Austin Brown

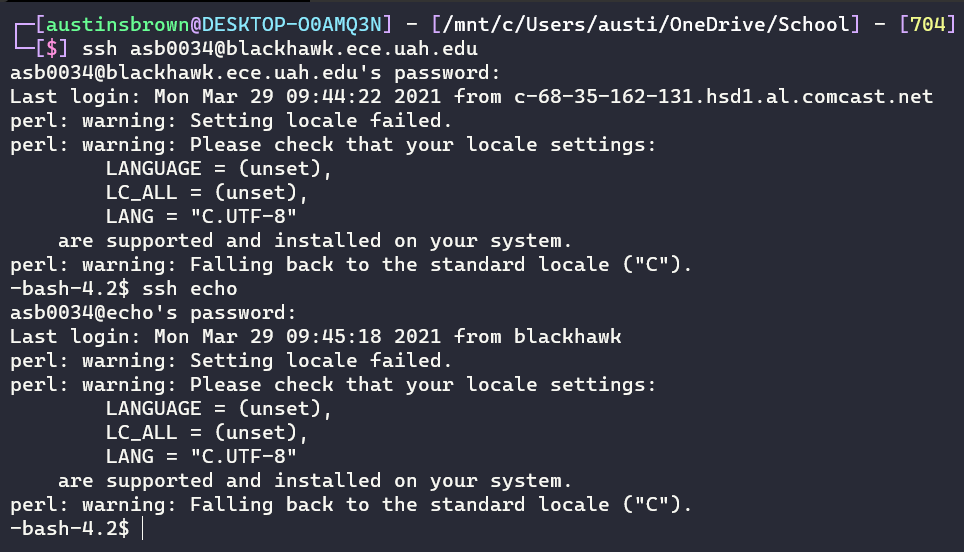
CPE 434-01

3/29/2021

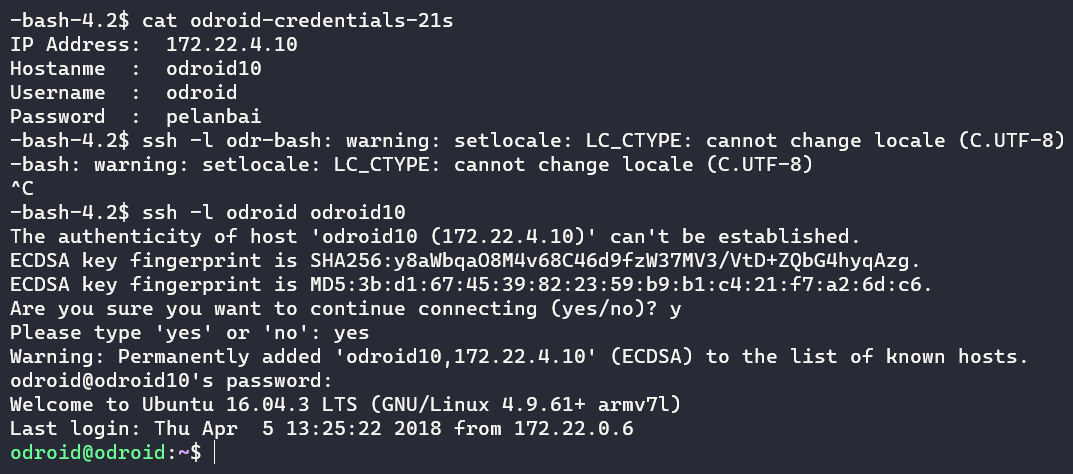
Lab11 Part 1

**Subtask 1**

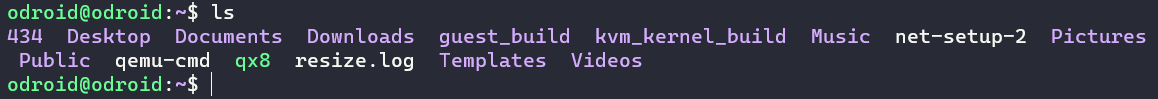
1.

****

2.

