Lab 3

Mohammed and I added a subnet over spring break, your job is to find out what's there. You'll be working from Ba (remember to ssh to Alef and then to Ba) using your newly acquired root priveleges on that machine. ICMP is dropped by the firewall between Ba's subnet (10.0.0.0/24) and the new subnet (192.168.33.0/24), and the connection between these two subnets is not so great, *i.e.*, there is a lot of packet loss, so you'll need to use more targeted scans and some of the more advanced features of nmap (see, our tuntap setup is a feature, not a bug ;-). Before you get started, here's a few things to keep in mind:

- Don't trust what nmap tells you, *especially when packet loss is high*. If you think nmap might have missed an open port or a machine that should be there, try it again.
- Try, if possible, to do your tests when not a lot of other people are logged into Ba and working on this lab (you can type the command “w” to see who else is logged in and what they're doing). Network congestion may become a problem, it's already an issue with only one person logged in and doing nmaps. Don't be shy about working on your lab, but if packet loss seems to be making your results inaccurate and half a dozen people are logged in, consider trying again later.
- Scan for specific ports. Due to the packet loss rate on shasta's virtual networks, a vanilla nmap scan of the basic Nmap 101 variety is going to take forever and probably miss everything.
- If you see open ports, chances are other machines on the subnet also listen on that port.
- Don't assume machines aren't there because you did one kind of scan and nmap says nothing's there except for the machines it found open ports on. Some firewall rules drop SYN packets destined for particular machines that aren't servers, for example. Nmap has other types of scans besides ICMP and SYN packets. Consider SYN/FIN or Christmas scans, for example.

To get you started. here is an example command to scan every IP address from 192.168.33.0 to 192.168.33.255 on port 80 using a SYN scan (`-PN` disables ping, which you'll want to do in general since ICMP packets are filtered), with DNS disabled (`-n`, you should always do this since DNS is not setup on Ba and allowing reverse DNS queries will cause nmap to hang for a while), and to give you verbose output (`-vvv`) and write the results in grepable format (`-oG`) to the file openport80.log.

```
sudo nmap -n --scan-delay 1s -vvv -PN -p80 192.168.33.0/24 -oG
openport80.log
```

Since all machines on the subnet are between 192.168.33.2 and 192.168.33.100, you can speed up your scan by replacing 192.168.33/0/24 with 192.168.33.2-100.

Here is a command that does “the works” (`-A`) on Alef, which includes service detection, NMAP scripting engine, OS detection, *etc*.

```
sudo nmap -n -PN -A 192.168.254.2
```

I'll send an email with some resources about Nmap, you can also find out a lot from “man nmap”. There is at least one web server and one BSD server that is running SSH on the 192.168.33.0/24 subnet, finding those is a good place to start. Here are questions you should be able to answer in your blog posts:

What are the IP addresses of all machines on the subnet? How many are there (if you think you've found them all, e-mail me to confirm rather than wasting your time looking for more since there really aren't that many)?

What kind of BSD distribution is the BSD server running (e.g., OpenBSD? FreeBSD? NetBSD?)? Can you tell me the exact version?

What other ports is the web server listening on besides the HTTP port 80? What else can you tell me about the web server?

Are there any other machines on the subnet besides these two servers? What can you tell me about that/those machine/machines and the firewall rules that protect it/them? Is it likely intended to be a server or a client?

If you've answered all of these questions, then try to find something that nmap can tell you about shasta's virtual environment that will surprise me (as in, I'll be surprised that nmap can do that, though if you tell me something about shasta itself that surprises me that's even more of a bonus). Nmap has a lot of features, I'm sure if you play with it you can tell me something about my firewall rules, about how packets are routed, or about how to make the scanning more efficient that I don't know, and the input will be much appreciated. **You will be expected to blog about nmap for at least two weeks in a row so if answering the basics doesn't keep you busy, read up and experiment a bit.**

You should answer all the questions above and tell me other information you find in your blog posts, and you should be done with this lab by March 8th, when I plan to assign lab 4.