Hacking Job Interview Questions And Answers

Interview Questions Answers

https://interviewquestionsanswers.org/

About Interview Questions Answers

Interview Questions Answers . ORG is an interview preparation guide of thousands of Job Interview Questions And Answers, Job Interviews are always stressful even for job seekers who have gone on countless interviews. The best way to reduce the stress is to be prepared for your job interview. Take the time to review the standard interview questions you will most likely be asked. These interview questions and answers on Hacking will help you strengthen your technical skills, prepare for the interviews and quickly revise the concepts.

If you find any **question or answer** is incorrect or incomplete then you can **submit your question or answer** directly with out any registration or login at our website. You just need to visit Hacking Interview Questions And Answers to add your answer click on the *Submit Your Answer* links on the website; with each question to post your answer, if you want to ask any question then you will have a link *Submit Your Question*; that's will add your question in Hacking category. To ensure quality, each submission is checked by our team, before it becomes live. This Hacking Interview preparation PDF was generated at **Wednesday 29th November, 2023**

You can follow us on FaceBook for latest Jobs, Updates and other interviews material.
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter for latest Jobs and interview preparation guides.
https://twitter.com/InterviewQA

If you need any further assistance or have queries regarding this document or its material or any of other inquiry, please do not hesitate to contact us.

Best Of Luck.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
Support@InterviewQuestionsAnswers.ORG

Hacking Interview Questions And Answers Guide.

Question - 1:

List the types of ethical hackers?

Ans:

The types of ethical hackers are:
* Grey Box hackers or Cyberwarrior
* Black Box penetration Testers
* White Box penetration Testers
* Certified Ethical hacker

View All Answers

Question - 2:

How to stop website getting hacked?

Ans:

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.

View All Answers

Question - 3:

what are the tools Burp Suite consist of?

Ans:

The tools that Burp Suite has:
* Proxy
* Spider
* Scanner
* Intruder
* Repeater
* Decoder
* Comparer
* Sequencer

View All Answers

Question - 4:

What is Burp Suite?

Ans:

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.

View All Answers

Question - 5:

What is CSRF (Cross Site Request Forgery)?

Ans:

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.

View All Answers

Question - 6:

What are the types of hacking stages?

Ans:

The types of hacking stages are:
* Gaining AccessEscalating
* PrivilegesExecuting
* ApplicationsHiding
* FilesCovering Tracks

View All Answers

Question - 7:

What are the types of password cracking techniques?

Ans:

The types of password cracking technique includes:
* AttackBrute Forcing
* AttacksHybrid
* AttackSyllable
* AttackRule

View All Answers

Question - 8:

What is MIB?

Ans:

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).

View All Answers

Question - 9:

What is NTP?

Ans:

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.

View All Answers

Question - 10:

Define Enumeration?

Ans:

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

View All Answers

Question - 11:

What is Keylogger Trojan?

Ans:

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.

View All Answers

Question - 12:

Define Mac Flooding?

Ans:

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.

View All Answers

Question - 13:

What is Defacement?

Ans:

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.

View All Answers

Question - 14:

What is Pharming?

Ans:

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.

View All Answers

Question - 15:

List the types of Cross site scripting?

Ans:

There are three types of Cross-site scripting:
* Non-persistent
* Persistent
* Server side versus DOM based vulnerabilities

View All Answers

Question - 16:

Define Cross-site scripting?

Ans:

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.

View All Answers

Question - 17:

What is DHCP Rogue Server?

Ans:

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.

View All Answers

Question - 18:

List the common forms of DOS attack?

Ans:

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

View All Answers

Question - 19:

What is DOS (Denial of service) attack?

Ans:

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.

View All Answers

Question - 20:

How to avoid or prevent ARP poisoning?

Ans:

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.

View All Answers

Question - 21:

What is ARP Spoofing or ARP poisoning?

Ans:

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.

View All Answers

Question - 22:

Define SQL injection?

Ans:

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.

View All Answers

Question - 23:

What is Network Sniffing?

Ans:

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.

View All Answers

Question - 24:

List the types of computer based social engineering attacks?

Ans:

Computer based social engineering attacks are:
* Phishing
* Baiting
* On-line scams

View All Answers

Question - 25:

Define Phishing?

Ans:

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

View All Answers

Question - 26:

Define footprinting in ethical hacking?

Ans:

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.

View All Answers

Question - 27:

Define Stack Fingerprinting?

Ans:

Once the hosts and port have been mapped by scanning the network, the final footprinting step can be performed. This is called Stack fingerprinting.

View All Answers

Question - 28:

What is Brute Force Hack?

Ans:

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".

View All Answers

Question - 29:

Define Network Enumeration?

