Austin Brown

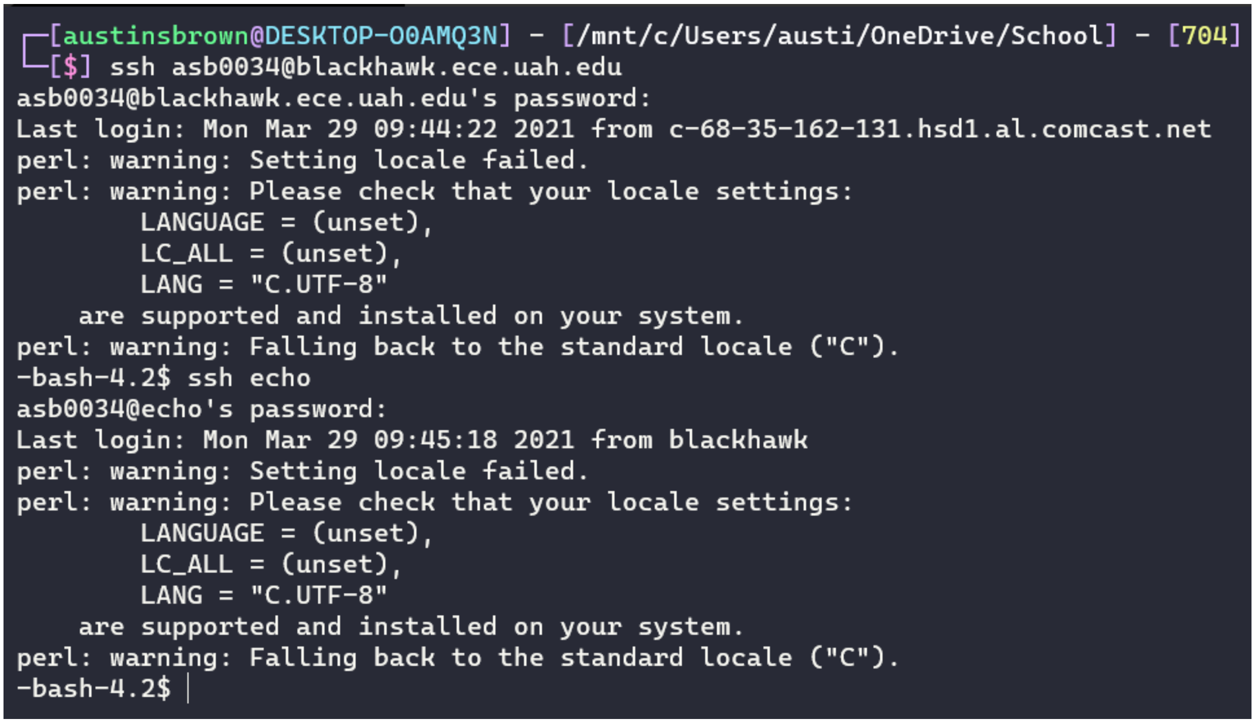
CPE 434-01

3/29/2021

Lab11 Part 1

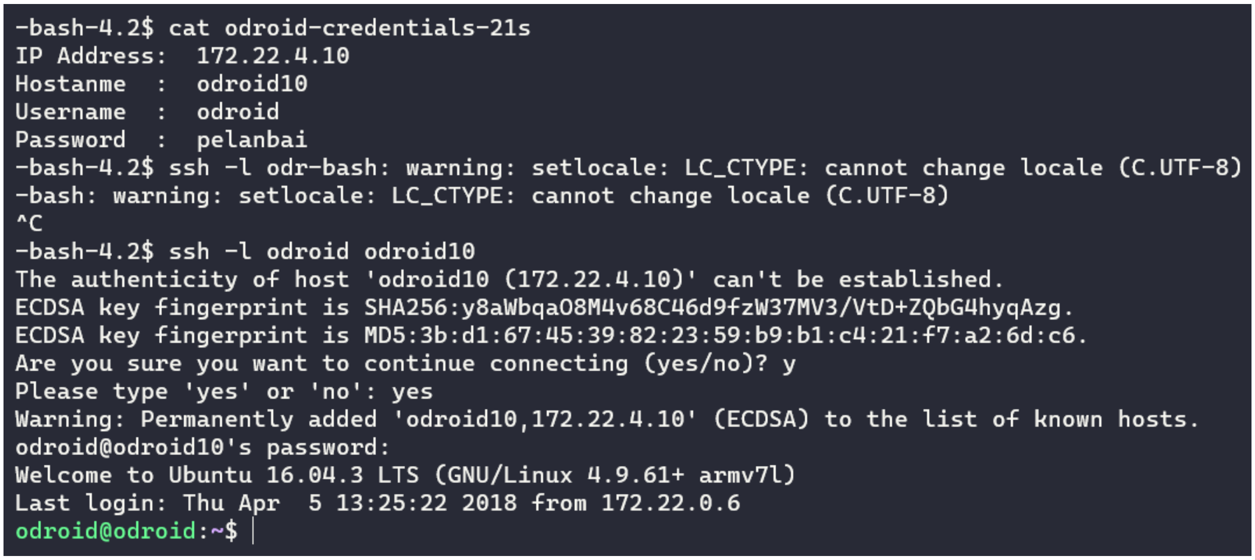
Subtask 1

1.



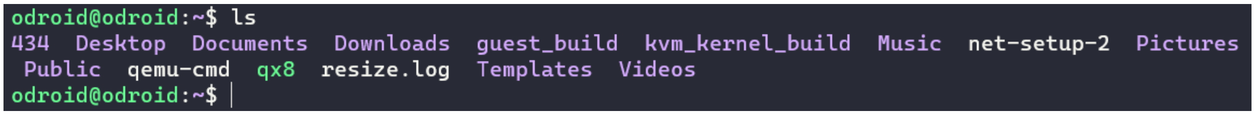
```
┌─[austinsbrown@DESKTOP-O0AMQ3N] - [/mnt/c/Users/austi/OneDrive/School] - [704]
└─[$] ssh asb0034@blackhawk.ece.uah.edu
asb0034@blackhawk.ece.uah.edu's password:
Last login: Mon Mar 29 09:44:22 2021 from c-68-35-162-131.hsd1.al.comcast.net
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "C.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
-bash-4.2$ ssh echo
asb0034@echo's password:
Last login: Mon Mar 29 09:45:18 2021 from blackhawk
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "C.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
-bash-4.2$
```

