

**Prerequisites:**

1. Review Week 6 discussion of virtualization and virtualized networking (slide content).
2. Review Week 6 discussion and working knowledge of Linux commands (slide content and tutorials).
3. Kali Linux Virtual Machine or Kali Natively Installed  
Note: If you have difficulties using Kali, you can download NMAP and install it on any modern operating system natively.
4. You need to be connected to some network. Home networks are perfect for this.

**Objectives:**

The main purpose of this week's exercise is getting started with Kali, understanding NMAP, and showing how it can be used for basic reconnaissance.

**Call for Help:**

Do your best to try the tasks below, if you're confused, or need help, feel free to email or text me at any point and I will gladly try to help you. If you're having an Issue, chances are, other people are as well, and I can update the instructions/comments/add content as necessary.

**Background:**

Nmap (Network Mapper) is a free and open-source security scanner, originally written by Gordon Lyon, used to discover hosts and services on a computer network, thus building a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host(s) and then analyzes the responses.

**Tasks:****Fundamentals/Setup:**

1. If you're using a virtual machine, make sure your Virtual Machine is in Bridged Mode.  
*Note: Recall that you may need to restart your virtual machine for things to take effect.*
2. Confirm your Virtual Machine and Physical Machine have different IP Addresses (**ipconfig** on most windows variants, and **ifconfig** on your Kali Linux Virtual Machine)
3. Confirm you can ping a well-known URL or IP Address.

**Deliverable:** Provide a screenshot of the ping.

```
root@kali:~# ping 139.130.4.5
PING 139.130.4.5 (139.130.4.5) 56(84) bytes of data.
64 bytes from 139.130.4.5: icmp_seq=1 ttl=118 time=251 ms
64 bytes from 139.130.4.5: icmp_seq=2 ttl=118 time=250 ms
64 bytes from 139.130.4.5: icmp_seq=3 ttl=118 time=250 ms
^C
--- 139.130.4.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 250.656/250.826/251.019/0.149 ms
root@kali:~#
```

4. Recall you can learn about Nmap if you have any challenges using the linux command **man nmap**. Feel free to look over nmap's options. Use Page Up/Down to scroll through the many options.

#### Finding Hosts on Your Network:

1. **REVIEW THIS ENTIRE TUTORIAL ON IP ADDRESSES AND SUBNETTING (Introduction to Conclusion). You need to understand how IP Addressing works.**

<https://www.techopedia.com/6/28587/internet/8-steps-to-understanding-ip-subnetting>

2. Use the command `nmap -sn <Network>` to identify hosts on your network.

*Note: As an example, my home network is 192.168.1.XXX, where XXX changes for every device I have. To find 192.168.1.0 to 192.168.1.255 I would use **nmap -sn 192.168.1.0/24***

Provide a screenshot of what you found.

```

root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-25 02:27 EDT
Nmap scan report for FIOS_Quantum_Gateway.fios-router.home (192.168.1.1)
Host is up (0.00036s latency).
MAC Address: 48:5D:36:D0:E7:5F (Verizon)
Nmap scan report for Commander.fios-router.home (192.168.1.22)
Host is up (0.00014s latency).
MAC Address: 30:9C:23:DF:DE:3A (Micro-star Intl)
Nmap scan report for android-d81effe03b3cc1fc.fios-router.home (192.168.1.23)
Host is up (0.099s latency).
MAC Address: 70:05:14:7E:66:B0 (LG Electronics (Mobile Communications))
Nmap scan report for android-bf755bf772ef4e33.fios-router.home (192.168.1.183)
Host is up (0.100s latency).
MAC Address: D0:13:FD:63:A1:80 (LG Electronics (Mobile Communications))
Nmap scan report for amazon-7157a3134.fios-router.home (192.168.1.186)
Host is up (0.098s latency).
MAC Address: 68:54:FD:95:B3:C8 (Amazon Technologies)
Nmap scan report for 192.168.1.217
Host is up (0.089s latency).
MAC Address: D0:04:01:12:A7:6B (Motorola Mobility, a Lenovo Company)
Nmap scan report for 192.168.1.233
Host is up (0.11s latency).
MAC Address: 04:03:D6:DA:4F:4E (Nintendo)
Nmap scan report for HP6DE6FF.fios-router.home (192.168.1.236)
Host is up (0.11s latency).
MAC Address: 5C:B9:01:6D:E6:FF (Hewlett Packard)
Nmap scan report for Skylar-PC.fios-router.home (192.168.1.253)
Host is up (0.032s latency).
MAC Address: F8:63:3F:80:DA:A4 (Intel Corporate)
Nmap scan report for kali.fios-router.home (192.168.1.26)
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 2.93 seconds
root@kali:~#

