

# CPE 435: OPERATING SYSTEMS LABORATORY.

## **Lab11**

### **Introduction to nMap and Hydra.**

**Submitted by:** Dan Otieno.

**Date of Experiment:** 03/31/23.

**Report Deadline:** 04/07/23.

**Demonstration Deadline:** 04/07/23.

## Introduction:

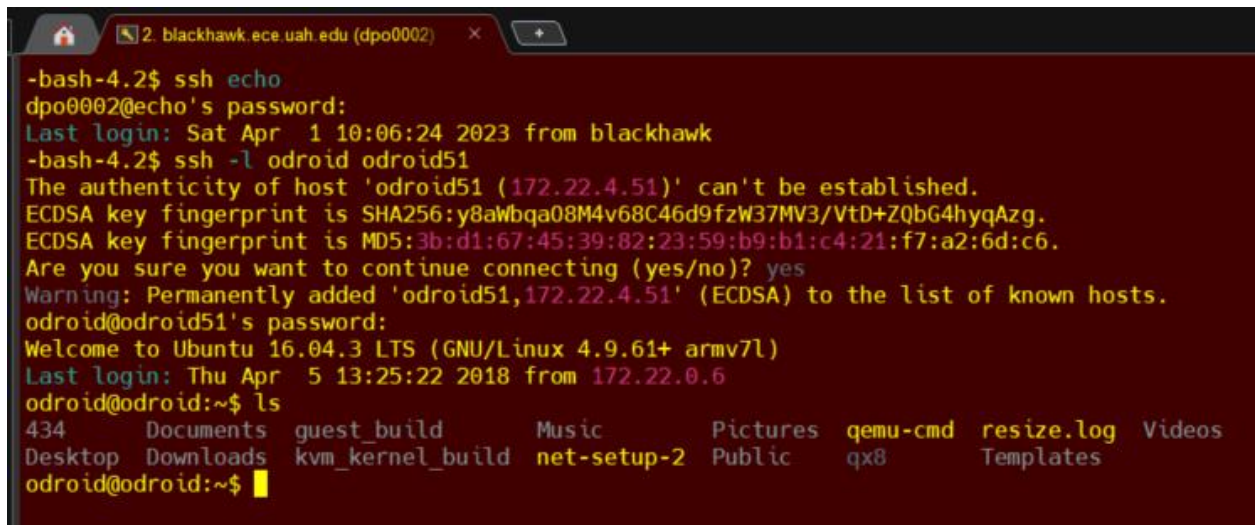
The purpose of this lab was to understand the nMap and Hydra utilities.

## Results & Observation:

### Subtask 1:

#### Description:

1. You must log into Blackhawk using `ssh <username>@blackhawk.ece.uah.edu` . Provide your password. If you are on lab machines, you are already logged into Blackhawk . Once you are on Blackhawk, you need to ssh into echo. In your terminal, type `ssh echo` and provide your Blackhawk password. The file system is shared, so you should be able to see the same files as you would see on Blackhawk. ([see screenshot on step 3](#)).
2. From Echo, you will log into another computer. You will be given a machine number and password. Please keep this with you in a place that you can remember. You can change your password if you want. This machine that you are logged in right now will be referred to as the HOST in this text from now on. SSH into the host using the following command: `ssh -l odroid odroidx` . Replace the x with your number. Provide a password when prompted. Your odroidx can be anything from odroid1 to odroid91 . ([Mine is Odroid51, see screenshot on step 3](#)).
3. Do `ls` in your terminal. Take a screenshot of what you see. Put this in your report:



```
-bash-4.2$ ssh echo
dpo0002@echo's password:
Last login: Sat Apr  1 10:06:24 2023 from blackhawk
-bash-4.2$ ssh -l odroid odroid51
The authenticity of host 'odroid51 (172.22.4.51)' can't be established.
ECDSA key fingerprint is SHA256:y8aWbqa08M4v68C46d9fzW37MV3/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)? yes
Warning: Permanently added 'odroid51,172.22.4.51' (ECDSA) to the list of known hosts.
odroid@odroid51'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:~$ ls
434      Documents  guest_build  Music      Pictures  qemu-cmd  resize.log  Videos
Desktop  Downloads  kvm_kernel_build net-setup-2 Public     qx8        Templates
```