2.



```
-bash-4.2$ cat odroid-credentials-21s
IP Address:  172.22.4.10
Hostanme   :  odroid10
Username   :  odroid
Password   :  pelanbai
-bash-4.2$ ssh -l odr-bash: warning: setlocale: LC_CTYPE: cannot change locale (C.UTF-8)
-bash: warning: setlocale: LC_CTYPE: cannot change locale (C.UTF-8)
^C
-bash-4.2$ ssh -l odroid odroid10
The authenticity of host 'odroid10 (172.22.4.10)' can't be established.
ECDSA key fingerprint is SHA256:y8aWbqaO8M4v68C46d9fzW37MV3/VtD+ZQbG4hyqAzg.
ECDSA key fingerprint is MD5:3b:d1:67:45:39:82:23:59:b9:b1:c4:21:f7:a2:6d:c6.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added 'odroid10,172.22.4.10' (ECDSA) to the list of known hosts.
odroid@odroid10's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.9.61+ armv7l)
Last login: Thu Apr  5 13:25:22 2018 from 172.22.0.6
odroid@odroid:~$
```

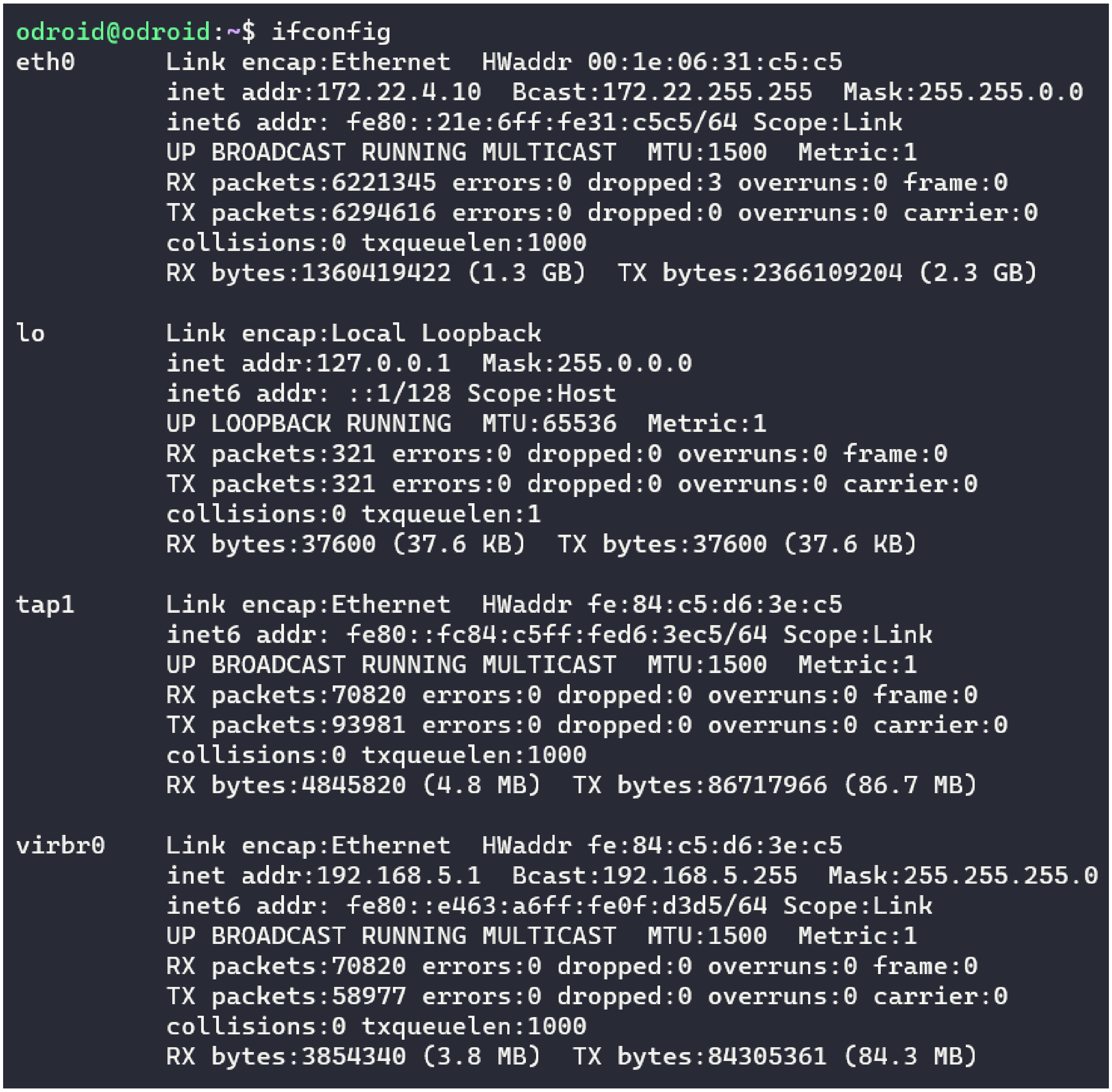
3.



```
odroid@odroid:~$ ls
434  Desktop  Documents  Downloads  guest_build  kvm_kernel_build  Music  net-setup-2  Pictures
 Public  qemu-cmd  qx8  resize.log  Templates  Videos
odroid@odroid:~$
```

Subtask 2

4.



```
odroid@odroid:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1e:06:31:c5:c5
          inet addr:172.22.4.10  Bcast:172.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::21e:6ff:fe31:c5c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6221345 errors:0 dropped:3 overruns:0 frame:0
          TX packets:6294616 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1360419422 (1.3 GB)  TX bytes:2366109204 (2.3 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:321 errors:0 dropped:0 overruns:0 frame:0
          TX packets:321 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:37600 (37.6 KB)  TX bytes:37600 (37.6 KB)

tap1      Link encap:Ethernet  HWaddr fe:84:c5:d6:3e:c5
          inet6 addr: fe80::fc84:c5ff:fed6:3ec5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70820 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93981 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4845820 (4.8 MB)  TX bytes:86717966 (86.7 MB)

virbr0    Link encap:Ethernet  HWaddr fe:84:c5:d6:3e:c5
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::e463:a6ff:fe0f:d3d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70820 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58977 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3854340 (3.8 MB)  TX bytes:84305361 (84.3 MB)
```

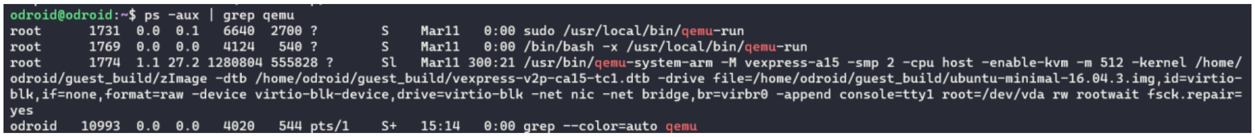
Virtual bridges are just virtual connections between virtual machines.

5.

KVM converts the VM into a type 1 hypervisor. This means it can run directly on the host’s hardware.

