Alexander Cannell

CSIA 6200

3/25/2016

**Vulnerability Management 2.0 Hands On**

Write-up your VA report in Word format. Use the previous ISACA report format. Your report must include (40 pts/section):

* Executive summary Should be in narrative form and understandable by a non-technical audience

A vulnerability assessment is the process of defining, identifying, and classifying the security holes in a system. During this assignment we have used many different tools to assess the vulnerabilities, including nmap, nessus, and wireshark. Nmap(network mapper) is a security scanner that discovers who is on the network, and what services are being run on your network. Nessus is a comprehensive website that tests the vulnerability of your network. Personally I think this is the best tool I tested. Wireshark is a packet scanner and analyzer. Packets are conversations on a network.

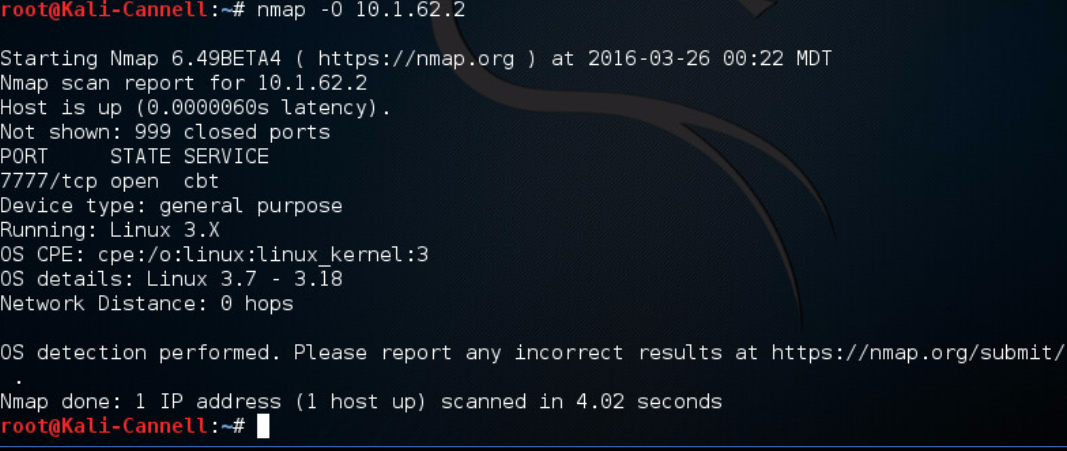
Using nmap I discovered which machines were windows 2012 servers, Kali, and other boxes on our network. Their were three other boxes on the network 10.1.62.55, 10.1.62.50, and 10.1.62.60. On these boxes is what I performed my vulnerability assessment on. I discovered that each of these three boxes are not secure what so ever. From my nmap each one of theses VM’s have multiple tcp and udp ports open, which is like leaving doors open leading to your vault. We know that each of these boxes are running windows. From the Nessus we discover that each of these boxes have multiple vulnerabilities. Looking at 10.1.62.50 it has 19 critical vulnerablilities, which is alot, I would think this is box is a honeypot. A honeypot is a trap for hackers, which looks like a vulnerable box and easy to hack, but it is an informational gathering tool to see how the boxes are compromised. A honeypot logs all the hackers actions, to be studied by a security professional later.

My Windows 2012 server IP address is 10.1.62.21. My Kali VM IP address is 10.1.62.2. What I discovered is that My Kali box has two SSL Certificate that are vulnerable, I can see only one port have open is port 7777 and for linux you need port 7777 open. I can see several ports that are filtered but we don't have to worry about filtered ports. For my Windows 2012 server I see only informational exceptions from Nessus. Nmap we can see no open ports. So I believe that My kali and windows 2012 server is secure.

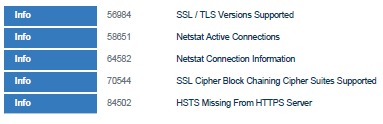
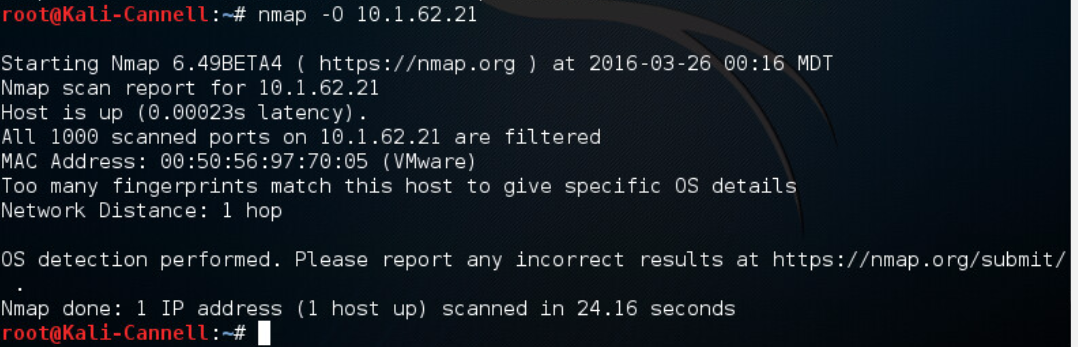
* Vulnerability Assessment of your VM
  + Needs to include a sample [2-3] of researched exploits associated with vulnerabilities found, and what those exploits do

Looking at my own target server 2012 which is 10.1.62.21 I can look at what my target server looks like in a nmap scan. I also did a nmap scan on my kali box to see what it looks like too.

