

---

---

---

---

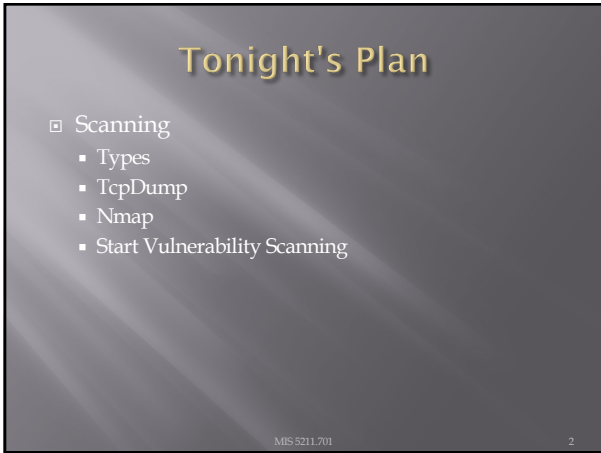
---

---

---

---

1



---

---

---

---

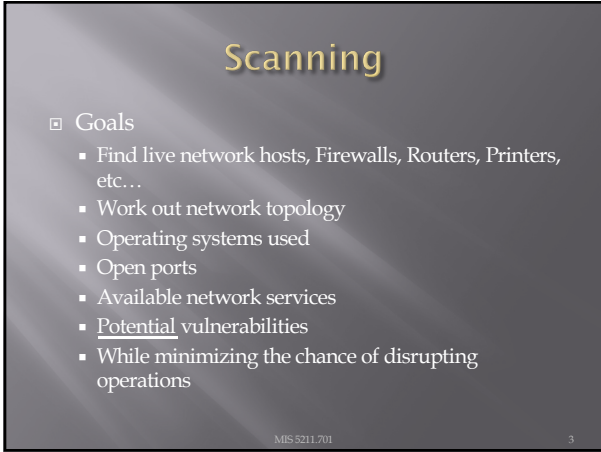
---

---

---

---

2



---

---

---

---

---

---

---

---

3

## 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

MIS 5211.701

4

4

---

---

---

---

---

---

---

---

## 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

MIS 5211.701

5

5

---

---

---

---

---

---

---

---

## Targeting

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

MIS 5211.701

6

6

---

---

---

---

---

---

---

---

## Big Scans

- ❑ Targeting large numbers 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 address space or all ports consider:
  - Multiple scanners
  - Distributed scanners (Closer to Targets)

MIS 5211.701 7

7

---

---

---

---

---

---

---

---

---

---

## Sniffers for Scanning

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

MIS 5211.701 8

8

---

---

---

---

---

---

---

---

---

---

## tcpdump

- ❑ Linux sniffer tool is tcpdump



MIS 5211.701 9

9

---

---

---

---

---

---

---

---

---

---

## tcpdump

- ❑ Remember Man page for tcpdump is already installed

```

TCPDUMP(8)                                TCPDUMP(8)
NAME
tcpdump - dump traffic on a network

SYNOPSIS
tcpdump [ -AbdDefHhJKLlNnOpqRSrStuvvxX ] [ -B buffer_size ] [ -c count ]
[ -C file_size ] [ -G rotate_seconds ] [ -F file ]
[ -i interface ] [ -j timestamp_type ] [ -M module ] [ -N secret ]
[ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
[ -W filecount ]
[ -E sni@ipaddr algo:secret.... ]
[ -y statlinktype ] [ -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.
    
```

MIS 5211.701 10

10

---

---

---

---

---

---

---

---

---

---

## 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 126
    
```

- ❑ 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
23:41:09.132937 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
    
```

MIS 5211.701 11

11

---

---

---

---

---

---

---

---

---

---

## 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/>

MIS 5211.701 12

12

---

---

---

---

---

---

---

---

---

---

## 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 data bytes
len=66 ip=192.168.233.133 ttl=64 DF id=61878 sport=0 flags=RA seq=0 win=0 rtt=0.7 ms
len=66 ip=192.168.233.133 ttl=64 DF id=61879 sport=0 flags=RA seq=1 win=0 rtt=0.3 ms
len=66 ip=192.168.233.133 ttl=64 DF id=61880 sport=0 flags=RA seq=2 win=0 rtt=0.5 ms
len=66 ip=192.168.233.133 ttl=64 DF id=61881 sport=0 flags=RA seq=3 win=0 rtt=0.4 ms
len=66 ip=192.168.233.133 ttl=64 DF id=61882 sport=0 flags=RA seq=4 win=0 rtt=0.4 ms
^C

```

MIS 5211.701 13

13

---

---

---

---

---

---

---

---

---

---

## 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

MIS 5211.701 14

14

---

---

---

---

---

---

---

---

---

---

## Nmap

- ❑ Now we take it up a notch
- ❑ 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: 00:50:56:00:80:08 (VMware)
Nmap scan report for 192.168.233.2
Host is up (0.00039s latency).
MAC Address: 00:50:56:02:CA:77 (VMware)
Nmap scan report for 192.168.233.133
Host is up (0.00025s 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:~#