Ans:

The hacker tries to identify the domain names and the network blocks of the target network.

View All Answers

Question - 30:

Define Open Source Footprinting?

Ans:

It will look for the contact information of administrators that will be used in guessing the password in Social engineering.

View All Answers

Question - 31:

Define Scanning?

Ans:

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.

View All Answers

Question - 32:

What are the common tools which are used by Ethical hackers?

Ans:

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

View All Answers

Question - 33:

What is MAC (Machine Access Control) address?

Ans:

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.

View All Answers

Question - 34:

What is IP address?

Ans:

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.

View All Answers

Question - 35:

What is Ethical Hacking?

Ans:

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.

View All Answers

Question - 36:

How hard would it be to hack into a google voice account and change the owners google voice number?
im not trying to do this, it just "supposedly" happened to one of my friends and im wondering how possible this actually is?

Ans:

No Answer is Posted For this Question

Be First To **Post Your Answer Now.**

Question - 37:

What is a trojan/worm/virus?

Ans:

Trojan: A program that when run by a user does an action that the users did not expect, or the program was not designed to do.
Virus: A portion of code that attaches it self to other executable files in the attempt to replicate and spread itself.
Worm: A stand alone program that acomplishes a task in the background by replicating and moving though a computer

network.

View All Answers

Question - 38:

What is a hacking loop?

Ans:

A loop is two phone numbers connected together by the phone company for testing purposes. A loop has a high end and a low end. If you dial the high end, you will hear nothing. Not even a ring. If you dial the low end, you will hear an annoying 1,000hz tone for several seconds. If you connect to the high end and someone dials the low end, you can speak to each other.

View All Answers

Question - 39:

What is a ringback number?

Ans:

A ringback number is a number that you call that will immediately ring the telephone from which it was called.

View All Answers

Question - 40:

How do I modify the IRC client to hide my real username?

Ans:

Get the IRC client from cs.bu.edu /irc/clients. Look at the source code files irc.c and ctcp.c. The code you are looking for is fairly easy to spot. Change it. Change the username code in irc.c and the ctcp information code in ctcp.c. Compile and run your client.

View All Answers

Question - 41:

How do I hack ChanOp on IRC?

Ans:

Find a server that is split from the rest of IRC and create your own channel there using the name of the channel you want ChanOp on. When that server reconnects to the net, you will have ChanOp on the real channel. If you have ServerOp on a server, you can cause it to split on purpose.

View All Answers

Question - 42:

What are some IRC channels of interest to hackers?

Ans:

#hack
#phreak
#linux
#unix
#warez

View All Answers

Question - 43:

What is a Black Box?

Ans:

A Black Box is a 10k ohm resistor placed across your phone line to cause the phone company equipment to be unable to detect that you have answered your telephone. People who call you will then not be billed for the telephone call.

View All Answers

Question - 44:

Do Blue Boxes still work?

Ans:

Blue Boxes still work in areas using in-band signalling. Modern phone signalling switches using ESS (Electronic Signalling Systems) use out-of-band-signalling. Nothing you send over the voice portion of bandwidth can control the switch.

View All Answers

Question - 45:

What is a Blue Box?

Ans:

Blue boxes use a 2600hz tone to convince telephone switches that use in-band signalling that the caller is actually a telephone operator. The caller may then access special switch functions, with the usual purpose of making free long distance phone calls, using the Multi-Frequency tones provided by the Blue Box.

View All Answers

Question - 46:

Which payphones will a Red Box work on?

Ans:

Red Boxes will work on TelCo owned payphones, but not on COCOT's (Customer Owned Coin Operated Telephones).

View All Answers

Question - 47:

How do I build a Red Box?

Ans:

Red boxes are commonly manufactured from modified Radio Shack tone dialers, Hallmark greeting cards, or made from scratch from readily available electronic components.
To make a Red Box from a radio shack tone dialer, open the dialer and replace the crystal (the largest shiny metal component) with a crystal close to 6.5Mhz. The most popular choice is the 6.5536Mhz crystal. When you are finished, program the P1 button with five *'s. That will simulate a quarter tone. Note that the tone dialer you start with must have programmable buttons.

View All Answers

Question - 48:

What is a Red Box?

Ans:

When a coin is inserted into a payphone, the phone emits a set of tones. A red box is a device that simulates those tones, with the purpose of fooling the payphone into believing you have inserted an actual coin.

View All Answers

Question - 49:

How do I fake posts to UseNet?