**My Kali Nmap 10.1.62.2:**



**My nmap of my Windows 2012 server 10.1.62.21:**





NMAP:

Nmap scan report for 10.1.62.21

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.21 are filtered

MAC Address: 00:50:56:97:70:05 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

**Nmap scan report for 10.1.62.21**

**Host is up (-0.100s latency).**

**All 2000 scanned ports on 10.1.62.21 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:70:05 (VMware)**

Nmap scan report for 10.1.62.2

Host is up (0.0000050s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

7777/tcp open cbt

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.7 - 3.18

Network Distance: 0 hops

**Nmap scan report for 10.1.62.2**

**Host is up (0.0000030s latency).**

**Not shown: 1996 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

**5353/udp open|filtered zeroconf**

**Nmap done: 256 IP addresses (21 hosts up) scanned in 1299.83 seconds**

**root@Kali-Cannell:~#**

* + Include citations for your exploits

<http://cyberpedia.in/using-whois-a-command-for-information-gathering/>

<https://uwnthesis.wordpress.com/2013/07/31/kali-how-to-install-nessus-on-kali/>

<https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/>

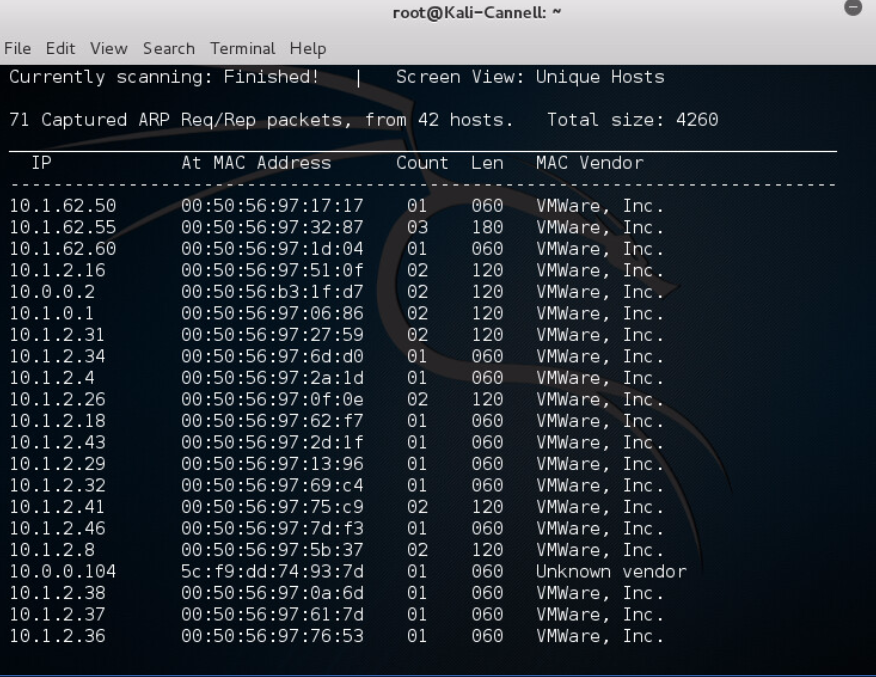
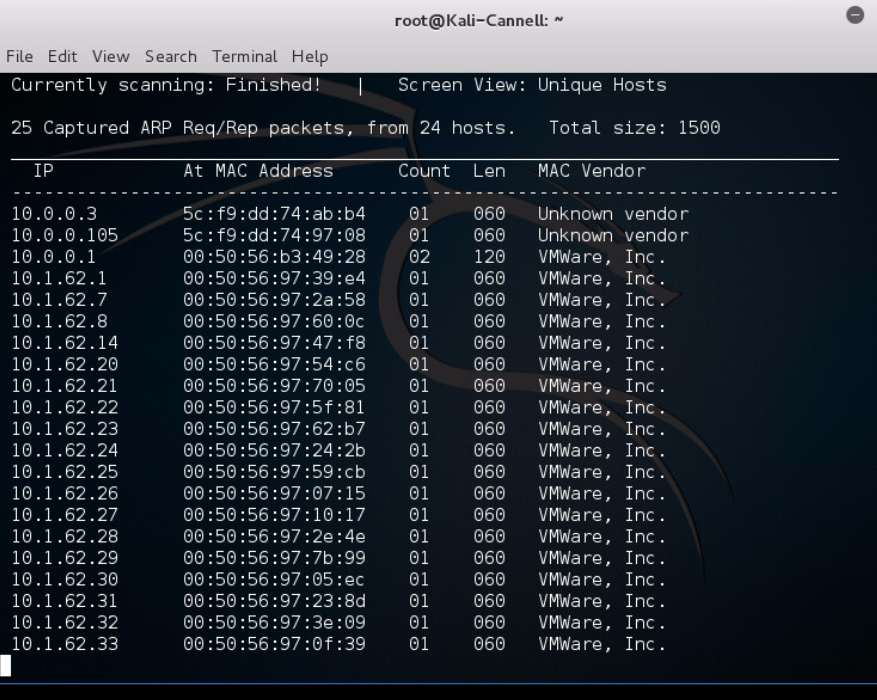
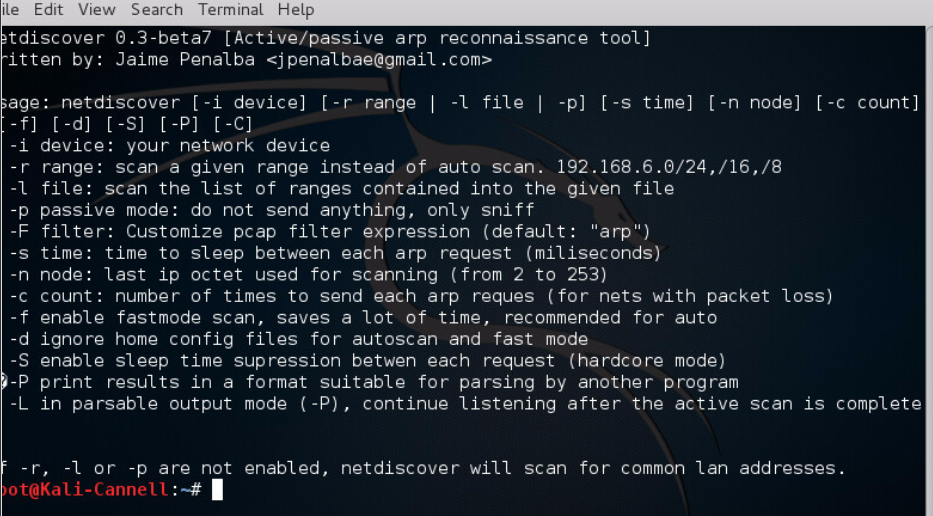
[http://null-byte.wonderhowto.com/how-to/hack-like-pro-advanced-nmap-for-reconnaissance-0151619](http://null-byte.wonderhowto.com/how-to/hack-like-pro-advanced-nmap-for-reconnaissance-0151619/)