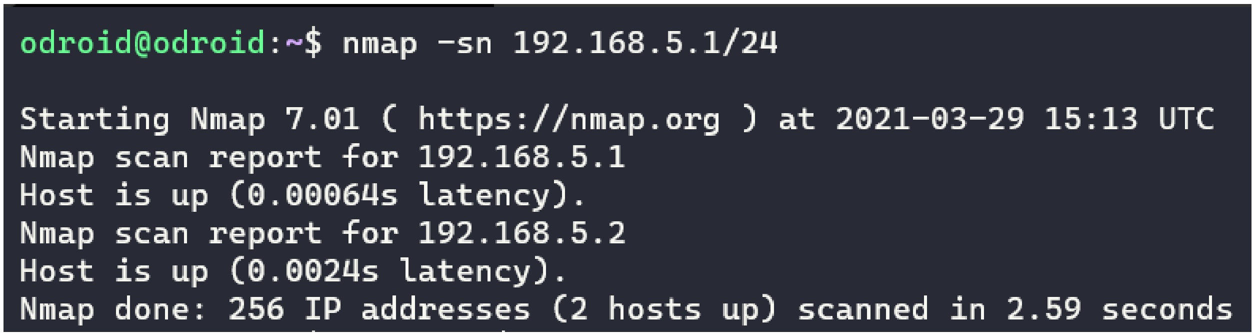
QEMU is a type 2 hypervisor. It can virtualize disks, USB, PCI, networks, etc.

6.

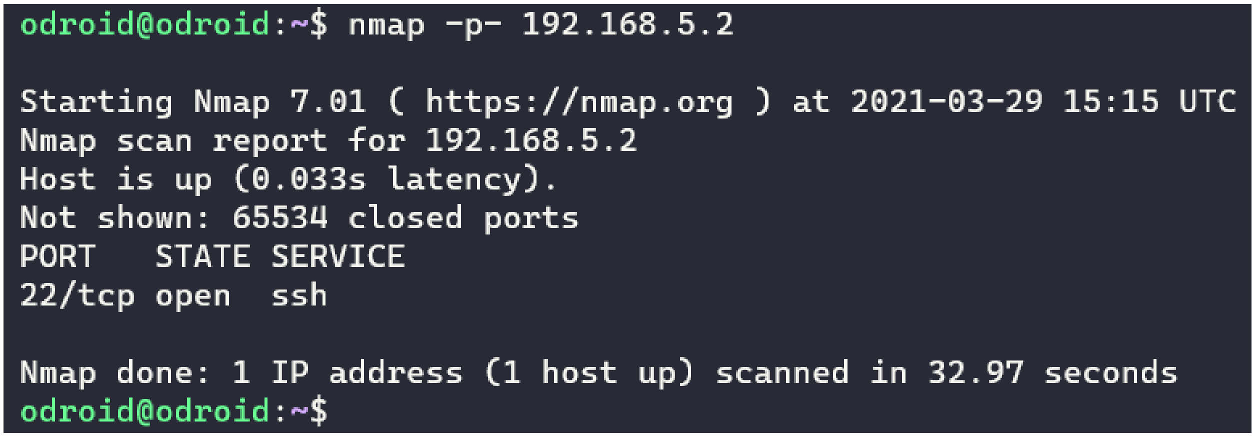


```
odroid@odroid:~$ ps -aux | grep qemu
root      1731  0.0  0.1   6640  2700 ?        S    Mar11   0:00 sudo /usr/local/bin/qemu-run
root      1769  0.0  0.0   4124   540 ?        S    Mar11   0:00 /bin/bash -x /usr/local/bin/qemu-run
root      1774  1.1 27.2 1280804 555828 ?      Sl   Mar11 300:21 /usr/bin/qemu-system-arm -M vexpress-a15 -smp 2 -cpu host -enable-kvm -m 512 -kernel /home/
odroid/guest_build/zImage -dtb /home/odroid/guest_build/vexpress-v2p-ca15-tc1.dtb -drive file=/home/odroid/guest_build/ubuntu-minimal-16.04.3.img,id=virtio-
blk,if=none,format=raw -device virtio-blk-device,drive=virtio-blk -net nic -net bridge,br=virbr0 -append console=tty1 root=/dev/vda rw rootwait fsck.repair=
yes
odroid   10993  0.0  0.0   4020   544 pts/1    S+   15:14   0:00 grep --color=auto qemu
```

7.



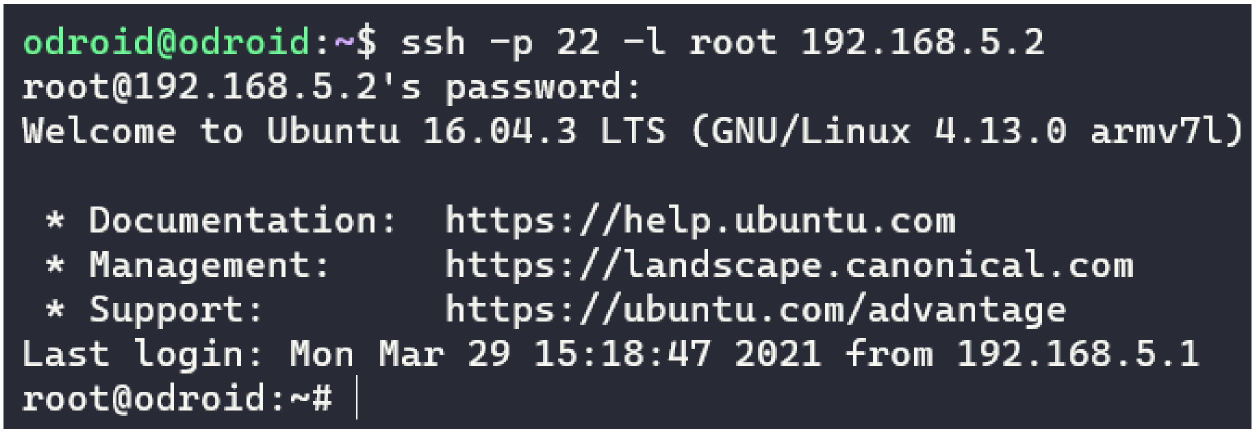
```
odroid@odroid:~$ nmap -sn 192.168.5.1/24

Starting Nmap 7.01 ( https://nmap.org ) at 2021-03-29 15:13 UTC
Nmap scan report for 192.168.5.1
Host is up (0.00064s latency).
Nmap scan report for 192.168.5.2
Host is up (0.0024s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.59 seconds
```



```
odroid@odroid:~$ nmap -p- 192.168.5.2

Starting Nmap 7.01 ( https://nmap.org ) at 2021-03-29 15:15 UTC
Nmap scan report for 192.168.5.2
Host is up (0.033s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 32.97 seconds
odroid@odroid:~$
```

8.

