to be patched.

Q35) What is the difference between a false positive and false negative in IDS?

Ans.

- A false positive is considered to be a false alarm and false negative is considered to be the most complicated state.
- A false positive occurs when an IDS fires an alarm for legitimate network activity.
- A false negative occurs when IDS fails to identify malicious network traffic.

Compared to both, a false positive is more acceptable than false-negative as they lead to intrusions without getting noticed.

Q36) what is the difference between the Red team and Blue team?

Ans.

- Red team and blue team refers to cyberwarfare. Many organizations split the security team into two groups as red team and blue team.
- The red team refers to an attacker who exploits weaknesses in an organization's security.
- The blue team refers to a defender who identifies and patches vulnerabilities into successful breaches.

Q37) Explain System hardening?

Ans.

- Generally, system hardening refers to a combination of tools and techniques for controlling vulnerabilities in systems, applications, firmware, and more in an organization.
- The purpose of system hardening is to decrease the security risks by reducing the potential attacks and condensing the system’s attack surface.

The following are the various types of system hardening:

1. Database hardening
2. Operating system hardening
3. Application hardening
4. Server hardening
5. Network hardening

Q38) What is a cybersecurity risk assessment?

Ans. A cybersecurity risk assessment refers to detecting the information assets that are prone to cyber-attacks(including customer data, hardware, laptop, etc.) and also evaluates various risks that could affect those assets.

It is mostly performed to identify, evaluate, and prioritize risks across organizations.

The best way to perform cybersecurity risk assessment is to detect:

- Relevant threats in your organization
- Internal and external vulnerabilities
- Evaluate vulnerabilities impact if they are exploited

Q39) What are the seven layers of the OSI model?

Ans. The main objective of the OSI model is to process the communication between two endpoints in a network.

The seven open systems interconnection layers are listed below:

- **Application layer (layer 7) -** It allows users to communicate with network/application whenever required to perform network-related operations.
- **Presentation layer (layer 6) -** It manages encryption and decryption of data required for the application layer. It translates or formats data for the application layer based on the syntax of the application that accepts.
- **Session layer (layer 5) -** It determines the period of a system that waits for other application to respond.
- **Transport layer (layer 4) -** It is used for sending data across a network and also offers error checking practices and data flow controls.
- **Network layer (layer 3) -** It is used to transfer data to and fro through another network.
- **Data-link layer (layer 2) -** It handles the flow of data to and fro in a network. It also controls problems that occur due to bit transmission errors.
- **Physical layer (layer 1) -** It transfers the computer bits from one device to another through the network. It also controls how physical connections are set up to the network and also bits represented into signals while transmitting either optically, electrically, or radio waves.

Q40) How to reset or remove the BIOS password?

Ans. There are many ways to reset or remove the BIOS password:

- By removing CMOS battery
- By using software
- By using MS-DOS command
- By using motherboard jumper
- By using Backdoor BIOS password

Q41) What is the use of Address Resolution Protocol (ARP)?

Ans. ARP is a protocol specifically used to map IP network addresses to physical addresses, such as Ethernet addresses.

It translates 32-bits addresses to 48-bits addresses and vice versa. This is needed because the most common level of internet protocol(IP) we use today is 32-bits long and MAC addresses are 48-bits long.

Q42) How to protect data in transit Vs rest?

Ans.

Description	Data in Transit	Data in Rest

Definition of data	Here data moves actively from one location to another across the internet or private network.	Here data is not transferred from one location to another as data is stored on hard drives, flash drive, etc.
Encryption in data protection	It encrypts sensitive data before sending or using encrypted connections(SSL, HTTPS, TLS, etc.)	It encrypts sensitive files before storing or choosing the encrypted storage drive itself.

Q43) What are the several indicators of compromise(IOC) that organizations should monitor?

Ans. The key indicators of compromise that organizations should monitor are listed below:

- Unusual Outbound Network Traffic
- HTML Response Sizes
- Geographical Irregularities
- Increases in Database Read Volume
- Log-In Red Flags
- Unexpected Patching of Systems
- Large Numbers of Requests for the Same File
- Web Traffic with Unhuman Behavior
- Suspicious Registry or System File Changes
- Unusual DNS Requests
- Mobile Device Profile Changes
- Bundles of Data in the Wrong Place
- Mismatched Port-Application Traffic
- Signs of DDoS Activity
- Anomalies in Privileged User Account Activity

Q44) What is Remote Desktop Protocol (RDP)?

Ans.

- RDP (Remote Desktop Protocol) is a Microsoft protocol specifically designed for application data transfer security and encryption between client devices, users, and a virtual network server.
- It allows administrators to remotely evaluate and resolve issues individual subscribers encounter.
- It supports up to 64,000 separate data channels with a provision for multipoint transmission.

Q45) What is the difference between Diffie Hellman and RSA?

Ans.

- **Diffie-Helman:** It’s a key exchange protocol where two parties exchange a shared key that either one can use to encrypt/decrypt messages between them.
- **RSA:** It’s asymmetric key encryption where it has two different keys. The public key can be given to anyone and decrypted with another, which is kept private.

Q46) What is Forward Secrecy and how does it work?

Ans.

- Forward secrecy is a feature of specific key agreement protocols which gives assurance that even if the private key of the server is compromised the session keys will not be compromised. It is also known as perfect forward secrecy(PFS).
- The Algorithm that helps in achieving this is called "Diffie–Hellman key exchange".

Q47) What is an active reconnaissance?

Ans.

- Active reconnaissance is a kind of computer attack where an intruder engages the target system for collecting data about vulnerabilities.
- The attackers mostly use port scanning to identify vulnerable ports and then exploit the vulnerabilities of services that are associated with open ports.

Q48) What is security misconfiguration?

Ans. Security misconfiguration is a vulnerability that could happen if an application/network/device is susceptible to attack due to an insecure configuration option. It can be as simple as keeping the default username/password unchanged.

Q49) What is the difference between information protection and information assurance?

Ans.

- **Information protection:** It protects the data using encryption, security software, etc., from unauthorized access.
- **Information Assurance:** It keeps the data reliable by ensuring availability, authentication, confidentiality, etc.

Q50) What do you mean by Chain of Custody?

- Chain of custody refers to the probability of data provided as originally acquired and has not been changed before admission into evidence.
- In legal terms, it’s a chronological documentation/paper trail that records a proper sequence of custody, control, analysis, and disposition of electronic or physical evidence.