Ans:

Use inews to post. Give inews the following lines:
From:
Newsgroups:
Subject:
Message-ID:
Date:
Organization:
For a moderated newsgroup, inews will also require this line:
Approved:
Then add your post and terminate with <Control-D>.
Example:
From: Dale Drew
Newsgroups: alt.2600
Subject: Please forgive me
Message-ID: <d_drew.123@tymnet.com>
Date: Fri, 13 Jun 1994 12:15:03
Organization: Tymnet Insecurity

View All Answers

Question - 50:

How do I gain root from a suid script or program?

Ans:

1. Change IFS.
If the shell script calls any other programs using the system()

function call, you may be able to fool it by changing IFS. IFS is the
Internal Field Seperator that the shell uses to delimit arguments.
If the program contains a line that looks like this:
system("/bin/date")
and you change IFS to '/' the shell will them interpret the
proceeding line as:
bin date
Now, if you have a program of your own in the path called "bin" the
suid program will run your program instead of /bin/date.
To change IFS, use this command:
set IFS '/'
2. link the script to -i
Create a symbolic link named "-i" to the program. Running "-i"
will cause the interpreter shell (/bin/sh) to start up in interactive
mode. This only works on suid shell scripts.
Example:
% ln suid.sh -i
% -i
#
3. Exploit a race condition
Replace a symbolic link to the program with another program while the
kernel is loading /bin/sh.
Example:
nice -19 suidprog ; ln -s evilprog suidroot
4. Send bad input the the program.
Invoke the name of the program and a seperate command on the same
command line.
Example:
suidprog ; id

View All Answers

Question - 51:

How do I break out of a restricted shell?

Ans:

On poorly implemented restricted shells you can break out of the
restricted environment by running a program that features a shell
function. A good example is vi. Run vi and use this command:
:set shell=/bin/sh
then shell using this command:
:shell

View All Answers

Question - 52:

What is password shadowing?

Ans:

Password shadowing is a security system where the encrypted password
field of /etc/password is replaced with a special token and the
encrypted password is stored in a seperate file which is not readable
by normal system users.
To defeat password shadowing on many systems, write a program that
uses successive calls to getpwent() to obtain the password file.
Example:
#include <pwd.h>
main()
{
struct passwd *p;
while(p=getpwent())
printf("%s:%s:%d:%d:%s:%s:%sn", p->pw_name, p->pw_passwd,
p->pw_uid, p->pw_gid, p->pw_gecos, p->pw_dir, p->pw_shell);
}

View All Answers

Question - 53:

What is NIS/yp?

Ans:

NIS (Network Information System) in the current name for what was once
known as yp (Yellow Pages). The purpose for NIS is to allow many
machies on a network to share configuration information, including
password data. NIS is not designed to promote system security. If
your system uses NIS you will have a very short /etc/passwd file with
a line that looks like this:
+::0:0:::
To view the real password file use this command "cd/etc;ypcat passwd"

View All Answers

Question - 54:

How do I crack VMS passwords?

Ans:

Write a program that uses the SYS$GETUAF functions to compare the results of encrypted words against the encrypted data in SYSUAF.DAT. Two such programs are known to exist, CHECK_PASSWORD and GUESS_PASSWORD.

View All Answers

Question - 55:

How do I access the password file under VMS?

Ans:

Under VMS, the password file is SYS$SYSTEM:SYSUAF.DAT. However, unlike Unix, most users do not have access to read the password file.

View All Answers

Question - 56:

How do I crack Unix passwords?

Ans:

Contrary to popular belief, Unix passwords cannot be decrypted. Unix passwords are encrypted with a one way function. The login program encrypts the text you enter at the "password:" prompt and compares that encrypted string against the encrypted form of your password. Password cracking software uses wordlists. Each word in the wordlist is encrypted with each of the 2600 possible salt values and the results are compared to the encrypted form of the target password. The best cracking program for Unix passwords is currently Crack by Alec Muffett. For PC-DOS, the best package to use is currently CrackerJack.

View All Answers

Question - 57:

How do I access the password file under Unix?

Ans:

In standard Unix the password file is /etc/passwd. On a Unix system with either NIS/yp or password shadowing, much of the password data may be elsewhere.

View All Answers

Basic Common Most Popular & Related Interview Guides

1 : **Targeted Selection Interview Questions and Answers.**

2 : Business intelligence Interview Questions and Answers.

3 : Puzzles Interview Questions and Answers.

4 : Behavioral Interview Questions and Answers.

5 : Freshers Graduate Interview Questions and Answers.

6 : Visa Interview Questions and Answers.

7 : Aptitude Interview Questions and Answers.

8 : Basic Common Interview Questions and Answers.

9 : Funny Interview Questions and Answers.

10 : Logical Interview Questions and Answers.

Follow us on FaceBook
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter
https://twitter.com/InterviewQA

For any inquiry please do not hesitate to contact us.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
support@InterviewQuestionsAnswers.ORG