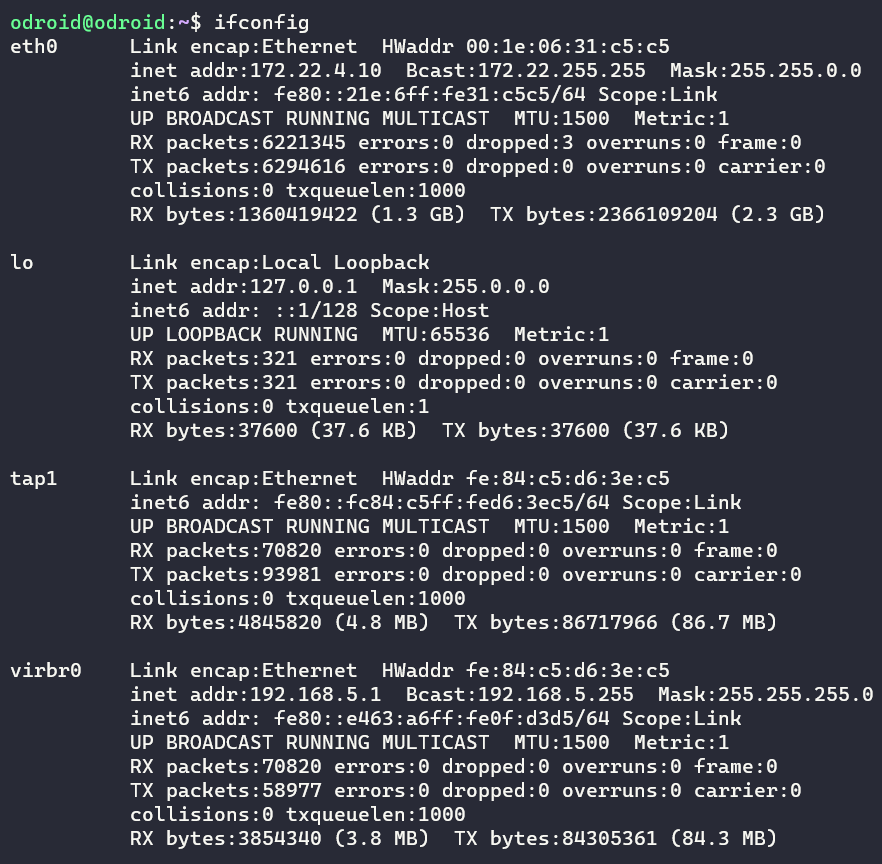
****

3.



**Subtask 2**

4.



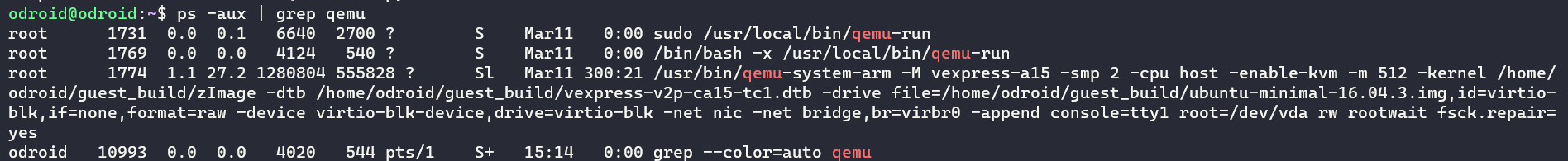
Virtual bridges are just virtual connections between virtual machines.

5.

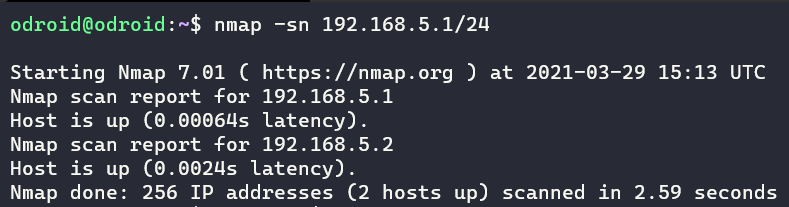
KVM converts the VM into a type 1 hypervisor. This means it can run directly on the host’s hardware.

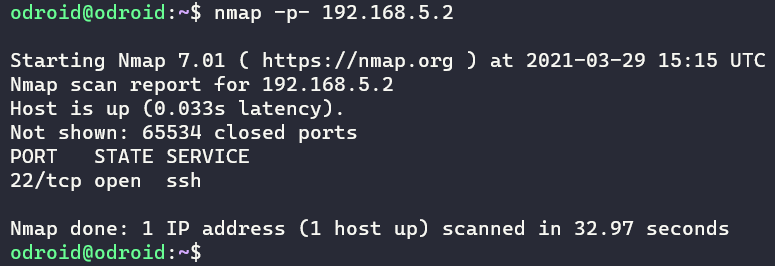
QEMU is a type 2 hypervisor. It can virtualize disks, USB, PCI, networks, etc.

6.