<http://www.geekyshows.com/2013/07/how-to-use-nmap-in-kali-linux.html>

<https://steamcommunity.com/app/217140/discussions/2/616198623979610110/>

* List of devices on the network - provide IP addresses and as much identifying information that you can obtain on those devices. (i.e. host names, etc.)

**Netdiscover:**



**Nmap:**

Starting Nmap 6.49BETA4 ( [https://nmap.org](https://nmap.org/) ) at 2016-03-25 17:24 MDT

Nmap scan report for 10.1.62.1

Host is up (0.000090s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

7777/tcp open cbt

MAC Address: 00:50:56:97:39:E4 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.7

Host is up (0.00010s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

7777/tcp open cbt

MAC Address: 00:50:56:97:2A:58 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.8

Host is up (0.000086s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

7777/tcp open cbt

MAC Address: 00:50:56:97:60:0C (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.11

Host is up (0.000094s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

7777/tcp open cbt

MAC Address: 00:50:56:97:29:1A (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.14

Host is up (0.000081s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

7777/tcp open cbt

MAC Address: 00:50:56:97:47:F8 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.20

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.20 are filtered

MAC Address: 00:50:56:97:54:C6 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.21

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.21 are filtered

MAC Address: 00:50:56:97:70:05 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.22

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.22 are filtered

MAC Address: 00:50:56:97:5F:81 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.23

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.23 are filtered

MAC Address: 00:50:56:97:62:B7 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.24

Host is up (0.00040s latency).

All 1000 scanned ports on 10.1.62.24 are filtered

MAC Address: 00:50:56:97:24:2B (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.25

Host is up (0.00040s latency).

All 1000 scanned ports on 10.1.62.25 are filtered

MAC Address: 00:50:56:97:59:CB (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.26

Host is up (0.00049s latency).

All 1000 scanned ports on 10.1.62.26 are filtered

MAC Address: 00:50:56:97:07:15 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.27

Host is up (0.00026s latency).

All 1000 scanned ports on 10.1.62.27 are filtered

MAC Address: 00:50:56:97:10:17 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.28

Host is up (0.00039s latency).

All 1000 scanned ports on 10.1.62.28 are filtered

MAC Address: 00:50:56:97:2E:4E (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.29

Host is up (0.00040s latency).

All 1000 scanned ports on 10.1.62.29 are filtered

MAC Address: 00:50:56:97:7B:99 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.30

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.30 are filtered

MAC Address: 00:50:56:97:05:EC (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.31

Host is up (0.00016s latency).

All 1000 scanned ports on 10.1.62.31 are filtered

MAC Address: 00:50:56:97:23:8D (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.32

Host is up (-0.10s latency).

All 1000 scanned ports on 10.1.62.32 are filtered

MAC Address: 00:50:56:97:3E:09 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.33

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.33 are filtered

MAC Address: 00:50:56:97:0F:39 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.50

Host is up (0.000092s latency).

Not shown: 989 closed ports

PORT STATE SERVICE

21/tcp open ftp

25/tcp open smtp

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

1027/tcp open IIS

3372/tcp open msdtc

MAC Address: 00:50:56:97:17:17 (VMware)

Device type: general purpose

Running: Microsoft Windows 2000|XP|Me

OS CPE: cpe:/o:microsoft:windows\_2000::- cpe:/o:microsoft:windows\_2000::sp2 cpe:/o:microsoft:windows\_2000::sp4 cpe:/o:microsoft:windows\_xp::- cpe:/o:microsoft:windows\_xp::sp1 cpe:/o:microsoft:windows\_me

OS details: Microsoft Windows 2000 SP0/SP2/SP4 or Windows XP SP0/SP1, Microsoft Windows 2000 SP1, Microsoft Windows 2000 SP2, Microsoft Windows Millennium Edition (Me)

Network Distance: 1 hop

Nmap scan report for 10.1.62.55

Host is up (0.000094s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

MAC Address: 00:50:56:97:32:87 (VMware)

Device type: general purpose

Running: Microsoft Windows XP|2003

OS CPE: cpe:/o:microsoft:windows\_xp::sp2:professional cpe:/o:microsoft:windows\_server\_2003

OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003

Network Distance: 1 hop

Nmap scan report for 10.1.62.60

Host is up (0.00012s latency).

