INTRO TO ETHICAL HACKING

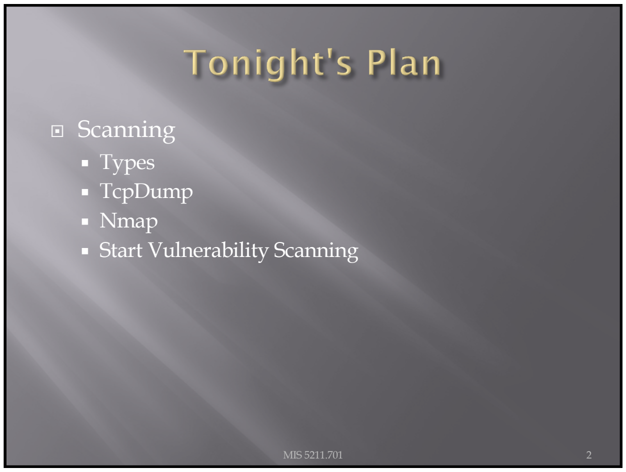
MIS 5211.701

Week 4

Site:

https://community.mis.temple.edu/mis5211sec701fall2019/

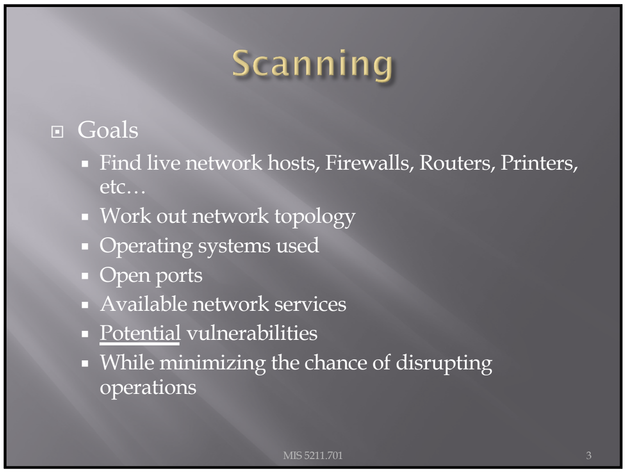
1



Tonight's Plan

- Scanning
  - Types
  - TcpDump
  - Nmap
  - Start Vulnerability Scanning

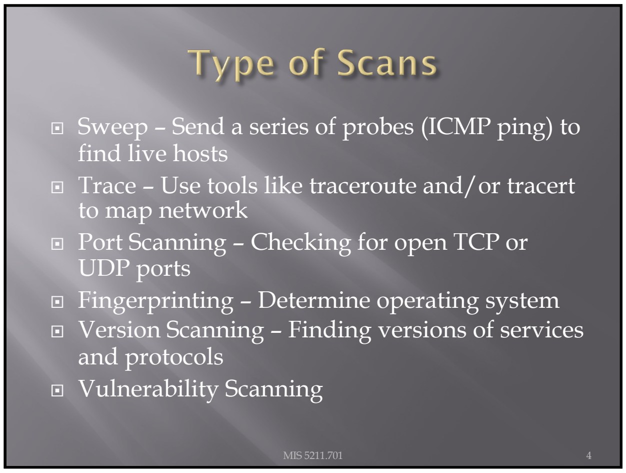
2



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

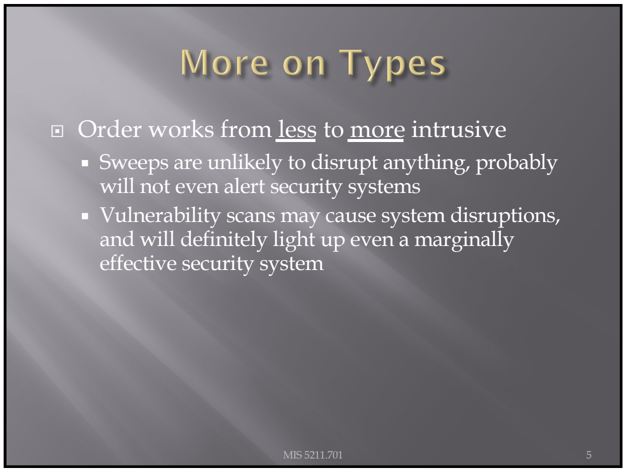
3



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

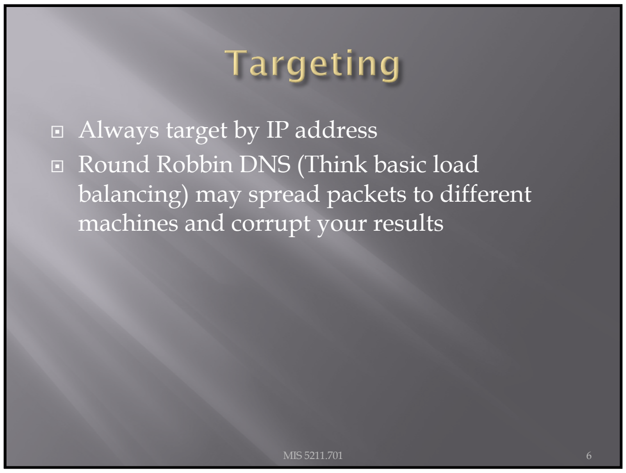
4



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

5



Targeting

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

6

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)

