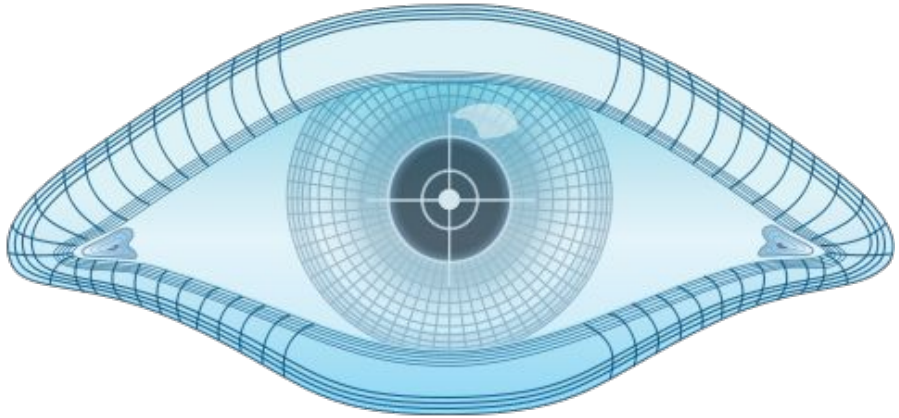
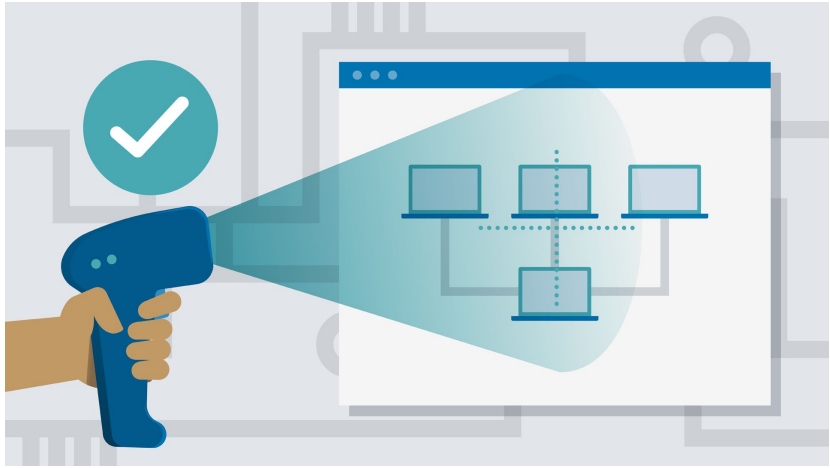
Who's Knocking?
A Brief Intro to Network Scanning



Greg Horie

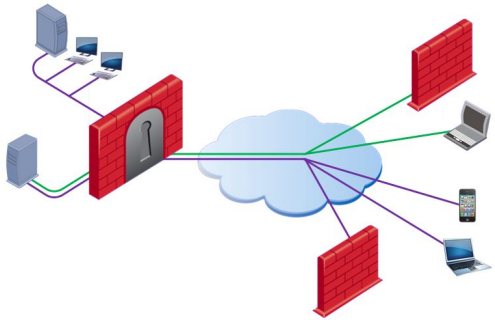
What is Network Scanning?

- A method for identifying active devices in a network
- Uses network protocols to signal devices and await a response
  - e.g. Sending a ICMP echo request (i.e. ping)
- Typically uses:
  - Security assessments
  - Discovery / Identification
  - Monitoring
- Nefarious uses are also common



Network vs. Vulnerability Scanning

- Network Scanning
  - Discover available network services running on the targeted hosts
  - Determine the operating systems (OSs) in use by assessing network responses
  - Helpful for troubleshooting and hardening a system
- Vulnerability Scanning
  - Scan system for weak spots
  - Preliminary step before attempting to compromise, crash or DoS a system
    - Attacks based on known vulnerabilities
- Today's focus will be network scanning
  - **Goal** - Understand how to protect your systems



Prep

Ubuntu 18.04

```
$ sudo apt update
$ sudo apt install -y wireshark netcat nmap
```

CentOS 7

```
$ sudo yum check-update
$ sudo yum install -y wireshark netcat nmap
```

