15 Linux Things you Should know before a Linux Interview

by Aaron Grothe
Security+/CISSP/NSA
IAM/NSA IEM/CSA+

Introduction

I’ve interviewed and been interviewed by a lot of people for Linux positions. A question I get asked every now and then is do you have a list of questions you ask someone?

I don’t normally have a formal list of questions preferring to wing it, but here are the ones I tend to keep asking all the time

A lot of them will seem pretty basic to you guys, but if you don’t know a couple of them hopefully it’ll be worthwhile for you

Introduction (cont'd)

A lot of places want to hear your thought process so talking out loud while you're thinking about something can be helpful. Of course if it is gibberish it might not be as helpful.

Introduction (Continued)

This is laid out in a Q & A - format. My answers might not be the best ones so please feel free to contribute :-)

These are more terminal based. A lot of these things can you can also do through the gui, but you'll always have a terminal maybe not always a gui

If there are other questions similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

Interviewers

The interviewers don't know everything either. They may use incorrect or different terms to define things as well.

An Example

In an interview with a certain search company and they start asking me about "slash addressing". Huh? After going back and forth with them I realize they are asking about CIDR notation. Using the phrase slash notation would also have worked.

Question #1

What Linux Distribution do you use and why do you use it?

I used to say there isn't a right or wrong answer here. A couple of years I was interviewing someone asked this question and I realized there was a wrong answer here.

Answer #1

This is a classic softball question to show thought process. You should be able to give a bit of background about it.

E.g. I use Debian because I like the package manager, the testing distribution seems to keep things up to date pretty well and most things are available for it. Stable doesn't change and works well for servers.

I like Arch Linux because it has the latest version of packages, including things like grails, groovy, kernel, etc.

I like CentOS because it is what I learned at work and it just stays out of my way.

Answer #1 (cont'd)

I consider all of these valid answers. The idea is you should be able to explain a bit behind your answer.

Of course if you bad-mouth Ubuntu and it is an Ubuntu shop it might not be the wisest course of action, so try to keep it positive and not distro bashing usually.

Question #2

How do you update a system? Or install a package?

You should at least know how to do this for your favorite distro. Using the automated tools are also good.

Answer #2

You should know how to update a system.

Fedora/CentOS

```
# dnf/yum upgrade
```

Debian/Ubuntu

```
# apt update; apt upgrade vs. dist-upgrade; etc
```

Arch

```
# pacman -Syu
```

Answer #2 (cont’d)

You should know how to install a package on the system

Fedora/CentOS

```
# yum/dnf install # rpm -ivh
```

Debian/Ubuntu

```
# apt install, #dpkg -i
```

Arch

```
# pacman -Sy
```

Question #3

How do you determine the distro & kernel that are running on a system?

Answer #3

For Kernel - the best answer is probably “uname -a” or some variation of that

For Distro - “lsb_release -a” isn’t a bad answer it will usually tell you, that you are running Arch, Debian, CentOS, etc

For Distro there is usually a file in the /etc/ folder with something along the lines of /etc/*release* which usually contains some information

Bonus points for mentioning rpm -qa, etc as additional options, but lsb_release/uname are probably best

Question #4

How do you determine the IP address of your system?

Answer #4

A lot of the time with this question you can figure out when someone got into linux.

The classic answer is ‘# ifconfig” - old timer

The new/correct answer is “# ip addr show” - more recent person, or less set in their ways

If the person answers “# /sbin/ifconfig” odds are they know they should be using ip but are being stubborn

Question #5

Who has logged into the system?

Answer #5

The usual answer here is “# last”
bonus points for “# lastb” which shows bad login attempts

If you want to get fancy you can mention about grepping through logs, wtmp, etc for additional info but 99% of people will be happy with last

Question #6

What are Linux permissions and how do you figure them out and how do you set them?

This is one of the longer answers

Answer #6

The basics here are to explain that basic Linux Permissions work out into 3 groups and 3 types.

Groups: Owner, Group, Everybody
Types: Read, Write, Execute

The command you usually use to see what they are is “# ls -l” and the command you use to set them is “# chmod”

Answer #6 (cont'd)

Example for a while

```
# ls -l myfile

-rw-r--r-- 1 grothe grothe 1095 Sep 1   03:39 a.txt
```

The permissions here are

Owner (grothe) can read/write the file
Group (grothe) can read the file
Everybody else can read the file

Answer #6 (cont'd)

Changing permissions

```
% chmod 0666 myfile
```

Changes permissions so anyone can read/write to the file. Leading 0 is for Octal, not needed, but is a pet-peeve of mine

```
% ls -l

-rw-rw-rw- 1 grothe grothe 1095 Sep 1   03:39 a.txt
```

Answer #6 (cont'd)

There are also extended attributes, SUID, SGID

Set Owner ID (SUID) is used when a program needs to run as that person.

