Local Network Audit with Nmap

Larsen Close[*a]*

[a]*Computer Science, Metropolitan State University, Denver, CO*
Student: lclose@msudenver.edu

ABSTRACT
Extensive Nmap scanning to fingerprint a local network is demonstrated and areas of interest are identified. Anomolies, security concerns and unexpected results prompt further investigation. Actions taken upon the basis of the findings are then discussed.

MOTIVATION
We often only pay attention to our internet connected devices when we lose connectivity. We then try and restore the connection as quickly as possible. The truth is that as the Internet Of Things expands and our world increasingly digitizes the danger of these devices to our safety, privacy and security increases. The steps clearly demonstrated in this paper are steps everyone should take regulary on their home network for their sake and for their families sake.

INTRODUCTION
I started fingerprinting my network with a few areas of heightened interest. In order to ensure a thorough investigation I first used widespread scanning and looked for abnormalties, anything which surprised me or that raised security concerns. I made sure to turn on and log into every device on the network before conducting the scans. Also in order to asses the behavior of a new automated system for the door lock and thermostat, mandated by the poperty owner, I connected to the network for the first time. The device has been running on cellular connection but has both options.

How does Tails handle local traffic?
To research the local network scan response of Tails, The Amnesic Incognito Live System (a security-focused Debian based distribution of Linux) I booted a machine with the live system during the scans. Starting with cursory scans and increasing the intensity each time while saving the results allowed for a detailed fingerprint of the local network.

Let shodan.io scan for you
To gain information about my public IP address and check for any outward facing access I used shodan.io. After using their search function I created a monitor with triggers to notify me of any any unexpected activity. After scanning extensively I created the graphs below to organize the findings, visualize them and decide upon which areas to increasingly focus. Host data from the scans is combined with DHCP Reservations from the routers to verify the identity of devices and fill gaps left by scans.

METHODS AND MEASUREMENT
To begin scanning we needed to know which IP addresses to tell nmap to scan. Using the command:

```
ifconfig | grep broadcast
```

We determined the local networks and the subnet ranges. As can be seen in **Figure 1**, the networks are `10.0.0.0/24` `192.168.0.0/24`. The `netmask 0xffffff00` tells us the range for hosts is limited the last octet, digits 1-254.

Figure 1. First the command 'ifconfig | grep broadcast' identifies the local networks.

Super user privileges for scanning

Next I ran a ping scan of both networks to quickly get a list of the hosts. It's likely that you will not get a full list if you do not run this command with super user privileges. Testing this without the sudo command resulted in 1 host and 9 hosts respectively. To run ping scans for both networks we used commands:

```
sudo nmap -sn 192.168.0.0/24
sudo nmap -sn 10.0.0.0/24
```

