INTRO TO ETHICAL HACKING

MIS 5211.701

Week 4

Site:

http://community.mis.temple.edu/mis5211sec701fall17/

Tonight's Plan

- Scanning
  - Types
  - TcpDump
  - Hping3
  - Beginning Nmap

Scanning

- Goals
  - Find live network hosts, Firewalls, Routers, Printers, etc…
  - Work out network topology
  - Operating systems used
  - Open ports
  - Available network services
  - Potential vulnerabilities
  - While minimizing the chance of disrupting operations

Type of Scans

- Sweep – Send a series of probes (ICMP ping) to find live hosts
- Trace – Use tools like traceroute and/or tracert to map network
- Port Scanning – Checking for open TCP or UDP ports
- Fingerprinting – Determine operating system
- Version Scanning – Finding versions of services and protocols
- Vulnerability Scanning

More on Types

- Order works from less to more intrusive
  - Sweeps are unlikely to disrupt anything, probably will not even alert security systems
  - Vulnerability scans may cause system disruptions, and will definitely light up even a marginally effective security system

Targeting

- Always target by IP address
- Round Robbin DNS (Think basic load balancing) may spread packets to different machines and corrupt your results

Big Scans

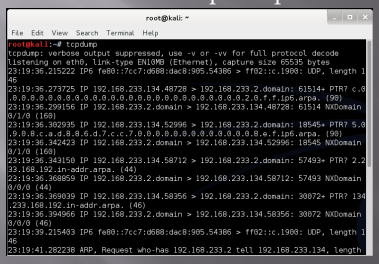
- Targeting a large number of addresses and/or ports will create a very long scan
- Need to focus on smaller scope of addresses and a limited number of ports
- If you have to scan large addresses space or all ports consider:
  - Multiple scanners
  - Distributed scanners (Closer to Targets)

Sniffers for Scanning

- Some Pen Testers suggest running a sniffer to watch activity
  - Detect errors
  - Visualize what is happening

tcpdump

- Linux sniffer tool is tcpdump



tcpdump

- Remember Man page for tcpdump is already installed

```
TCPDUMP(8)                                                    TCPDUMP(8)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqRStuUvxX ] [ -B buffer_size ] [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ expression ]

DESCRIPTION
       Tcpdump  prints  out a description of the contents of packets on a net-
       work interface that match the boolean expression.  It can also  be  run
       with the -w flag, which causes it to save the packet data to a file for
       later analysis, and/or with the -r flag, which causes it to read from a
       saved packet file rather than to read packets from a network interface.
       In all cases, only packets that match expression will be  processed  by
       tcpdump.
```


tcpdump

- Basic Communications
  - Try tcpdump -nS

```
root@kali:~# tcpdump -nS
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

23:32:59.311921 IP 192.168.233.1.54390 > 239.255.255.250.1900: UDP, length 128
```

- Looking for pings

```
root@kali:~# tcpdump -nS icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
23:41:09.132837 IP 192.168.233.1 > 192.168.233.134: ICMP echo request, id 1, seq
 5, length 40
23:41:09.132886 IP 192.168.233.134 > 192.168.233.1: ICMP echo reply, id 1, seq 5
, length 40
23:41:10.134663 IP 192.168.233.1 > 192.168.233.134: ICMP echo request, id 1, seq
 6, length 40
23:41:10.134700 IP 192.168.233.134 > 192.168.233.1: ICMP echo reply, id 1, seq 6
, length 40
```


tcpdump

- If you are not root:
  - Remember: sudo tcpdump
- Can filter for specific IP
  - Try: tcpdump –nn tcp and dst 10.10.10.10
  - Try: tcpdump –nn udp and src 10.10.10.10
  - Try: tcpdump –nn tcp and port 443 and host 10.10.10.10
  - FYI
    - -n : Don't resolve hostnames.
    - -nn : Don't resolve hostnames or port names.
- More detailed How To:
  - http://danielmiessler.com/study/tcpdump/

