Ethical hacking interview questions

Ethical hacking:

Ethical hacking can be described as the hacking procedure done by professionals to identify the potential threats on the computer network. The Ethical hacker actually hacks his way through the system for finding the loop holes present in the system and the bad security arrangements so that the companies can rectify them. This the organization does to reduce if not eliminate any potential threats to the organization. here are Ethical hacking interview questions.

In order to authenticate the hacking to be ethical one has to follow the rules:

1. One need to take permission first to probe the network to find the potential threats to the security of the network.

2. One needs to respect the companies privacy policy and not intrude.

3. You need to report all the security venerability found to the company. Leaving none.

4. You must inform the software developer about any security issue in the software.

Following these rules could make you a good ethical hacker. Also, Ethical hackers are trusted people in the organization and thus the trust factor enables them to have hefty salaries. Thus, the career as an ethical hacker is great. Ethical hacking interview questions.

So here for your help are the Ethical hacking questions:

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) Who is hacker?

Answer: A hacker is an intelligent individual with excellent programming skills, and who would have the ability to create and explore computer software.

6) What is footprinting ?

Answer: Foot printing is known as uncovering and collecting as much as information about a target network as possible about a target network.

7) Definition and types of scanning.

Answer: Scanning may be referred to as a set of procedures for identifying hosts, ports and the services attached to a network. Scanning is a very important component for information gathering for the hacker to create a profile in the site or the organization to be hacked.

Types of scanning:

There are 3 types of scanning-

a. Port scanning

b. Venerability scanning

c. Network scanning.

8) What is Enumeration ?

Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an Intranet Environment.

9) What is SNMP(Simple Network Management Protocol) ?

the Simple network management program can be defined as a simple TCP/IP protocol used for remote monitoring and managing hosts, routers and other such devices on the network.

10) What is MIB (Management Information Base)?

It is a database (virtual) that contains information about all the network objects that are their in the SNMP. This data base in hierarchic and all the objects contained in it are addressed by object identifier.

11) What is LDAP (Lightweight Directory Access Protocol) ?

It is a protocol that is used for getting access to the directory listing in the present active directory or also from the other directory services.

12) What is NTP ?

This is protocol whose main function is to synchronize the clocks in the networked or connected computers.

13) What are the types of hacking stages ?

a. Gain access

b. Getting privilages

c. Executing applications

d. Hiding the files

e. Covering the tracks

14) Types of password cracking techniques?

a. Dictionary attacks

b. Brute Forcing Attacks

c. Hybrid Attack

d. Syllable Attack

e. Rule – based Attack

15) 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.

16) 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”.

17) 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

18) 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

19) 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.

20) 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.