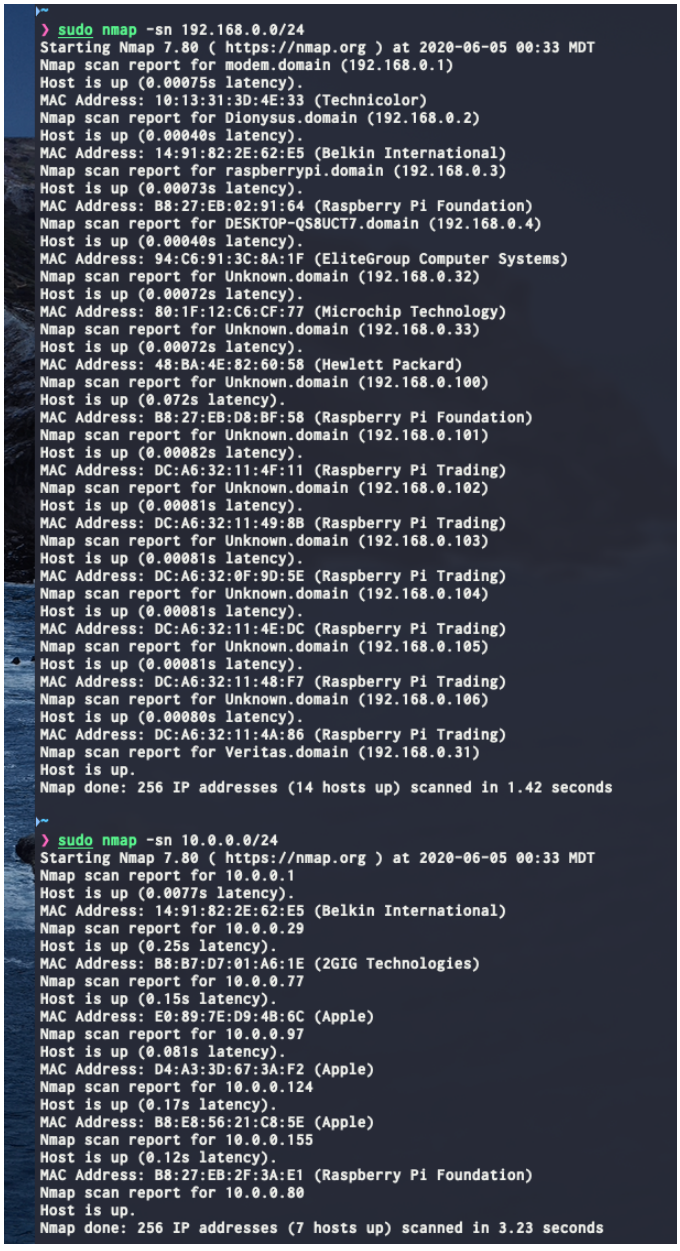

Figure 2. A ping scan of both networks returns a list of 14 and 7 hosts.

As we can see in **Figure 2**, the ping scan with sudo returned a list of 14 hosts and 7 hosts respectively.

Nmap flags for more thorough scans

After completing the quick and simple ping scan we scanned both networks using nmap with the flag `-A` to initiate an agressive scan. We also included `-v` to increase the verbosity of our results and `-T5` to turn the scans speed all the way up. The commands used here:

```
sudo nmap -T5 -A -v 192.168.0.0/24
sudo nmap -T5 -A -v 10.0.0.0/24
```

At this point it was necessary to create **Table 1** to organize the results and create an overview that could actually be visualized. These types of scans return so much information that it demands systematic organization. Zenmap can do a good job of helping with this but it has not been running well for me on macOS Catalina. Another option which I employed is to use an additional flag when running nmap `-oX 'scan-%T-%D.xml'` which outputs the scan in xml format named by the date and time. To give some full examples:

```
sudo nmap -oX 'scan-%T-%D.xml' -T5 -A -v 192.168.0.0/24
sudo nmap -oX 'scan-%T-%D.xml' -T5 -A -v 10.0.0.0/24
```

Checking and monitoring public IP addresses with shodan.io

Due to the ethical and legal restrictions on scanning the public IP owned by Century Link I used shodan.io to search for my IP and set up a monitor for the address. An easy what to determine your public IP address is with command:

```
curl ifconfig.me
```

RESULTS

To begin with, shodan.io allowed us to determine that our router has an open outward facing port. It is running http with authentication. **Figure 3** shows a screen shot from their webservice.

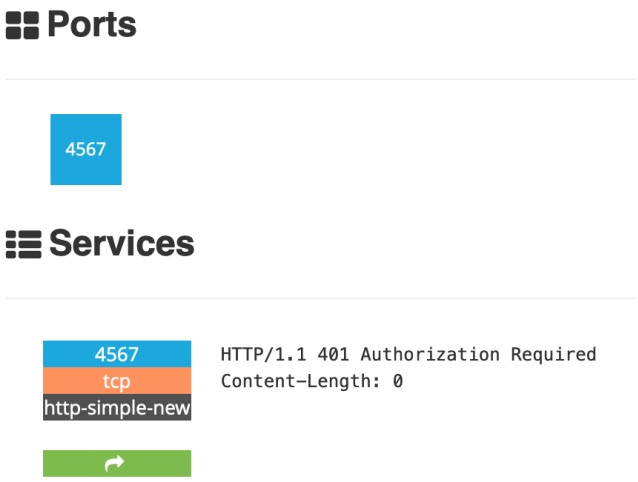

Figure 3. From website https://www.shodan.io/ often called "the most dangerous search engine in the world"

Compiling all of the findings

The table below, **Table 1**, is a compilation of all the scans. The aggressive scans discovered more hosts missed by the privileged ping scan. Immediately some interesting things are visible from the table. First, my HomePod has two IP addresses on the same network. After logging into and checking the router it appeared that both were running on the 5G wifi. Nmap guessed the