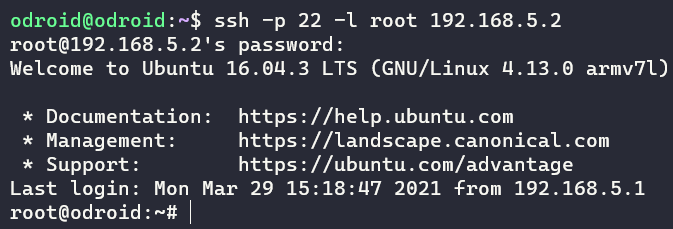
7.





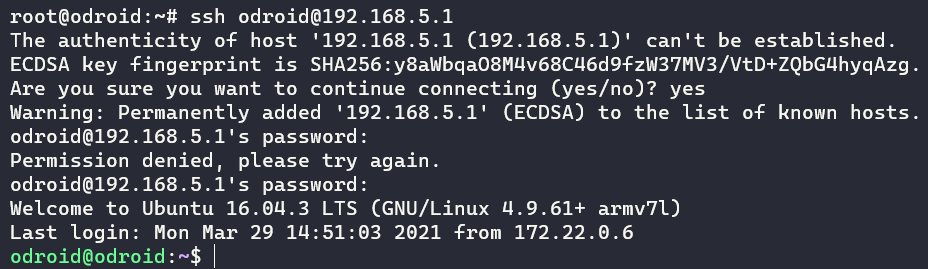
8.

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



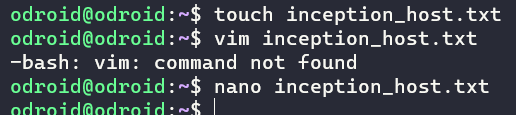
**Subtask 3**

9.



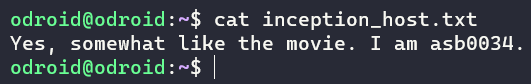
I used 192.168.5.1.

10.

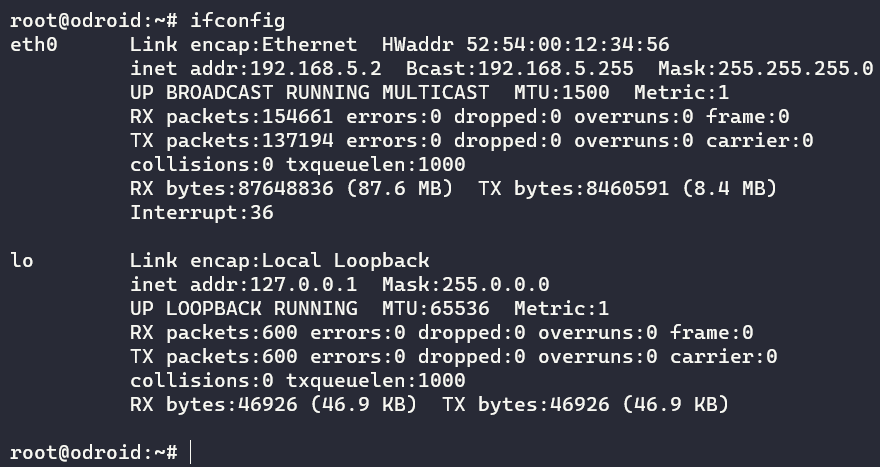


11. This file was created on HOST.

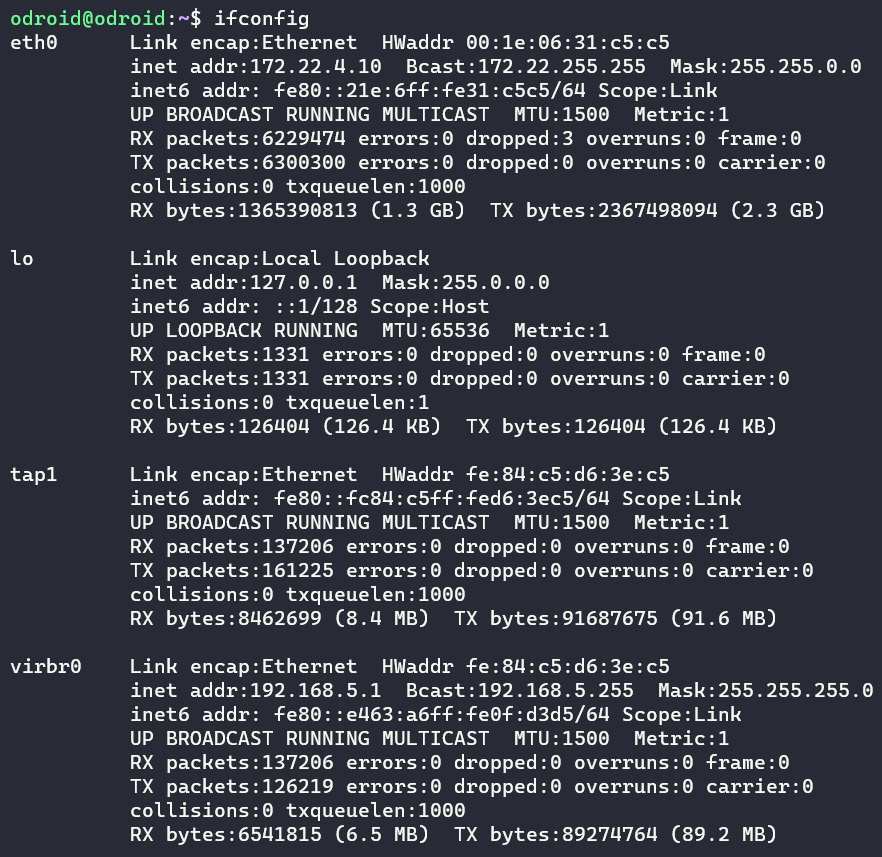
12.