Not shown: 980 closed ports

PORT STATE SERVICE

21/tcp open ftp

53/tcp open domain

80/tcp open http

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

1028/tcp open unknown

1040/tcp open netsaint

1041/tcp open danf-ak2

1051/tcp open optima-vnet

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3389/tcp open ms-wbt-server

MAC Address: 00:50:56:97:1D:04 (VMware)

Device type: general purpose

Running: Microsoft Windows XP|2003

OS CPE: cpe:/o:microsoft:windows\_xp cpe:/o:microsoft:windows\_server\_2003

OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003

Network Distance: 1 hop

Nmap scan report for 10.1.62.2

Host is up (0.0000050s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

7777/tcp open cbt

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.7 - 3.18

Network Distance: 0 hops

root@Kali-Cannell:~# nmap -sS -sU -PN [10.1.62.0/24](http://10.1.62.0/24)

Starting Nmap 6.49BETA4 ( [https://nmap.org](https://nmap.org/) ) at 2016-03-25 21:42 MDT

Nmap scan report for 10.1.62.1

Host is up (0.00014s latency).

Not shown: 1995 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

1124/udp open|filtered hpvmmcontrol

5353/udp open zeroconf

MAC Address: 00:50:56:97:39:E4 (VMware)

Nmap scan report for 10.1.62.5

Host is up (0.00011s latency).

Not shown: 1993 closed ports

PORT STATE SERVICE

22/tcp open ssh

111/tcp open rpcbind

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

111/udp open rpcbind

5353/udp open zeroconf

MAC Address: 00:50:56:97:3F:CB (VMware)

Nmap scan report for 10.1.62.7

Host is up (0.00012s latency).

Not shown: 1996 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

5353/udp open zeroconf

MAC Address: 00:50:56:97:2A:58 (VMware)

Nmap scan report for 10.1.62.8

Host is up (0.00013s latency).

Not shown: 1996 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

5353/udp open zeroconf

MAC Address: 00:50:56:97:60:0C (VMware)

Nmap scan report for 10.1.62.12

Host is up (0.00013s latency).

Not shown: 1994 closed ports

PORT STATE SERVICE

111/tcp open rpcbind

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

111/udp open rpcbind

5353/udp open zeroconf

MAC Address: 00:50:56:97:07:B1 (VMware)

Nmap scan report for 10.1.62.14

Host is up (0.00014s latency).

Not shown: 1996 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

5353/udp open zeroconf

MAC Address: 00:50:56:97:47:F8 (VMware)

Nmap scan report for 10.1.62.20

Host is up (-0.100s latency).

All 2000 scanned ports on 10.1.62.20 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:54:C6 (VMware)

Nmap scan report for 10.1.62.21

Host is up (-0.100s latency).

All 2000 scanned ports on 10.1.62.21 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:70:05 (VMware)

Nmap scan report for 10.1.62.22

Host is up (-0.100s latency).

All 2000 scanned ports on 10.1.62.22 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:5F:81 (VMware)

Nmap scan report for 10.1.62.23

Host is up (-0.100s latency).

All 2000 scanned ports on 10.1.62.23 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:62:B7 (VMware)

Nmap scan report for 10.1.62.24

Host is up (0.00049s latency).

All 2000 scanned ports on 10.1.62.24 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:24:2B (VMware)

Nmap scan report for 10.1.62.25

Host is up (0.00040s latency).

All 2000 scanned ports on 10.1.62.25 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:59:CB (VMware)

Nmap scan report for 10.1.62.26

Host is up (0.00026s latency).

All 2000 scanned ports on 10.1.62.26 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:07:15 (VMware)

Nmap scan report for 10.1.62.27

Host is up (0.00029s latency).

All 2000 scanned ports on 10.1.62.27 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:10:17 (VMware)

Nmap scan report for 10.1.62.28

Host is up (0.00039s latency).

All 2000 scanned ports on 10.1.62.28 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:2E:4E (VMware)

Nmap scan report for 10.1.62.29

Host is up (0.00038s latency).

All 2000 scanned ports on 10.1.62.29 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:7B:99 (VMware)

Nmap scan report for 10.1.62.31

Host is up (-0.100s latency).

All 2000 scanned ports on 10.1.62.31 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:23:8D (VMware)

Nmap scan report for 10.1.62.32

Host is up (-0.100s latency).

All 2000 scanned ports on 10.1.62.32 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:3E:09 (VMware)

Nmap scan report for 10.1.62.33

Host is up (-0.087s latency).

All 2000 scanned ports on 10.1.62.33 are filtered (1000) or open|filtered (1000)

MAC Address: 00:50:56:97:0F:39 (VMware)

Nmap scan report for 10.1.62.50

Host is up (0.00011s latency).

Not shown: 1990 closed ports

PORT STATE SERVICE

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

3372/tcp open msdtc

137/udp open netbios-ns

138/udp open|filtered netbios-dgm

445/udp open|filtered microsoft-ds

500/udp open|filtered isakmp

1029/udp open solid-mux

MAC Address: 00:50:56:97:17:17 (VMware)

Nmap scan report for 10.1.62.2

Host is up (0.0000030s latency).

