Linux Fundamentals Part 3

Task 1 ✅ Intro

This room is the third part in the Linux Fundamental rooms designed to teach you about various Linux concepts, and in-built tools. This room covers the following topics:

- Advanced File Operators (Continued From Linux Fundamentals Part 2)
- Users & Groups
- Introduction To Shell Scripting

Deploy the machine and SSH into the room using the following credentials (these credentials will be available from the last task of the Linux Fundamentals Part2 room):

- username: shiba3
- password: happynootnoises

Answer the questions below

Read the above.

No answer needed [Correct Answer]

Deploy the machine attached to this task!

NOTE: *If you have a machine open in the Welcome room (or any other room) please go to that room and terminate it before deploying the machine attached to this task. These machines are not the same, and only the one attached to this room will work.*

No answer needed [Correct Answer]

Task 2 ✅ [Section 5: Advanced File Operations] - cp

cp does mainly the same thing as mv, except instead of moving the file it duplicates(copies) it. The syntax is also the same as mv, meaning the syntax is `cp <file> <destination>`.

```
shiba3@nootnoot:/tmp/aa$ cp file ~/
.bash_history  .bash_logout  .bashrc        .profile       test/
shiba3@nootnoot:/tmp/aa$ cp file ~/ghdfs
shiba3@nootnoot:/tmp/aa$ ls ~
ghdfs  test
shiba3@nootnoot:/tmp/aa$
```

Answer the questions below

No answer needed [Correct Answer]

Task 3 ○ [Section 5: Advanced file Operations] - cd && mkdir

Task 4 ○ [Section 5: Advanced File Operations] ln

Task 5 ○ [Section 5 - Advanced File Operations]: find

```
root@parabox:/tmp# cd aa
root@parabox:/tmp/aa#
```

Relative Paths are supported, as well as absolute paths. Our command line provides a nice section for seeing exactly what directory you're in, so you'll never be lost!

This brings us to mkdir, occasionally you'll want to make a new directory to store files in, and that is done using mkdir, the syntax of mkdir is `mkdir <directory name>`.

```
root@parabox:/tmp/aa# ls
root@parabox:/tmp/aa# mkdir a
root@parabox:/tmp/aa# ls
a
root@parabox:/tmp/aa# cd a
root@parabox:/tmp/aa/a#
```

Note: As you might have noticed, ls shows directories aswell

Answer the questions below

Using relative paths, how would you cd to your home directory.

cd ~	Correct Answer

Using absolute paths how would you make a directory called test in /tmp

mkdir /tmp/test	Correct Answer

Task 4 ○ [Section 5: Advanced File Operations] ln ⌄

```
shiba3@nootnoot: ~
File  Edit  View  Search  Terminal  Help
  Memory usage: 19%              IP address for ens5: 10.10.39.182
  Swap usage:   0%

11 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


Command 'aa' not found, but can be installed with:

apt install astronomical-almanac
Please ask your administrator.

shiba3@nootnoot:~$
shiba3@nootnoot:~$
```

THM AttackBox   54m 28s

```
lrwxrwxrwx  1 root root     4 Feb 20 21:32 file3 -> file
root@parabox:/tmp/aa#
```

ls even shows that its a symbolic link with the arrow pointing to what the link is referencing. It is important to note the permissions on the symlink. It has full 777 perms meaning that in theory you can execute the symlink, however since it is just a reference, in reality it has the same perms as the original file.

```
root@parabox:/tmp/aa# ls -al
total 12
drwxr-xr-x  2 root root 4096 Feb 20 21:32 .
drwxrwxrwt 14 root root 4096 Feb 20 21:25 ..
-rw-r--r--  1 root root   11 Feb 20 21:26 file
lrwxrwxrwx  1 root root    4 Feb 20 21:32 file3 -> file
root@parabox:/tmp/aa# ./file3
bash: ./file3: Permission denied
root@parabox:/tmp/aa#
```

