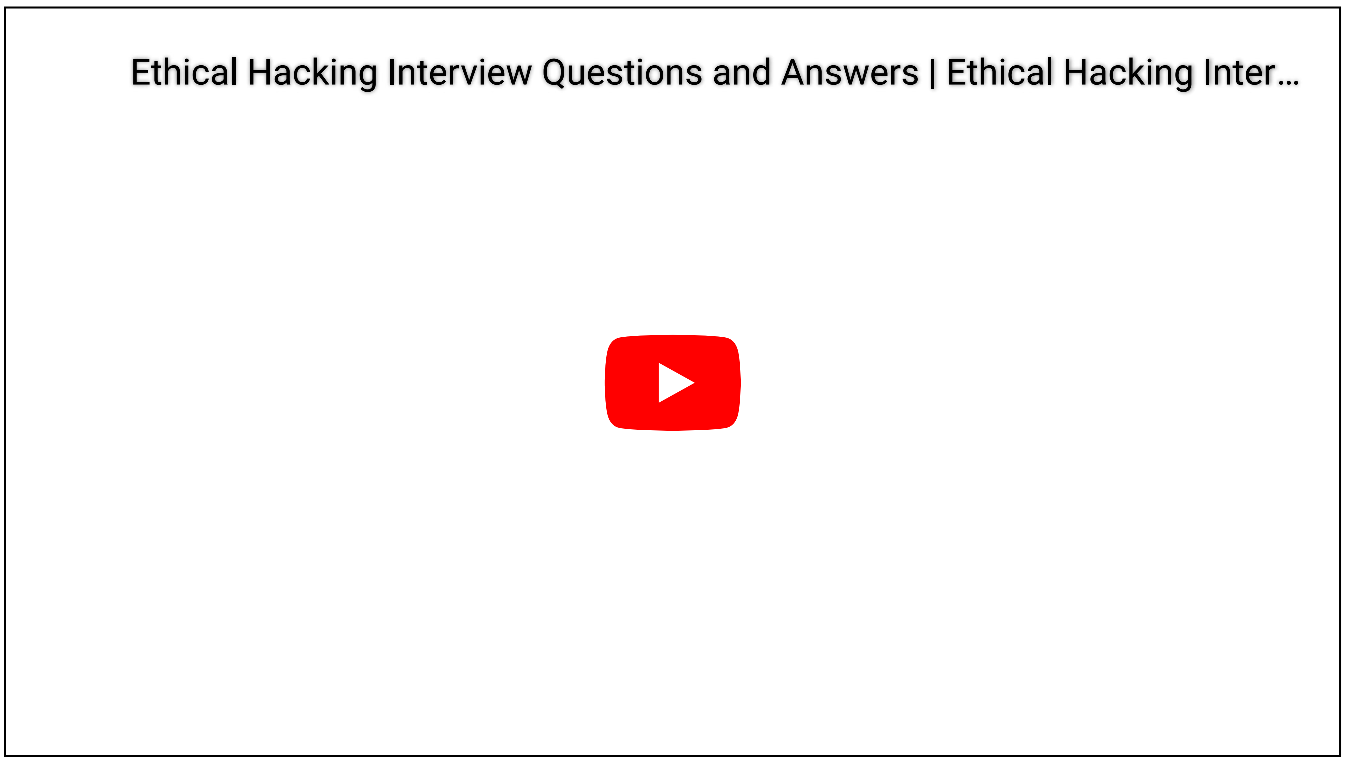
Ethical Hacking is one of the fastest-growing fields of cyber security which deals with finding vulnerabilities of a system and resolving them before any malware or black hat hackers find them. The Ethical Hacking Interview Questions blog is curated for both beginners and experts. With the assistance of SMEs from major organizations around the world, we have collected a list of the most frequently asked questions, along with their solutions, to help you give you an edge and prepare you for your Ethical Hacking job interview. Let's look at the top Ethical Hacking interview questions that companies generally ask:

Below are the three categories into which this Ethical Hacking Interview Questions and Answers blog is divided:

Check out this video on Ethical Hacking Interview Questions and Answers



Ethical Hacking Interview Questions and Answers | Ethical Hacking Inter…

Basic Ethical Hacking Interview Questions

1. What is Ethical Hacking?

Ethical Hacking is the practice of bypassing system security legally and with the permission of the owner to identify potential threats and vulnerabilities in a network.