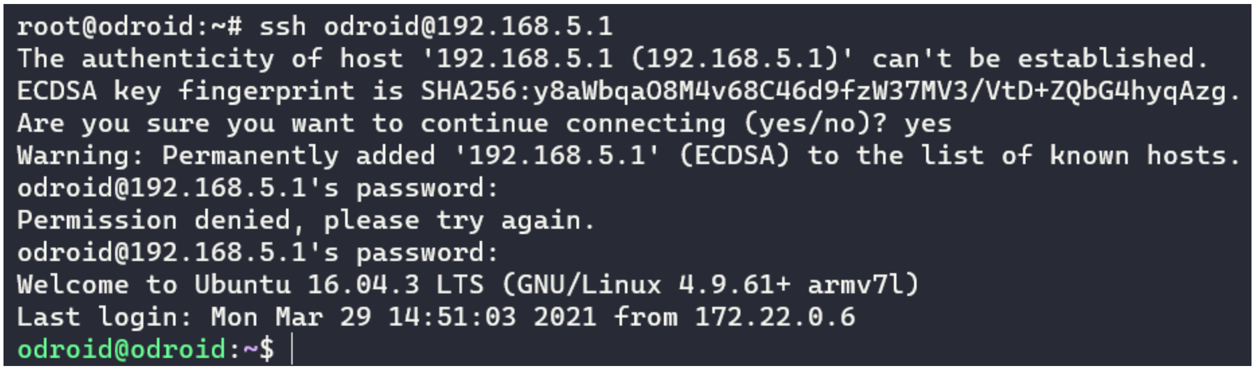
The VM has an IP of 192.168.5.2. It is using port 22.



```
odroid@odroid:~$ ssh -p 22 -l root 192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Mar 29 15:18:47 2021 from 192.168.5.1
root@odroid:~#
```

Subtask 3

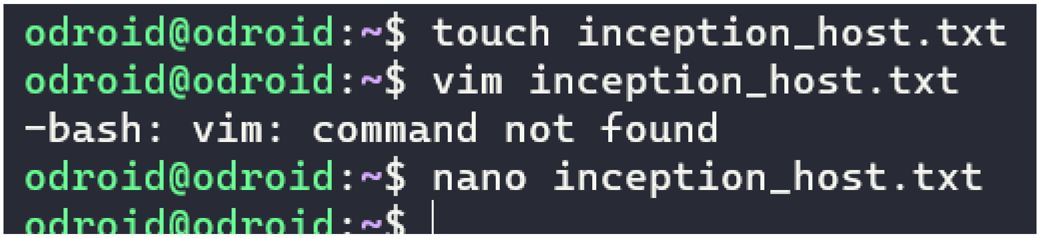
9.



```
root@odroid:~# ssh odroid@192.168.5.1
The authenticity of host '192.168.5.1 (192.168.5.1)' can't be established.
ECDSA key fingerprint is SHA256:y8aWbqaO8M4v68C46d9fzW37MV3/VtD+ZQbG4hyqAzg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.5.1' (ECDSA) to the list of known hosts.
odroid@192.168.5.1's password:
Permission denied, please try again.
odroid@192.168.5.1's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.9.61+ armv7l)
Last login: Mon Mar 29 14:51:03 2021 from 172.22.0.6
odroid@odroid:~$
```

I used 192.168.5.1.

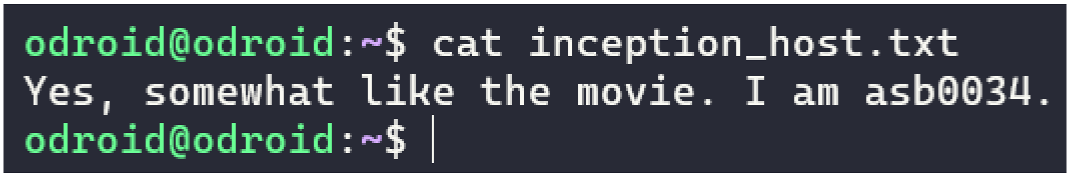
10.



```
odroid@odroid:~$ touch inception_host.txt
odroid@odroid:~$ vim inception_host.txt
-bash: vim: command not found
odroid@odroid:~$ nano inception_host.txt
odroid@odroid:~$
```

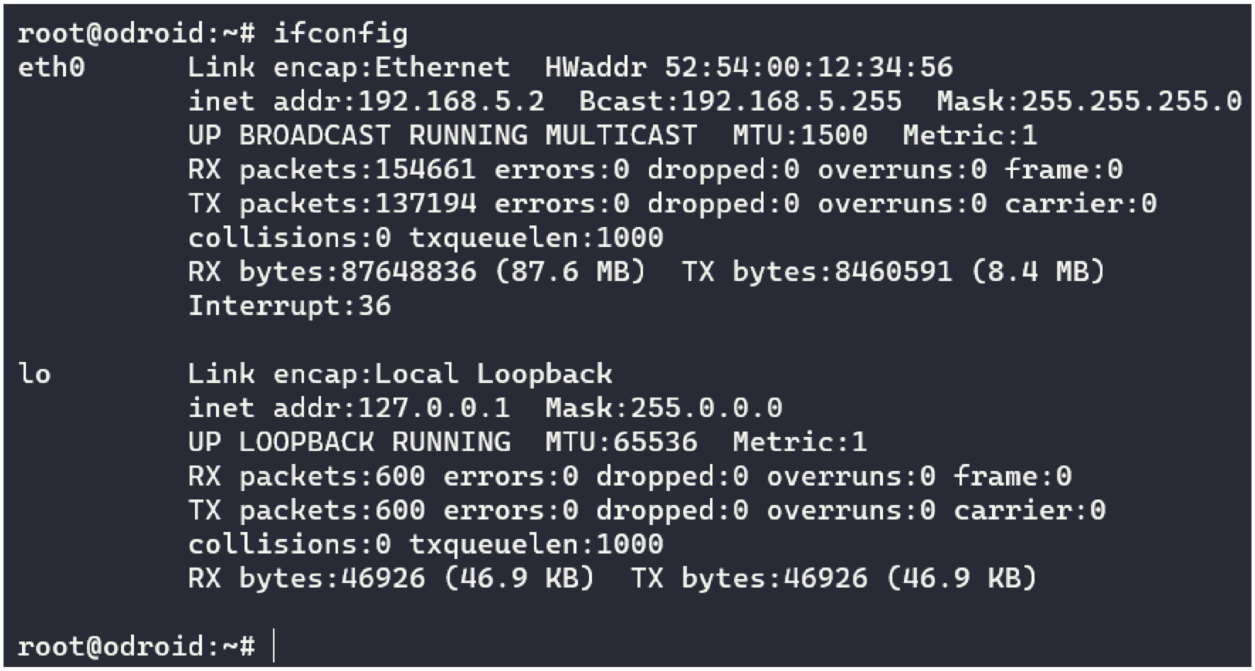
11. This file was created on HOST.

12.