Answer the questions below

How would I link /home/test/testfile to /tmp/test

ln /home/test/testfile /tmp/test	Correct Answer

Task 5 ○ [Section 5 - Advanced File Operations]: find ⌄

Task 6 ○ [Section 5: Advanced File Operations] - grep ⌄

Task 7 ○ Binary - Shiba3 ⌄

Woop woop! Your answer is correct.   ✕

```
shiba3@nootnoot: ~
File  Edit  View  Search  Terminal  Help
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Command 'aa' not found, but can be installed with:

apt install astronomical-almanac
Please ask your administrator.

shiba3@nootnoot:~$
shiba3@nootnoot:~$ ls
test
shiba3@nootnoot:~$ ls -al
total 36
drwxr-xr-x 5 shiba3 shiba3 4096 Sep 18 07:46 .
drwxr-xr-x 8 root   root   4096 Feb 22 2020 ..
-rw------- 1 shiba3 shiba3  726 Feb 22 2020 .bash_history
-rw-r--r-- 1 shiba3 shiba3  220 Feb 20 2020 .bash_logout
-rw-r--r-- 1 shiba3 shiba3 3771 Feb 20 2020 .bashrc
drwx------ 2 shiba3 shiba3 4096 Sep 18 07:46 .cache
drwx------ 3 shiba3 shiba3 4096 Sep 18 07:46 .gnupg
-r-xr--r-- 1 shiba3 shiba3  810 Feb 20 2020 .profile
drwxrwxr-x 2 shiba3 shiba3 4096 Feb 22 2020 test
shiba3@nootnoot:~$
```

THM AttackBox   52m 34s

This is one command I highly recommend reading the manual page on to learn all of it's options. This command is invaluable when working with files.

Answer the questions below

How do you find files that have specific permissions?

```
-perm
```
Correct Answer   💡 Hint

How would you find all the files in /home

```
find /home
```
Correct Answer

How would you find all the files owned by paradox on the whole system

```
find /-user paradox
```
Correct Answer

Task 6 ○ [Section 5: Advanced File Operations] - grep ⌄

```
shiba3@nootnoot: ~

File  Edit  View  Search  Terminal  Help
drwxr-xr-x 8 root   root   4096 Feb 22  2020 ..
-rw------- 1 shiba3 shiba3  726 Feb 22  2020 .bash_history
-rw-r--r-- 1 shiba3 shiba3  220 Feb 20  2020 .bash_logout
-rw-r--r-- 1 shiba3 shiba3 3771 Feb 20  2020 .bashrc
drwx------ 2 shiba3 shiba3 4096 Sep 18 07:46 .cache
drwx------ 3 shiba3 shiba3 4096 Sep 18 07:46 .gnupg
-r-xr--r-- 1 shiba3 shiba3  810 Feb 20  2020 .profile
drwxrwxr-x 2 shiba3 shiba3 4096 Feb 22  2020 test
shiba3@nootnoot:~$ find
.
./.profile
./test
./test/test1234
./test/1234
./.gnupg
./.gnupg/private-keys-v1.d
./.bashrc
./.bash_history
./.cache
./.cache/motd.legal-displayed
./.bash_logout
shiba3@nootnoot:~$ find dir -user
find: missing argument to `-user'
shiba3@nootnoot:~$
```

---

grep comes and saves the day! What about if you have a bunch of data, and you wanna see if the string hello is in it, and if so what line number it's at.

```
root@nootnoot:/tmp# grep hello test -n
148:hello
root@nootnoot:/tmp# grep hello test -n
```

I'm sure you can see just how useful this command is. When searching logs for the cause of an error message, when parsing large amounts of data for that specific piece, when searching every file in a directory for that one line that you may need to change.

Another important thing to note is that grep supports regular expressions, you see I wasn't being entirely truthful with you(props if you get the reference) when I says the syntax is `grep <string> <file>`, the syntax is actually `grep <regular expression> <file>`. Unfortunately regular expressions are out of the scope of this room, but I highly encourage you to read up on regular expressions, as they increase the power of grep tenfold.

Answer the questions below

What flag lists line numbers for every string found?

```
-n
```
Correct Answer

How would I search for the string boop in the file aaaa in the directory /tmp

```
grep boop /tmp/aaaa
```
Correct Answer

Task 7 ○ Binary - Shiba3 ⌄

Woop woop! Your answer is correct. ✕

```
shiba3@nootnoot: ~

File  Edit  View  Search  Terminal  Help
-r-xr--r-- 1 shiba3 shiba3  810 Feb 20  2020 .profile
drwxrwxr-x 2 shiba3 shiba3 4096 Feb 22  2020 test
shiba3@nootnoot:~$ find
.
./.profile
./test
./test/test1234
./test/1234
./.gnupg
./.gnupg/private-keys-v1.d
./.bashrc
./.bash_history
./.cache
./.cache/motd.legal-displayed
./.bash_logout
shiba3@nootnoot:~$ find dir -user
find: missing argument to `-user'
shiba3@nootnoot:~$ grep test1234

^C
shiba3@nootnoot:~$ grep hello test -n
grep: test: Is a directory
shiba3@nootnoot:~$
```

Screenshot 1

We've been through a lot in this section, and the challenge for this binary will reflect that. The first step is actually finding the binary, I'm not heartless though, so I'll give you the name of the binary. The name of the binary is shiba4.