```

**Question:** What do you notice about the types of devices? Did nmap associate a MAC address to a Vendor?

Devices are listed with the Network ID with the router name attached to the end of the name. MAC addresses were associated and given with a known product name

- How it works: The Nmap option `-sn` disables port scanning, leaving the discovery phase enabled, which makes Nmap perform a ping sweep. Depending on the privileges, Nmap by default uses different techniques to achieve this task: sending a TCP SYN packet to port 443, TCP ACK packet to port 80 and ICMP echo and timestamp requests if executed as a privileged user, or a SYN packets to port 80 and 443 via the `connect()` syscall if executed by users who can't send raw packets. ARP/Neighbor Discovery is also enabled when scanning local Ethernet networks as privileged users. MAC addresses and vendors are identified from the ARP requests sent during the ARP/Neighbor Discovery phase.

### Tracing Routes:

- Run the command `nmap -sn --traceroute google.com microsoft.com`

**What did you find:**

- How Many Hops?**

Google had 9 hops

Microsoft had 24 hops

- b. Were there other hosts associated with microsoft.com and google.com? If so, why is this the case?

The other hosts associated in both cases are most likely different Microsoft and google servers along with domain names claimed by Microsoft and google

- c. Anything else of interest?

Scanned using TCP to find that it went to new York and then London ("nyc30" to "lon30") then to Dublin servers ("dub07") presumably

### Finding Open Ports On a Given Host:

1. Run the command **nmap scanme.nmap.org**

#### Produce a Screenshot

- a. What ports are open?

22/tcp open ssh  
80/tcp open http  
9929/tcp open nping-echo  
31337/tcp open Elite

- b. What are the services likely for?

Ssh is secure shell used for encrypted wireless data transfer

HTTP is unsecure hypertext transfer protocol used for hosting web addresses

nping-echo is likely for pinging the site

Elite I assume allows for administrative privileges to this unsecure site

2. How it works: The basic default Nmap scan `nmap <target>` executes a simple port scan that returns a list of ports. In addition, it returns a service name from a database distributed with Nmap and the port state for each of the listed ports.

Nmap categorizes ports into the following states:

- a. Open: Open indicates that a service is listening for connections on this port.
- b. Closed: Closed indicates that the probes were received, but it was concluded that there was no service running on this port.
- c. Filtered: Filtered indicates that there were no signs that the probes were received and the state could not be established. It also indicates that the probes are being dropped by some kind of filtering.
- d. Unfiltered: Unfiltered indicates that the probes were received but a state could not be established.
- e. Open/Filtered: This indicates that the port was filtered or open but the state could not be established.
- f. Close/Filtered: This indicates that the port was filtered or closed but the state could not be established.