```

MIS 5211.701 15

15

---

---

---

---

---

---

---

---

---

---

## A Little Refresher

- ☐ Recall, two principal 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)

MIS 5211.701 16

16

---

---

---

---

---

---

---

---

## TCP Protocol

Offset	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160	164	168	172	176	180	184	188	192	196	200	204	208	212	216	220	224	228	232	236	240	244	248	252	256	260	264	268	272	276	280	284	288	292	296	300	304	308	312	316	320	324	328	332	336	340	344	348	352	356	360	364	368	372	376	380	384	388	392	396	400	404	408	412	416	420	424	428	432	436	440	444	448	452	456	460	464	468	472	476	480	484	488	492	496	500	504	508	512																																																																																																																															
Octet	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	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255
Bit	Source Port				Destination Port				Sequence Number								Acknowledgement Number (if ACK set)								Data Offset								Reserved								N S R								C W S								E R E								U A C								R C S								S S S								Y I I								F I I								Window Size								Checksum								Urgent Pointer (if URG set)								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

17

17

---

---

---

---

---

---

---

---

## 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](http://en.wikipedia.org/wiki/Transmission_Control_Protocol)

MIS 5211.701 18

18

---

---

---

---

---

---

---

---

### 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

MIS 5211.701 19

---

---

---

---

---

---

---

---

19

### 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

MIS 5211.701 20

---

---

---

---

---

---

---

---

20

### Behaviors

- Port Open
- Port Closed or Blocked by Firewall

MIS 5211.701 21

---

---

---

---

---

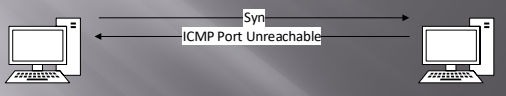
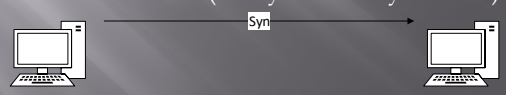
---

---

---

21

## Behaviors 2

- ❑ Port Inaccessible (Likely Blocked by Firewall)
 
- ❑ Port Inaccessible (Likely Blocked by Firewall)
 
- ❑ Note: Nmap will mark both as "filtered"

MIS 5211.701 22

22

---

---

---

---

---

---

---

---

## UDP Protocol

Offset	Octet	0	1	2	3
Octet	Bit	0	1	2	3
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

MIS 5211.701 23

23

---

---

---

---

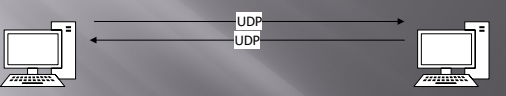
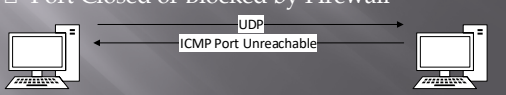
---

---

---

---

## Behaviors

- ❑ Port Open
 
- ❑ Port Closed or Blocked by Firewall
 

MIS 5211.701 24

24

---

---

---

---

---

---


---

---



## 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

MIS 5211.701 25

25

---

---

---

---

---

---

---

---

## 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](http://www.amazon.com/Nmap-Network-Scanning-Official-Discovery/dp/0979958717/ref=sr_1_1?ie=UTF8&qid=1411443925&sr=8-1&keywords=nmap)

MIS 5211.701 26

26

---

---

---

---

---

---

---

---

## NMAP New



MIS 5211.701 27

27

---

---

---

---

---

---

---

---

## 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.
- ❑ <https://sourceforge.net/projects/metasploitable/files/latest/download>
  - May download immediately upon landing on page
- ❑ UserID: msfadmin Password: msfadmin

MIS 5211.701 28

28



## 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 "Copied"
- ❑ Once started, login and issue command ifconfig to get you IP address and your done.

