

Description

Nmap is a utility that allows you to check all the devices that are connected to the network. You can basically check the open ports in those devices also. You can also find a multitude of other information regarding those devices connected to the network. Please check more about nmap in <https://linux.die.net/man/1/nmap>. This assignment has 33 steps and **you are required to have at least 33 screenshots to support your answers**. You can have more as needed, but no less.

Use of Odroids and Paired Programing

For the remaining labs students will be using the Odroid machines that are connected to the ECE department's server. The odroids are located on echo, which is reachable through blackhawk following the instructions below. Students will obtain login credentials for an Odroid by doing one of the following; completing the survey on canvas, messaging the lab TA directly, or requesting an Odroid in person in the lab or during office hours. Otherwise, students will be assigned an Odroid and sent its credentials on the day of the next lab section after this lab is issued if no response was chosen.

For the remaining labs due to limited hardware students may work in pairs of two or alone. Students working in pairs should put both names on the submission and will be issued a single Odroid to be used between them.

Subtask I:

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.
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`.
3. Do `ls` in your terminal. Take a **screenshot** of what you see. Put this in your report.

Subtask II:

4. Type in `ifconfig` . Take a **screenshot** of what you see. What is a virtual bridge?
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.
6. Type `ps -aux | grep qemu` in terminal. Take a **screenshot** of what you see and paste the output.
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 user name 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. 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?
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.

Subtask III:

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.
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>".
11. Where do you think you created this file?
12. Cat the content of the file using `cat <filename>` and take a **screenshot**.
13. Hit `exit` on the terminal. Where are you now after exit? Perform `ifconfig` as a proof and take a **screenshot**.
14. Exit from here. Where are you now after exit?
15. Do you see 'inception_host.txt'? Cat the content of the file and take a **screenshot**.

Subtask IV:

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.
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.
18. Create a file named "inception_secondguest.txt" and write whatever you want. Cat the content of the file and take **screenshot**.
 19. Exit from the second guest.
 20. Exit from the first guest.

Subtask V:

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.
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!!)
 2. What OS is your friend using?
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.

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.
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.

29. Repeat 27 for the first user account `root` on the **GUEST** machine. You may need to modify the password file.

30. Take a **screenshot** of successful login.

31. Exit from your odroid onto echo.

32. Perform 27 and **attempt** to perform an attack on your odroid from echo using hydra.

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.

You have immense power from this moment on. You are more powerful than the greatest lock cracker in the world, make wise use of your power.

Deliverables

Lab Report

The following material in each section is expected:

1. Cover page with your name, lab number, course name, and dates
2. The following sections from the assignment are expected along with their answers and supporting screenshots:
 - a. Subtask 1
 - b. Subtask 2
 - c. Subtask 3
 - d. Subtask 4
 - e. Subtask 5
 - f. The Real Deal

The report should be submitted as a single pdf document with the source code for your program within it.

Recorded Demonstration

The following material in each section is expected:

1. Introduce yourself and give the name of the lab
2. Walk through the final steps of The Real Deal section

The demonstration may be in person or recorded and submitted as an mp4 file alongside the report.