### Subtask 2:

4. Type in `ifconfig` . Take a screenshot of what you see. What is a virtual bridge? **A virtual bridge is a networking component that allows communication between two or more virtual or physical network segments, commonly used in virtualized environments such as cloud computing, where multiple virtual machines may be running on a single physical server.**

```

odroid@odroid:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1e:06:32:68:7b
          inet addr:172.22.4.51  Bcast:172.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::21e:6ff:fe32:687b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:591122460  errors:0  dropped:2  overruns:0  frame:0
          TX packets:1762311973  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2492496964 (2.4 GB)  TX bytes:3144808124 (3.1 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:398  errors:0  dropped:0  overruns:0  frame:0
          TX packets:398  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1
          RX bytes:47159 (47.1 KB)  TX bytes:47159 (47.1 KB)

tap1      Link encap:Ethernet  HWaddr fe:53:91:91:03:2c
          inet6 addr: fe80::fc53:91ff:fe91:32c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:96282  errors:0  dropped:0  overruns:0  frame:0
          TX packets:55568  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8177847 (8.1 MB)  TX bytes:31814662 (31.8 MB)

virbr0    Link encap:Ethernet  HWaddr fe:53:91:91:03:2c
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::b413:fff:fe5a:8826/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:96282  errors:0  dropped:0  overruns:0  frame:0
          TX packets:45639  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6829899 (6.8 MB)  TX bytes:31014991 (31.0 MB)

odroid@odroid:~$ █

```

5. The odroid that you just logged in already has a virtual machine running. Write a short note on KVM and QEMU highlighting what each does. **KVM (Kernel-based Virtual Machine) is built into the Linux kernel and provides hardware-assisted virtualization capabilities that allows for multiple virtual machines to run on a single Linux-based host. QEMU (Quick Emulator) is a machine emulator and virtualizer that supports a wide range of operating systems and architectures. It is often used with KVM to help achieve complete virtualization.**

6. Type `ps -aux | grep qemu` in terminal. Take a screenshot of what you see and paste the output.

```

odroid@odroid:~$ ps -aux | grep qemu
root    1628  0.0  0.1  6640  2720 ?        S   Mar09   0:00 sudo /usr/local/bin/qemu-run
root    1643  0.0  0.0   4124   576 ?        S   Mar09   0:00 /bin/bash -x /usr/local/bin/qemu-run
root    1644 51.5 27.1 1428260 555352 ?        Sl  Mar09 16933:34 /usr/bin/qemu-system-arm -M vexpress-a15 -smp 2 -cpu ho
st -enable-kvm -m 512 -kernel /home/odroid/guest_build/zImage -dtb /home/odroid/guest_build/vexpress-v2p-ca15-tc1.dtb -dri
ve file=/home/odroid/guest_build/ubuntu-minimal-16.04.3.img,id=virtio-blk,if=none,format=raw -device virtio-blk-device,dri
ve=virtio-blk -net nic -net bridge,br=virbr0 -append console=tty1 root=/dev/vda rw rootwait fsck.repair=yes
odroid  32291  0.0  0.0   4020   532 pts/1    S+  15:43   0:00 grep --color=auto qemu
odroid@odroid:~$

```

7. The virtual machine that is running in your machine will be referred to as the GUEST in this text. Log into the GUEST machine. The username is root and the password is odroid . However we do not know the IP. Let us use nmap to detect all live hosts in our network. Verify nmap is installed by typing nmap in your terminal. We will look into the virtual bridge interface. Use nmap to scan the IP address that starts with 192.168.xxx.xxx and provide a screenshot of the result.

```

Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.9.61+ armv7l)
Last login: Thu Apr  6 21:50:44 2023 from 172.22.0.6
odroid@odroid:~$ nmap 192.168.5.1/24

Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-06 21:55 UTC
Nmap scan report for 192.168.5.1
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap scan report for 192.168.5.2
Host is up (0.018s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.62 seconds
odroid@odroid:~$

```

This might be the GUEST machine. You may need to know the idea of subnet masking. Please search online on how to scan a network using nmap . Does knowing a part of the GUEST IP help? **Knowing part of the GUEST IP helps because we can use that information to determine the exact IP address we need to access for the guest. Ifconfig sends back multiple addresses, and it may be more challenging to determine the exact one needed for the guest interface.**

8. What is the virtual machine that you discovered? What are the ports that are open in the machine? Log into that virtual machine that you discovered. Paste screenshot of successful login and the open ports. **Virtual Machine: Ubuntu 16.04.3 LTS, open port is 22.**

```

Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-06 21:55 UTC
Nmap scan report for 192.168.5.1
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap scan report for 192.168.5.2
Host is up (0.018s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.62 seconds
odroid@odroid:~$ ssh 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: Thu Apr  6 21:50:55 2023 from 192.168.5.1
root@odroid:~# █