Network Sweeps

- Hping3
  - One target at a time
- Caution: Windows firewalls may block functionality

```
root@kali:~# hping3 192.168.233.133
HPING 192.168.233.133 (eth0 192.168.233.133): NO FLAGS are set, 40 headers + 0 d
ata bytes
len=46 ip=192.168.233.133 ttl=64 DF id=61878 sport=0 flags=RA seq=0 win=0 rtt=0.
7 ms
len=46 ip=192.168.233.133 ttl=64 DF id=61879 sport=0 flags=RA seq=1 win=0 rtt=0.
3 ms
len=46 ip=192.168.233.133 ttl=64 DF id=61880 sport=0 flags=RA seq=2 win=0 rtt=0.
5 ms
len=46 ip=192.168.233.133 ttl=64 DF id=61881 sport=0 flags=RA seq=3 win=0 rtt=0.
4 ms
len=46 ip=192.168.233.133 ttl=64 DF id=61882 sport=0 flags=RA seq=4 win=0 rtt=0.
4 ms
^C
```


Hping3

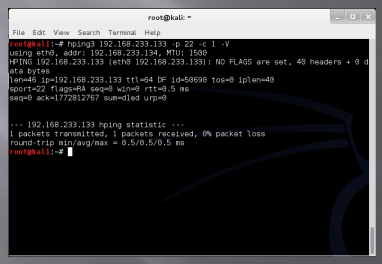
- Can spoof source
  - --spoof
  - Example
    - Hping3 –spoof 10.10.10.10 10.10.10.20
    - Sets source to 10.10.10.10
    - Sets destination to 10.10.10.20

Hping3

- Targets ports
  - -- destport [port]
  - Example
    - Hping3 10.10.10.10 –p 53
    - Targets port 53 on 10.10.10.10
- Target multiple port

Hping3

- Example targeting port 22 with count "-c" and verbose "-V"



Nmap

- Nmap is a network mapper
- Very basic example

```
root@kali:~# nmap -sP 192.168.233.133

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-17 01:26 EDT
Nmap scan report for 192.168.233.133
Host is up (0.00056s latency).
MAC Address: 00:0C:29:28:06:5B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
root@kali:~#
```

- Just pings a machine and confirms it exists

- Now we take it up a notch
- Lets check an entire class "C" address
- Example:
  - Try: nmap –sP 192.168.1-255

```
root@kali:~# nmap -sP 192.168.233.1-255

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-17 01:31 EDT
Nmap scan report for 192.168.233.1
Host is up (0.00027s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.233.2
Host is up (0.00039s latency).
MAC Address: 00:50:56:E9:CA:77 (VMware)
Nmap scan report for 192.168.233.133
Host is up (0.00026s latency).
MAC Address: 00:0C:29:28:06:5B (VMware)
Nmap scan report for 192.168.233.254
Host is up (0.00024s latency).
MAC Address: 00:50:56:FE:A6:A8 (VMware)
Nmap scan report for 192.168.233.134
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 1.77 seconds
root@kali:~#
```

Targeting

- Always target by IP address
- Round Robbin DNS (Think basic load balancing) may spread packets to different machines and corrupt your results

Big Scans

- Targeting a large number of addresses and/or ports will create a very long scan
- Need to focus on smaller scope of addresses and a limited number of ports
- If you have to scan large addresses space or all ports consider:
  - Multiple scanners
  - Distributed scanners (Closer to Targets)

Sniffers for Scanning

- Some Pen Testers suggest running a sniffer to watch activity
  - Detect errors
  - Visualize what is happening

A Little Refresher

- Recall, two principle packet types
  - TCP (Transmission Control Protocol)
    - Connection oriented
    - Reliable
    - Sequenced
  - UDP (User Datagram Protocol)
    - Connectionless
    - Best effort (Left to higher level application to detect loss and request retransmission if needed)
    - Independent (un-sequenced)

TCP Protocol

Offset	Octet	0								1								2								3			
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source Port																Destination Port														
4	32	Sequence Number																														
8	64	Acknowledgement Number (if ACK set)																														
12	96	Data Offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size													
16	128	Checksum																														
20 ...	160 ...	Options (if data offset > 5. Padded at the end with "0" bytes if necessary.)																														

