By OnlineInterviewQuestions.com

Ethical hacking Interview Questions

Ethical hacking is also known as the Penetration test. This penetration testing is a type of activity that is being introduced in the systems or the network. The main aim of Ethical hacking is to test to find out the threats, vulnerabilities in the system that a malicious hacker may find and exploit and cause to lose data, financial loss or the other major damages. The main motto of Ethical hacking is also to improve the security of the internet or the network by solving the vulnerabilities that are found during the testing. There are lots of **Ethical hacking interview questions** and answers that will help you a lot.

Ethical hacking is done by Ethical Hackers. Ethical hackers are also known as the White hat hackers. They are mainly networking security experts who consistently attempt to crack a computer system, network, application or the other computing resources. Ethical hacking is mainly done by the company or an individual to help to analyze the threat in the computer or the network. Below are some of the **Ethical hacking interview questions** and answers.

Q1. What is Ethical Hacking?

Ethical Hacking is also known as white hat hacking. This type of hacking is mainly performed by the company or an individual. This Ethical hacking helps to identify all the hidden threats and the vulnerabilities in the system and the networks.

Q2. What are the works of ethical hackers?

The main work of the Ethical hacker is to attempt the circumventing of any of the weak point in the network or the system that can be exploited by the malignant hackers.

Q3. What are the constitutes an Ethical hacker should always follow?

The following are some of the constitutes an Ethical hacker should follow and they are:

- The ethical hackers should have written permission to examine the network or the systems and attempt to identify all the hidden risk factors.
- Ethical hackers should respect the individuals or any of the company’s privacy.
- At the time of leaving the office, Ethical hackers main work is to shut down each and everything without leaving them open.

Q4. What are the types of tools that are used by the Ethical hackers?

The following are some of the tools being used by the Ethical hackers:

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

Q5. What is burp suit in the Ethical hacking?

Burp suite is mainly a type of a unified platform that is generally used for the invading in the web application. Burp suite contains all the desirable tools that the Ethical hackers need to attack an application.

Q6. What are the types of tools you will get in the Ethical hacking?

The following are some of the types of tools that you will get in the ethical hacking:

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Decoder
- Comparer
- Sequencer

Q7. What are the different types of hacking stages?

There are different types of hacking stages. Some of them are:

- Reconnaissance: The Reconnaissance is the first phase of the hacking system. In this stage, the hackers used as much information as possible about the purpose.
- Scanning: The scanning is the second stage. This stage mainly involves exploiting of the information being gathered during the Reconnaissance stage and it is also used to investigate the victim.
- Gaining access: Gaining access is the stage at which the real hacking mainly takes place. In this stage, the hackers will exploit all the vulnerabilities that are being discovered during the reconnaissance.
- Maintaining access: At maintaining access stage, the hackers will maintain access for future exploration.

- Covering tracks: This is the final phase of the hacking stages. Once the hackers have succeeded in gaining and maintaining access, they will cover the track and the traces so that further detection can be avoided.

Q8. What are the types of scannings used in Ethical hacking?

The following are some of the types of scanning that are used in Ethical hacking:

- Port scanning
- Vulnerability scanning
- Network scanning

Q9. What is the port scanning in ethical hacking?

Port scanning is one of the frequent reconnaissance techniques that is used by Ethical hackers to discover the threats and the vulnerabilities that are exploited by computer hackers.

Q10. What is vulnerability scanning in Ethical hacking?

Vulnerability scanning is the type of a computer program that is mainly designed to approach the networks, connections or the applications that are known for the weakness.

Q11. What is network scanning in Ethical hacking?

Network scanning is the type of procedure that is used to identify the entire active hosts that are active on the network. They may be present either for the purpose of attacking in the network or for the network security assessment.

Q12. What is a footprint in the ethical hacking?

The footprint is the type of technique that is used to gather all the information about the computer system and all the individuals they belong to. To get all the information, ethical hackers should use various tools and all the techniques of the footprint.

Q13. What are the different types of techniques that are used in the footprint?

The following are different types of techniques that are used in the footprint:

- Open source footprint

- Network enumeration
- Scanning
- Stack fingerprint

Q14. What is network sniffing in ethical hacking?

Network sniffing is the type of process of monitoring and capturing all the packets that are passing through the given network using the sniffing tools.

Q15. What are the types of hackers?

The following are the different types of hackers:

- White hat hackers, also known as the Ethical hackers
- Black hat hackers, also known as the computer or network hackers
- Grey hat Hackers are the blend of the two hackers that are ethical hackers and the network hackers
- Miscellaneous hackers

Q16. What are the different types of software used by hackers?

The following are the different types of software being used by hackers:

- Metasploit framework
- NMAP
- OpenSSH
- Wireshark
- Nessus
- Aircrack NG
- Snort
- John the ripper

Q17. What are the different types of the programming languages used by hackers?

The following are different types of the programming languages used by hackers:

- Python
- C
- C++
- Perl
- Lisp

Q18. What is the differences between Ethical hacking and computer hacking?

Ethical Hacking	Computer Hacking
Ethical hacking is the type of methodology to find out any of the threats or the vulnerabilities in the system or in the network.	The computer hacking mainly refers to the breaking into someone's system for the personal and commercial gains.
The hackers who do ethical hacking are mainly known as white hat hackers.	The hackers who do computer hacking are mainly known as grey hat hackers.

Q19. What is sniffing in hacking?

Sniffing in hacking is the monitoring and deriving of every packet that goes through a specific network. This process is achieved by making use of sniffing tools. Sniffing of information can take place in Web traffic, router configuration, chat sessions, email and DNS traffic, FTP and Telnet password. Sniffing in hacking can also be described as tapping telephone wires in order to know or hear a conversation. This is broadly known as wiretapping. With sniffing, you can see both the protected and unprotected traffic. An individual working in an organization can sniff all the traffic of the network in the physical location.