7

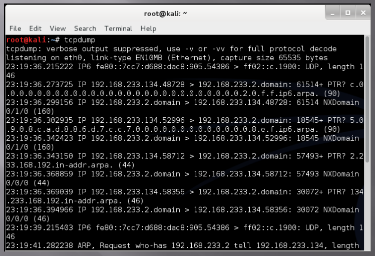
Sniffers for Scanning

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

8

tcpdump

- Linux sniffer tool is tcpdump

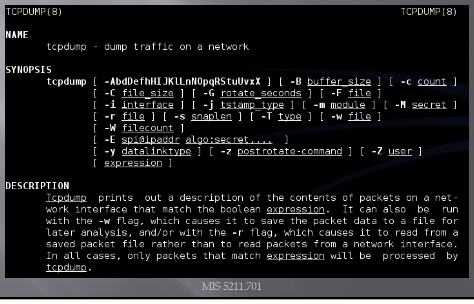


```
root@kali:~# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
23:19:36.215222 IP6 fe80::7cc7:d688:dac8:905.54386 > ff02::c.1900: UDP, length 1
46
23:19:36.273725 IP 192.168.233.134.48728 > 192.168.233.2.domain: 61514+ PTR? c.0
.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
23:19:36.299156 IP 192.168.233.2.domain > 192.168.233.134.48728: 61514 NXDomain
0/1/0 (160)
23:19:36.302935 IP 192.168.233.134.52996 > 192.168.233.2.domain: 18545+ PTR? 5.0
.9.0.8.c.a.d.8.8.6.d.7.c.c.7.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
23:19:36.342423 IP 192.168.233.2.domain > 192.168.233.134.52996: 18545 NXDomain
0/1/0 (160)
23:19:36.343150 IP 192.168.233.134.58712 > 192.168.233.2.domain: 57493+ PTR? 2.2
33.168.192.in-addr.arpa. (44)
23:19:36.368859 IP 192.168.233.2.domain > 192.168.233.134.58712: 57493 NXDomain
0/0/0 (44)
23:19:36.369039 IP 192.168.233.134.58356 > 192.168.233.2.domain: 30072+ PTR? 134
.233.168.192.in-addr.arpa. (46)
23:19:36.394966 IP 192.168.233.2.domain > 192.168.233.134.58356: 30072 NXDomain
0/0/0 (46)
23:19:39.215403 IP6 fe80::7cc7:d688:dac8:905.54386 > ff02::c.1900: UDP, length 1
46
23:19:41.282238 ARP, Request who-has 192.168.233.2 tell 192.168.233.134, length
```

9

tcpdump

- Remember Man page for tcpdump is already installed

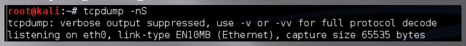


```
TCPDUMP(8)                                                          TCPDUMP(8)

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.
```

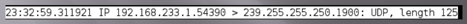
10

tcpdump

- Basic Communications
  - Try tcpdump -nS

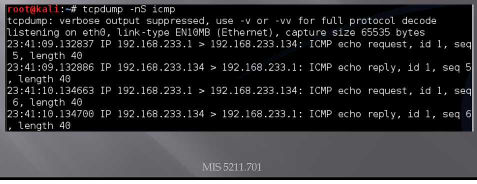


```
root@kali:~# tcpdump -nS
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```



```
23:32:59.311921 IP 192.168.233.1.54390 > 239.255.255.250.1900: UDP, length 125
```

- 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
```

11

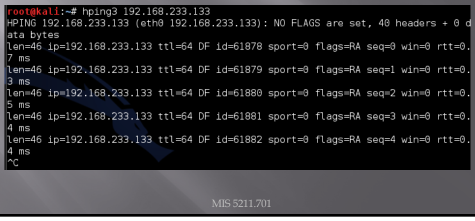
tcpdump

- 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/

12

Network Sweeps

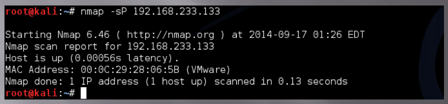
- Hping3
  - One target at a time
- Caution: Windows firewalls may block functionality



```
root@kali:~# hping3 192.168.233.133
HPING 192.168.233.133 (eth0 192.168.233.133): NO FLAGS are set, 40 headers + 0 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
```

Nmap

- Nmap is a network mapper
- Very basic example

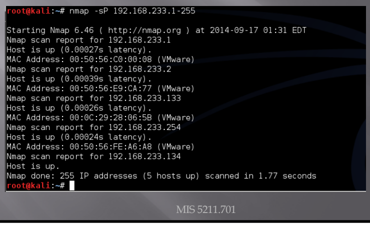


```
root@kali:~# nmap -sP 192.168.233.133

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:~# 
```

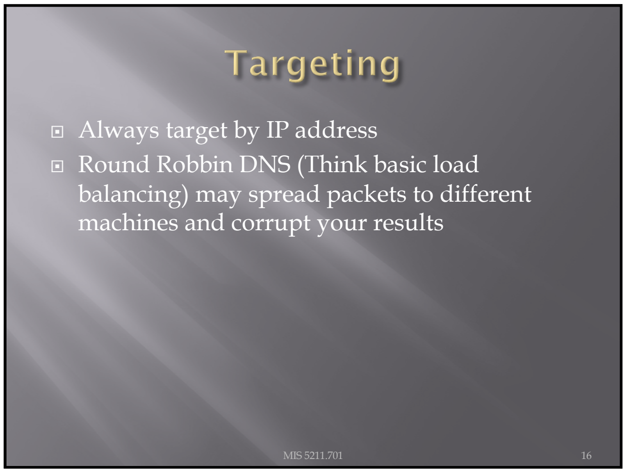
- Just pings a machine and confirms it exists