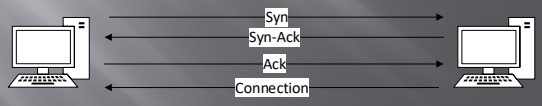
- Number of flags have grown over the years, adding flags to the left as new ones are approved
- With nine flags, there are 512 unique combinations of 1s and 0s
- Add the three reserved flags and the number grows to 4096

TCP Control Bits

- Control bits also called "Control Flags"
- Defined by RFCs 793, 3168, and 3540
- Currently defines 9 bits or flags
  - See: http://en.wikipedia.org/wiki/Transmission_Control_Protocol

Three Way Handshake

- Every "Legal" TCP connection begins with a three way handshake.
- Sequence numbers are exchanged with the Syn, Syn-Ack, and Ack packets

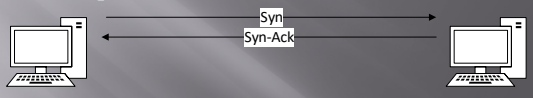


How This Applies to Scanning

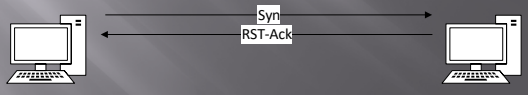
- Per the RFC (793)
- A TCP listener on a port will respond with Ack, regardless of the payload
- Listener responds with a Syn-Ack
- Therefore, if you get a Syn-Ack, something that speaks TCP was listening on that port

Behaviors

- Port Open

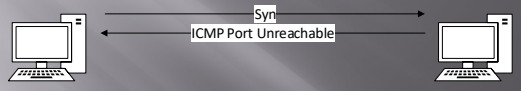


- Port Closed or Blocked by Firewall

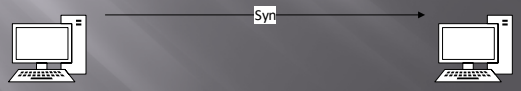


Behaviors 2

- Port Inaccessible (Likely Blocked by Firewall)



- Port Inaccessible (Likely Blocked by Firewall)



- Note: Nmap will mark both as "filtered"

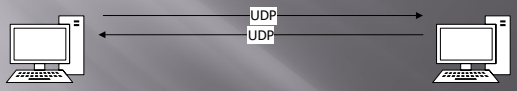
UDP Protocol

Offset	Octet	0								1								2								3			
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source Port																Destination Port														
4	32	Length																Checksum														
8	64	Payload																														
...	...																															

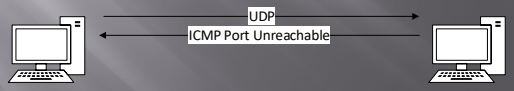
- As you can see, UDP is a lot simpler.
  - No Sequence Numbers
  - No flags or control bits
  - No "Connection"
- As a result
  - Slower to scan
  - Less reliable scanning

Behaviors

- Port Open



- Port Closed or Blocked by Firewall



Behaviors 2

- Port Inaccessible

- Could be:
  - Closed
  - Blocked going in
  - Blocked coming out
  - Service not responding (Looking for a particular payload)
  - Packet simply dropped due to collision

On to Nmap the Tool

- Written and maintained by Fyodor
- http://nmap.org/
- Note: Lots of good info on the site, but the tutorial is a bit out of date. Latest info was put in a book and is sold on Amazon
  - http://www.amazon.com/Nmap-Network-Scanning-Official-Discovery/dp/0979958717/ref=sr_1_1?ie=UTF8&qid=1411443925&sr=8-1&keywords=nmap

Nmap Location On Kali (old)

NMAP New

A Suitable Target

- Metasploitable
  - Deliberately vulnerable version of Linux developed for training on Metasploit
  - We'll use it here since there will be worthwhile things to find with nmap.
- http://sourceforge.net/projects/virtualhacking/files/os/metasploitable/metasploitable-linux-2.0.0/download
- UserID: msfadmin Password: msfadmin

Heads Up

- After downloading the zip file, extract to a convenient location. VMWare should have created a folder in "My Documents" called "Virtual Machines"
- Let Kali get started first
- Then, select "Open a Virtual Machine" and navigate to the folder for metasploitable. Then launch.
- You get a prompt asking if you moved or copied the VM, select "Moved"
- Once started, login and issue command ifconfig to get you IP address and your done.

