

## Using NMAP to scan networks

Virtual Box Kali Linux Bridge Mode

man nmap to see all of the documentation for the application.

nmap -A for OS Detection

Add -T4 for faster execution.

nmap -A -T4 (IP address) (CIDR)

**What are the letters called that we are adding to the command?**

First, use ip add to find your computer's network, and Kali Linux is on.

nmap -sn (network identifier/CIDR) will scan an entire network.

Your Linux Server firewall should be enabled.

```
sudo ufw enable
```

```
sudo ufw allow 20,21,22,990/tcp
```

nmap (your Linux Server address)

nmap -sV (yourLinuxserveraddress) [Service Versions]

searchsploit (name of the server)

```
sudo msfconsole
```

```
search service name for exploits
```

To map an entire network:

```
nmap -T5 -A -v network identifier/CIRD -oX network-map.xml
```

```
firefox network-map.xml
```

```
xsltproc ./network-map.xml -o ./network-map.html
```

```
firefox network-map.html
```