CSci 4271W (011 and 012 sections) Lab Instructions

Lab 8 **March 24th, 2025**

Ground Rules. You may choose to complete this lab in a group of up to three students. Before you leave the lab, **make sure you have submitted to Gradescope, you included all group members on the submission, and the autograder found all required files!**

1 `nmap`

In today's lab, we'll see a powerful network scanning tool, `nmap`. Nmap is used by administrators to scan networks for services that shouldn't be running, misconfigured firewalls and gateways, and other anomalies. It is also used by penetration testers to find possible entry points into a network and identify potential vulnerabilities to target, and of course some malicious hackers could do the same. For this reason, its use on networks that you don't have permission to scan can be seen as an attack by some network administrators. (So don't go around scanning other people's networks with `nmap`.)

2 Installing `nmap`

Once you've logged in to your VM, you can install nmap (and another utility we'll use) in your VM by running the following command:

```
$ sudo apt-get install nmap pcregrep
```

This will download about several packages and may take a minute to finish. Once it does, we're ready to start using nmap.

3 Nmap modes

3.1 Hostname scanning

One of the simplest capabilities nmap has is to find the host names for a block of IP addresses. This is accomplished using the `-sL` flag; let's use it find out what the hostnames are for other IP addresses related to the Walter B28 lab. First we can find out the IP address for a machine in the lab using `host`: (if you want, you can replace the `07` with the number of the machine you're sitting at, or you can use `dig` instead of `host`, as in Homework 4, to see more DNS details)

```
$ host csel-wb28-07.cselabs.umn.edu
```

The result will give a 4 byte IP address, something like `134.84.xxx.yyy`. We can guess that the other machines in the lab have the same value of `xxx` but different values of `yyy`. Let's ask nmap to find out all of the hostnames that start with the same first 24 bytes, and redirect the output to the file `csel-hostnames` as follows:

```
$ nmap -sL -oN csel-hostnames 134.84.xxx.0/24
```

(Substitute the correct value for `xxx`) Here the `-sL` option is asking nmap just to list hostnames, and the `-oN csel-hostnames` argument is asking nmap to write its output in (`N`)ormal format to the file `csel-hostnames`, and the argument `134.84.xxx.yyy/24` is telling nmap to scan all of the IP addresses matching the first 24 bits of `134.84.xxx.yyy`. (So we will be scanning $2^{32}/2^{24} = 2^8 = 256$ addresses. If we wanted to scan everything matching the first 23 bits, what would we replace? How many addresses would be scanned?)

We can find just the other hosts in Walter B28 by `grep`ing this output for the string `wb28`:

```
$ grep wb28 csel-hostnames
```

And we can make a file containing just the IP addresses for these hosts using a regular expression as follows:

```
$ pcregrep -o1 'wb28.*\((.*)\)' csel-hostnames > wb28-ips
```

If you open this file with, e.g. `less`, you'll see a list of IP addresses.

3.2 Liveness scanning

Another simple but useful tool `nmap` supports is "liveness" scanning, using the `-sn` option. Run the following command to see which of the lab workstations are currently running:

```
$ nmap -sn -iL wb28-ips
```

Here the `-iL wb28-ips` option is telling nmap to scan the list of hosts in the `wb28-ips` file. What is the output telling you?

3.3 Port scanning

Nmap's primary purpose is "port scanning", to find out which ports and services might be running on a (list of) host(s). As the introduction mentioned, many network administrators consider port scanning to be an attack on their network, so you should never run a port scan against a machine you're not authorized to contact. In today's lab we will scan the machines we're using for the lab, our VMs, and the OIT proxy server. You might find it useful to be able to do a port scan for later labs or homeworks. But you should not run around port scanning the Internet, or any network without permission.

3.3.1 Scanning specific ports

Nmap has a variety of options for scanning a target host. Options that start with `-s` specify a "type" of scan: e.g. `-sS` for `SYN` packets, `-sT` for TCP connect, and `-sU` for UDP; `-sX` is a "stealth scan" option as well. In addition to the type of scan, we can specify which *ports* to scan with the `-p` option. Ports can be specified by their "typical" service names (e.g., `ssh`, `http`, `dns`) or numerically, and ranges can be specified with dashes (e.g. `1-15`) and joined with commas (such as `20-30,80-127` or `ssh,dns,http`). Let see some examples.

- Test whether NTP (the network time protocol) is running on your VM with the command:

```
$ sudo nmap -sU -p ntp localhost
```

- Test whether the ssh or http ports are open on a lab machine (from your VM) by picking some value `xx` in 01-27 and entering the command:

```
$ sudo nmap -sS -p ssh,http csel-wb28-xx.cselabs.umn.edu
```

3.3.2 Operating system detection

Nmap can also guess what OS a host might be running, using the `-O` option (there are sub-options for how "aggressively" nmap should attempt to probe this, see `man nmap` for more details). Let's see what OS nmap thinks is running on the same machine:

```
$ sudo nmap -O csel-wb28-xx.cselabs.umn.edu
```

3.3.3 Service version, traceroute, and output formats

Nmap can also try to guess what *version* of services like ssh, http, etc are running on a host, and trace the network-layer route to a host; using the `-A` option will tell nmap to do all of these things at once. Nmap will also produce a variety of output formats (some of which are easier to consume programatically); we can get (`A`)ll of the output formats using the `-oA prefix` option. Let's scan the proxy our VMs use to talk to the rest of the internet:

```
$ sudo nmap -A -oA proxy proxy.oit.umn.edu
```

This will take 2-3 minutes and produce files named `proxy.{xml,nmap,gnmap}`. Take a look at each of these with `vim` or `less`.

Nmap has one more "fun" output format: (`S`)cript-kiddie, or `1337`-speak. See what it looks like by doing a connect scan of the proxy:

```
$ nmap -oS proxy.sk proxy.oit.umn.edu
```

L0l l00k @ th3 pr0xy.$k f|l3 1n l3ss.

3.4 All done!

Once you've laughed at the script kiddie format, you're done with Lab 8! Use `scp` to copy the `proxy.xml`, `proxy.nmap`, `proxy.gnmap` and `proxy.sk` files off of your VM, so you can submit these files to the Lab 8 assignment on Gradescope. Make sure you include all of your group members in the submission!

Once you've submitted the files, the autograder will test to make sure the proper files were submitted, check that they include the right information, and notify you if any files were missing, within a few minutes.

Congratulations, you've finished Lab 8!