MIS 5211.701 29

29



## Back to Nmap

- ❑ Lets try something simple
- ❑ Nmap 192.168.233.135

```

root@kali:~# nmap 192.168.233.135
Starting Nmap 5.46 ( http://nmap.org ) at 2014-09-29 20:54 EDT
Nmap scan report for 192.168.233.135
Host is up (0.0000s latency).
Not shown: 997 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  xcp
513/tcp   open  login
514/tcp   open  smb1
1099/tcp  open  msiregistry
1524/tcp  open  drpstock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
2365/tcp  open  msq1
5432/tcp  open  postgresql
5889/tcp  open  irc
6889/tcp  open  x11
6889/tcp  open  x11
6889/tcp  open  x11
8080/tcp  open  http-alt
MAC Address: 08:00:2B:24:10:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@kali:~#

```

MIS 5211.701 30

30



## What This Tells Us

- ❑ There are a number of interesting ports here
  - ftp
  - Ssh
  - telnet
  - Sntp (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>

MIS 5211.701 31

31

---

---

---

---

---

---

---

---

---

---

## 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”

MIS 5211.701 32

32

---

---

---

---

---

---

---

---

---

---

## --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 (0.0000s) TCP 192.168.233.134:52390 → 192.168.233.135:80 S ttl=64 id=19972
ipLen=44 seq=3481881639 win=1024 mss=1460
RVD (0.0795s) TCP 192.168.233.135:80 → 192.168.233.134:52390 SA ttl=64 id=0 ipL
en=44 seq=1296729268 win=6840 mss=1460
RVD (0.0795s) TCP 192.168.233.135:21 → 192.168.233.134:52390 SA ttl=64 id=0 ipL
en=44 seq=1291239770 win=6840 mss=1460
RVD (0.0798s) TCP 192.168.233.135:110 → 192.168.233.134:52390 RA ttl=64 id=0 ipL
en=44 seq=0 win=0
RVD (0.0800s) TCP 192.168.233.135:23 → 192.168.233.134:52390 SA ttl=64 id=0 ipL
en=44 seq=1292961072 win=6840 mss=1460
RVD (0.0800s) TCP 192.168.233.135:22 → 192.168.233.134:52390 SA ttl=64 id=0 ipL
en=44 seq=1291239770 win=6840 mss=1460
    
```

MIS 5211.701 33

33

---

---

---

---

---

---

---

---

---

---

## 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
            
```

MIS 5211.701 34

34

---

---

---

---

---

---

---

---

---

---

## 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
            
```

MIS 5211.701 35

35

---

---

---

---

---

---

---

---

---

---

## 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
            
```

MIS 5211.701 36

36

---

---

---

---

---

---

---

---

---

---

## 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
MIS 5211.701

```

37

---

---

---

---

---

---

---

---

## Roll Your Own

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

38

---

---

---

---

---

---

---

---

## 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  tomcat
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

39

---

---

---

---

---

---

---

---

## 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 uplLite
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap done: 1 IP address (1 host up) scanned in 264.23 seconds
  
```

MIS 5211.701 40

40

---

---

---

---

---

---

---

---

---

---

## 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: 577 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian Bubuntu (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 rpsbind 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 rxsed
513/tcp open login?
514/tcp open tcpwrapped
1699/tcp open mircregistry GNU Classpath gmicregistry
  
```

MIS 5211.701 41

41

---

---

---

---

---

---

---

---

---

---

## 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.
LMI: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
  
```

MIS 5211.701 42

42

---

---

---

---

---

---

---

---

---

---

## Still More on Version Scan

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

MIS 5211.701 43

---

---

---

---

---

---

---

---

43

## Nmap Scripting Engine

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

MIS 5211.701 44

---

---

---

---

---

---

---

---

44

## Script Location

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

```

root@kali:~/nmap/share/nmap/scripts# cat ike-version.nse
local nmap = require "nmap"
local stdios = require "stdios"
local httpport = require "httpport"
local table = require "table"
local ike = require "ike"

description[[
Obtains information (such as vendor and device type where available) from an IKE
service by sending four packets to the host. This script tests with both Main
and Aggressive Mode and sends multiple transforms per request.
]]

...
-- @usage
-- nmap -sV -sV -p 598 <target>
-- nmap -sU -p 500 --script ike-version <target>
...
-- @output
-- PORT STATE SERVICE REASON VERSION