```

### Subtask 3:

9. From your GUEST machine, where you are currently, log back into the HOST machine using ssh. Use the HOST IP on the virtual bridge interface. Use `ssh odroid@<host ip>`. The HOST IP that you provide is the IP on virtual interface, and not the IP you used to login from echo. What IP should you use now? Take a screenshot of successful login.

```

root@odroid:~# ssh odroid@192.168.5.1
odroid@192.168.5.1's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.9.61+ armv7l)
Last login: Thu Apr  6 21:54:14 2023 from 192.168.5.2
odroid@odroid:~$ █

```

blackhawk	0%	6.18 GB / 125.36 GB	0.63 Mb/s
-----------	----	---------------------	-----------

10. At this instance, you should be logged into HOST from GUEST which you logged in from HOST. Create a file named "inception\_host.txt". Open the file and write "Yes, somewhat like the movie. I am <charger id>".

```

odroid@odroid:~$ touch inception_host.txt
odroid@odroid:~$ ls -l
total 60
drwxr-xr-x 2 odroid odroid 4096 Mar 23 2018 434
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Desktop
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Documents
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Downloads
drwxr-xr-x 4 odroid odroid 4096 Mar 22 2018 guest_build
-rw-rw-r-- 1 odroid odroid 0 Apr 6 22:13 inception_host.txt
drwxr-xr-x 3 odroid odroid 4096 Feb 5 2018 kvm_kernel_build
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Music
-rw-rw-r-- 1 odroid odroid 375 Feb 19 2018 net-setup-2
-rw-rw-r-- 1 odroid odroid 224 Apr 5 23:56 nmap_output
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Pictures
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Public
-rw-r--r-- 1 odroid odroid 501 Feb 9 2018 qemu-cmd
-rwxr-xr-x 1 odroid odroid 572 Feb 19 2018 qx8
-rw-r--r-- 1 root root 0 Feb 11 2016 resize.log
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Templates
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Videos
odroid@odroid:~$ vi inception_host.txt
odroid@odroid:~$ cat inception_host.txt
Yes, somewhat like the movie. I am dpo0002.
odroid@odroid:~$ █

```

11. Where do you think you created this file? **The file is created in the home directory for HOST user (odroid's home directory).**
12. Cat the content of the file using cat <filename> and take a screenshot. **See screenshot above with cat command.**
13. Hit exit on the terminal. Where are you now after exit? Perform ifconfig as a proof and take a screenshot. **After typing exit in the terminal, I log back into GUEST IP.**

```
odroid@odroid:~$ exit
logout
Connection to 192.168.5.1 closed.
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:9394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7627 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1071170 (1.0 MB)  TX bytes:654408 (654.4 KB)
          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:663 errors:0 dropped:0 overruns:0 frame:0
          TX packets:663 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50643 (50.6 KB)  TX bytes:50643 (50.6 KB)

root@odroid:~# █
```

14. Exit from here. Where are you now after exit? **When I exit from here, I log back into the HOST IP.**

```
root@odroid:~# exit
logout
Connection to 192.168.5.2 closed.
odroid@odroid:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1e:06:32:68:7b
          inet addr:172.22.4.51  Bcast:172.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::21e:6ff:fe32:687b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1269090  errors:0  dropped:2  overruns:0  frame:0
          TX packets:629480  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:593778963 (593.7 MB)  TX bytes:560091944 (560.0 MB)

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:6074  errors:0  dropped:0  overruns:0  frame:0
          TX packets:6074  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1
          RX bytes:382607 (382.6 KB)  TX bytes:382607 (382.6 KB)

tap1      Link encap:Ethernet  HWaddr fe:d1:ac:68:cf:6b
          inet6 addr: fe80::fcd1:acff:fe68:cf6b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7703  errors:0  dropped:0  overruns:0  frame:0
          TX packets:10632  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:663244 (663.2 KB)  TX bytes:1394447 (1.3 MB)

virbr0    Link encap:Ethernet  HWaddr fe:d1:ac:68:cf:6b
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::24eb:d7ff:fedc:80bb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7703  errors:0  dropped:0  overruns:0  frame:0
          TX packets:10190  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:555402 (555.4 KB)  TX bytes:1320569 (1.3 MB)

odroid@odroid:~$ █
```