Not shown: 1996 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

5353/udp open|filtered zeroconf

Nmap done: 256 IP addresses (21 hosts up) scanned in 1299.83 seconds

root@Kali-Cannell:~#

**Classes Server 2012:**

Nmap scan report for 10.1.62.20

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.20 are filtered

MAC Address: 00:50:56:97:54:C6 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.21

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.21 are filtered

MAC Address: 00:50:56:97:70:05 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.22

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.22 are filtered

MAC Address: 00:50:56:97:5F:81 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.23

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.23 are filtered

MAC Address: 00:50:56:97:62:B7 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.24

Host is up (0.00040s latency).

All 1000 scanned ports on 10.1.62.24 are filtered

MAC Address: 00:50:56:97:24:2B (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.25

Host is up (0.00040s latency).

All 1000 scanned ports on 10.1.62.25 are filtered

MAC Address: 00:50:56:97:59:CB (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.26

Host is up (0.00049s latency).

All 1000 scanned ports on 10.1.62.26 are filtered

MAC Address: 00:50:56:97:07:15 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.27

Host is up (0.00026s latency).

All 1000 scanned ports on 10.1.62.27 are filtered

MAC Address: 00:50:56:97:10:17 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.28

Host is up (0.00039s latency).

All 1000 scanned ports on 10.1.62.28 are filtered

MAC Address: 00:50:56:97:2E:4E (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.29

Host is up (0.00040s latency).

All 1000 scanned ports on 10.1.62.29 are filtered

MAC Address: 00:50:56:97:7B:99 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.30

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.30 are filtered

MAC Address: 00:50:56:97:05:EC (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.31

Host is up (0.00016s latency).

All 1000 scanned ports on 10.1.62.31 are filtered

MAC Address: 00:50:56:97:23:8D (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.32

Host is up (-0.10s latency).

All 1000 scanned ports on 10.1.62.32 are filtered

MAC Address: 00:50:56:97:3E:09 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.1.62.33

Host is up (-0.100s latency).

All 1000 scanned ports on 10.1.62.33 are filtered

MAC Address: 00:50:56:97:0F:39 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

**Classes Kali machines:**

Nmap scan report for 10.1.62.1

Host is up (0.00014s latency).

Not shown: 1995 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

1124/udp open|filtered hpvmmcontrol

5353/udp open zeroconf

MAC Address: 00:50:56:97:39:E4 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.5

Host is up (0.00011s latency).

Not shown: 1993 closed ports

PORT STATE SERVICE

22/tcp open ssh

111/tcp open rpcbind

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

111/udp open rpcbind

5353/udp open zeroconf

MAC Address: 00:50:56:97:3F:CB (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.7

Host is up (0.00012s latency).

Not shown: 1996 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

5353/udp open zeroconf

MAC Address: 00:50:56:97:2A:58 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.8

Host is up (0.00013s latency).

Not shown: 1996 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

5353/udp open zeroconf

MAC Address: 00:50:56:97:60:0C (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.12

Host is up (0.00013s latency).

Not shown: 1994 closed ports

PORT STATE SERVICE

111/tcp open rpcbind

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

111/udp open rpcbind

5353/udp open zeroconf

MAC Address: 00:50:56:97:07:B1 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

Nmap scan report for 10.1.62.14

Host is up (0.00014s latency).

Not shown: 1996 closed ports

PORT STATE SERVICE

7777/tcp open cbt

68/udp open|filtered dhcpc

69/udp open|filtered tftp

5353/udp open zeroconf

MAC Address: 00:50:56:97:47:F8 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3

OS details: Linux 3.2 - 3.19

Network Distance: 1 hop

**Different machines:**

Nmap scan report for 10.1.62.50

Host is up (0.00011s latency).

Not shown: 1990 closed ports

PORT STATE SERVICE

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

3372/tcp open msdtc

137/udp open netbios-ns

138/udp open|filtered netbios-dgm

445/udp open|filtered microsoft-ds

500/udp open|filtered isakmp

1029/udp open solid-mux

MAC Address: 00:50:56:97:17:17 (VMware)

Nmap scan report for 10.1.62.50

Host is up (0.000092s latency).

Not shown: 989 closed ports

PORT STATE SERVICE

21/tcp open ftp

25/tcp open smtp

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

1027/tcp open IIS

3372/tcp open msdtc

MAC Address: 00:50:56:97:17:17 (VMware)

Device type: general purpose

Running: Microsoft Windows 2000|XP|Me

OS CPE: cpe:/o:microsoft:windows\_2000::- cpe:/o:microsoft:windows\_2000::sp2 cpe:/o:microsoft:windows\_2000::sp4 cpe:/o:microsoft:windows\_xp::- cpe:/o:microsoft:windows\_xp::sp1 cpe:/o:microsoft:windows\_me

OS details: Microsoft Windows 2000 SP0/SP2/SP4 or Windows XP SP0/SP1, Microsoft Windows 2000 SP1, Microsoft Windows 2000 SP2, Microsoft Windows Millennium Edition (Me)

Network Distance: 1 hop

Nmap scan report for 10.1.62.55

Host is up (0.000094s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

MAC Address: 00:50:56:97:32:87 (VMware)

Device type: general purpose

Running: Microsoft Windows XP|2003

OS CPE: cpe:/o:microsoft:windows\_xp::sp2:professional cpe:/o:microsoft:windows\_server\_2003

OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003

Network Distance: 1 hop

Nmap scan report for 10.1.62.60

Host is up (0.00012s latency).