Exercise - **`ping`** & capture

Setup:

```
$ sudo wireshark
```

capture on your wireless interface - e.g. wlan0

display filter: **`icmpv6 or icmp`**

Try:

```
$ ping -6 vicpimakers.ca
$ ping -4 vicpimakers.ca
```

`ping` & ICMP

- Is `ping` a network scanning tool?
- Why do we need it?
- What is ICMP (ICMPv6) ?
  - ICMP - **I**nternet **C**ontrol **M**essage **P**rotocol
  - The “admin assistant” of the Internet Protocol
  - Carries both informational and error messages
  - ICMP = Typical starting point for many network scan

Exercise - `traceroute` & capture

Setup:

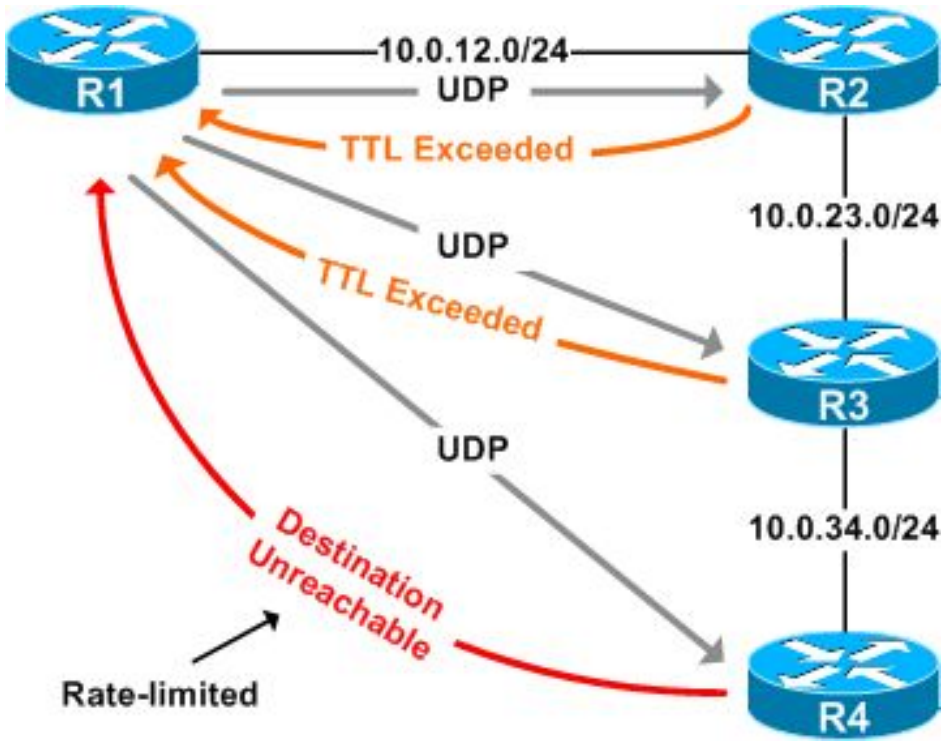
```
$ nslookup vicpimakers.ca
    # collect IPv4 and / or IPv6
$ sudo wireshark
    # again, capture on your wireless interface - e.g. wlan0
    # display filters:
        ip.addr == <IP> or icmp          # for IPv4
        ipv6.addr == <IP> or icmpv6      # for IPv6
```

Try:

```
$ traceroute -4 vicpimakers.ca -m 16
$ traceroute -6 vicpimakers.ca -m 16
```

`traceroute`

- Is `traceroute` a network scanning tool?
- Why do we need it?
- How does it work?
  - **TTL !**



Exercise - **`netcat`** & capture

Setup:

```
$ nslookup vicpimakers.ca
    # collect IPv4 and / or IPv6
$ sudo wireshark
    # again, capture on your wireless interface - e.g. wlan0
    # display filters:
        ip.addr == <IP>        # for IPv4
        ipv6.addr == <IP>      # for IPv6
```

Try:

```
$ nc -v -4 vicpimakers.ca 80
$ nc -v -6 vicpimakers.ca 80
```

`netcat` & TCP

- Is `netcat` a network scanning tool?
- Why do we need it?
  - Swiss army knife of network troubleshooting
- What did we illustrate in this exercise?
  - TCP 3-way handshake
    - Both session setup and teardown