Nmap

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



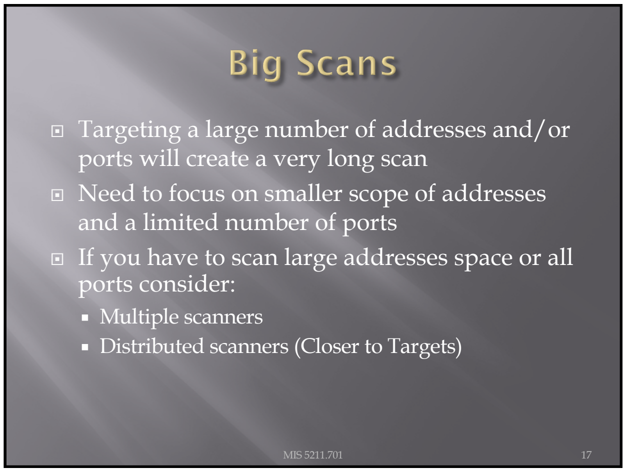
```
root@kali:~# nmap -sP 192.168.233.1-255

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

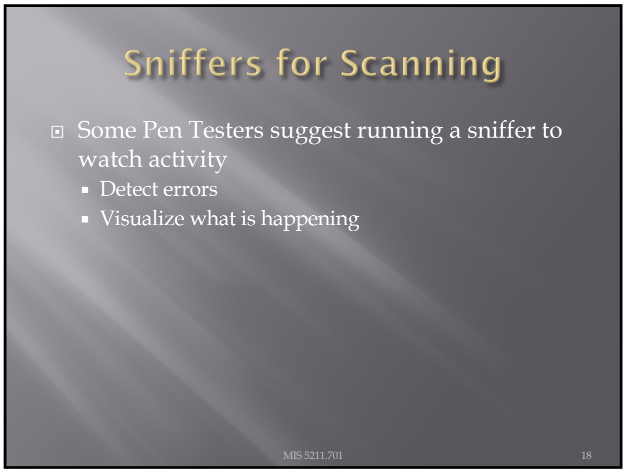
16



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)

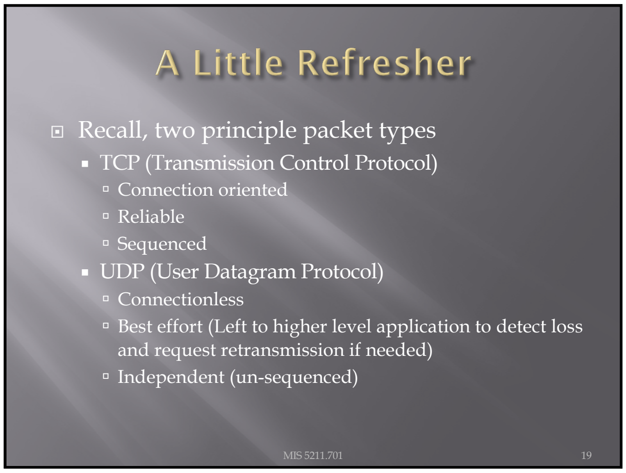
17



Sniffers for Scanning

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

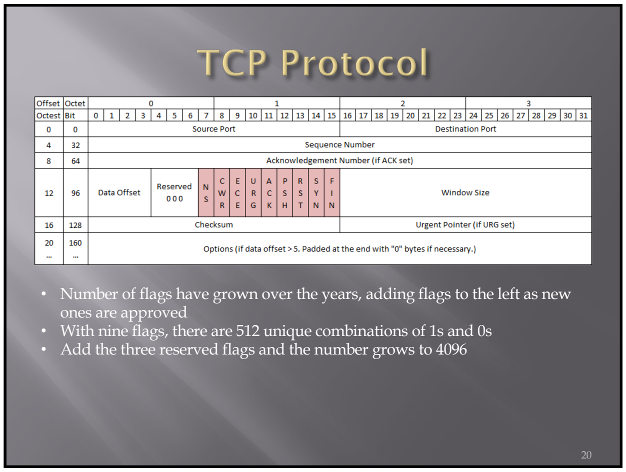
18



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)

19

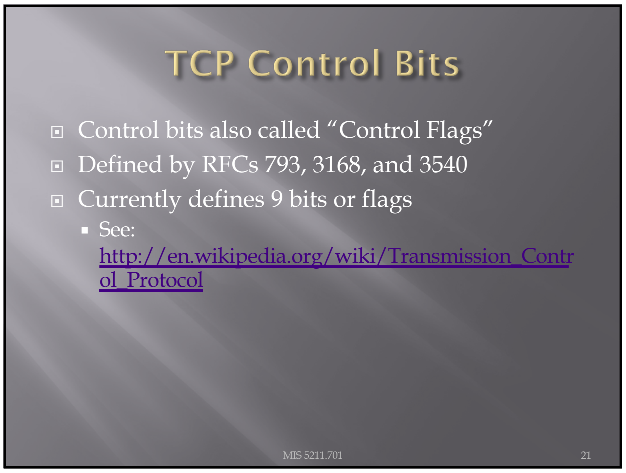


TCP Protocol

Offset	Octet	0								1								2								3							
Octest	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																Urgent Pointer (if URG set)															
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

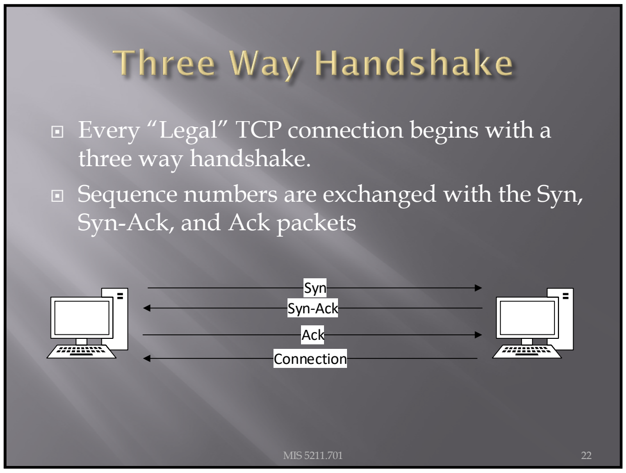
20



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

21

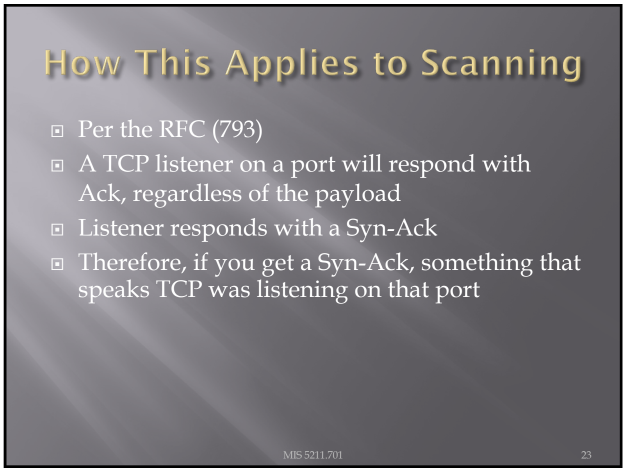


Three Way Handshake

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

Syn
Syn-Ack
Ack
Connection

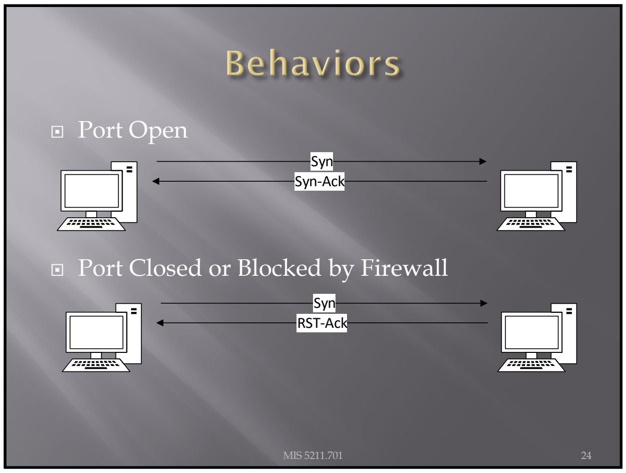
22



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

23



Behaviors

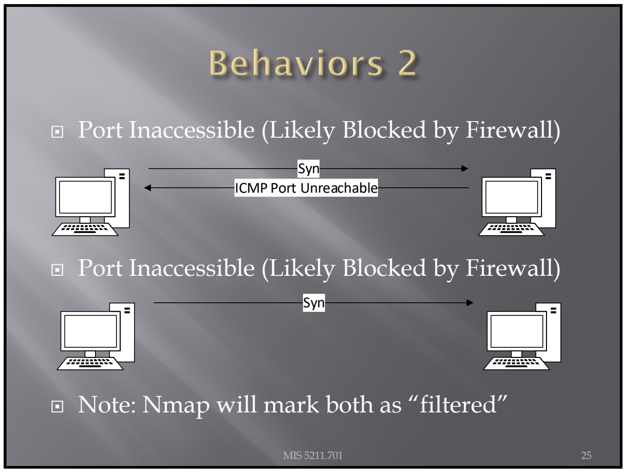
- Port Open

Syn
Syn-Ack

- Port Closed or Blocked by Firewall

