

# security questions for interview and exam preparation

---

- what are the components of security ?
- what is CIA triad ?
- what is ethical hacking ?
- what is ethical hacking required ?
- what is penetration testing ?
- what is a ethical hacker ?
- what skills are required to be a hacker ?
- what are the types of hackers ?
- what are the differences between offensive and defensive security ?
- what are the differences between black hat and white hat hackers ?
- what is the difference between cyber terrorist and state sponsored hackers ?
- what are the phases of hacking ?
- what is cyber kill chain ? and what are the phases of cyber kill chain ?
- what are the tools used in ethical hacking ?
- what is a cyber attack ?
- what is vulnerability ?
- what are the motives or goals behind the attacks ?
- what are the classes of attacks ?
- what is the difference between passive and active attacks ?
- what is PCI DSS and where is it used ?
- what is HIPPA ?
- what is DMCA and why is it important ?
- what is the difference between red team and blue team ?
- what is a malware ?
- what are the types of malware ?
- what is the difference between a virus and a worm ?
- what is the difference between virus and trojan ?
- what is used to open backdoor on a computer ?
- how virus works ?
- how worm works ?
- how trojan works ?
- what are ways for malware to enter the system ?
- how the hacker spreads the malware ?
- what are the components of malware ?
- what are the characteristics of virus ?
- what could be a purpose of creating virus ?
- how do you know if your machine is infected with a virus ?
- what is virus lifecycle and what are the stages in it ?
- what are the types of viruses ?
- what is logic bomb virus ? is the same as the bomb used in the war ?
- what is ransomware ? how critical it is compared with trojan ?
- which tools are used to create a virus ?
- what are the types of trojan ?

- how does a hacker use the trojan ?
- what is RAT ?
- what is rootkit ?
- what is scanning ?
- what are the types of scanning ?
- why scanning is required ?
- what is the size of TCP header ?
- what is three way handshaking ?
- what are the communication flags in TCP header ?
- which tools are used for scanning ?
- what is social engineering ?
- which are the targets of social engineering ?
- why social engineering is possible ?
- what are the phases of social engineering attacks ?
- what are the types of social engineering ?
- what are the types of phishing ?
- how hackers carry out man-in-the middle attack ? which tool can be used to perform this attack ?
- what is ARP and reverse ARP ?
- what is ARP spoofing ?
- what is ARP poisoning ?
- what is DNS spoofing ?
- what are different types of DNS records exist ?
- what are the methods of windows authentication ?
- what is the difference between NTLM and kerberos ?
- what are the types of password cracking ?
- which tools are used to crack password ?
- how to defend against password attacks ?
- what is the buffer overflow ? what are the types of buffer overflow?
- what are popular web server attacks ? how to carry them out ?
- what is DoS and DDoS attack ? how to carry them out ?
- what is botnet ?
- what is directory traversal attack ?
- what is SQL injection attack ? why it is possible ? how to protect against it ?
- what is CSRF attack ?
- what is XSS attack ? what are the types of it ?
- what are the netBIOS attacks ?
- what is website defacement ?
- what are server hardening methods ?
- what is network sniffer ? which tools can be used to sniff the network ?
- what is session hijacking ? how to protect against it ?
- what is SSID in wireless networking ?
- what is google hacking database ?
- which tools can be used for enumeration ?
- what is target of evaluation ?
- what is steganography ? what are types ?
- what is OWASP ? what are top 10 web vulnerabilities ?

- which are intrusion detection systems ?
- what is the difference between Smurf attack and Syn Flood attack ?
- what do you mean by privilege escalation ? how do you achieve it ?
- which are the tools used for network scanning and analysis ?
- what is MIB ?
- what is footprinting ?
- what do you mean by fingerprinting ?
- what is cowpatty ?
- why and where python is needed in ethical hacking ?
- what are the tools used for wireless hacking ?
- what do you mean by Oday attacks and Oday vulnerability ?
- what is firewall ? where is it used ? what are the types of firewall ? give some popular examples of firewall ?