Exercise - **`nmap`** host port scan

Setup:

```
$ nslookup vicpimakers.ca
    # collect IPv4 and / or IPv6
$ sudo wireshark
    # again, capture on your wireless interface - e.g. wlan0
    # display filter:
        ipv6.addr == <IP>    # for IPv6
        ip.addr == <IP>      # for IPv4
```

Try:

```
$ nmap -6 vicpimakers.ca
$ nmap -4 vicpimakers.ca
```

`nmap`

- Is `nmap` a network scanning tool?
- Why do we need it?
  - De facto standard for port scanning
  - Makes discovery easy
- What happened in this exercise?

Exercise - **`nmap`** subnet discovery

Setup:

```
$ ip -4 route    # record local IPv4 subnet
$ ip -6 route    # record local IPv6 subnet
$ sudo wireshark
    # any suggestions ?
```

Try:

```
$ nmap -4 -sn <IPv4 subnet>
$ nmap -6 -sn <IPv6 subnet>
$ subnetcalc <IPv6 subnet>
```

`nmap` - Subnet discovery

- What happened in this exercise?
- Default “ping” scan uses:
  - ICMP
  - SYN TCP-80
  - SYN TCP-443
  - ICMP timestamp
- Specific observations on v6 scanning?

Exercise - **nmap** OS and service detection

Setup:

```
$ default4=$(ip -4 route | grep ^default | awk '{print $3}')
$ default6=$(ip -6 route | grep ^default | awk '{print $3}')
$ echo $default4 $default6
$ sudo wireshark
    # any suggestions ?
```

Try:

```
$ nmap -4 -A -T4 $default4
$ nmap -6 -A -T4 $default6
```

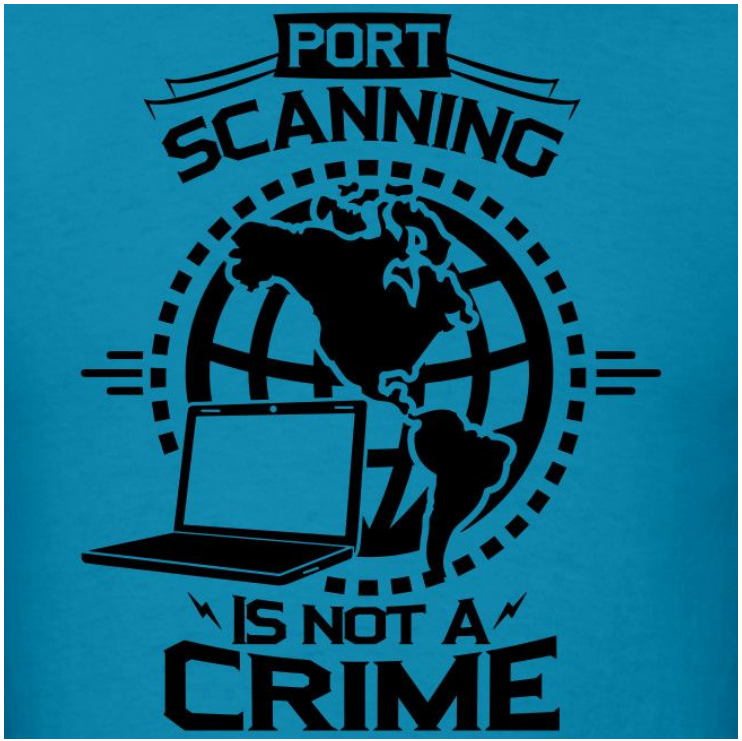
`nmap` - OS and service detection

- What happened in this exercise?
- OS detection with TCP/IP stack fingerprinting
  - Compares results with known OS fingerprints
  - ~2600 OSes in the nmap database
- Specific observations on v6 scanning?