Back to Nmap

- Lets try something simple
- Nmap 192.168.233.135

What This Tells Us

- There are a number of interesting ports here
  - ftp
  - Ssh
  - telnet
  - Smtp (Mail)
  - domain (DNS)
  - http (Web Server)
- Keep in mind, ports are "commonly associated" with these services, but not guaranteed
- http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Points to Remember

- -n – Don't resolve host names
- -nn – Don't resolve host names OR port names
- -v – Verbose, tell me more
- -vv – Really Verbose, tell me lots more
- -iL – Input from list, get host list from a text file
- --exclude – Don't scan a particular host
- --excludefile – Don't scan hosts from a text file
- Remember – "man nmap"

--packet-trace

- Nmap prints a summary of every packet sent or received
- May want to limit ports "-p1-1024" or less
- There are also
  - --version-trace
  - --script-trace

```
SENT (0.0080s) TCP 192.168.233.134:52390 > 192.168.233.135:80 S ttl=52 id=19972
iplen=44  seq=3481801639 win=1024 <mss 1460>
RCVD (0.0795s) TCP 192.168.233.135:25 > 192.168.233.134:52390 SA ttl=64 id=0 ipl
en=44  seq=1296729268 win=5840 <mss 1460>
RCVD (0.0797s) TCP 192.168.233.135:21 > 192.168.233.134:52390 SA ttl=64 id=0 ipl
en=44  seq=1289797711 win=5840 <mss 1460>
RCVD (0.0798s) TCP 192.168.233.135:110 > 192.168.233.134:52390 RA ttl=64 id=0 ip
len=40  seq=0 win=0
RCVD (0.0800s) TCP 192.168.233.135:23 > 192.168.233.134:52390 SA ttl=64 id=0 ipl
en=44  seq=1292961672 win=5840 <mss 1460>
RCVD (0.0802s) TCP 192.168.233.135:22 > 192.168.233.134:52390 SA ttl=64 id=0 ipl
en=44  seq=1291239770 win=5840 <mss 1460>
```


Basic Scan Types

- -sT – TCP connect() scanning
  - If connect succeeds, port is open

```
root@kali:~# nmap -sT 192.168.233.135

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 21:44 EDT
Nmap scan report for 192.168.233.135
Host is up (0.0079s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
```


Basic Scan Types

- -sS – SYN stealth Scan
  - If SYN-ACK is received, port is open

```
root@kali:~# nmap -sS 192.168.233.135

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 21:48 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00013s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
```

FIN Scan

- -sF – Like SYN Scan, less likely to be flagged
  - Closed port responds w/ RST, Open port drops
  - Works on RFC 793 compliant systems
    - Windows not compliant, could differentiate a Windows system

```
root@kali:~# nmap -sF 192.168.233.135

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 21:53 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00041s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
```


Other Options

- -sN – Null scan
  - Similar to FIN
- -sX – Xmas tree scan
  - Sets FIN, PSH, and URG
- -sM – Maiman scan
  - sets FIN and ACK
- All work by looking for the absence of a RST

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```


Roll Your Own

- --scanflags
  - Example:
    - Nmap –scanflags SYNPSHACK –p 80 19

UDP Scans

- -sU – 0 Byte UDP Packet
  - Port unreachable – Port is closed
  - No response – Port assumed open
  - Very time consuming

```
root@kali:~# nmap -sU 192.168.233.135 -p1-20

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 22:18 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00031s latency).
PORT   STATE         SERVICE
1/udp  open|filtered tcpmux
2/udp  open|filtered compressnet
3/udp  open|filtered compressnet
4/udp  closed        unknown
5/udp  closed        rje
```

  - 20 ports took 5.46 seconds, -sT scan only took 0.15

Protocol Scan

- -sO – Looks for IP Protocols supported
  - Sends raw IP packets without additional header information
  - Takes time

```
root@kali:~# nmap -sO 192.168.233.135

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 22:23 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00039s latency).
Not shown: 251 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
136      open|filtered udplite
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 264.23 seconds
```


Version Detection

- -sV – Attempts to determine version of services running

```
root@kali:~# nmap -sV 192.168.233.135

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 22:24 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00016s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
```

