Carleton
Cyber
Security
Club

Week 1: Scanning

Where to Start?

```
crazyeights@superchicken: ~
File  Edit  View  Search  Terminal  Help
crazyeights@superchicken:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.182  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::e2d5:5eff:fea8:8422  prefixlen 64  scopeid 0x20<link>
        ether e0:d5:5e:a8:84:22  txqueuelen 1000  (Ethernet)
        RX packets 87149  bytes 99689352 (95.0 MiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 54751  bytes 11792330 (11.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xf7600000-f761ffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

crazyeights@superchicken:~$
```

ifconfig

ifconfig with no args displays the status of currently active interfaces.

Use inet address, and netmask to determine range of addresses to scan

Where to Start?

```
crazyeights@superchicken: ~
File  Edit  View  Search  Terminal  Help
crazyeights@superchicken:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.182  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::e2d5:5eff:fea8:8422  prefixlen 64  scopeid 0x20<link>
        ether e0:d5:5e:a8:84:22  txqueuelen 1000  (Ethernet)
        RX packets 87149  bytes 99689352 (95.0 MiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 54751  bytes 11792330 (11.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xf7600000-f761ffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

crazyeights@superchicken:~$
```

For Example:

inet: 192.168.0.182
netmask:
255.255.255.0

Gives the range:
192.168.0.0 -
192.168.0.255

Tools for Scanning networks and devices:

ping

Single Device:
 ping 192.168.0.182

The Entire Network: (Range 192.168.0.0 - 192.168.0.255)

for i in {0..255}; do ping -c 192.117.247.$i | grep ‘from’; done

Tools for Scanning networks and devices:

fping - a linux tool for ping sweeps

Syntax: (Range 192.168.0.0 - 192.168.0.255)

fping -a -g 192.168.0.0 192.168.0.255

Or using the netmask:

fping -a -g 192.168.0.0/24

Parameters:

-a - force tool to show only live hosts
-g - specifies ping sweep

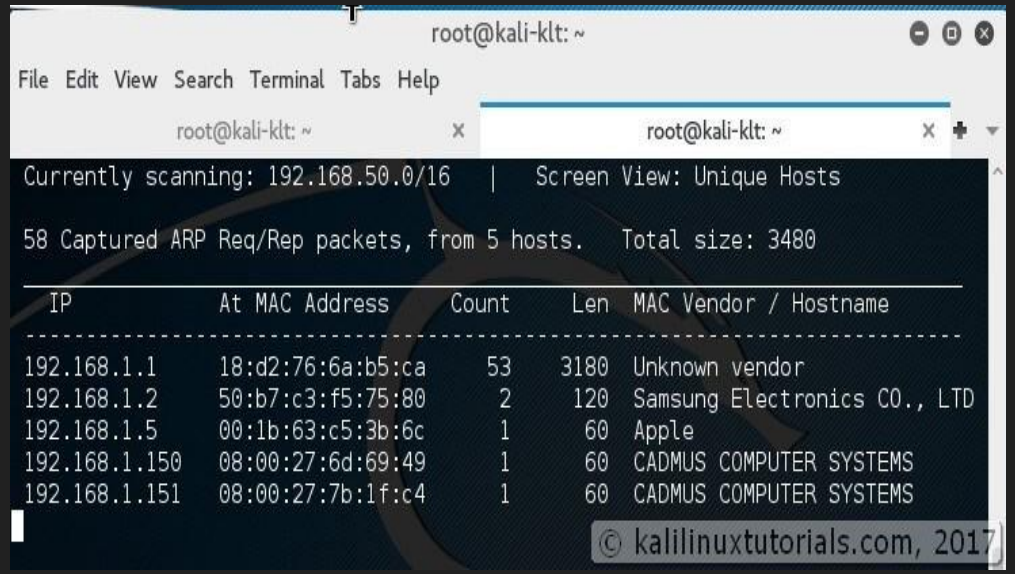
Tools for Scanning networks and devices:

Netdiscover - simple ARP Scanner to scan for live hosts in a network
Usage: For finding a device without knowing the IP (ie. a VM).

Syntax: (Range 192.168.0.0 - 192.168.0.255)

netdiscover -r 192.168.0.0/24

More:
https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/



Tools for Scanning networks and devices:

Masscan - fast, good for discovering open ports

Syntax: Device: 192.168.0.182

masscan -p1-65535, U:1-65535 192.168.0.182 --rate=500 -e eth0

More:

https://kalilinuxtutorials.com/masscan/

Tools for Scanning networks and devices:

Nmap

Some Examples: (Range 192.168.0.0 - 192.168.0.255)

Ping Sweep:

```
nmap -PS 192.168.0.0-192.168.0.255
```

Stealth Scan: (TCP services)

```
nmap -sS 192.168.0.182
```

Service Scan, with versions:

```
nmap -sV 192.168.0.182
```

Scan well known/top ports:

```
Nmap --top-ports 10 192.168.0.182
```

Tools for Scanning networks and devices:

Nmap

Some Examples: (Range 192.168.0.0 - 192.168.0.255)

Read from list:

```
nmap -iL /tmp/test.txt
```

Version and OS Detection Scanning:

```
nmap -v -A 192.168.0.182
```

Find out if host is protected by a firewall

```
nmap -sA 192.168.0.182
```

Scan a host when protected by the firewall

```
nmap -PN 192.168.0.182
```

Tools for Scanning networks and devices:

Nmap

Some Examples: (Range 192.168.0.0 - 192.168.0.255)

Show all packets sent and received:

```
nmap --packet-trace 192.168.0.182
```

Show interfaces and routes:

```
nmap --iflist
```

Scanning Specific Ports:

```
nmap -p [port] hostname
nmap -p T:80 192.168.0.182
nmap -p U:53 192.168.0.182
```

Combining Options:

```
nmap -v -sU -sT -p U:53, 111, 137, T:21-25, 80 192.168.0.182
```

Tools for Scanning networks and devices:

Nmap

Some Examples: (Range 192.168.0.0 - 192.168.0.255)

Fast Scanning:

```
nmap -T5 192.168.0.0/24
```

How to detect remote OS:

```
nmap -v -O --osscan-guess 192.168.0.182
```

Nmap TCP ACK(PA) and TCP SYN (PS) ping

(Firewall blocking ICMP pings)

```
nmap -PS 192.168.0.182
nmap -PA 192.168.0.182
```

Scan using IP Protocol ping

```
nmap -PO 192.168.0.182
```

Tools for Scanning networks and devices:

Nmap
Some Examples: (Range 192.168.0.0 - 192.168.0.255)

Scan using UDP Ping:
nmap -PU 192.168.0.182
Scan for UDP Services:
Nmap -sU 192.168.0.182
Scan firewall for security weaknesses using: -sF, -sN, and -sX
Scan for packet fragments: -f
Cloak scan with decoys:
nmap -n -Ddecoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip
nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5

Tools for Scanning networks and devices:

Nmap
Some Examples: (Range 192.168.0.0 - 192.168.0.255)

Scan for MAC Spoofing:
Spoof your MAC address

```
nmap --spoof-mac MAC-ADDRESS-HERE 192.168.1.1
```

Add other options

```
nmap -v -sT -PN --spoof-mac MAC-ADDRESS-HERE 192.168.1.1
```

Use a random MAC address
The number 0, means nmap chooses a completely random MAC address

```
nmap -v -sT -PN --spoof-mac 0 192.168.1.1
```

Tools for Scanning networks and devices:

Nmap

Source: https://www.cyberciti.biz/security/nmap-command-examples-tutorials/

Tools for Scanning networks and devices:

And More...