Syn
RST-Ack

24



Behaviors 2

- Port Inaccessible (Likely Blocked by Firewall)

Syn

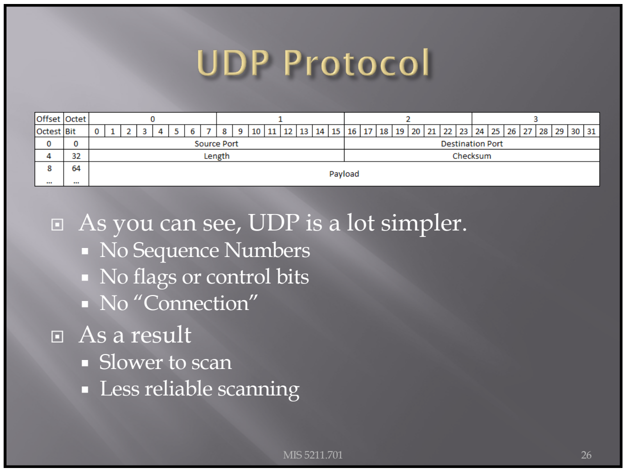
ICMP Port Unreachable

- Port Inaccessible (Likely Blocked by Firewall)

Syn

- Note: Nmap will mark both as “filtered”

25

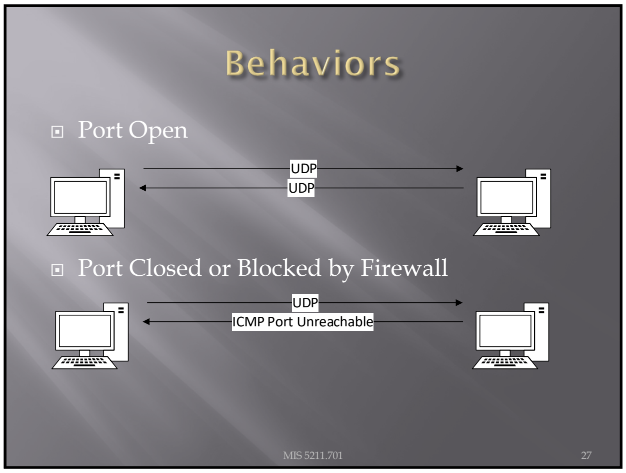


UDP Protocol

Offset	Octet	0								1								2								3							
Octest	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

26



Behaviors

- Port Open

UDP

UDP

- Port Closed or Blocked by Firewall

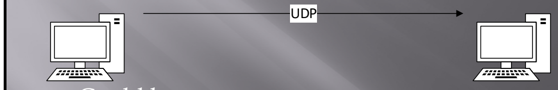
UDP

ICMP Port Unreachable

27

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

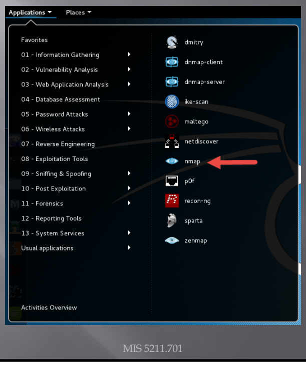
28

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

29

NMAP New



30

A Suitable Target

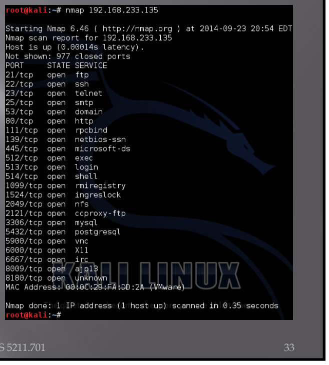
- Metasploitable
  - Deliberately vulnerable version of Linux developed for training on Metasploit
  - We'll use it here since there will be worthwhile things to find with nmap.
- https://sourceforge.net/projects/metasploitable/files/latest/download
  - May download immediately upon landing on page
- UserID: msfadmin Password: msfadmin

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.

Back to Nmap

- Lets try something simple
- Nmap 192.168.233.135