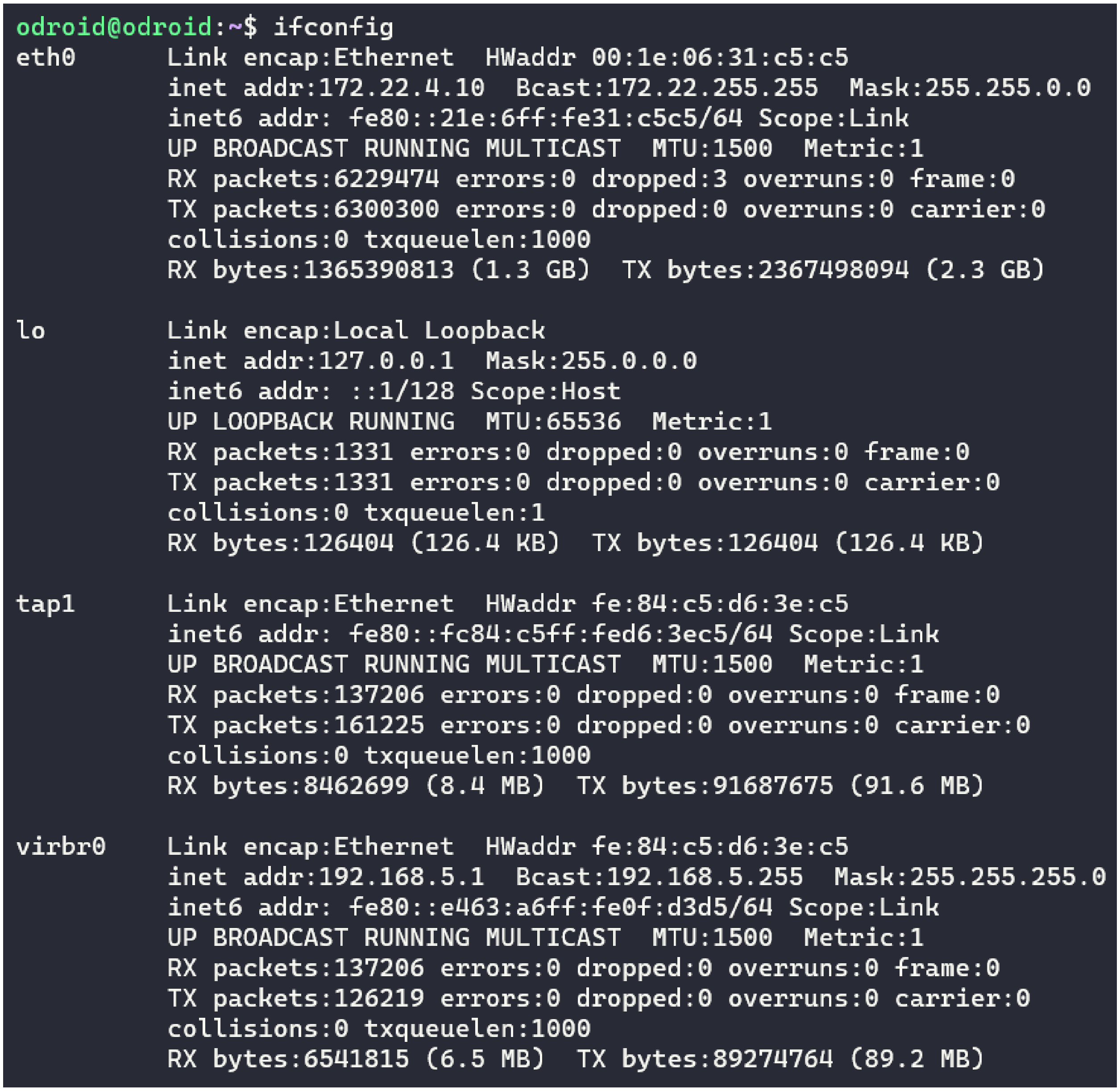
```
odroid@odroid:~$ cat inception_host.txt
Yes, somewhat like the movie. I am asb0034.
odroid@odroid:~$
```

13.



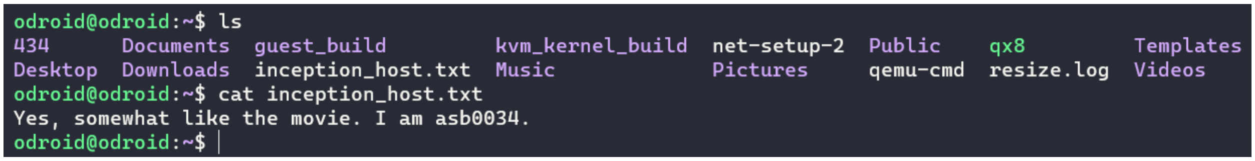
```
root@odroid:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:12:34:56
          inet addr:192.168.5.2  Bcast:192.168.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:154661 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:87648836 (87.6 MB)  TX bytes:8460591 (8.4 MB)
          Interrupt:36

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:600 errors:0 dropped:0 overruns:0 frame:0
          TX packets:600 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:46926 (46.9 KB)  TX bytes:46926 (46.9 KB)

root@odroid:~# 
```

14. I am now on the HOST.



```
odroid@odroid:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1e:06:31:c5:c5
          inet addr:172.22.4.10  Bcast:172.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::21e:6ff:fe31:c5c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6229474 errors:0 dropped:3 overruns:0 frame:0
          TX packets:6300300 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1365390813 (1.3 GB)  TX bytes:2367498094 (2.3 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1331 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1331 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:126404 (126.4 KB)  TX bytes:126404 (126.4 KB)

tap1      Link encap:Ethernet  HWaddr fe:84:c5:d6:3e:c5
          inet6 addr: fe80::fc84:c5ff:fed6:3ec5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137206 errors:0 dropped:0 overruns:0 frame:0
          TX packets:161225 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8462699 (8.4 MB)  TX bytes:91687675 (91.6 MB)

virbr0    Link encap:Ethernet  HWaddr fe:84:c5:d6:3e:c5
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::e463:a6ff:fe0f:d3d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137206 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126219 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6541815 (6.5 MB)  TX bytes:89274764 (89.2 MB)
```

