Lab Exercise 4

Due: June 3, 2021 **Points:** 100

This laboratory exercise has you use a network probing tool called *nmap* to see what services a host is running, along with some other information. *nmap* is on the CSIF, so we will begin with those systems. The documentation is available online, at `https://nmap.org/docs.html`; please refer to it as needed.

Do not run *nmap* against a host unless (1) you have permission of the system managers; or (2) you are the system manager. We have obtained the permission of the CSIF manager, the College of Engineering security team, and the campus security team for these exercises, so as long as you run *nmap* with the source and target as described below, you will not be violating any rules.

For this set of exercises, you will need to log into two CSIF systems. Please use pc12.cs.ucdavis.edu and pc13.cs.ucdavis.edu. If they are not up, use pc22.cs.ucdavis.edu and pc23.cs.ucdavis.edu; then if needed, pc32.cs.ucdavis.edu and pc33.cs.ucdavis.edu. If none of those pairs are up, pick any 2 CSIF systems.

Hosts on the Same Subnet

On the CSIF, log into your two systems. We'll use pc12 and pc13, but if you use different systems, replace the names accordingly.

Step 1

On pc13, run the command

```
nmap localhost
```

and then

```
nmap pc13.cs.ucdavis.edu
```

1. Are there any different services in the output? If so, what are they, and why do they occur?

By default, *nmap* looks only at common ports. The option `-p` allows you to specify which ports to look at. The forms are a comma-separated list of ports or a range. If the beginning of the range is omitted it is 1, the first port; if the end is omitted, it is 65535, the last port. So the following command checks all the ports.

```
nmap -p- localhost
```

Execute it and compare the output to that of "nmap localhost".

2. Do they report different services and if so, how and why do they differ?

Step 2

Next, look at probing another system. From pc13, run

```
nmap pc12.cs.ucdavis.edu
```

Then on pc12, run

```
nmap localhost
```

and then

```
nmap pc12.cs.ucdavis.edu
```

3. Are there any different services in the output? If so, what are they, and why do they occur?

Hosts on Different Networks at UC Davis

The above tests were all run on the same subnet. Now we will experiment with hosts on 2 different networks. For these experiments, there is a firewall between the two networks; this will affect how *nmap* runs.

Step 1

On pc12, run:

```
nmap nob.cs.ucdavis.edu
```

You will notice that some ports are labeled "filtered".

4. What does that mean?

Step 2

The *nmap* option `-A` provides information about the servers, including version number and associated data. Please use it to scan nob.cs.ucdavis.edu (warning: it may take as long as 5 minutes, so be patient).

5a. What version of *ssh* is nob.cs.ucdavis.edu running?
5b. What programs are running as the servers for SMTP and HTTP, and what are their version numbers?
5c. What operating system is nob.cs.ucdavis.edu running?

Repeat this for the system noevalley.cs.ucdavis.edu.

6a. What version of *ssh* is noevalley.cs.ucdavis.edu running?
6b. What other server(s) is noevalley.cs.ucdavis.edu running, and what are their version numbers?

Hosts Crossing the UC Davis Boundary

Now let's see what happens when a probe crosses a network boundary. We'l also try a couple of options that you can't use on the CSIF because you have to be *root* or the administrator to run them. So you will need to use *nmap* on on a system where you do have those privileges (in what follows, this system will be called "your system").

If you need to install it, download it from `https://www.nmap.org` and follow the instructions.

There are different ways to scan a system. The first is to attempt to open a TCP connection to the port on the host. This does not require *root* privileges, and the option is `-sT`. Execute the command:

```
nmap -sT nob.cs.ucdavis.edu
```

Compare this result with the result of step 1 of the previous section.

7. Do the two report different services? If so, how? Look at the state column in particular.

Many services are UDP-based, such as DNS and DHCP. The option `-sU` sends a UDP packet to the port. The reply tells *nmap* about the state of the port. As it writes directly to the raw network socket, *root* privileges are required. Execute this command.

```
nmap -sU nob.cs.ucdavis.edu
```

Warning: it will be slow. If you get a response that nob.cs.ucdavis.edu seems down, run the command with the additional option `-Pn`. When *nmap* starts a UDP scan, it pings the host to maki sure it is up. The `-Pn` option says to skip that check. You may see some messages about "Offending packet". You can ignore these.

8. The state of the syslog server is given as "open—filtered". What does this mean?

Another probe sends malformed TCP packets to ports and determines their possible states from the response. The option `-sX` causes three TCP flags (FIN, URG, PSH) to be set; such a packet is commonly called a "Christmas tree packet". Execute the following command:

```
nmap -sX nob.cs.ucdavis.edu
```

9. Compare the results of this with the results from the first scan in this step. Why are the states of the services shown differently?

Finally, look at the actual packets. Start *wireshark* and use the following filter:

```
ip.addr==169.237.6.105&&ip.addr==your IP address
```

Execute the command

```
nmap -r -p1-1024 nob.cs.ucdavis.edu
```

10. What port does your system send the SYN that nob.cs.ucdavis.edu receives on ports 1 and 2? With what packets does nob.cs.ucdavis.edu respond? Enclose a screen shot to show this.