```
root@kali:~# nmap 192.168.233.135

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-23 20:54 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00014s 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
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

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

What This Tells Us

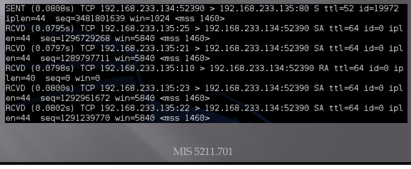
- There are a number of interesting ports here
  - ftp
  - Ssh
  - telnet
  - Smtp (Mail)
  - domain (DNS)
  - http (Web Server)
- Keep in mind, ports are "commonly associated" with these services, but not guaranteed
- http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

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

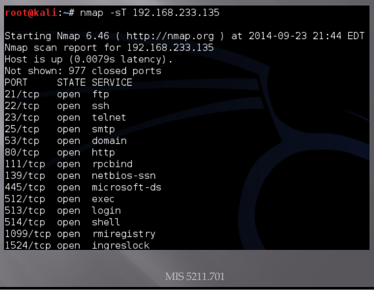
- Nmap prints a summary of every packet sent or received
- May want to limit ports "-p1-1024" or less
- There are also
  - --version-trace
  - --script-trace



```
SENT (0.0808s) 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

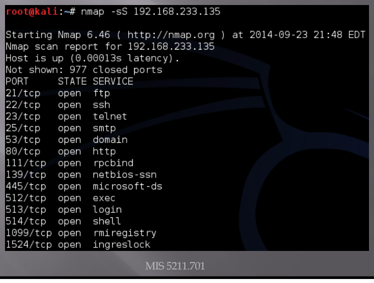


```
root@kali:~# nmap -sT 192.168.233.135

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
```

37

Basic Scan Types

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

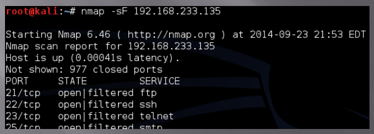


```
root@kali:~# nmap -sS 192.168.233.135

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
```

38

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

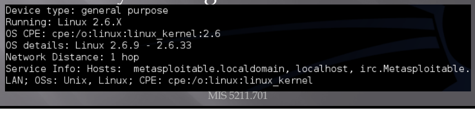


```
root@kali:~# nmap -sF 192.168.233.135

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
```

39

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
```

40

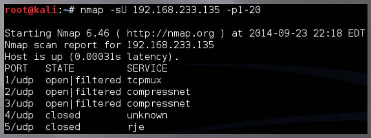
Roll Your Own

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

41

UDP Scans

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



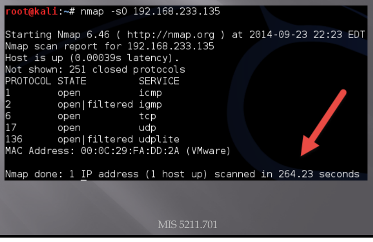
```
root@kali:~# nmap -sU 192.168.233.135 -p1-20

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

42

Protocol Scan

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

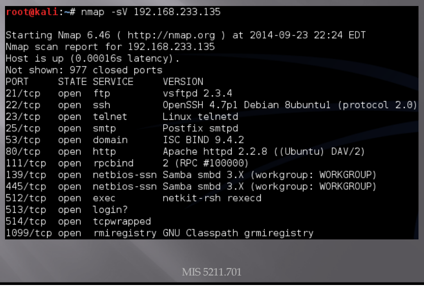


```
root@kali:~# nmap -sO 192.168.233.135

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
```

43

Version Detection

- -sV – Attempts to determine version of services running

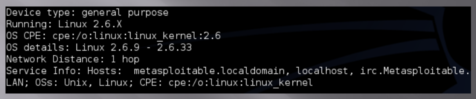


```
root@kali:~# nmap -sV 192.168.233.135

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
```

44

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
```

45

Still More on Version Scan

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

46

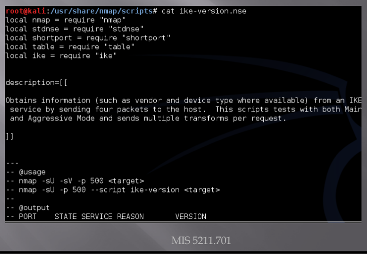
Nmap Scripting Engine

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

47

Script Location

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

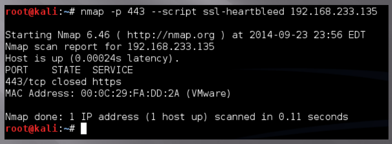


```
root@kali:/usr/share/nmap/scripts# cat ike-version.nse
local nmap = require "nmap"
local stdnse = require "stdnse"
local shortport = require "shortport"
local table = require "table"
local ike = require "ike"


description=[[

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

]]


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

48

Script Example

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

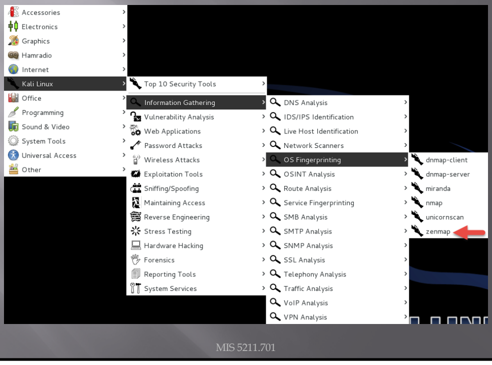


