Lab Exercise 1

Due: Friday, October 18, 2019 **Points:** 100

This laboratory exercise is straightforward. It is designed to get you comfortable with running virtual machines using a hypervisor called VirtualBox. We will use these in future labs. It also introduces you to a powerful network probing tool, *nmap*(1).

Background

When attackers target a system, one of the first things they do is see what services the system makes available over the Internet. Once the attackers learn the services the system provides, they attempt to exploit vulnerabilities in the services to gain access to the system and the information on it.

The goal of this exercise is to carry out such an analysis (called a *port scan*) so you can see how attackers do it, and how you can hinder it.

What You Will Need

All the virtual machines and/or resources are available via the web at

http://nob.cs.ucdavis.edu/classes/ecs153-2019-04/labs/lab1

You will also need a virtual machine, VirtualBox. You can download it from

https://www.virtualbox.org/wiki/Downloads

Also, get the VirtualBox Extension Pack. Install both VirtualBox and the extension pack.

Part 1

You will need the virtual machine `nmap1` (*nmap1.ova*). This is a big file (about 2.86 gigabytes), so it's best not to do this on a slow link.

To run it, start VirtualBox, and go to *Import Appliance* (it's under the *File* menu item). Select *nmap1.ova*. Then in the settings, change RAM to be 4096 MB. Click *Import* to load the virtual machine.

You will also find a shared folder to be useful. With it, you can copy a file into that folder on the guest (`nmap`) and it will appear on your host system. To do this, first click on the virtual machine `nmap1` in the left column, and then on *Display*, and make sure the *Video Memory* (under *Screen*) is set to at least 32MB. Then click on *Shared Folders*, and the folder with the green plus sign. Set *Folder Path* to the shared folder on the host system, and click on *Auto-mount*. Then click *OK*, and then *OK* again. The shared folder will be mounted under */media* and have the prefix *sf_*. So if you named the folder *Shared*, on the guest `nmap1`, it is the directory */media/sf_Shared*.

Once you start it, you can log in with the user name `Ubuntu` (it is the one that comes up) and the password `ubuntu` (note the initial "u" is in lower case). Now you're ready to begin!

The first exercise is to use *nmap* to see what services the virtual machine `nmap1` is providing. The IP address of this system is 127.0.0.1, or you can refer to it by name as "localhost".

Use the command:

```
nmap -p1-1024 localhost
```

to see what servers are running on the ports numbered 1 to 1024 inclusive.

What to turn in: Turn in a ".zip" or ".tgz" file of the output of your command and the contents of the file *nmap1-submit-me* in your home directory. Call the file "part1.zip" or "part1.tgz".

Part 2

You can also use *nmap* to see what servers are running on other systems, too — which is exactly what attackers do. ***Never do this to another system without the permission of the system manager; otherwise you can, and usually will, be mistaken for someone who is trying to break into the system.***

To do this, we have to set up the networking within VirtualBox. First, go to the VirtualBox preferences (*not* the settings for any system!), click on *Network*, then on the green icon with the plus sign at the right. A network called "NatNetwork" should appear. Click *OK*.

When you start the virtual machines, look at the bottom right, and you will see an icon with 2 screens. Click on that; it's the network setting. Click on *Network Settings*, then in the *Attached to:*, choose "NAT Network". Click *OK*.

You will need to get another virtual machine, `nmap2` (*nmap2.ova*). Like *nmap1.ova*, this is a big file (about 3.15 gigabytes), so it's best not to do this on a slow link. Once you download it and start it, you can log in with the user name "Ubuntu" and the password "ubuntu" (the same as for `nmap1`).

Now, you are to determine what servers are running on `nmap2` from your login on `nmap1`. To do this, you need to get the IP address of `nmap2`. Log on to the `nmap2` virtual machine (same account name and password as for `nmap1`) and open up the command prompt. Type the command

```
ifconfig -a
```

to `nmap2`'s command prompt. This command may take a few minutes to run, so be patient. When it finishes, look for the section labeled `enp0s3`. The IP address you want is in that section, next to the label `inet addr`.

The next step is to use *nmap* to see what services the virtual machine `nmap2` is providing. Take the same commands you used in part 1, replace the IP address or name (127.0.0.1 or "localhost") with the IP address you just found (call it *ip-address*).

What servers are running on the ports numbered 1 to 1024 inclusive?

Next, see if *nmap* got the list correct. Log into `nmap2` and run the same commands as you did in Part 1. Are the lists the same as what you got for part 2?

What to turn in: Label your lists as from `nmap1` and `nmap2`. Turn in a ".zip" or ".tgz" file of both lists and the contents of the file *nmap2-submit-me* in your home directory. Call the file "part2.zip" or "part2.tgz".

Part 3

Now that you have the IP address of `nmap2`, we're going to use *nmap* to determine what operating system is running on `nmap2`.

First, log back into `nmap1`.

Use the command:

```
nmap -O nmap2-address
```

where *nmap2-address* is the IP address of `nmap2` that you found in part 2.

Now log onto `nmap2` and see if it got the operating system correct. Type the command

```
uname -a
```

Did *nmap* get it right?

What to turn in: Turn in the output from *nmap*. Call the file "part3.txt" or "part3.pdf".