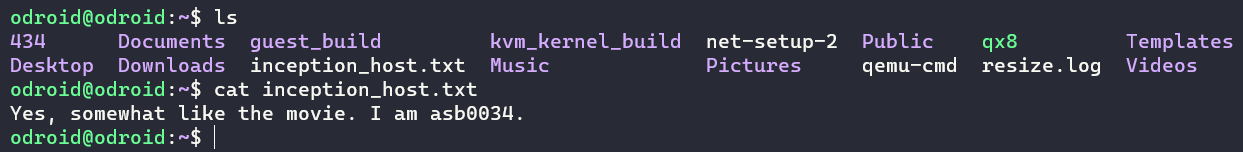
13.



14. I am now on the HOST.

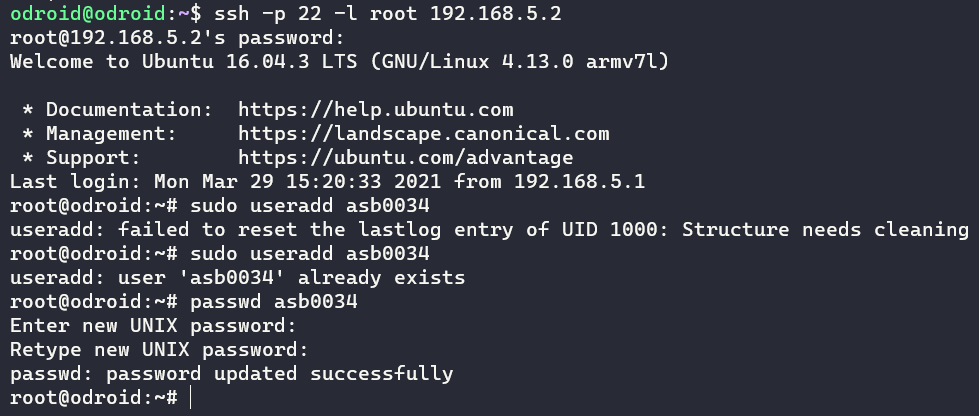


15.



**Subtask 4**

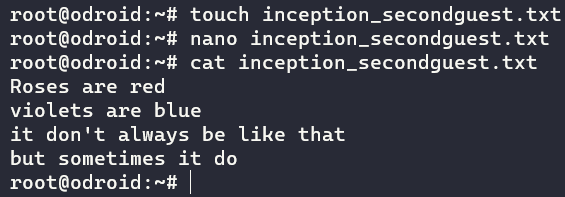
16.



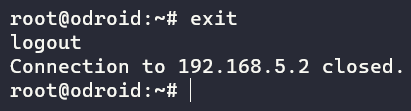
17.



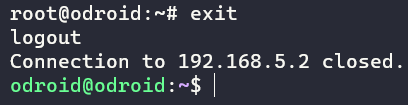
18.



19.



20.

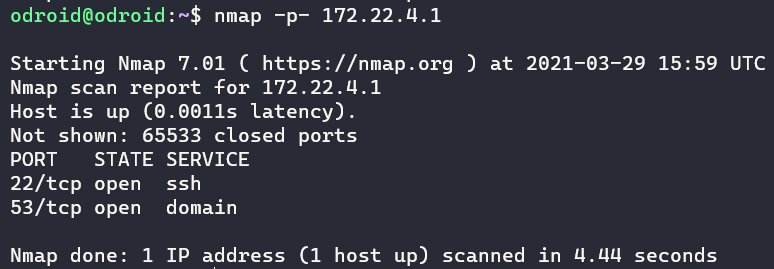


**Subtask 5**

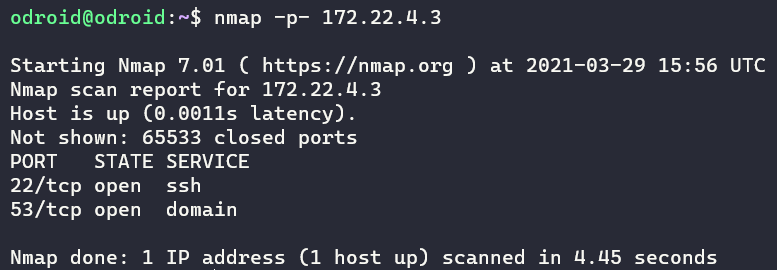
21.