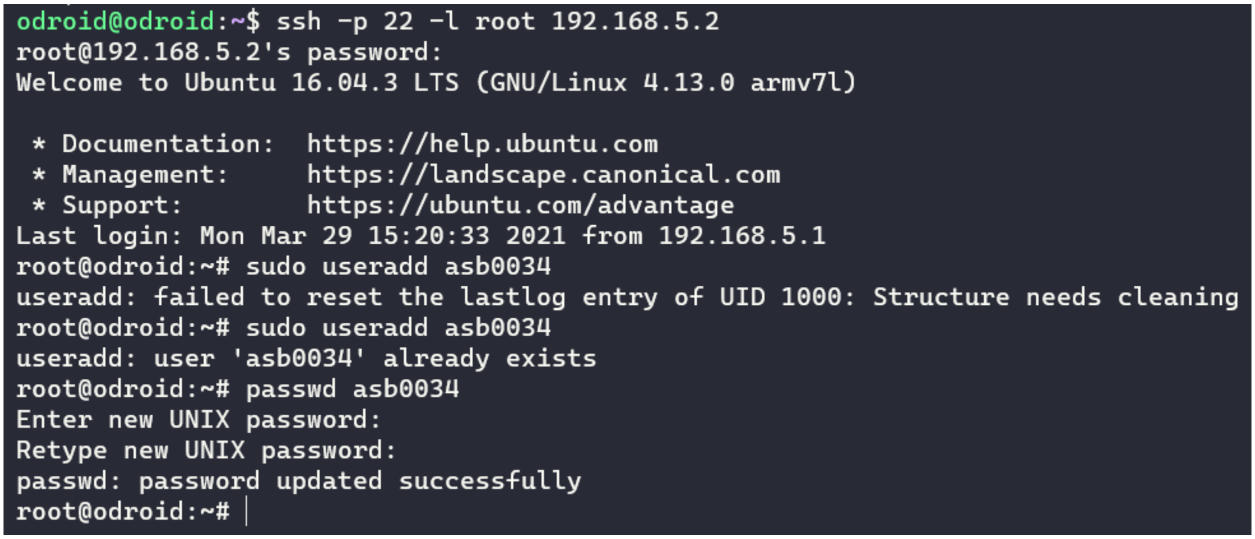
15.



```
odroid@odroid:~$ ls
434      Documents  guest_build         kvm_kernel_build  net-setup-2  Public    qx8         Templates
Desktop  Downloads  inception_host.txt  Music             Pictures     qemu-cmd  resize.log  Videos
odroid@odroid:~$ cat inception_host.txt
Yes, somewhat like the movie. I am asb0034.
odroid@odroid:~$
```

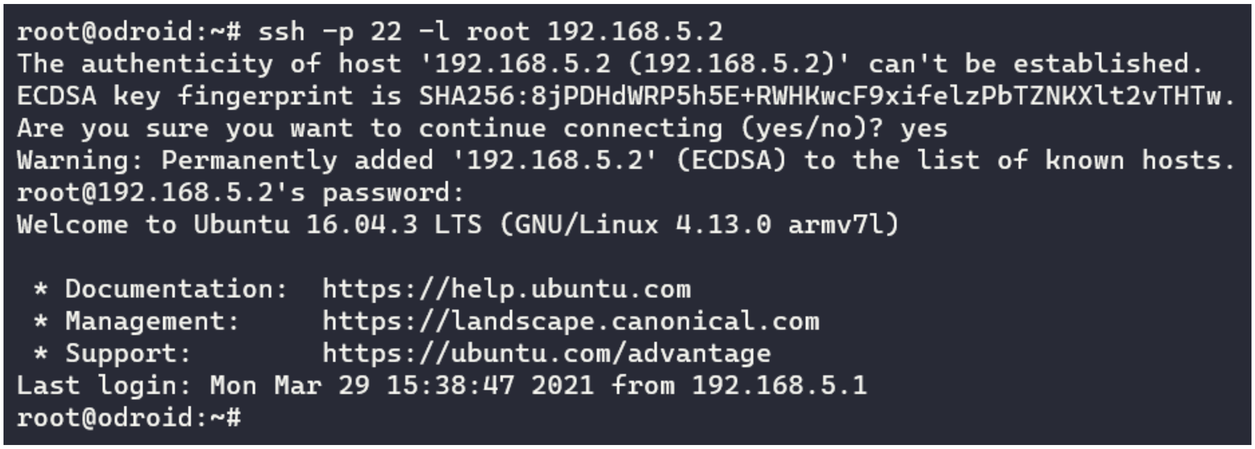
Subtask 4

16.



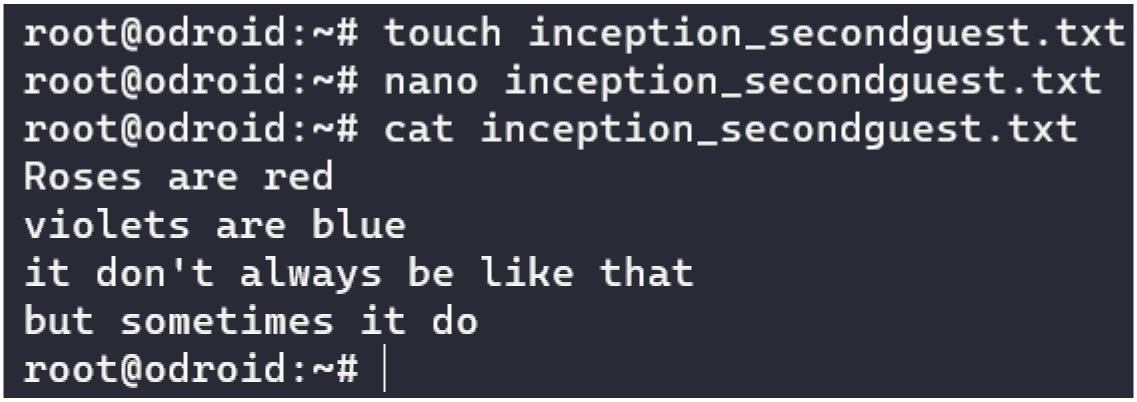
```
odroid@odroid:~$ ssh -p 22 -l root 192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Mar 29 15:20:33 2021 from 192.168.5.1
root@odroid:~# sudo useradd asb0034
useradd: failed to reset the lastlog entry of UID 1000: Structure needs cleaning
root@odroid:~# sudo useradd asb0034
useradd: user 'asb0034' already exists
root@odroid:~# passwd asb0034
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@odroid:~#
```

17.



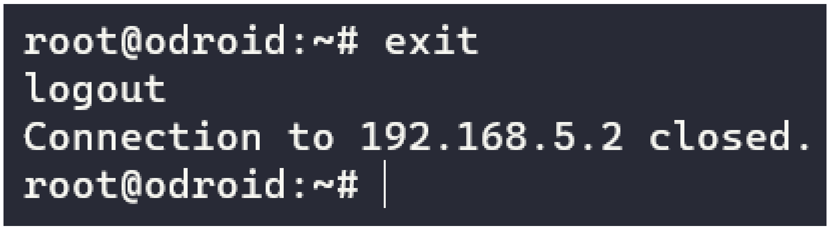
```
root@odroid:~# ssh -p 22 -l root 192.168.5.2
The authenticity of host '192.168.5.2 (192.168.5.2)' can't be established.
ECDSA key fingerprint is SHA256:8jPDHdWRP5h5E+RWHKwcF9xifelzPbTZNKXlt2vTHTw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.5.2' (ECDSA) to the list of known hosts.
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Mar 29 15:38:47 2021 from 192.168.5.1
root@odroid:~#
```

18.



