Top 25 Ethical hacking Interview Questions & Answers

1) Explain what is Ethical Hacking?

Ethical Hacking is when a person is allowed to hacks the system with the permission of the product owner to find weakness in a system and later fix them.

2) What is the difference between IP address and Mac address?

IP address: To every device IP address is assigned, so that device can be located on the network. In other words IP address is like your postal address, where anyone who knows your postal address can send you a letter.

MAC (Machine Access Control) address: A MAC address is a unique serial number assigned to every network interface on every device. Mac address is like your physical mail box, only your postal carrier (network router) can identify it and you can change it by getting a new mailbox (network card) at any time and slapping your name (IP address) on it.

3) List out some of the common tools used by Ethical hackers?

- Meta Sploit
- Wire Shark
- NMAP
- John The Ripper
- Maltego

4) What are the types of ethical hackers?

The types of ethical hackers are

- Grey Box hackers or Cyberwarrior
- Black Box penetration Testers
- White Box penetration Testers
- Certified Ethical hacker

5) What is footprinting in ethical hacking? What is the techniques used for footprinting?

Footprinting refers accumulating and uncovering as much as information about the target network before gaining access into any network. The approach adopted by hackers before hacking

- Open Source Footprinting : It will look for the contact information of administrators that will be used in guessing the password in Social engineering
- Network Enumeration : The hacker tries to identify the domain names and the network blocks of the target network
- Scanning : Once the network is known, the second step is to spy the active IP addresses on the

network. For identifying active IP addresses (ICMP) Internet Control Message Protocol is an active IP addresses
- Stack Fingerprinting : Once the hosts and port have been mapped by scanning the network, the final footprinting step can be performed. This is called Stack fingerprinting.

6) Explain what is Brute Force Hack?

Brute force hack is a technique for hacking password and get access to system and network resources, it takes much time, it needs a hacker to learn about JavaScripts. For this purpose, one can use tool name “Hydra”.

7) Explain what is DOS (Denial of service) attack? What are the common forms of DOS attack?

Denial of Service, is a malicious attack on network that is done by flooding the network with useless traffic. Although, DOS does not cause any theft of information or security breach, it can cost the website owner a great deal of money and time.

- Buffer Overflow Attacks
- SYN Attack
- Teardrop Attack
- Smurf Attack
- Viruses

8) Explain what is SQL injection?

SQL is one of the technique used to steal data from organizations, it is a fault created in the application code. SQL injection happens when you inject the content into a SQL query string and the result mode content into a SQL query string, and the result modifies the syntax of your query in ways you did not intend

9) What are the types of computer based social engineering attacks? Explain what is Phishing?

Computer based social engineering attacks are

- Phishing
- Baiting
- On-line scams

Phishing technique involves sending false e-mails, chats or website to impersonate real system with aim of stealing information from original website.

10) Explain what is Network Sniffing?

A network sniffer monitors data flowing over computer network links. By allowing you to capture and view the packet level data on your network, sniffer tool can help you to locate network problems. Sniffers can be used for both stealing information off a network and also for legitimate network management.

11) Explain what is ARP Spoofing or ARP poisoning?

ARP (Address Resolution Protocol) is a form of attack in which an attacker changes MAC (Media Access Control) address and attacks an internet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets.

12) How you can avoid or prevent ARP poisoning?

ARP poisoning can be prevented by following methods

- Packet Filtering : Packet filters are capable for filtering out and blocking packets with conflicting source address information
- Avoid trust relationship : Organization should develop protocol that rely on trust relationship as little as possible
- Use ARP spoofing detection software : There are programs that inspects and certifies data before it is transmitted and blocks data that is spoofed
- Use cryptographic network protocols : By using secure communications protocols like TLS, SSH, HTTP secure prevents ARP spoofing attack by encrypting data prior to transmission and authenticating data when it is received

13) What is Mac Flooding?

Mac Flooding is a technique where the security of given network switch is compromised. In Mac flooding the hacker or attacker floods the switch with large number of frames, then what a switch can handle. This make switch behaving as a hub and transmits all packets at all the ports. Taking the advantage of this the attacker will try to send his packet inside the network to steal the sensitive information.