```

MIS 5211.701 45

---

---

---

---

---

---

---

---

45

## Script Example

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

```

root@kali:~# nmap -p 443 --script ssl-heartbleed 192.168.233.135
Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 23:56 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00024s latency).
PORT      STATE SERVICE
443/tcp   closed https
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#

```

MIS 5211.701

46

46

---

---

---

---

---

---

---

---

---

---

## Zenmap

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

MIS 5211.701

47

47

---

---

---

---

---

---

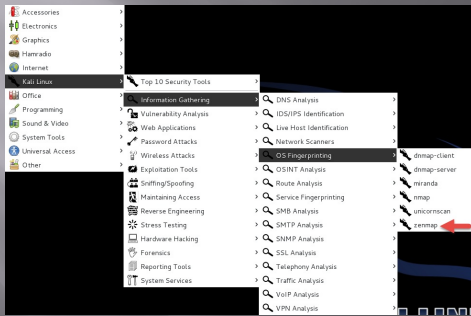
---

---

---

---

## Zenmap Location



MIS 5211.701

48

48

---

---

---

---

---

---

---

---

---

---





49

---

---

---

---

---

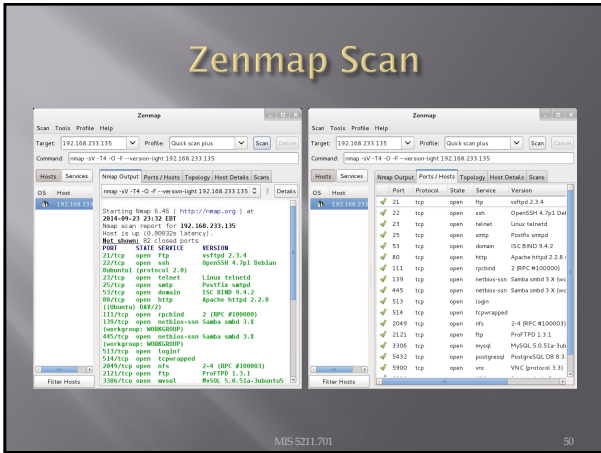
---

---

---

---

---



50

---

---

---

---

---

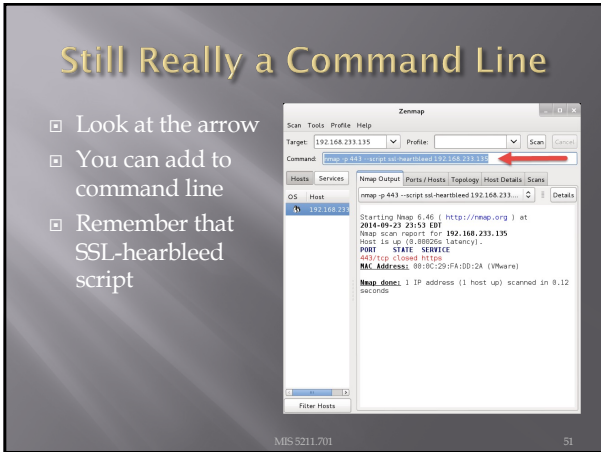
---

---

---

---

---



51

---

---

---

---

---

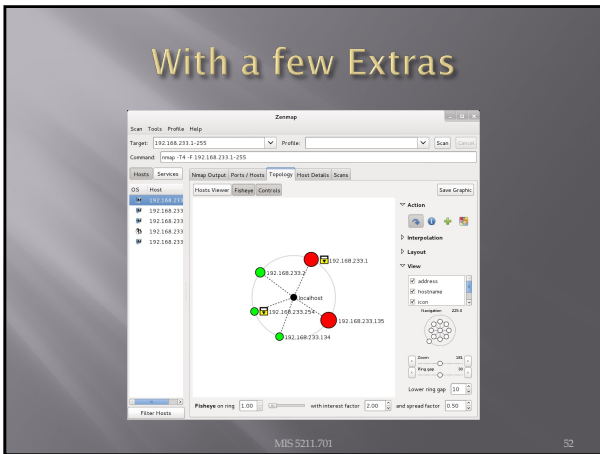
---

---

---

---

---



52

---

---

---

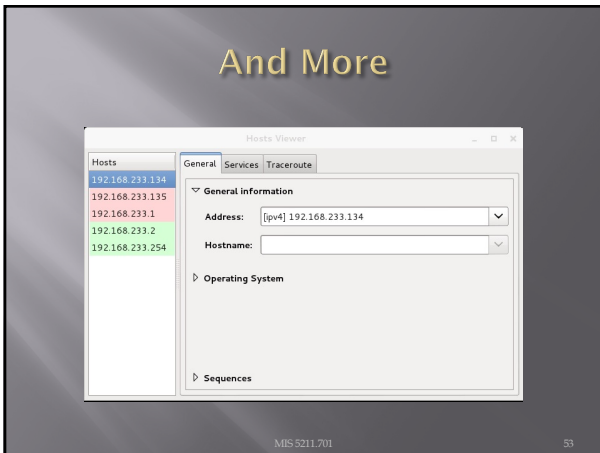
---

---

---

---

---



53

---

---

---

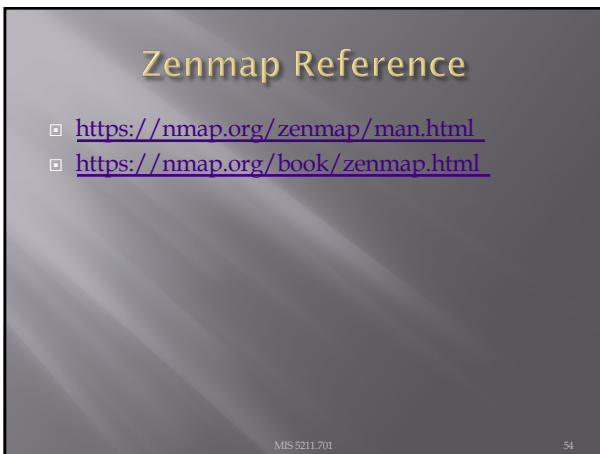
---

---

---

---

---



54

---

---

---

---

---

---

---

---

## Nessus

- ❑ Started in 1998 as an open source security scanning tool
- ❑ Changed to a close sourced tool in 2005, but has remained “free” for personal use.
- ❑ Surveys by sectools.org indicate Nessus remains the most popular vulnerability scanners