15. Do you see 'inception\_host.txt'? Cat the content of the file and take a screenshot.



```

odroid@odroid:~$ ls -l
total 64
drwxr-xr-x 2 odroid odroid 4096 Mar 23 2018 434
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Desktop
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Documents
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Downloads
drwxr-xr-x 4 odroid odroid 4096 Mar 22 2018 guest_build
-rw-rw-r-- 1 odroid odroid 44 Apr 6 22:15 inception_host.txt
drwxr-xr-x 3 odroid odroid 4096 Feb 5 2018 kvm_kernel_build
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Music
-rw-rw-r-- 1 odroid odroid 375 Feb 19 2018 net-setup-2
-rw-rw-r-- 1 odroid odroid 224 Apr 5 23:56 nmap_output
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Pictures
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Public
-rw-r--r-- 1 odroid odroid 501 Feb 9 2018 qemu-cmd
-rwxr-xr-x 1 odroid odroid 572 Feb 19 2018 qx8
-rw-r--r-- 1 root root 0 Feb 11 2016 resize.log
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Templates
drwxr-xr-x 2 odroid odroid 4096 Jul 3 2016 Videos
odroid@odroid:~$ cat inception_host.txt
Yes, somewhat like the movie. I am dpo0002.
odroid@odroid:~$ █

```

#### Subtask 4:

16. Log into the GUEST machine again. You are root, which means you can do whatever you want. Create a user account with the same name as your chargerid. Please search online on how to create a user account on a linux machine. At this moment you should have two user accounts on the GUEST machine. Give a password that you will remember. Screenshot.

```

root@odroid:~# useradd dpo0002
root@odroid:~# sudo useradd dpo0002
useradd: user 'dpo0002' already exists
root@odroid:~# ssh 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: Thu Apr 6 21:55:43 2023 from 192.168.5.1
root@odroid:~# pwd
/root

```

17. Log into the second guest from the first guest. You can ssh into the second guest using the same IP as the first guest. Take a screenshot of the successful login. [See screenshot above for](#)

useradd dpo0002 command, but for later parts of the lab, I created a second user called "labdpo0002", you may see that in later screenshots.

18. Create a file named "inception\_secondguest.txt" and write whatever you want. Cat the content of the file and take screenshot.

```
root@odroid:~# touch inception_secondguest.txt
root@odroid:~# ls-l
-bash: ls-l: command not found
root@odroid:~# ls -l
total 0
-rw-r--r-- 1 root root 0 Apr  6 22:35 inception_secondguest.txt
root@odroid:~# vi inception_secondguest.txt
root@odroid:~# cat inception_secondguest.txt
ABCDEFGHIJKLMNOPQRSTUVWXYZ
CatsDinosaursDogsetcetcetc:W
This is actually fun, not so bad, but its fun when things work!
root@odroid:~# █
```

19. Exit from the second guest. (exited)

20. Exit from the first guest. (exited)

## Subtask 5:

21. You are already familiar with using nmap for live host discovery. Here you will use the same concept but you will find how many of your friends' machines are live at this particular moment. You should look at the interface eth0 . How many live machines did you find? Screenshot. This might take some time (a couple of minutes). Your screenshot should clearly indicate the number of machines that are up. **89 Machines are Up!**

```
odroid@odroid:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1e:06:32:68:7b
          inet addr:172.22.4.51  Bcast:172.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::21e:6ff:fe32:687b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1759061 errors:0 dropped:3 overruns:0 frame:0
          TX packets:607806 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:734371867 (734.3 MB)  TX bytes:453271279 (453.2 MB)
```

```
odroid@odroid:~$ nmap 172.22.4.51/24

Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-08 15:38 UTC
Nmap scan report for 172.22.4.1
Host is up (0.0016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
```

```

Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap scan report for 172.22.4.86
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap scan report for 172.22.4.87
Host is up (0.0019s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap scan report for 172.22.4.89
Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap scan report for 172.22.4.90
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap scan report for 172.22.4.91
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap done: 256 IP addresses (89 hosts up) scanned in 10.27 seconds
odroid@odroid:~$

```

22. Based on scan from above, for any two of your friend's machine write following information

1. What ports are open? If you know the password, can you attack their machine? (Do not actually attack any of these machines/ports!!) **Ports 22 and 53 are open (see above screenshot), and yes, you can attack their machines if you know the password.**
2. What OS is your friend using? **Linux.**