```
root@kali:~# nmap -p 443 --script ssl-heartbleed 192.168.233.135

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:~#
```

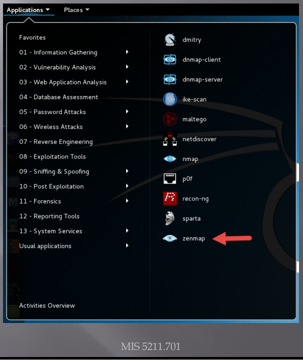
Zenmap

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

Zenmap Location

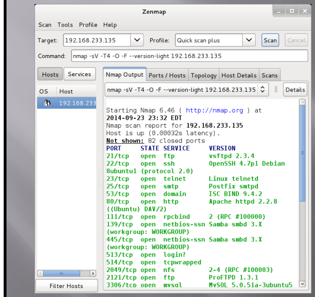


Zenmap New



52

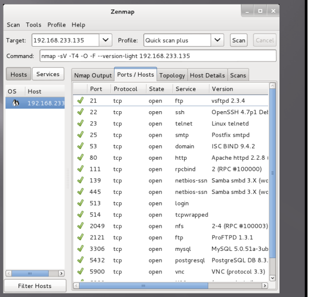
Zenmap Scan



Target: 192.168.233.135 Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 192.168.233.135

```
Starting Nmap 6.46 ( http://nmap.org ) at
2014-09-23 23:32 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00032s latency).
Not shown: 82 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)
513/tcp  open  login?
514/tcp  open  tcpwrapped
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```



Target: 192.168.233.135 Profile: Quick scan plus

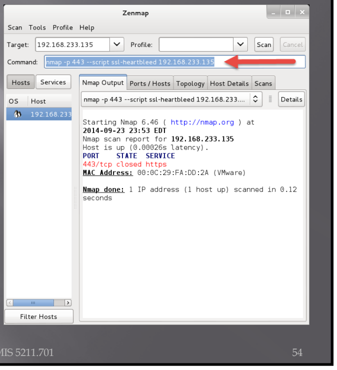
Command: nmap -sV -T4 -O -F --version-light 192.168.233.135

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	vsftpd 2.3.4
✓	22	tcp	open	ssh	OpenSSH 4.7p1 Del
✓	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 (
✓	111	tcp	open	rpcbind	2 (RPC #100000)
✓	139	tcp	open	netbios-ssn	Samba smbd 3.X (wc
✓	445	tcp	open	netbios-ssn	Samba smbd 3.X (wc
✓	513	tcp	open	login	
✓	514	tcp	open	tcpwrapped	
✓	2049	tcp	open	nfs	2-4 (RPC #100003)
✓	2121	tcp	open	ftp	ProFTPD 1.3.1
✓	3306	tcp	open	mysql	MySQL 5.0.51a-3ub
✓	5432	tcp	open	postgresql	PostgreSQL DB 8.3.
✓	5900	tcp	open	vnc	VNC (protocol 3.3)

53

Still Really a Command Line

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



Target: 192.168.233.135 Profile:

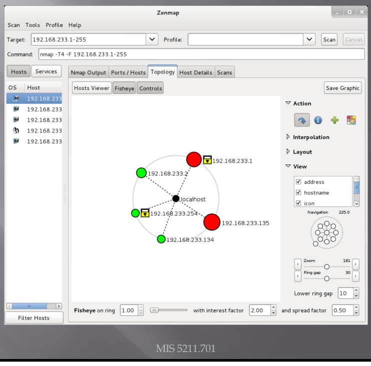
Command: nmap -p 443 --script ssl-heartbleed 192.168.233.135

nmap -p 443 --script ssl-heartbleed 192.168.233....

```
Starting Nmap 6.46 ( http://nmap.org ) at
2014-09-23 23:53 EDT
Nmap scan report for 192.168.233.135
Host is up (0.00026s 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 0.12
seconds
```

54

With a few Extras



Target: 192.168.233.1-255

Command: nmap -T4 -F 192.168.233.1-255

☑ address
☑ hostname
☑ icon

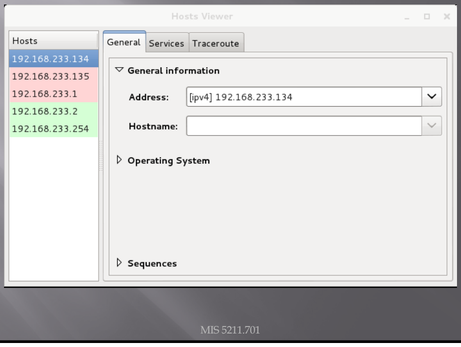
Zoom 181

Ring gap 30

Lower ring gap 10

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

And More

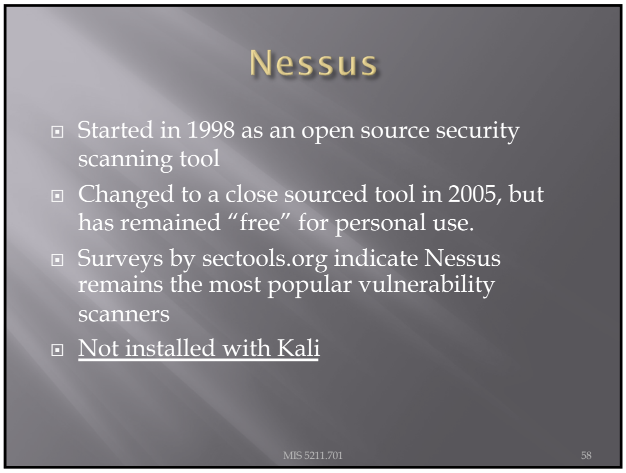


Address: [ipv4] 192.168.233.134

Hostname:

Zenmap Reference

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

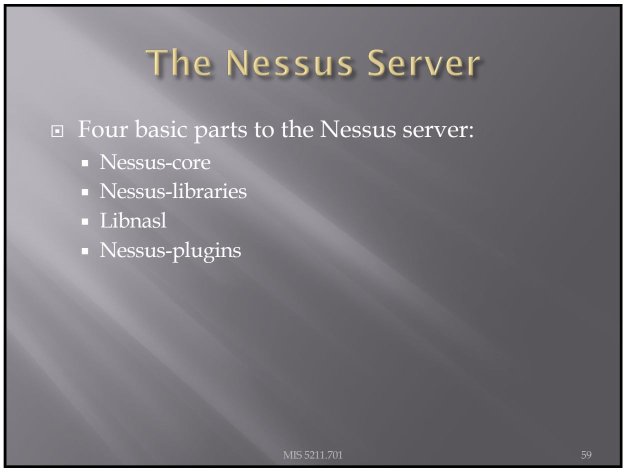


Nessus

- 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 58

58

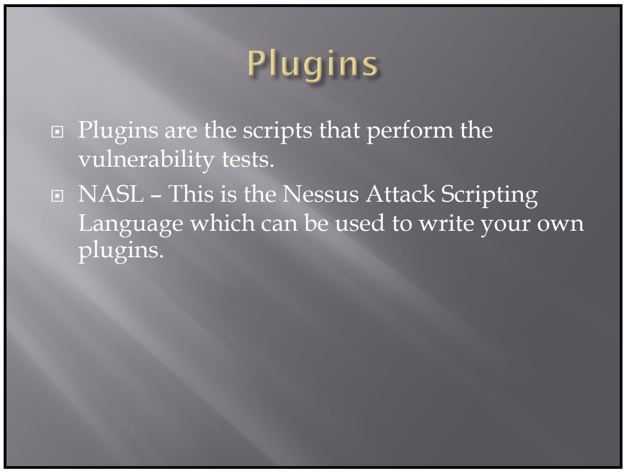


The Nessus Server

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

MIS 5211.701 59

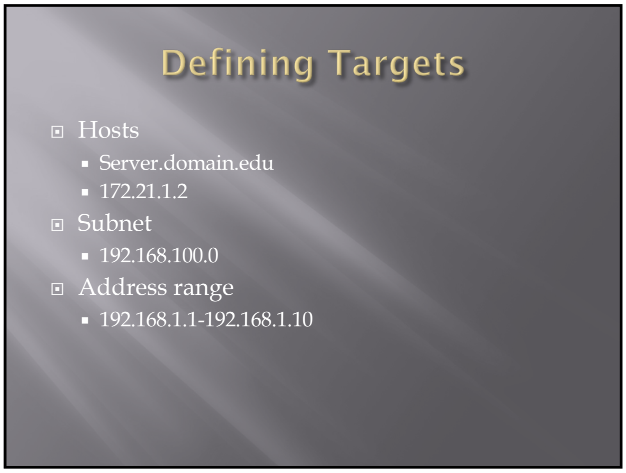
59



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.

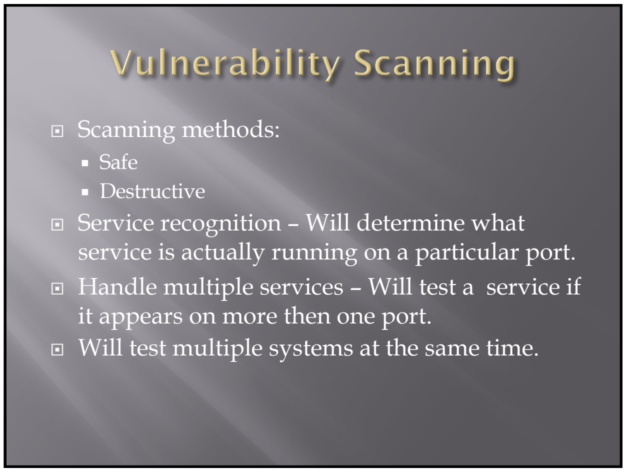
60



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

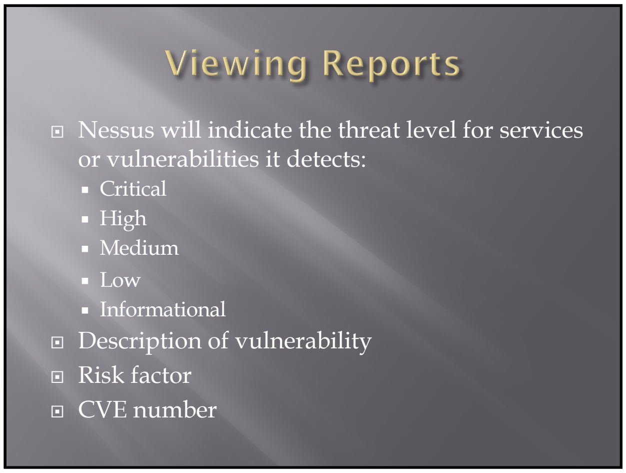
61



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 then one port.
- Will test multiple systems at the same time.