The actual binary will check for two things, it will be checking that there's a directory called test in your home directory, how you create that is up to you. It will also be checking that inside the directory there's a file called test1234.

Answer the questions below

What is shiba4's password

test1234	Correct Answer

Task 8 ○ [Section 6: Miscellaneous]: Intro ⌄

Task 9 ○ [Section 6: Miscellaneous]: sudo ⌄

Task 10 ○ [Section 6: Miscellaneous]: Adding users and groups ⌄

Task 11 ○ [Section 6: Miscellaneous]: nano ⌄

Terminal (Screenshot 1)

```
Applications  Places         Mon 18 Sep, 08:58 AttackBox IP:10.10.114.132

                        Woop woop! Your answer is correct.        ✕

                        shiba3@nootnoot: ~                 _  □  ✕
File  Edit  View  Search  Terminal  Help
find: '/proc/1525/map_files': Permission denied
find: '/proc/1525/fdinfo': Permission denied
find: '/proc/1525/ns': Permission denied
find: '/run/lxcfs': Permission denied
find: '/run/sudo': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lvm': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/fuse/connections/49': Permission denied
find: '/tmp/systemd-private-d364eb2b223a4ba5a301b547a9631bc5-systemd-timesyncd.s
ervice-AlI9oo': Permission denied
find: '/tmp/systemd-private-d364eb2b223a4ba5a301b547a9631bc5-systemd-resolved.se
rvice-s3xzUr': Permission denied
shiba3@nootnoot:~$ find / -name shiba4 2> /dev/null
/opt/secret/shiba4
/home/shiba4
/etc/shiba/shiba4
shiba3@nootnoot:~ $ /opt/secret/shiba4
test1234
shiba3@nootnoot:~$

   ⤢  +  ⏻  —  i    THM AttackBox                          45m 46s
```

Screenshot 2

Task 7 ✓ Binary - Shiba3 ⌄

Even though we've gone over how the Linux operating system works, and some of it's most useful features and commands, there are some useful commands and concepts that haven't been covered in previous sections. So this section is dedicated to all those miscellaneous commands and concepts that are useful to know.

Answer the questions below

Read the above

No answer needed	Correct Answer

Task 9 ○ [Section 6: Miscellaneous]: sudo ⌄

Task 10 ○ [Section 6: Miscellaneous]: Adding users and groups ⌄

Task 11 ○ [Section 6: Miscellaneous]: nano ⌄

Task 12 ○ [Section 6: Miscellaneous]: Basic shell scripting ⌄

Terminal (Screenshot 2)

Note: whoami is just a command that states your current user.

As you can see when using sudo the command is run as root. It is important to note that you need to have your current user's password to use it. Again like Windows, not every user has permission to use sudo, but most Linux OS' set up a user that has permissions when you install it.

Assuming you create a new user that you also want to give sudo permissions to, the man page for sudo has a section on how to add user permissions. It is also worth noting you can configure sudo to run commands as other users, again the man page has a section on that(sudo has a very nice man page)

Answer the questions below

How do you specify which user you want to run a command as.

-u	Correct Answer

How would I run whoami as user jen?

sudo -u jen whoami	Correct Answer

How do you list your current sudo privileges(what commands you can run, who you can run them as etc.)

-l	Correct Answer

Task 10 ○ [Section 6: Miscellaneous]: Adding users and groups   ⌄

It's important to note that only root has permissions to add users and groups, as seen with the failure when I attempted to run the commands without sudo. You may be wondering how to add a user to a group. that is done with the usermod command, the syntax for that is `usermod -a -G <groups seperated by commas> <user>` . Meaning if I wanted to add the user noot to b I would run `usermod -a -G b noot` .

```
nootnoot@nootnoot:~$ usermod -a -G b noot
usermod: Permission denied.
usermod: cannot lock /etc/passwd; try again later.
nootnoot@nootnoot:~$ sudo usermod -a -G b noot
nootnoot@nootnoot:~$ id noot
uid=1005(noot) gid=1006(noot) groups=1006(noot),1007(b)
nootnoot@nootnoot:~$
```

Note: id is a command that allows you to view basic information about a user.