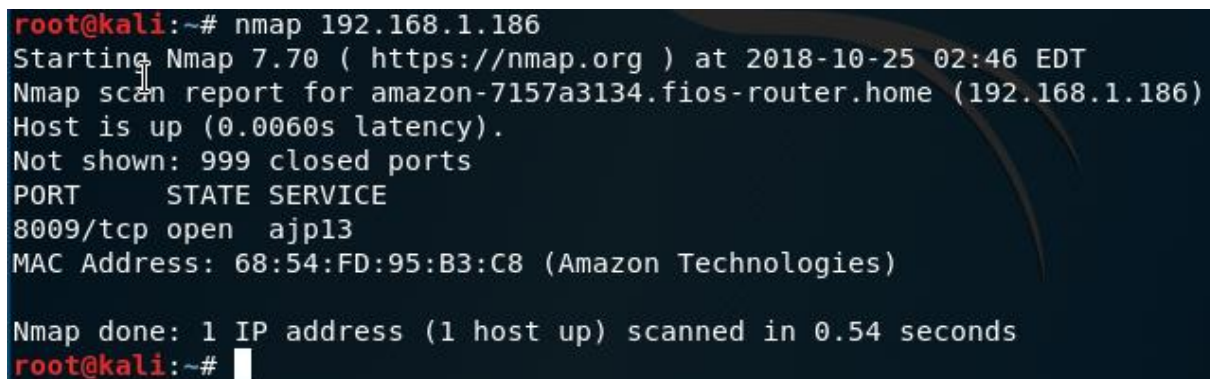
Even for this simplest port scan, Nmap does many things in the background that can be configured as well.

### Scan a friend:

1. Work with a friend, or utilize another computer or asset (google home, alexa, playstation, etc., etc.) you own.

2. Use NMAP to scan the host.

Provide a screenshot.



```
root@kali:~# nmap 192.168.1.186
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-25 02:46 EDT
Nmap scan report for amazon-7157a3134.fios-router.home (192.168.1.186)
Host is up (0.0060s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
8009/tcp  open  ajp13
MAC Address: 68:54:FD:95:B3:C8 (Amazon Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
root@kali:~#
```

- a. From a cybersecurity perspective, what did you learn? Are there any ports open, possibly vulnerable services, was it blocked by a firewall, etc.?

So this is an Amazon firestick. I chose this device because I recently ran a Nessus scan and found that, through Metasploit, I am able to gain remote access to this device using a Day Zero hack. From this I learn that 8009 is the open port likely that allowed remote access. This is the most vulnerable thing on my home network but for testing purposes I wanted to show my housemates how this worked. (Then promptly install a firmware update and block the device until further notice)

### Your Mission:

1. Discover hosts with a TCP SYN ping scan.

What command did you use?

```
nmap -sP -PS 192.168.1.0/24
```

2. Discover hosts with a TCP ACK ping scan.

What command did you use?

```
nmap -sP -PA 192.168.1.0/24
```

3. Discover hosts with a UDP ping scan.

What command did you use?

```
nmap -sP -PU
```

4. Discover hosts with a SCTP INIT ping scan.

What command did you use?

```
nmap -sn -PY
```

5. Discover hosts with a IP protocol ping scan.

What command did you use?

```
nmap -sP -PO
```

### Advanced Work:

Your mission, is to attempt to use nmap, and its geolocation scripts to find the physical location of a give IP. You can use a shodan IP Address (like a webcam). This will take some time, and I encourage you to figure it out.

```
root@kali:~# nmap 95.226.165.10
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-25 12:13 EDT
Nmap scan report for host10-165-static.226-95-b.business.telecomitalia.it (95.226.165.10)
Host is up (0.13s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
25/tcp    filtered  smtp
53/tcp    filtered  domain
80/tcp    open       http
```

Business.telecomitalia.it – probably means its in Italy

```
root@kali:~# curl https://api.hackertarget.com/geoiip/?q=95.225.165.10
IP Address: 95.225.165.10
Country: IT
State: Toscana
City: Empoli
Latitude: 43.684601
Longitude: 10.907600root@kali:~#
```

Here is a long and latitude for the address.

### Wrap Up/Additional Content/Required Watching:

Watch the DEFCON 13 video. Note it is from circa 2005.

<https://tinyurl.com/ya58tfwo>