62



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

63

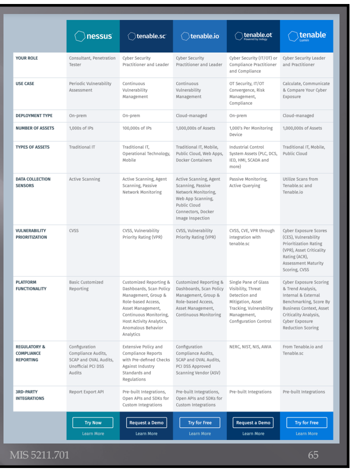
Common Vulnerabilities and Exposures

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

64

Tenable Products

- Nessus Essentials
  - 16 Nodes (devices)
  - Non-Commercial / Personal Use

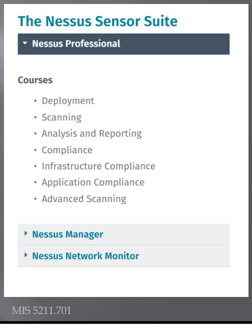


	nessus	tenable.sc	tenable.io	tenable.ot Powered by Indegy	tenable Lumin
YOUR ROLE	Consultant, Penetration Tester	Cyber Security Practitioner and Leader	Cyber Security Practitioner and Leader	Cyber Security (IT/OT) or Compliance Practitioner and Compliance	Cyber Security Leader and Practitioner
USE CASE	Periodic Vulnerability Assessment	Continuous Vulnerability Management	Continuous Vulnerability Management	OT Security, IT/OT Convergence, Risk Management, Compliance	Calculate, Communicate & Compare Your Cyber Exposure
DEPLOYMENT TYPE	On-prem	On-prem	Cloud-managed	On-prem	Cloud-managed
NUMBER OF ASSETS	1,000s of IPs	100,000s of IPs	1,000,000s of Assets	1,000's Per Monitoring Device	1,000,000s of Assets
TYPES OF ASSETS	Traditional IT	Traditional IT, Operational Technology, Mobile	Traditional IT, Mobile, Public Cloud, Web Apps, Docker Containers	Industrial Control System Assets (PLC, DCS, IED, HMI, SCADA and more)	Traditional IT, Mobile, Public Cloud
DATA COLLECTION SENSORS	Active Scanning	Active Scanning, Agent Scanning, Passive Network Monitoring	Active Scanning, Agent Scanning, Passive Network Monitoring, Web App Scanning, Public Cloud Connectors, Docker Image Inspection	Passive Monitoring, Active Querying	Utilize Scans from Tenable.sc and Tenable.io
VULNERABILITY PRIORITIZATION	CVSS	CVSS, Vulnerability Priority Rating (VPR)	CVSS, Vulnerability Priority Rating (VPR)	CVSS, CVE, VPR through integration with tenable.sc	Cyber Exposure Scores (CES), Vulnerability Prioritization Rating (VPR), Asset Criticality Rating (ACR), Assessment Maturity Scoring, CVSS
PLATFORM FUNCTIONALITY	Basic Customized Reporting	Customized Reporting & Dashboards, Scan Policy Management, Group & Role-based Access, Asset Management, Continuous Monitoring, Host Activity Analytics, Anomalous Behavior Analytics	Customized Reporting & Dashboards, Scan Policy Management, Group & Role-based Access, Asset Management, Continuous Monitoring	Single Pane of Glass Visibility, Threat Detection and Mitigation, Asset Tracking, Vulnerability Management, Configuration Control	Cyber Exposure Scoring & Trend Analysis, Internal & External Benchmarking, Score By Business Context, Asset Criticality Analysis, Cyber Exposure Reduction Scoring
REGULATORY & COMPLIANCE REPORTING	Configuration Compliance Audits, SCAP and OVAL Audits, Unofficial PCI DSS Audits	Extensive Policy and Compliance Reports with Pre-defined Checks Against Industry Standards and Regulations	Configuration Compliance Audits, SCAP and OVAL Audits, PCI DSS Approved Scanning Vendor (ASV)	NERC, NIST, NIS, AWIA	From Tenable.io and Tenable.sc
3RD-PARTY INTEGRATIONS	Report Export API	Pre-built Integrations, Open APIs and SDKs for Custom Integrations	Pre-built Integrations, Open APIs and SDKs for Custom Integrations	Pre-built Integrations	Pre-built Integrations
	Try Now Learn More	Request a Demo Learn More	Try for Free Learn More	Request a Demo Learn More	Try for Free Learn More

65

Free Training

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



The Nessus Sensor Suite

▾ Nessus Professional

Courses

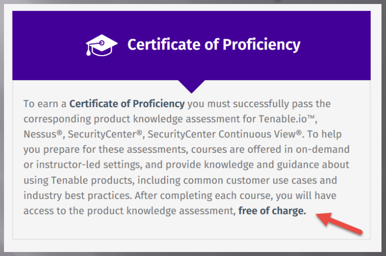
- Deployment
- Scanning
- Analysis and Reporting
- Compliance
- Infrastructure Compliance
- Application Compliance
- Advanced Scanning

▸ Nessus Manager

▸ Nessus Network Monitor

66

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

67

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

68

Getting Nessus

- Download from Tenable Security
  - https://www.tenable.com/products/nessus
  - Before installing, go to registration page and get the activation code
  - https://www.tenable.com/products/nessus/nessus-essentials
- 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

69

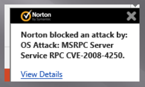
Documentation

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

70

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:



Norton blocked an attack by:
OS Attack: MSRPC Server
Service RPC CVE-2008-4250.

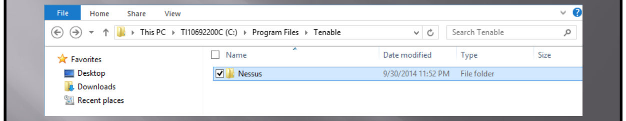
View Details

- 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.

71

Location

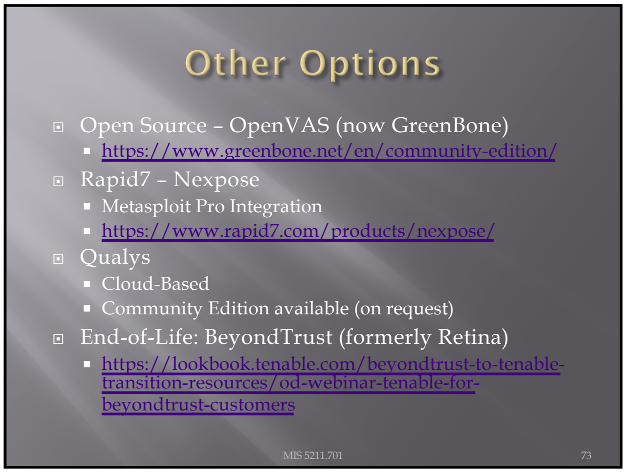
- Nessus is installed here:



This PC › TI10692200C (C:) › Program Files › Tenable

☐ Name	Date modified	Type	Size
☑ Nessus	9/30/2014 11:52 PM	File folder	

72



Other Options

- Open Source – OpenVAS (now GreenBone)
  - https://www.greenbone.net/en/community-edition/
- Rapid7 – Nexpose
  - Metasploit Pro Integration
  - https://www.rapid7.com/products/nexpose/
- Qualys
  - Cloud-Based
  - Community Edition available (on request)
- End-of-Life: BeyondTrust (formerly Retina)
  - https://lookbook.tenable.com/beyondtrust-to-tenable-transition-resources/od-webinar-tenable-for-beyondtrust-customers

MIS 5211.701 73

73

STOP

- We will continue next week.

MIS 5211.701 74

74

Next Week

- Complete Nessus
- Begin Metasploit

MIS 5211.701 75

75

Questions

?

MIS 5211.701

76

76