Answer the questions below

How would I add the user test to the group test

sudo usermod -a -G test test\	Correct Answer

Task 11 ○ [Section 6: Miscellaneous]: nano   ⌄

Up until this point you may have seen me only using >> to add content to a file. Luckily that's not the only way to do things, nano is a terminal based text editor. The syntax for nano is `nano <file you want to write to>`. For example typing nano test will take you to this screen.

```
GNU nano 2.9.3                              test

-





                           [ New File ]
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text    ^J Justify    ^C Cur Pos    ^Y Undo
^X Exit       ^R Read File   ^\ Replace    ^U Uncut Text  ^T To Spell   ^_ Go To Line ^E Redo
```

```
nootnoot@nootnoot:/tmp$ ls
test
nootnoot@nootnoot:/tmp$ cat test
sadfasdfjiasdijkfasdhijkfasdhkjgfhlxujadsfmdsk1:jvnsadfjklvn :sajkldvnkls:djvn:jsdklvnjaksvnjklasdvh
sadlkjhfgasjkidfjkldsahfaisdjkhfasdhjlfasd
f
dsafaj'isdfkijadshfjaisdkf
asdfhjkasdjhfdsa
jofhj'lasdf
hasdfh
iasdjhfasd
fsdahjkf'jhlsadfha
:sdf
hasdhjfk
as
hk1:fdasd:h
k1fhk
adsfh
asd
fhas
aahdfh
asd
hfisdai'hkfhklasd
lk:hfjs
da:jof
hjo:sdk:
jhifsdai:hk
fhkldsafhi:sda
nootnoot@nootnoot:/tmp$ _
```

Now you can actually edit text files! :)

Answer the questions below

Read the above

| No answer needed | Correct Answer |

```
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/fuse/connections/49': Permission denied
find: '/tmp/systemd-private-d364eb2b223a4ba5a301b547a9631bc5-systemd-timesyncd.s
ervice-AlI9oo': Permission denied
find: '/tmp/systemd-private-d364eb2b223a4ba5a301b547a9631bc5-systemd-resolved.se
rvice-s3xzUr': Permission denied
shiba3@nootnoot:~$ find / -name shiba4 2> /dev/null
/opt/secret/shiba4
/home/shiba4
/etc/shiba/shiba4
shiba3@nootnoot:~$ /opt/secret/shiba4
test1234
shiba3@nootnoot:~$ whoami
shiba3
shiba3@nootnoot:~$ sudo whoami
[sudo] password for shiba3:
Sorry, try again.
[sudo] password for shiba3:
shiba3 is not in the sudoers file.  This incident will be reported.
shiba3@nootnoot:~$ adduser noot
adduser: Only root may add a user or group to the system.
shiba3@nootnoot:~$ nano
shiba3@nootnoot:~$ nano
shiba3@nootnoot:~$
```

$PATH - Stores all the binaries you're able to run - same as $PATH on Windows

$PATH is an environment variable that contains all the binaries you're able to execute.

```
root@parabox:~# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
root@parabox:~#
```

It is worth noting that the paths in $PATH(hah!) are separated by colons. Every executable file that is in any of those paths you are able to run just by typing the name of the executable instead of the full path.

```
root@parabox:~# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
root@parabox:~# which ls
/bin/ls
root@parabox:~#
```

Note: which is just a command that shows you where an executable is in any of the PATH directories.
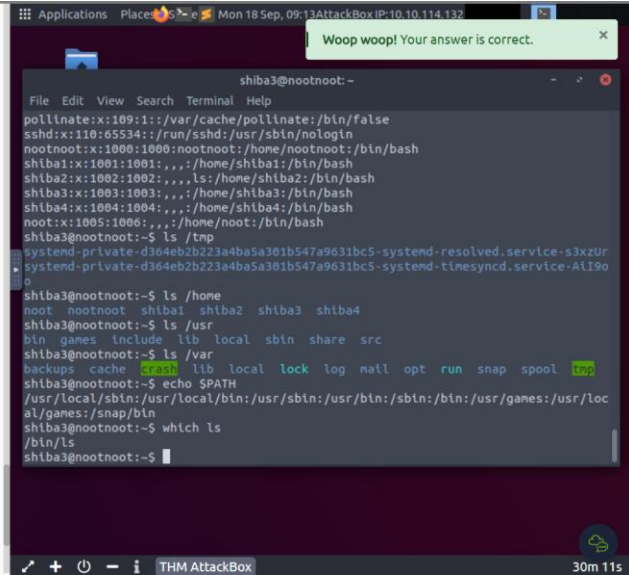
Answer the questions below