2. What is the difference between Ethical Hacking and Cybersecurity?

Ethical Hacking is performed by Ethical Hackers to assess and provide a report based on the insights gained during the hack. Cyber Security is managed by Cyber Security experts whose responsibility is to defend the system from malicious activities and attacks.

3. What are the advantages and disadvantages of hacking?

Advantages	Disadvantages
It can be used to foil security attacks	It creates massive security issues
To plug the bugs and loopholes	Get unauthorized system access
It helps to prevent data theft	Stealing private information
Hacking prevents malicious attacks	Violating privacy regulations

Download Salary Trends
Learn how professionals like you got upto 100% hike!
Email Address
+91 IN
Phone Number
Submit

The types of hackers:

1. **Black Hat Hackers or Crackers:** Illegally, they hack systems to gain unauthorized access and cause disruptions in operations or breach data privacy.
2. **White Hat Hackers or Ethical Hackers:** These hackers hack systems and networks for the assessment of potential vulnerabilities or threats legally and with prior permission.
3. **Grey Box Hackers:** They assess the security weakness of a computer system or network without the owner’s permission but bring it to their attention later.

Aside from these three types, there are also other types of miscellaneous hackers.

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

Asymmetric encryption	Symmetric encryption
Asymmetric encryption uses different keys for encryption and decryption.	Symmetric encryption uses the same key for both encryption and decryption.
Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred.	Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel.

6. How can you avoid ARP poisoning?

ARP poisoning is a type of network attack that can be resolved through these techniques:

Using Packet filtering: Packet filters can filter out & block packets with clashing source address data.

Keeping away from trust relationship: Organizations ought to develop a protocol that depends on trust relationship as little as they can.

Utilize ARP spoofing software: Some programs assess and certify information before it is transmitted and blocks any information that is spoofed.

Get 100% Hike!

Master Most in Demand Skills Now !

Email Address

+91 IN

Phone Number

Submit

7. What can an ethical hacker do?

An ethical hacker is a computer system and networking master who systematically endeavours to infiltrate a PC framework or network for the benefit of its owners to find security vulnerabilities that a malicious hacker could potentially exploit.

8. Why is Python utilized for hacking?

Most broadly utilized scripting language for Hackers is Python. Python has some very critical highlights that make it especially valuable for hacking, most importantly, it has some pre-assembled libraries that give some intense functionality.

9. What is Pharming and Defacement?

Pharming : In this strategy the attacker compromises the DNS (Domain Name System) servers or on the user PC with the goal that traffic is directed towards malicious site

Defacement : In this strategy the attacker replaces the firm’s site with an alternate page. It contains the hacker’s name, images and may even incorporate messages and background music.

10. What is Cowpatty?

Cowpattyis implemented on an offline dictionary attack against WPA/WPA2 networks utilizing PSK-based verification (e.g. WPA-Personal). Cowpatty can execute an enhanced attack if a recomputed PMK document is accessible for the SSID that is being assessed.

11. What is Network Enumeration?

Network Enumeration is the revelation of hosts/gadgets on a network, they tend to utilize obvious disclosure protocols, for example, ICMP and SNMP to gather data, they may likewise check different ports on remote hosts for looking for surely known services trying to further recognize the function of a remote host.

Want to learn more check out this Cyber Security Tutorial.

12. Distinguish between phishing and spoofing?

Phishing and spoofing are totally different beneath the surface. One downloads malware to your PC or network, and the other part tricks you into surrendering sensitive monetary data to a cyber-crook. Phishing is a technique for recovery, while spoofing is a method for delivery.

13. What is network sniffing?

System sniffing includes utilizing sniffer tools that empower real- time monitoring and analysis of data streaming over PC systems. Sniffers can be utilized for various purposes, regardless of whether it’s to steal data or manage systems. Network sniffing is utilized for ethical and unethical purposes. System administrators utilize these as system monitoring and analysis tool to analyze and avoid network-related issues, for example, traffic bottlenecks. These devices can be used a organize cybercrime for untrustworthy purposes, for example, character usurpation, email, delicate information hijacking, etc.

14. What is network security, and what are its types?

Network security is essentially a set of rules and configurations formulated to protect the accessibility, confidentiality, and integrity of computer networks and data with the help of software and hardware technologies.