14) Explain what is DHCP Rogue Server?

A Rogue DHCP server is DHCP server on a network which is not under the control of administration of network staff. Rogue DHCP Server can be a router or modem. It will offer users IP addresses , default gateway, WINS servers as soon as user's logged in. Rogue server can sniff into all the traffic sent by client to all other networks.

15) Explain what is Cross-site scripting and what are the types of Cross site scripting?

Cross site scripting is done by using the known vulnerabilities like web based applications, their servers or plug-ins users rely upon. Exploiting one of these by inserting malicious coding into a link which appears to be a trustworthy source. When users click on this link the malicious code will run as a part of the client's web request and execute on the user's computer, allowing attacker to steal information.

There are three types of Cross-site scripting

- Non-persistent
- Persistent
- Server side versus DOM based vulnerabilities

16) Explain what is Burp Suite, what are the tools it consist of?

Burp suite is an integrated platform used for attacking web applications. It consists of all the Burp tools required for attacking an application. Burp Suite tool has same approach for attacking web applications like framework for handling HTTP request, upstream proxies, alerting, logging and so on.

The tools that Burp Suite has

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

17) Explain what is Pharming and Defacement?

- **Pharming:** In this technique the attacker compromises the DNS (Domain Name System) servers or on the user computer so that traffic is directed to a malicious site
- **Defacement:** In this technique the attacker replaces the organization website with a different page. It contains the hackers name, images and may even include messages and background music

18) Explain how you can stop your website getting hacked?

By adapting following method you can stop your website from getting hacked

- **Sanitizing and Validating users parameters:** By Sanitizing and Validating user parameters before submitting them to the database can reduce the chances of being attacked by SQL injection
- **Using Firewall:** Firewall can be used to drop traffic from suspicious IP address if attack is a simple DOS
- **Encrypting the Cookies:** Cookie or Session poisoning can be prevented by encrypting the content of the cookies, associating cookies with the client IP address and timing out the cookies after some time
- **Validating and Verifying user input :** This approach is ready to prevent form tempering by verifying and validating the user input before processing it
- **Validating and Sanitizing headers :** This techniques is useful against cross site scripting or XSS, this technique includes validating and sanitizing headers, parameters passed via the URL, form parameters and hidden values to reduce XSS attacks

19) Explain what is Keylogger Trojan?

Keylogger Trojan is malicious software that can monitor your keystroke, logging them to a file and sending them off to remote attackers. When the desired behaviour is observed, it will record the keystroke and captures your login username and password.

20) Explain what is Enumeration?

The process of extracting machine name, user names, network resources, shares and services from a system. Under Intranet environment enumeration techniques are conducted.

21) Explain what is NTP?

To synchronize clocks of networked computers, NTP (Network Time Protocol) is used. For its primary means of communication UDP port 123 is used. Over the public internet NTP can maintain time to within 10 milliseconds

22) Explain what is MIB?

MIB (Management Information Base) is a virtual database. It contains all the formal description about the network objects that can be managed using SNMP. The MIB database is hierarchical and in MIB each managed objects is addressed through object identifiers (OID).

23) Mention what are the types of password cracking techniques?

The types of password cracking technique includes

- AttackBrute Forcing
- AttacksHybrid
- AttackSyllable
- AttackRule

24) Explain what are the types of hacking stages?

The types of hacking stages are

- Gaining AccessEscalating
- PrivilegesExecuting
- ApplicationsHiding
- FilesCovering Tracks

25) Explain what is CSRF (Cross Site Request Forgery)? How you can prevent this?

CSRF or Cross site request forgery is an attack from a malicious website that will send a request to a web application that a user is already authenticated against from a different website. To prevent CSRF you can append unpredictable challenge token to each request and associate them with user's session. It will ensure the developer that the request received is from a valid source.

Refer our Ethical Hacking Tutorials for an extra edge in your interview.

Live Project	SoapUI	Photoshop	Manual Testing	Mobile Testing

Data Warehouse	R Tutorial	Tableau	DevOps	AWS

Jenkins	Agile Testing	RPA	JUnit	Software Engineering

Selenium	CCNA	AngularJS	NodeJS	PLSQL