Read the above

No answer needed	Correct Answer

Task 14 ○ [Section 6 - Miscellaneous]: Installing packages(apt)

```
Setting up libexpat1-dev:amd64 (2.2.5-3ubuntu0.2) ...
Setting up libpython2.7-stdlib:amd64 (2.7.17-1~18.04) ...
Setting up python2.7 (2.7.17-1~18.04) ...
Setting up libpython-stdlib:amd64 (2.7.15~rc1-1) ...
Setting up libpython2.7:amd64 (2.7.17-1~18.04) ...
Setting up libpython2.7-dev:amd64 (2.7.17-1~18.04) ...
Setting up python2.7-dev (2.7.17-1~18.04) ...
Setting up python (2.7.15~rc1-1) ...
Setting up libpython-dev:amd64 (2.7.15~rc1-1) ...
Setting up python-dev (2.7.15~rc1-1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
nootnoot@nootnoot:~$
```

apt has a lot of sub commands, and again warrants a room on it's own but most of the time you're going to be googling what you want and you'll find the name of the package to install.

Answer the questions below

Read the above
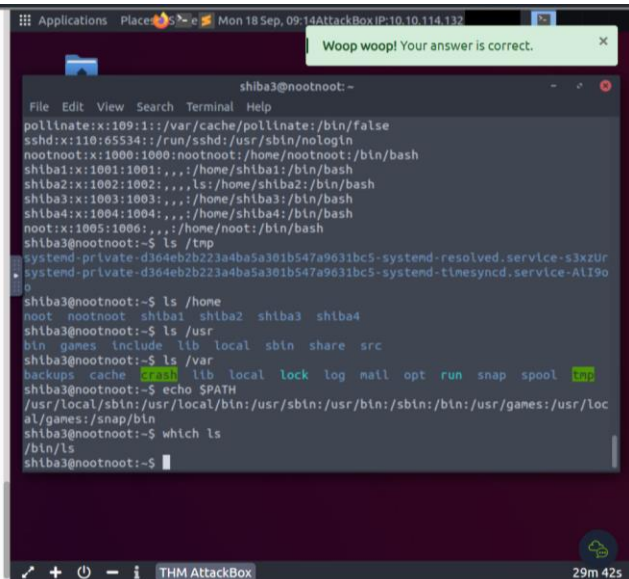
No answer needed	Correct Answer

Task 15 ○ [Section 6: Miscellaneous]: Processes

Created by 🔵 tryhackme

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 48626 users are in here and this room is 1294 days old.

```
11 root      rt    0       0      0      0 S  0.0  0.0   0:02.66 watchdog/0
12 root      20    0       0      0      0 S  0.0  0.0   0:00.00 cpuhp/0
13 root      20    0       0      0      0 S  0.0  0.0   0:00.00 kdevtmpfs
14 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 netns
15 root      20    0       0      0      0 S  0.0  0.0   0:00.00 rcu_tasks_kthre
16 root      20    0       0      0      0 S  0.0  0.0   0:00.00 kauditd
17 root      20    0       0      0      0 S  0.0  0.0   0:00.31 khungtaskd
18 root      20    0       0      0      0 S  0.0  0.0   0:00.03 oom_reaper
19 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 writeback
20 root      20    0       0      0      0 S  0.0  0.0   0:00.19 kcompactd0
21 root      25    5       0      0      0 S  0.0  0.0   0:00.00 ksmd
22 root      39   19       0      0      0 S  0.0  0.0   0:00.00 khugepaged
23 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 crypto
24 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 kin
25 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 kbl
26 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 ata
27 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 md
28 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 eda
29 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 dev
30 root       0  -20       0      0      0 I  0.0  0.0   0:00.00 wat
```

Note: The top man page has descriptions for what every value me
your system; I highly recommend reading it!

Answer the questions below

Read the above!

No answer needed

Created by 🐾 tryhackme

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 48626 users are in here and this room is 1294 days old.

Woop woop! Your answer is correct.

Congratulations

You've completed the room! Share this with your friends!

Share Awarded Badge   🐦 Twitter   f Facebook

in LinkedIn

Leave feedback

Linux Fundamentals Part 3

Learning Linux Part 3