Types of network security:

- **Network access control:** To prevent attackers and infiltrations in the network, network access control policies are in place for both users and devices at the most granular level. For example, access authority to network and confidential files can be assigned and regulated as needed.
- **Antivirus and antimalware software**: Antivirus and antimalware software are used to continuously scan and protect against malicious software, viruses, worms, ransomware, and trojans.
- **Firewall protection**: Firewalls act as a barrier between your trusted internal network and an untrusted external network. Administrators can configure a set of defined rules for the permission of traffic into the network.
- **Virtual private networks (VPNs):** VPNs form a connection to the network from another endpoint or site. For example, an employee working from home uses a VPN to connect to the organization's network. The user would need to authenticate to allow this communication. The data between the two points is encrypted.

Check out our Ethical Hacking Course in India now to learn about the concepts involved in the domain!

15. What are network protocols, and why are they necessary?

A network protocol is established as a set of rules to determine the way data transmissions take place between the devices in the same network. It basically allows communication between the connected devices regardless of any differences in their internal structure, design, or processes. Network protocols play a critical role in digital communications.

Career Transition

Intermediate Ethical Hacking Interview Questions

16. What do you understand by footprinting in ethical hacking? What are the techniques utilized for foot printing?

Footprinting is nothing but accumulating and revealing as much data about the target network before gaining access to any network. **Open Source Footprinting:** It will search for the contact data of administrators that will be utilized for guessing passwords in Social Engineering **Network Enumeration:** The hacker attempts to distinguish the domain names and the network blocks of the target network **Scanning:** After the network is known, the second step is to spy the active IP addresses on the network. For distinguishing active IP addresses (ICMP) Internet Control Message Protocol is a functioning IP address **Stack Fingerprinting:** the final stage of the footprinting step can be performed, once the hosts and port have been mapped by examining the network, this is called Stack fingerprinting.

17. What is the difference between encryption and hashing?

Encryption	Hashing
Encryption is reversible	Hashing is irreversible
Encryption ensures confidentiality	Hashing ensures Integrity

18. What is CIA Triad?

CIA triad is a popular information security model. It follows three principles mentioned below:

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

*Go through this **Ethical Hacker Training** to learn more about RPA.*

19. What is the difference between VA and PT?

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

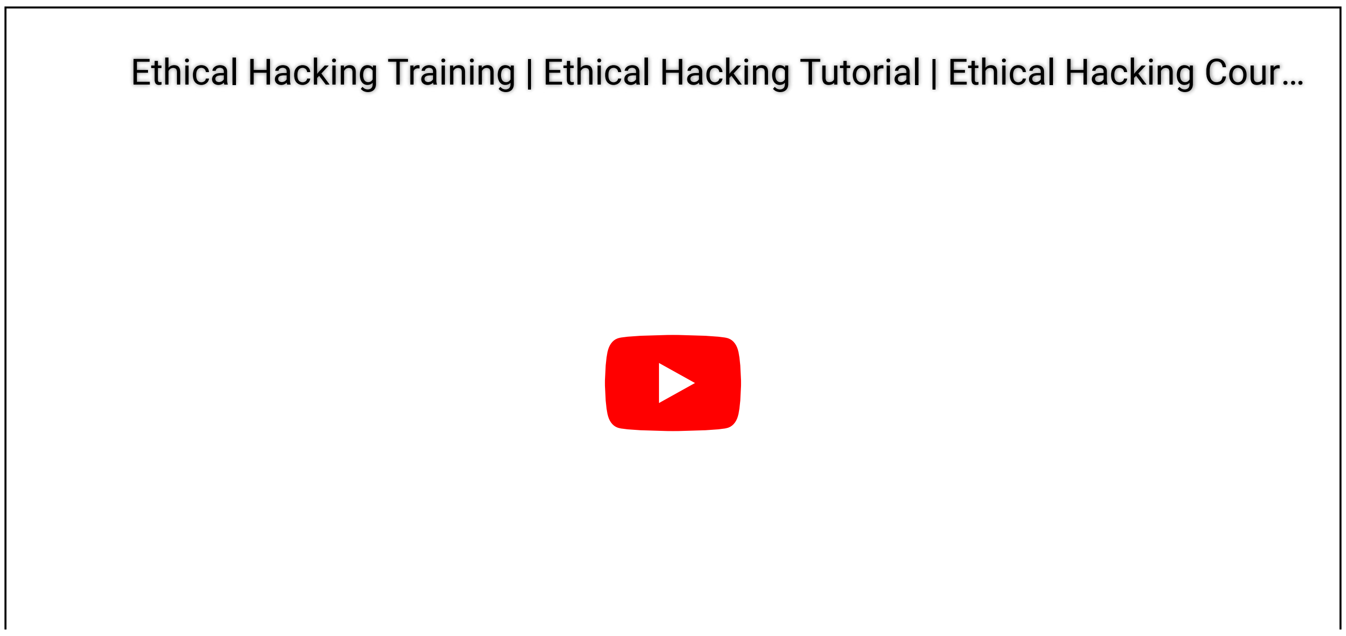
20. What is a firewall?