Summary

- Network scanning can help you discover the hosts in your networks
- Useful for troubleshooting
- Can reveal security gaps
- Note - It’s not illegal to port scan

  … but better to ask for permission :-)

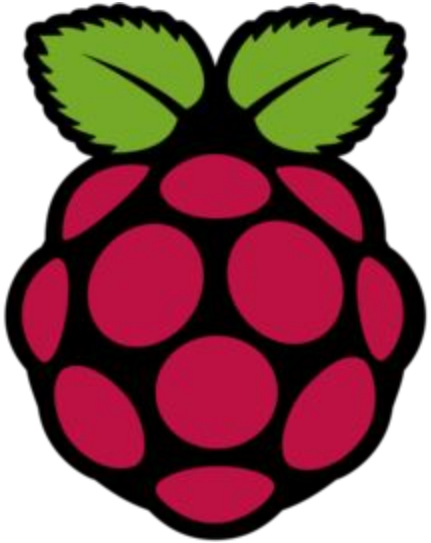


Possible Future Discussions

- Vulnerability scanning / Pen-testing
  - e.g. Metasploit, OpenVAS, etc.
- Intrusion Detection
  - e.g. Snort, etc.
- Network monitoring
  - e.g. Prometheus, Elastic Stack, Nagios, Cactus, etc.
- Honey Pots
- IPv6 with containers - k8s w/ calico ?
- Other ideas welcome!

VicPiMakers and Others Slack

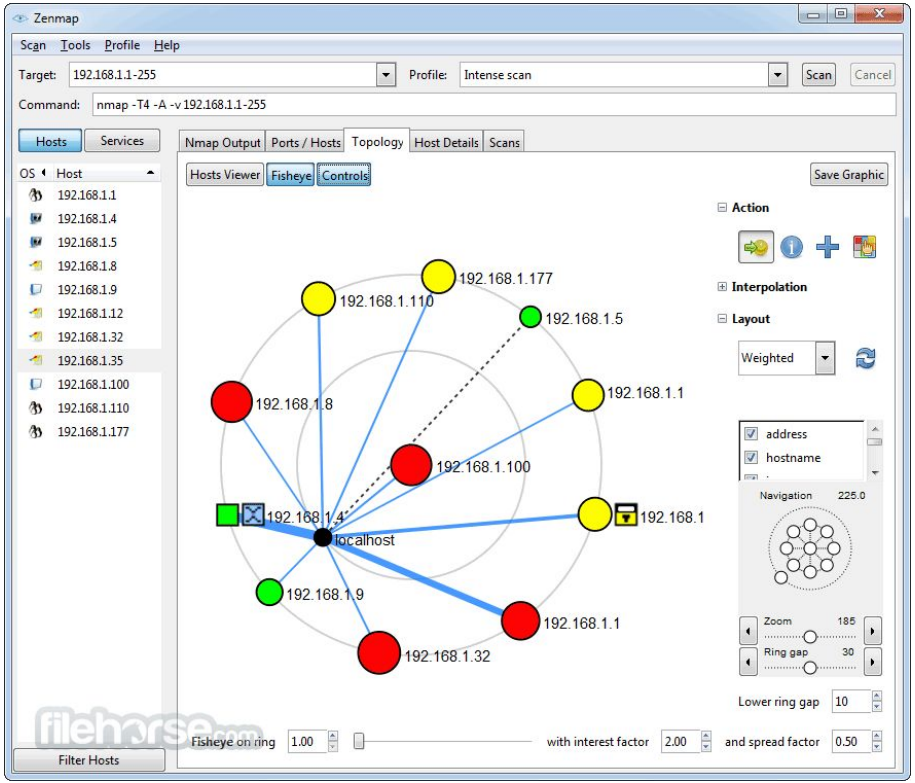
- Please let us know if you want an invite to this Slack group



Backup Slides

Zenmap

- `nmap` + GUI
- Standard scans without having to memorizing all the CLI options
- Topology views



Exercise - **`netcat`** client / server

Setup:

```
Terminal 1:
    $ nc -v -l 60001
Terminal 2:
    $ nc -v localhost 60001
```

Try:

```
Terminal 1:
    Hello !
Terminal 2:
    Hello to you too !
```

Exercise - Scan `netcat` server

Setup:

```
Terminal 1:
    $ nc -v -l 60001
```

Try:

```
$ nmap -4 <wlan0 v4 address>
```

Questions:

- How to fix this scan?