- ❑ Not installed with Kali

MIS 5211.701 55

---

---

---

---

---

---

---

---

55

## The Nessus Server

- ❑ Four basic parts to the Nessus server:
  - Nessus-core
  - Nessus-libraries
  - Libnasl
  - Nessus-plugins

MIS 5211.701 56

---

---

---

---

---

---

---

---

56

## Plugins

- ❑ Plugins are the scripts that perform the vulnerability tests.
- ❑ NASL - This is the Nessus Attack Scripting Language which can be used to write your own plugins.

---

---

---

---

---

---

---

---

57

### Defining Targets

- ❑ Hosts
  - Server.domain.edu
  - 172.21.1.2
- ❑ Subnet
  - 192.168.100.0
- ❑ Address range
  - 192.168.1.1-192.168.1.10

---

---

---

---

---

---

---

---

58

### Vulnerability Scanning

- ❑ Scanning methods:
  - Safe
  - Destructive
- ❑ Service recognition - Will determine what service is actually running on a particular port.
- ❑ Handle multiple services - Will test a service if it appears on more than one port.
- ❑ Will test multiple systems at the same time.

---

---

---

---

---

---

---

---

59

### Viewing Reports

- ❑ Nessus will indicate the threat level for services or vulnerabilities it detects:
  - Critical
  - High
  - Medium
  - Low
  - Informational
- ❑ Description of vulnerability
- ❑ Risk factor
- ❑ CVE number

---

---

---

---

---

---

---

---

60

## Common Vulnerabilities and Exposures

- ❑ CVE created by <https://cve.mitre.org>
  - Attempting to standardize the names for vulnerabilities.
- ❑ CVE search engine at <http://icat.nist.gov/>