Not shown: 980 closed ports

PORT STATE SERVICE

21/tcp open ftp

53/tcp open domain

80/tcp open http

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

1028/tcp open unknown

1040/tcp open netsaint

1041/tcp open danf-ak2

1051/tcp open optima-vnet

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3389/tcp open ms-wbt-server

MAC Address: 00:50:56:97:1D:04 (VMware)

Device type: general purpose

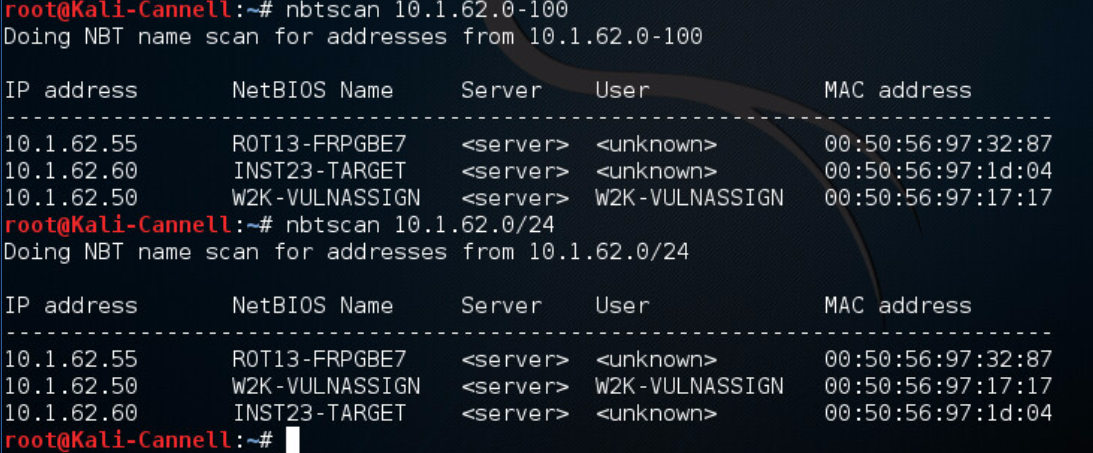
Running: Microsoft Windows XP|2003

OS CPE: cpe:/o:microsoft:windows\_xp cpe:/o:microsoft:windows\_server\_2003

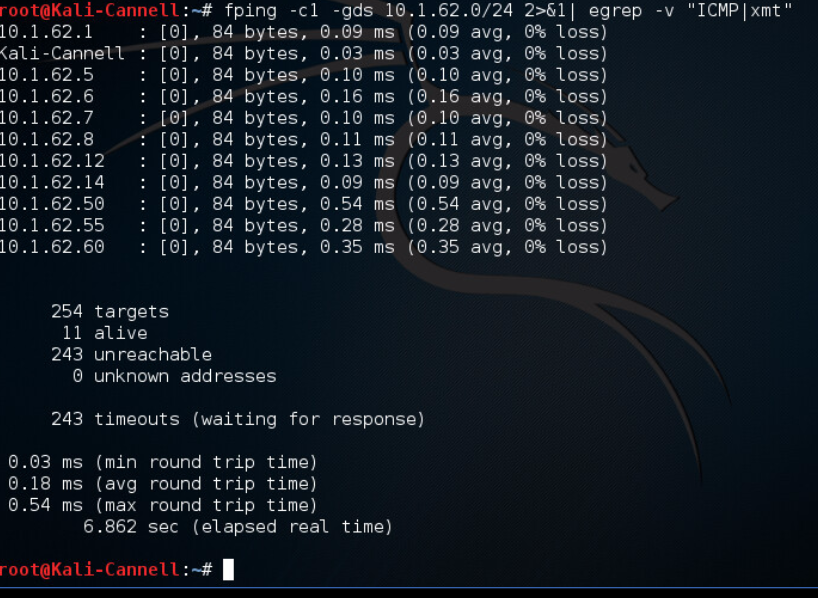
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003

Nbtscan:

With nbtscan we find out which boxes on the network are not student boxes



Fping:



**I decided to do a work all three.**

**NMAP:**

**Starting Nmap 6.49BETA4 (** [**https://nmap.org**](https://nmap.org/) **) at 2016-03-25 17:24 MDT**

**Nmap scan report for 10.1.62.1**

**Host is up (0.000090s latency).**

**Not shown: 999 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**MAC Address: 00:50:56:97:39:E4 (VMware)**

**Device type: general purpose**

**Running: Linux 3.X**

**OS CPE: cpe:/o:linux:linux\_kernel:3**

**OS details: Linux 3.2 - 3.19**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.7**

**Host is up (0.00010s latency).**

**Not shown: 999 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**MAC Address: 00:50:56:97:2A:58 (VMware)**

**Device type: general purpose**

**Running: Linux 3.X**

**OS CPE: cpe:/o:linux:linux\_kernel:3**

**OS details: Linux 3.2 - 3.19**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.8**

**Host is up (0.000086s latency).**

**Not shown: 999 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**MAC Address: 00:50:56:97:60:0C (VMware)**

**Device type: general purpose**

**Running: Linux 3.X**

**OS CPE: cpe:/o:linux:linux\_kernel:3**

**OS details: Linux 3.2 - 3.19**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.11**

**Host is up (0.000094s latency).**

**Not shown: 999 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**MAC Address: 00:50:56:97:29:1A (VMware)**

**Device type: general purpose**

**Running: Linux 3.X**

**OS CPE: cpe:/o:linux:linux\_kernel:3**

**OS details: Linux 3.2 - 3.19**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.14**

**Host is up (0.000081s latency).**

**Not shown: 999 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**MAC Address: 00:50:56:97:47:F8 (VMware)**

**Device type: general purpose**

**Running: Linux 3.X**

**OS CPE: cpe:/o:linux:linux\_kernel:3**

**OS details: Linux 3.2 - 3.19**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.20**

**Host is up (-0.100s latency).**

**All 1000 scanned ports on 10.1.62.20 are filtered**

**MAC Address: 00:50:56:97:54:C6 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.21**

**Host is up (-0.100s latency).**

**All 1000 scanned ports on 10.1.62.21 are filtered**

**MAC Address: 00:50:56:97:70:05 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.22**

**Host is up (-0.100s latency).**

**All 1000 scanned ports on 10.1.62.22 are filtered**

**MAC Address: 00:50:56:97:5F:81 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.23**

**Host is up (-0.100s latency).**

**All 1000 scanned ports on 10.1.62.23 are filtered**

**MAC Address: 00:50:56:97:62:B7 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.24**

**Host is up (0.00040s latency).**

**All 1000 scanned ports on 10.1.62.24 are filtered**

**MAC Address: 00:50:56:97:24:2B (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.25**

**Host is up (0.00040s latency).**

**All 1000 scanned ports on 10.1.62.25 are filtered**

**MAC Address: 00:50:56:97:59:CB (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.26**

**Host is up (0.00049s latency).**

**All 1000 scanned ports on 10.1.62.26 are filtered**

**MAC Address: 00:50:56:97:07:15 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.27**

**Host is up (0.00026s latency).**

**All 1000 scanned ports on 10.1.62.27 are filtered**

**MAC Address: 00:50:56:97:10:17 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.28**

**Host is up (0.00039s latency).**

**All 1000 scanned ports on 10.1.62.28 are filtered**

**MAC Address: 00:50:56:97:2E:4E (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.29**

**Host is up (0.00040s latency).**

**All 1000 scanned ports on 10.1.62.29 are filtered**

**MAC Address: 00:50:56:97:7B:99 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.30**

**Host is up (-0.100s latency).**

**All 1000 scanned ports on 10.1.62.30 are filtered**

**MAC Address: 00:50:56:97:05:EC (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.31**

**Host is up (0.00016s latency).**

**All 1000 scanned ports on 10.1.62.31 are filtered**

**MAC Address: 00:50:56:97:23:8D (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.32**

**Host is up (-0.10s latency).**

**All 1000 scanned ports on 10.1.62.32 are filtered**

**MAC Address: 00:50:56:97:3E:09 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.33**

**Host is up (-0.100s latency).**

**All 1000 scanned ports on 10.1.62.33 are filtered**

**MAC Address: 00:50:56:97:0F:39 (VMware)**

**Too many fingerprints match this host to give specific OS details**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.50**

**Host is up (0.000092s latency).**

**Not shown: 989 closed ports**

**PORT STATE SERVICE**

**21/tcp open ftp**

**25/tcp open smtp**

**80/tcp open http**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**443/tcp open https**

**445/tcp open microsoft-ds**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**1027/tcp open IIS**

**3372/tcp open msdtc**

**MAC Address: 00:50:56:97:17:17 (VMware)**

**Device type: general purpose**

**Running: Microsoft Windows 2000|XP|Me**

**OS CPE: cpe:/o:microsoft:windows\_2000::- cpe:/o:microsoft:windows\_2000::sp2 cpe:/o:microsoft:windows\_2000::sp4 cpe:/o:microsoft:windows\_xp::- cpe:/o:microsoft:windows\_xp::sp1 cpe:/o:microsoft:windows\_me**

**OS details: Microsoft Windows 2000 SP0/SP2/SP4 or Windows XP SP0/SP1, Microsoft Windows 2000 SP1, Microsoft Windows 2000 SP2, Microsoft Windows Millennium Edition (Me)**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.55**