23. Based on your scan from 21, you would not be able to know the OS. All you can do is guess. Find the command to detect OS of live hosts using nmap. Perform a new scan, and answer Q22 again. Take a screenshot of the scan that shows the OS also.

```

odroid@odroid:~$ sudo nmap -O 172.22.4.90

Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-08 15:46 UTC
Nmap scan report for 172.22.4.90
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:06:37:C1:5A (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
odroid@odroid:~$ sudo nmap -O 172.22.4.91

Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-08 15:46 UTC
Nmap scan report for 172.22.4.91
Host is up (0.00088s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
MAC Address: 00:1E:06:30:60:31 (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 4.70 seconds
odroid@odroid:~$ █

```

## The Real Deal:

24. Please read about Hydra at <https://tools.kali.org/password-attacks/hydra>. Write a short note on Hydra and its capabilities of at least five sentences. Add a sixth sentence saying that you will not use hydra for immoral or illegal purposes.

25. Log into your user account in the HOST machine.

26. Consider the following scenario:

1. You know that you have a machine that is live (means it is ON). You have the IP address, but you cannot log into it because you do not have a password. Your second user account on the GUEST is that machine for this case.
2. You also know that the ssh port is open in that machine. (Possible attack vector, right?)
3. What possible approach can you think of in this case to log into the second guest user account? Mention any two ways you can think of to log into the second guest user account without knowing the password. **You could create the second user without a password, or you could use a tool that can run through possible combinations and “guess” the password, perhaps.**

27. We will use a tool called Hydra. You might have studied this already.. Here we will create a password file that is fed into Hydra. In the file password.txt, put in at least 10 random passwords in 10 lines. Put an 11th line as the correct password for the second guest user account. Use the following command: hydra -l <secondguestusername> -P <password.txt> ssh://<ipofguest> -s <portnumber> Replace the secondguestusername with the actual username that you want to crack as, supply the ip of guest in ipofguest . portnumber is the port that you want to target. Default is 22 for ssh, so use 22.

28. Take a screenshot of successful login. (As previously mentioned, I created a second user for this part of the lab, user is labdpo0002, not dpo0002 in Question 17. I did this so I would not get confused with my regular blackhawk uah ID, this was also explained during lab demo). Password was odroid1.

```
odroid@odroid:~$ cat password.txt
rsenal1245688
ipass1236728:
pqodddueu8522
Dahayu192983e3
rhjshhwhw12jj
C
wjqgu
ChamsW92376
what897ghjs
ranj674892
odroid1
odroid@odroid:~$
```

```
odroid@odroid:~$ hydra -l labdpo0002 -P password.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 service organizations
, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2023-04-06 23:39:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2 login: labdpo0002 password: odroid1
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-04-06 23:39:54
odroid@odroid:~$
```

29. Repeat 27 for the first user account root on the GUEST machine. You may need to modify the password file. **Because of the issues in the screenshot below, where I was unable to get the GUEST IP, and therefore unable to log in to Root, both from my computer and the actual lab machine in EB246 I was unable to complete the remaining steps, I shared these issues with the Lab Instructor via email and attached screenshots. However, the demo for this lab was successfully completed on 04/07.**

```
Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-08 23:21 UTC
Nmap scan report for 192.168.5.1
Host is up (0.00062s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap done: 256 IP addresses (1 host up) scanned in 2.80 seconds
odroid@odroid:~$ ssh root@192.168.5.2
ssh: connect to host 192.168.5.2 port 22: No route to host
odroid@odroid:~$
```

30. Take a screenshot of successful login.

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

Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-09 13:49 UTC
Nmap scan report for 192.168.5.1
Host is up (0.00045s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap done: 256 IP addresses (1 host up) scanned in 2.80 seconds
```

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

Starting Nmap 7.01 ( https://nmap.org ) at 2023-04-08 23:29 UTC
Nmap scan report for 192.168.5.1
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap done: 256 IP addresses (1 host up) scanned in 2.70 seconds
odroid@odroid:~$
```

31. Exit from your odroid onto echo. **Unable to complete, no root access (see above screenshots).**

32. Perform 27 and attempt to perform an attack on your odroid from echo using hydra. **Unable to complete, no root access (see above screenshots).**

33. Were you able to attack your odroid from echo, why or why not? Note: do not attempt to install hydra on echo, especially with sudo. Take a screenshot of the result. **Unable to complete, no root access (see above screenshots).**