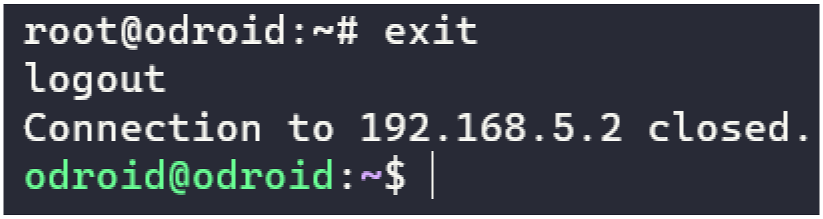
```
root@odroid:~# touch inception_secondguest.txt
root@odroid:~# nano inception_secondguest.txt
root@odroid:~# cat inception_secondguest.txt
Roses are red
violets are blue
it don't always be like that
but sometimes it do
root@odroid:~#
```

19.



```
root@odroid:~# exit
logout
Connection to 192.168.5.2 closed.
root@odroid:~#
```

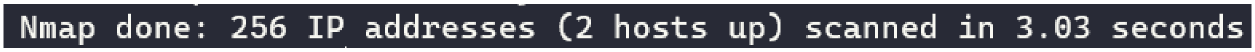
20.



```
root@odroid:~# exit
logout
Connection to 192.168.5.2 closed.
odroid@odroid:~$
```

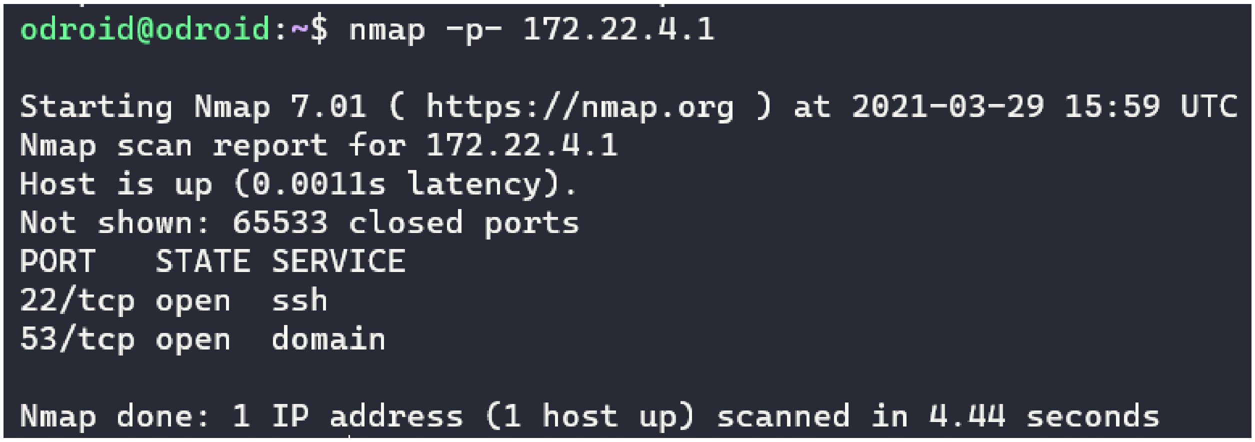
Subtask 5

21.



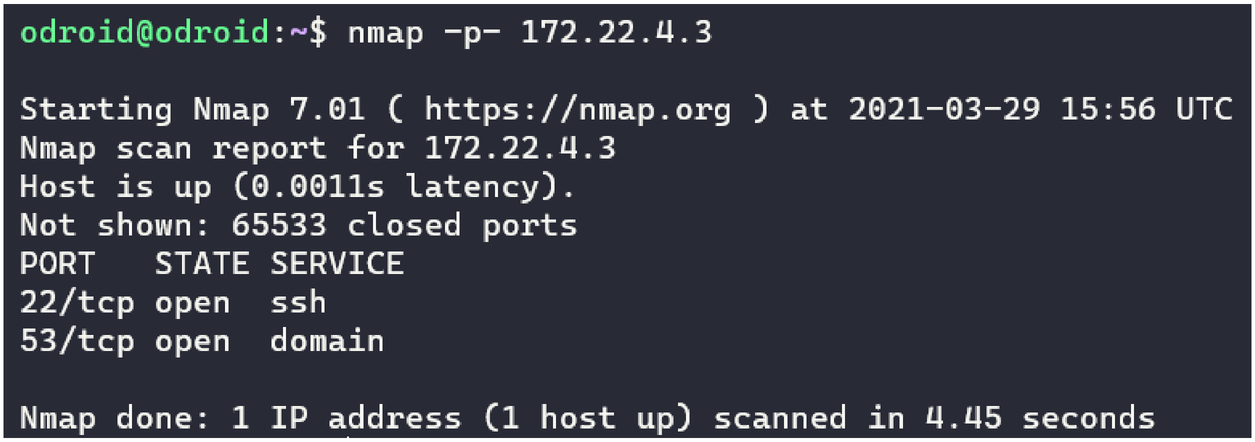
```
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.03 seconds
```

22.



```
odroid@odroid:~$ nmap -p- 172.22.4.1

Starting Nmap 7.01 ( https://nmap.org ) at 2021-03-29 15:59 UTC
Nmap scan report for 172.22.4.1
Host is up (0.0011s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.44 seconds
```

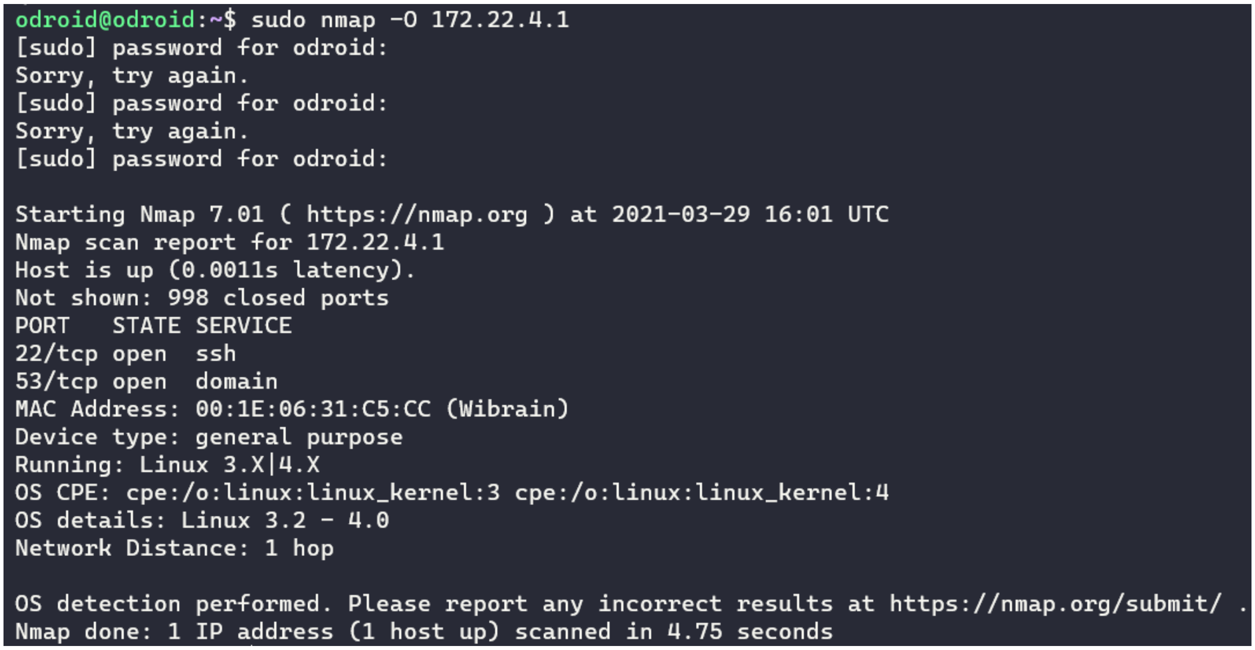
This machine as a ssh port open, so it is likely running Linux. It would be vulnerable to attack if the password were known.



```
odroid@odroid:~$ nmap -p- 172.22.4.3

Starting Nmap 7.01 ( https://nmap.org ) at 2021-03-29 15:56 UTC
Nmap scan report for 172.22.4.3
Host is up (0.0011s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.45 seconds
```