61

---

---

---

---

---

---

---

---

## Options

**THE NESSUS FAMILY**

Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

nessus essentials	nessus professional	tenable.io
<p><b>FREE DOWNLOAD</b> Scan 10 IPs</p> <ul style="list-style-type: none"> <li>✓ High-speed, in-depth assessments</li> <li>✓ Free training and guidance</li> <li>✓ Support via Tenable Community</li> <li>✓ On-demand training available</li> </ul> <p><small>Ideal for: Educators, students and individuals starting their careers in Cyber Security. Learn more about using Essentials in the classroom with the Tenable for Education program.</small></p> <p style="text-align: center;"><a href="#">Download</a></p>	<p><b>SUBSCRIPTION</b> Scan Unlimited IPs</p> <ul style="list-style-type: none"> <li>✓ Unlimited assessments</li> <li>✓ Use anywhere, annual subscription</li> <li>✓ Configuration assessment</li> <li>✓ Live Results</li> <li>✓ Configurable Reports</li> <li>✓ Community Support</li> <li>✓ Advanced Support available with subscription</li> <li>✓ On-demand training available</li> </ul> <p><small>Ideal for: Consultants, Pen Testers and Security Practitioners.</small></p> <p style="text-align: center;"><a href="#">Learn More</a> <a href="#">Try</a> <a href="#">Buy</a></p>	<p><b>SUBSCRIPTION</b> Deploy Unlimited Scanners</p> <ul style="list-style-type: none"> <li>✓ Unlimited Nessus Scanners</li> <li>✓ Managed in the Cloud</li> <li>✓ Flexible Predictive Prioritization</li> <li>✓ Advanced Dashboards and Reports</li> <li>✓ Role-Based Access Control</li> <li>✓ Advanced Support</li> <li>✓ Enterprise Scalability</li> <li>✓ Priced per asset, annual subscription</li> <li>✓ Instructor-led training course available</li> </ul> <p><small>Ideal for: Vulnerability Management for small, medium and enterprise organizations.</small></p> <p style="text-align: center;"><a href="#">Learn More</a> <a href="#">Try</a> <a href="#">Buy</a></p>

MIS 5211.701 62

62

---

---

---

---

---

---

---

---

## Free Training

- ❑ <http://www.tenable.com/education/on-demand-courses>

**The Nessus Sensor Suite**

- ▾ Nessus Professional

**Courses**

- Deployment
- Scanning
- Analysis and Reporting
- Compliance
- Infrastructure Compliance
- Application Compliance
- Advanced Scanning

- ▾ Nessus Manager
- ▾ Nessus Network Monitor

MIS 5211.701 63

63

---

---

---

---

---

---

---

---

## Certification Options

 **Certificate of Proficiency**

To earn a **Certificate of Proficiency** you must successfully pass the corresponding product knowledge assessment for Tenable.io™, Nessus®, SecurityCenter®, SecurityCenter Continuous View®,. To help you prepare for these assessments, courses are offered in on-demand or instructor-led settings, and provide knowledge and guidance about using Tenable products, including common customer use cases and industry best practices. After completing each course, you will have access to the product knowledge assessment, **free of charge**.

<http://www.tenable.com/education/certification>

MIS 5211.701 64

---

---

---

---

---

---

---

---

64

## Architecture

- ❑ Nessus is built on a classic client/server model.
- ❑ The server portion may reside on a separate machine, or on the same machine as the client
- ❑ The client is the interface that you will interact with to execute scans

MIS 5211.701 65

---

---

---

---

---

---

---

---

65

## Getting Nessus

- ❑ Download from Tenable Security
  - <https://www.tenable.com/products/nessus>
  - Before installing, go to registration page and get the activation code
  - <http://www.tenable.com/products/nessus-home>
- ❑ Run the MSI package and follow the prompts
- ❑ Install will also install PCAP and then take you to the registration page.
- ❑ Enter activation code and follow the prompts to get updates and plugins

MIS 5211.701 66

---

---

---

---

---

---

---

---

66

## Documentation

- ❑ Documentation for Nessus is available here:
  - <https://docs.tenable.com/Nessus.htm>
- ❑ You should also get a link to this location during the install.

MIS 5211.701 67

---

---

---

---

---


---

---

---

67

## AV and Firewalls

- ❑ You will need to turn off Anti-Virus and Firewall in order to get an effective scan or you will see this:  

- ❑ Before you do this, disconnect from any and all networks.
- ❑ You will likely still get some blocking as AV doesn't like to give up.

MIS 5211.701 68

---

---

---

---

---

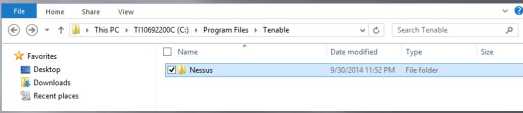
---

---

---

68

## Location

- ❑ Nessus is installed here:  


MIS 5211.701 69

---

---

---

---

---

---

---

---

69

**STOP**

- ▣ We will continue next week.

MIS 5211.701 70

70

---

---

---

---

---

---

---

---

**Next Week**

- ▣ Complete Nessus
- ▣ Begin Metasploit

MIS 5211.701 71

71

---

---

---

---

---

---

---

---

**Questions**

?

MIS 5211.701 72

72

---

---

---

---

---

---

---

---