22.

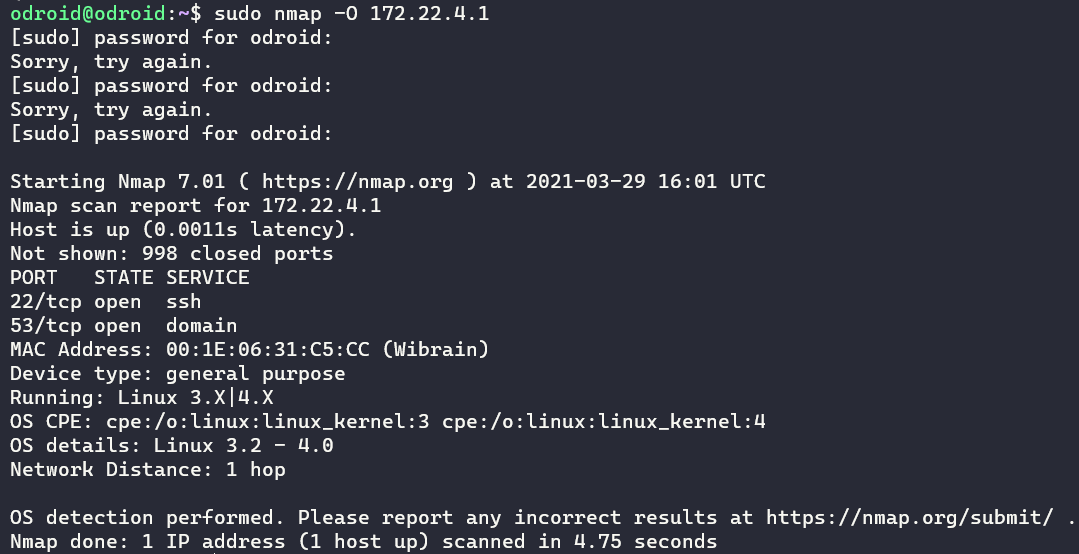


This machine as a ssh port open, so it is likely running Linux. It would be vulnerable to attack if the password were known.



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.



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

**The Real Deal**

24.

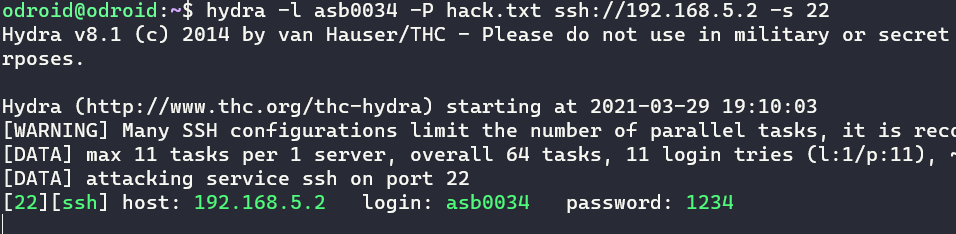
Hydra is a tool that is used for cracking passwords. It does so by guessing. It can do a brute force attack. This is just guessing random characters until you get a match. It can also try common passwords as a guess. This is far more efficient than a brute force. I will not use Hydra for nefarious purposes.

25.

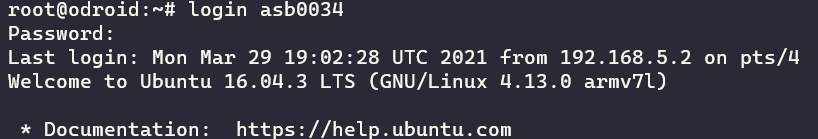


26. You could either use root privileges or brute force the password.

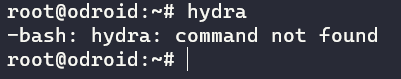
27.



28.

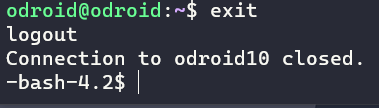


29.



Hydra is not installed on this machine.

31.



32. Hydra is not installed.

33. Hydra is not installed.