There are also optional extended attributes as well, such as append only, etc which are set via the chattr option.

There is a lot more to this topic, but we're just covering the basics here

Question #7

How much space is a user or a directory using?

Answer #7

For how much space a user is using the usual command you would use is “du -h directory”

E.g.

% du -h /home/grothe - will tell how much space I’m using

-h is human readable
-m is megabyte
-k is kilobyte, etc

% du -a - will tell you how much space each file is using

Question #8

How much disk space is available on the system?

Answer #8

To determine how much free space on a system you use the "df" command

E.g.

Free disk space on the current drive

```
% df -h .
```

Free space on all drives on system

```
% df -h
```

Question #9

How do you start/stop a service? How do you see if a service is running? How do you enable/disable a service?

Answer #9

There are two major answers here for this one

% service # is the old option, still being used in CentOS 6 and some holdouts

% systemd # is the new option, accepted by most distributions with a few notable holdouts, Devuan, Slackware, etc

There are other answers as well like chkconfig, /etc/init.d and others, but systemd should probably be mentioned.

Answer #9 (cont'd)

Seeing if a service is running

```
% service sshd status
```

```
% systemctl status sshd
```

Enabling/disabling a service

```
% service sshd enable/disable
```

```
% systemctl enable/disable sshd
```

Answer #9 (cont'd)

Stopping a service

```
% service sshd stop/start/restart
```

```
% systemctl status stop/start/restart
```

Question #10

How long has the system been up? When was it last rebooted?

Answer #10

The best answer here is "% uptime".

Uptime tells you how long the system has been up so you can figure out the last reboot. This is usually one of the go to commands if you are having weird issues on your system.

If your system is rebooting repeatedly and comes up quickly your monitoring solution might not always catch it.

Question #11

How to check for open ports on a system?

Answer #11

The usual answer here is a variation of netstat.

% netstat -tulpn is usually pretty good

This will tell you what has network connections on the system

% netstat -an | grep LISTEN - is also popular

Answer #11

Bonus points for doing the same with lsof

```
% lsof -i
```

Nmap isn't a bad answer, but typically not the best answer

Listen to the question carefully if it open on a remote system, nmap is the correct answer. Otherwise I'd probably go with netstat.

Better yet ask for clarification and explain your thought process

Question #12

How do you determine which process has a file open?

Answer #12

The usual answer here should be lsof

% lsof some_file - will tell you which process has the file open

% lsof -p process_id - will tell you which files have a process open

These are complementatry

Question #13

Miscellaneous

The following may also come up and should be reviewable

iptables/netfilter/ufw - firewalling
Favorite tools/utilities and so on
Security modules / apparmor/selinux/smack/tomoyo etc

Have an idea on these and be prepared to talk about them at least in general terms

Question #14

How do you give a person the ability to run a job as root?

Answer #14

The best answer here is probably sudo.

To give a user the ability to be able “% sudo bash” add the following /etc/sudoers

```
User  ALL=(ALL:ALL) ALL # can cut and paste root line from sudo
```

Answer #14b

To give a user the ability to run a command as root. Once again the best answer is probably sudo.

```
user ALL=(root) NOPASSWD: /usr/bin/rsync
```

Bonus points if you mention writing a script that can run rsync and do a Setuid on it. Bonus points, but not the best idea.

Question #15

What resources do you use for figuring out solutions to a problem?

Answer #15

This is another open ended question. Also tends to be a good way to finish up an interview.

Typical answers

% man or (info, if you're not old like me)

% google, duckduckgo or bing (pause for laughter)

% stack overflow

Answer #15b

Eric Raymond maintains an article at his site title “How To Ask Questions The Smart Way” which is a great resource for this

URL for it is catb.org/~esr/faqs/smart-questions.html

Favorite sections

“Dealing with rudeness” & “On Not Reacting Like A Loser”

Summary

That gives you kind of a quick idea of some of the types of questions you might get asked during a basic Linux interview.

The questions about kernel modules, /proc file systems, vfs, iptables and stuff are all out there as well but this is just a sampler of some of the kind of questions.

I'm hoping what people take away here is that you will never know everything about linux, but you should alway be learning.

Q & A

Questions???