	Hostname	Device	Purpose	OS	Open	Filtered	Services
10.0.0.001	Dionysus	Router	Gateway	-	53,80,443,10000	-	ssl,http
10.0.0.029	HD100	Webcam	Security	-	554,49152	-	rtsp,UPnP
10.0.0.077	Daemon	HomePod	Music	audioOS	62078	24 dif	c
10.0.0.080	Veritas	MacLaptop	PC	macOS	3000	c	c
10.0.0.097	Daemon	HomePod	Music	audioOS	6 dif	100 dif	wiretap
10.0.0.124	Mercury	Watch	Fitness	watchOS	c	17 dif	wiretap/tracke
10.0.0.155	raspberrypi	rpi	dev	Buster	22	-	ssh
192.168.0.001	Century Link	Router	Gateway	-	23,80,433,8085	-	telnet
192.168.0.001	Century Link	Outward	Outward	-	4576	-	auth http
192.168.0.002	Dionysus	Router	Secondary	-	All	-	-
192.168.0.003	raspberrypi	rpi	dev	Buster	22	-	ssh
192.168.0.004	DESKTOP-QS8UCT7	WindowsPC	PC	Windows	-	All	-
192.168.0.031	Veritas	MacLaptop	PC	macOS	3000	-	grafana
192.168.0.032	Unknown	?	80:1f:12:c6:cf:77	Linux	22	-	ssh
192.168.0.033	Unknown	HPLaptop	tails	tails live	-	All	-
192.168.0.100	Ares	rpi	motion	Buster	22,3389,8081	-	xrdp,motion
192.168.0.101	Master	rpi	Kubernetes	Buster	22,80,443	-	-
192.168.0.102	Node1	rpi	Kubernetes	Buster	22,80,443	-	-
192.168.0.103	Node2	rpi	Kubernetes	Buster	22,80,443	-	-
192.168.0.104	Node3	rpi	Kubernetes	Buster	22,80,443	-	-
192.168.0.105	Node4	rpi	Kubernetes	Buster	22,80,443	-	-
192.168.0.106	Node5	rpi	Kubernetes	Buster	22,80,443	-	-

Table 1. The table itself should be centered. The table title In AJUR goes below the table and ends with a period. Please bold column and row titles.

CONCLUSIONS

Describe major outcomes, novelty, and significance of your work. Future work may be noted.

NOTES ON REFERENCES

Use no indents. Follow the style given in the examples (journals and serial publications;[1] chapters and monographs;[2] web sources,[3] correspondingly) below. All references in text must be in order of appearance. Please include all authors, the complete title, and inclusive pagination, *e.g.*, 1234–1237, not 1234–7; please make sure to use en-dash (in LaTeX, use --) and not the regular dash or em-dash to indicate duration between page numbers or years. The publication year should follow authors in parentheses. Supply DOI numbers whenever possible. *Book titles* and *web sites* are italicized. *Titles of journals* should be abbreviated according to http://www.abbreviations.com/jas.php. **Reference accuracy is critical. It is authors responsibility to carefully check each reference.**

In the text, separate superscripted numbers by comma and space,[1, 2] they should be separated by an en-dash if the consecutive list of more than two numbers is used.[1–3] List them AFTER punctuation (be it comma or period) with no

space.

REFERENCES

1. Marquez, V., Frohlich, T., Armache, J. P., Sohmen, D., Donhofer, A., Mikolajka, A., Berninghausen, O., Thomm, M., Beckmann, R., Arnold, G. J., and Wilson, D. N. (2011) Proteomic characterization of archaeal ribosomes reveals the presence of novel archaeal-specific ribosomal proteins, *J Mol Biol* 405, 1215–1232. *https://doi.org/10.33697/ajur.2019.003*
2. Fierke, C. A., and Hammes, G. G. (1996) Transient Kinetic Approaches to Enzyme Mechanisms, in *Contemporary Enzyme Kinetics and Mechanism* (Purich, D., Ed.) 2nd ed., 1–35, Academic Press, New York.
3. Agricultural Research Service, U.S.D.A. National Nutrient Database for Standard Reference, Release 26, *http://ndb.nal.usda.gov/ndb/search/list* (accessed Mar 2014)

REFLECTION

Please rewrite your abstract so that it captures in few sentences the scope and focus of your publication but could be easily understood by the general public and hopefully shows why your work is exciting and important.

Once done, review these guidelines and the entire document. Make sure that images are exactly where you want them, not at the end of the text. Insert page brakes to avoid orphan titles, words, or sentences being separated out at the end or the top of a page. If any questions remain, please e-mail editor@ajuronline.org.

When you are ready to submit your article, use the share button above and send the read and edit link.