More on Version

- -A – Looks for version of OS as well

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```


Still More on Version Scan

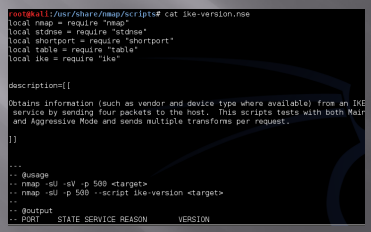
- -O – Fingerprint the operating system
- -A = -sV + -O

Nmap Scripting Engine

- Also known as NSE
  - Written in "Lua"
  - Activated with "-sC" or "- - script"
- Categories
  - Safe
  - Intrusive
  - Malware
  - Version
  - Discovery
  - Vulnerability

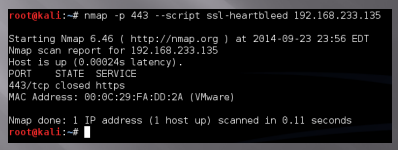
Script Location

- In Kali, nmap scripts are located in:
  - /usr/share/nmap/scripts
- Can view using either "cat" OR gedits



Script Example

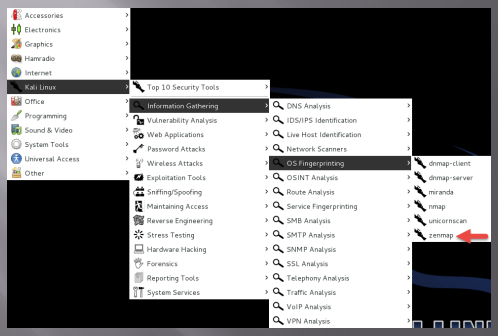
- SSL-Heartbleed
- Try: nmap –p 443 --script ssl-heartbleed {target}
- In this case, 443 is not even open



Zenmap

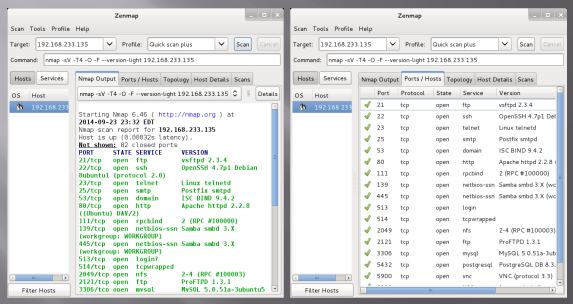
- Graphical User Interface for nmap
- Why did we just spend that time on the command line?
  - Better control
  - Better understanding

Zenmap Location



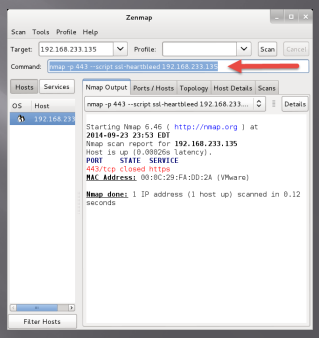
Zenmap New

Zenmap Scan

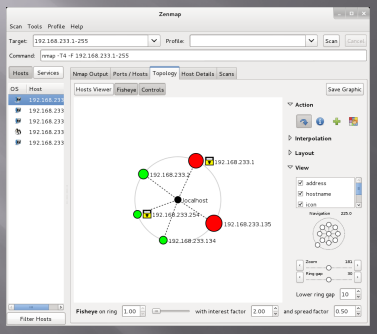


Still Really a Command Line

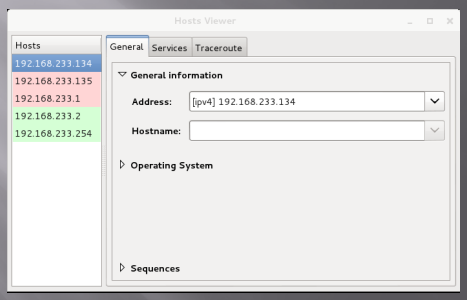
- Look at the arrow
- You can add to command line
- Remember that SSL-hearbleed script



With a few Extras



And More



Zenmap Reference

- https://www.linux.com/learn/tutorials/381794-audit-your-network-with-zenmap?format=pdf

Questions

?