This machine as a ssh port open, so it is likely running Linux. It would be vulnerable to attack if the password were known.

23.



```
odroid@odroid:~$ sudo nmap -O 172.22.4.1
[sudo] password for odroid:
Sorry, try again.
[sudo] password for odroid:
Sorry, try again.
[sudo] password for odroid:

Starting Nmap 7.01 ( https://nmap.org ) at 2021-03-29 16:01 UTC
Nmap scan report for 172.22.4.1
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
MAC Address: 00:1E:06:31:C5:CC (Wibrain)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds
```

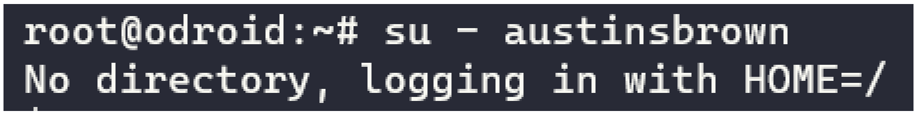
Nmap detected a Linux OS somewhere between 3.2 and 4. If I had the password then I could attack.

The Real Deal

24.

Hydra is a tool that is used for cracking passwords. It does so by guessing. It can do a brute force attack. This is just guessing random characters until you get a match. It can also try common passwords as a guess. This is far more efficient than a brute force. I will not use Hydra for nefarious purposes.

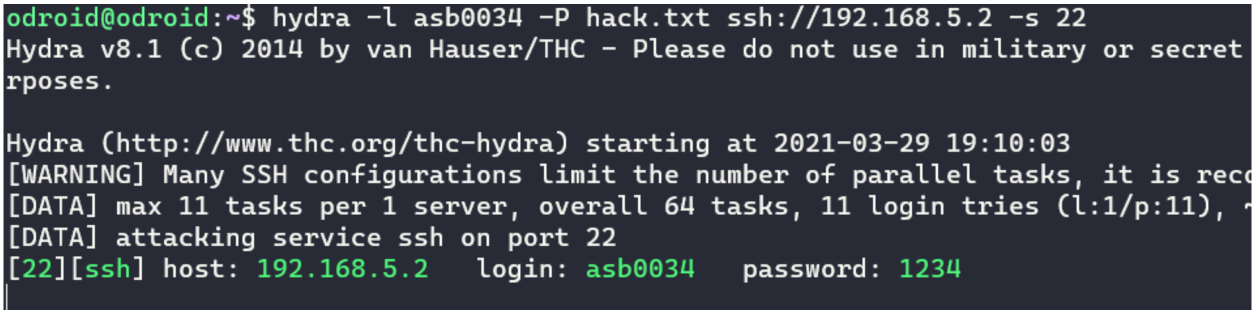
25.



```
root@odroid:~# su - austinsbrown
No directory, logging in with HOME=/
```

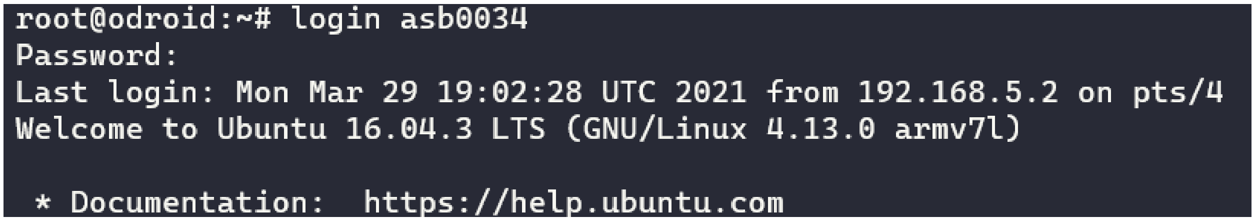
26. You could either use root privileges or brute force the password.

27.



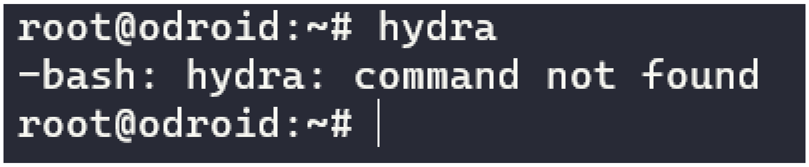
```
odroid@odroid:~$ hydra -l asb0034 -P hack.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
rposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-03-29 19:10:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is rec
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11),
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2   login: asb0034   password: 1234
```

28.



```
root@odroid:~# login asb0034
Password:
Last login: Mon Mar 29 19:02:28 UTC 2021 from 192.168.5.2 on pts/4
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
```

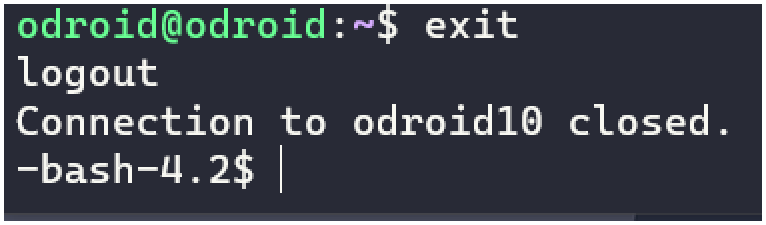
29.



```
root@odroid:~# hydra
-bash: hydra: command not found
root@odroid:~#
```

Hydra is not installed on this machine.

31.



```
odroid@odroid:~$ exit
logout
Connection to odroid10 closed.
-bash-4.2$
```

32. Hydra is not installed.

33. Hydra is not installed.