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

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

Data leak is nothing but data knowledge getting out of the organization in an unauthorized manner. Data will get leaked through numerous ways in which – emails, prints, laptops obtaining lost, unauthorized transfer of data to public portals, removable drives, pictures, etc. Security of data is very important nowadays so there are varied controls that may be placed to make sure that the info doesn't get leaked, many controls will be limiting upload on web websites, following an internal encryption answer, limiting the emails to the interior network, restriction on printing confidential data, etc.

Check out this video on Ethical Hacker


Ethical Hacking Training | Ethical Hacking Tutorial | Ethical Hacking Cour…

22. What are the hacking stages? Explain each stage.

Hacking, or targeting on a machine, should have the following 5 phases :

Surveillance : This is the principal stage where the hacker endeavours to gather as much data as possible about the target

Scanning : This stage includes exploiting the data accumulated amid Surveillance stage and utilizing it to inspect the casualty. The hacker can utilize computerized devices amid the scanning stage which can incorporate port scanners, mappers and vulnerability scanners.

Getting access : This is where the real hacking happens. The hacker attempts to exploit data found amid the surveillance and Scanning stage to get access.

Access Maintenance : Once access is gained, hackers need to keep that access for future exploitation and assaults by securing their exclusive access with backdoors, rootkits and Trojans.

Covering tracks : Once hackers have possessed the capacity to pick up and maintain access, they cover their tracks and to keep away from getting detected. This likewise enables them to proceed with the utilization of the hacked framework and keep themselves away from legitimate activities.

Looking to learn more about Ethical Hacking? Read our full guide on Ethical Hacking Tutorial.

23. What are the tools used for ethical hacking?

There are several moral hacking tools out there within the marketing for different purposes, they are:

- **NMAP –** NMAP stands for Network plotter. It's an associate degree open-source tool that's used widely for network discovery and security auditing.
- **Metasploit –** Metasploit is one of the most powerful exploit tools to conduct basic penetration tests.
- **Burp Suit –** Burp Suite could be a widespread platform that's widely used for playing security testing of internet applications.
- **Angry IP Scanner –** Angry information processing scanner could be a lightweight, cross-platform information processing address and port scanner.
- **Cain & Abel –** Cain & Abel is a password recovery tool for Microsoft operational Systems.
- **Ettercap –** Ettercap stands for local area network Capture. It is used for a Man-in-the-Middle attack using a network security tool.

24. What is MAC Flooding?

MAC Flooding is a kind of a technique wherever the protection of given network switch is compromised. In MAC flooding the hacker floods the switch with sizable amounts of frames, than what a switch can handle. This makes switch behaving as a hub and transmits all packetsto all the ports existing. Taking the advantage of this the attacker can attempt to send his a hub and transmits all packetsto all the ports existing. Taking the advantage of this the attacker can attempt to send his packet within the network to steal the sensitive information.

25. What is sniffing? Explain its types in Ethical Hacking.

Sniffing in Ethical Hacking is a method implemented for monitoring all the data packets that pass through a particular network. Sniffers are primarily used to oversee and troubleshoot network traffic, and Network/System Administrators are responsible for this role. Sniffers can be installed in the system in the form of software or hardware.

However, attackers can misuse sniffers to gain access to data packets that contain sensitive information, such as account information, passwords, etc. Packet sniffers on a network can give a malicious hacker the opportunity to intrude and access all of the network traffic.

There are two types of sniffing:

- **Active sniffing:** Sniffing in a point-to-point network device called the switch is referred to as active sniffing. The switch is responsible for the regulation of the data flow between its ports. This is done through the active monitoring of the MAC address on each port, which enables the passing of data only to the intended target. To activate the sniffing of the traffic between targets, sniffers have to inject traffic into the LAN.
- **Passive sniffing:** Passive sniffing happens when the sniffing is done through the hub. The traffic that goes through the unbridged network or the non-switched segment is transparent to all machines in that segment. Here, sniffers work at the network's data link layer. This is called passive sniffing as sniffers set up by the attackers passively wait for the data to capture them when they are sent.

26. What is an intrusion detection system (IDS)?

An intrusion detection system, or IDS for short, is a software application or device that monitors a network for the detection of malicious activities or policy violations. Any detected malicious activity or violation is reported or collected centrally with the help of a security information and event management system. An IDS that can respond to intrusions upon discovery is classified as an intrusion prevention system (IPS).

Looking for a CEH course? Have a look at our Ethical Hacking course in Bangalore!

27. What is Defense in Depth?

Defense in Depth (DiD) in Cybersecurity involves a series of defensive mechanisms that are layered for the purpose of securing valuable data and information. In case one mechanism fails, another one will start to work immediately to thwart unprecedented attacks. DiD's multi-layered approach, which is also referred to as the castle approach, tightens up the security of a system.

Courses you may like

28. What is a security operations center (SOC)?

A security operations center (SOC) as a facility houses the information security team. This team is set in place to continuously monitor and analyze an organization's security. The SOC team's responsibility includes detection, analysis, anc immediate response to Cybersecurity incidents through the implementation of various technology solutions and a set of processes. The team may include Security Analysts, Engineers, and Managers who work closely with the incident response team.

29. What is penetration testing? Mention some popular penetration testing tools.

A penetration test or a pen test is the simulation of a cyberattack on a computer to check for potential vulnerabilities in the system. It is commonly implemented to augment a web application firewall (WAF). It can involve a simulated attack on any number of application systems such as APIs, frontend servers, and backend servers to discover any vulnerabilities present. The insights gained through this kind of testing can be used to tighten the WAF security policies and fix the detected issues.

Following are a few popular tools used for penetration testing:

- Netsparker
- Wireshark
- Metasploit
- BeEF
- Aircrack

30. What is network traffic monitoring and analysis?

Network traffic monitoring and analysis is a security analytical technique and tool used by Network Security Administrators for the detection of issues that can affect accessibility, functionality, and network traffic security in connected devices.

31. What is the difference between RPO and RTO?

The recovery point objective (RPO) deals with the backup frequency and the recovery time objective (RTO) with the recovery timeline. During a system outage, RPO and RTO can determine the impact of the downtime on business operations.

RPO is a measure of how frequently you take backups and indicates the amount of data that will be lost or needed to be reentered after an outage. RTO, on the other hand, is the amount of downtime a business can afford. It determines how long it might take for a system to recover after a business disruption.

Advanced Ethical Hacking Interview Questions

32. Explain how you can stop your website getting hacked?

By adapting following methodology you'll be able to stop your web site from obtaining hacked

- Using Firewall : Firewall may be accustomed drop traffic from suspicious information processing address if attack may be an easy DOS
- Encrypting the Cookies : Cookie or Session poisoning may be prevented by encrypting the content of the cookies, associating cookies with the consumer information processing address and temporal arrangement out the cookies once it slow
- Validating and confirmative user input : This approach is prepared to stop the type tempering by confirmative and verifying the user input before processing it
- Header Sanitizing and validation : This technique is beneficial against cross website scripting or XSS, this method includes verifying and sanitizing headers, parameters passed via the address, type parameters and hidden values to cut back XSS attacks.

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

Burp Suite is an integrated platform used for attacking net applications. It contains all the tools a hacker would need for attacking any application. a number of these functionalities are

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

- Decoder
- Comparer
- Sequencer

34. What is SQL injection and its types?

If the application doesn't sanitize the user input then the SQL injection happens. Thus a malicious hacker would inject SQL queries to gain unauthorized access and execute administration operations on the database. SQL injections may be classified as follows:

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

35. What's 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 troublesome or not possible for legitimate users to access or use targeted sites.

Common DOS attacks include:

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

36. Which programming language is used for hacking?

It's best, actually, to master all 5 of Python, C/C++, Java, Perl, and LISP. Besides being the foremost vital hacking languages, they represent totally different approaches to programming, and each of it can educate you in valuable ways.

37. What is meant by spoofing attack?

A spoofing attack is when a malicious party impersonates another device or user on a network so as to launch attacks against network hosts, steal data, unfold malware or bypass access controls. Different Spoofing attacks are deployed by malicious parties to achieve this.

38. What are the different types of spoofing?

- ARP Spoofing Attack.
- DNS Spoofing Attack.
- IP Spoofing Attack.

Curious to know the difference between Cyber security and Ethical hacking? Have a look at our blog on Cyber security vs Ethical hacking.

39. What is active and passive reconnaissance?

Passive reconnaissance is nothing but to gain info regarding targeted computers and networks while not actively participating with the systems. In active reconnaissance, in distinction, the attacker engages with the target system, usually