**Host is up (0.000094s latency).**

**Not shown: 995 closed ports**

**PORT STATE SERVICE**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**MAC Address: 00:50:56:97:32:87 (VMware)**

**Device type: general purpose**

**Running: Microsoft Windows XP|2003**

**OS CPE: cpe:/o:microsoft:windows\_xp::sp2:professional cpe:/o:microsoft:windows\_server\_2003**

**OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.60**

**Host is up (0.00012s latency).**

**Not shown: 980 closed ports**

**PORT STATE SERVICE**

**21/tcp open ftp**

**53/tcp open domain**

**80/tcp open http**

**88/tcp open kerberos-sec**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**389/tcp open ldap**

**445/tcp open microsoft-ds**

**464/tcp open kpasswd5**

**593/tcp open http-rpc-epmap**

**636/tcp open ldapssl**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**1028/tcp open unknown**

**1040/tcp open netsaint**

**1041/tcp open danf-ak2**

**1051/tcp open optima-vnet**

**3268/tcp open globalcatLDAP**

**3269/tcp open globalcatLDAPssl**

**3389/tcp open ms-wbt-server**

**MAC Address: 00:50:56:97:1D:04 (VMware)**

**Device type: general purpose**

**Running: Microsoft Windows XP|2003**

**OS CPE: cpe:/o:microsoft:windows\_xp cpe:/o:microsoft:windows\_server\_2003**

**OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.2**

**Host is up (0.0000050s latency).**

**Not shown: 999 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**Device type: general purpose**

**Running: Linux 3.X**

**OS CPE: cpe:/o:linux:linux\_kernel:3**

**OS details: Linux 3.7 - 3.18**

**Network Distance: 0 hops**

**root@Kali-Cannell:~# nmap -sS -sU -PN** [**10.1.62.0/24**](http://10.1.62.0/24)

**Starting Nmap 6.49BETA4 (** [**https://nmap.org**](https://nmap.org/) **) at 2016-03-25 21:42 MDT**

**Nmap scan report for 10.1.62.1**

**Host is up (0.00014s latency).**

**Not shown: 1995 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

**1124/udp open|filtered hpvmmcontrol**

**5353/udp open zeroconf**

**MAC Address: 00:50:56:97:39:E4 (VMware)**

**Nmap scan report for 10.1.62.5**

**Host is up (0.00011s latency).**

**Not shown: 1993 closed ports**

**PORT STATE SERVICE**

**22/tcp open ssh**

**111/tcp open rpcbind**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

**111/udp open rpcbind**

**5353/udp open zeroconf**

**MAC Address: 00:50:56:97:3F:CB (VMware)**

**Nmap scan report for 10.1.62.7**

**Host is up (0.00012s latency).**

**Not shown: 1996 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

**5353/udp open zeroconf**

**MAC Address: 00:50:56:97:2A:58 (VMware)**

**Nmap scan report for 10.1.62.8**

**Host is up (0.00013s latency).**

**Not shown: 1996 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

**5353/udp open zeroconf**

**MAC Address: 00:50:56:97:60:0C (VMware)**

**Nmap scan report for 10.1.62.12**

**Host is up (0.00013s latency).**

**Not shown: 1994 closed ports**

**PORT STATE SERVICE**

**111/tcp open rpcbind**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

**111/udp open rpcbind**

**5353/udp open zeroconf**

**MAC Address: 00:50:56:97:07:B1 (VMware)**

**Nmap scan report for 10.1.62.14**

**Host is up (0.00014s latency).**

**Not shown: 1996 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

**5353/udp open zeroconf**

**MAC Address: 00:50:56:97:47:F8 (VMware)**

**Nmap scan report for 10.1.62.20**

**Host is up (-0.100s latency).**

**All 2000 scanned ports on 10.1.62.20 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:54:C6 (VMware)**

**Nmap scan report for 10.1.62.21**

**Host is up (-0.100s latency).**

**All 2000 scanned ports on 10.1.62.21 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:70:05 (VMware)**

**Nmap scan report for 10.1.62.22**

**Host is up (-0.100s latency).**

**All 2000 scanned ports on 10.1.62.22 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:5F:81 (VMware)**

**Nmap scan report for 10.1.62.23**

**Host is up (-0.100s latency).**

**All 2000 scanned ports on 10.1.62.23 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:62:B7 (VMware)**

**Nmap scan report for 10.1.62.24**

**Host is up (0.00049s latency).**

**All 2000 scanned ports on 10.1.62.24 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:24:2B (VMware)**

**Nmap scan report for 10.1.62.25**

**Host is up (0.00040s latency).**

**All 2000 scanned ports on 10.1.62.25 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:59:CB (VMware)**

**Nmap scan report for 10.1.62.26**

**Host is up (0.00026s latency).**

**All 2000 scanned ports on 10.1.62.26 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:07:15 (VMware)**

**Nmap scan report for 10.1.62.27**

**Host is up (0.00029s latency).**

**All 2000 scanned ports on 10.1.62.27 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:10:17 (VMware)**

**Nmap scan report for 10.1.62.28**

**Host is up (0.00039s latency).**

**All 2000 scanned ports on 10.1.62.28 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:2E:4E (VMware)**

**Nmap scan report for 10.1.62.29**

**Host is up (0.00038s latency).**

**All 2000 scanned ports on 10.1.62.29 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:7B:99 (VMware)**

**Nmap scan report for 10.1.62.31**

**Host is up (-0.100s latency).**

**All 2000 scanned ports on 10.1.62.31 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:23:8D (VMware)**

**Nmap scan report for 10.1.62.32**

**Host is up (-0.100s latency).**

**All 2000 scanned ports on 10.1.62.32 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:3E:09 (VMware)**

**Nmap scan report for 10.1.62.33**

**Host is up (-0.087s latency).**

**All 2000 scanned ports on 10.1.62.33 are filtered (1000) or open|filtered (1000)**

**MAC Address: 00:50:56:97:0F:39 (VMware)**

**Nmap scan report for 10.1.62.50**

**Host is up (0.00011s latency).**

**Not shown: 1990 closed ports**

**PORT STATE SERVICE**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**3372/tcp open msdtc**

**137/udp open netbios-ns**

**138/udp open|filtered netbios-dgm**

**445/udp open|filtered microsoft-ds**

**500/udp open|filtered isakmp**

**1029/udp open solid-mux**

**MAC Address: 00:50:56:97:17:17 (VMware)**

**Nmap scan report for 10.1.62.2**

**Host is up (0.0000030s latency).**

**Not shown: 1996 closed ports**

**PORT STATE SERVICE**

**7777/tcp open cbt**

**68/udp open|filtered dhcpc**

**69/udp open|filtered tftp**

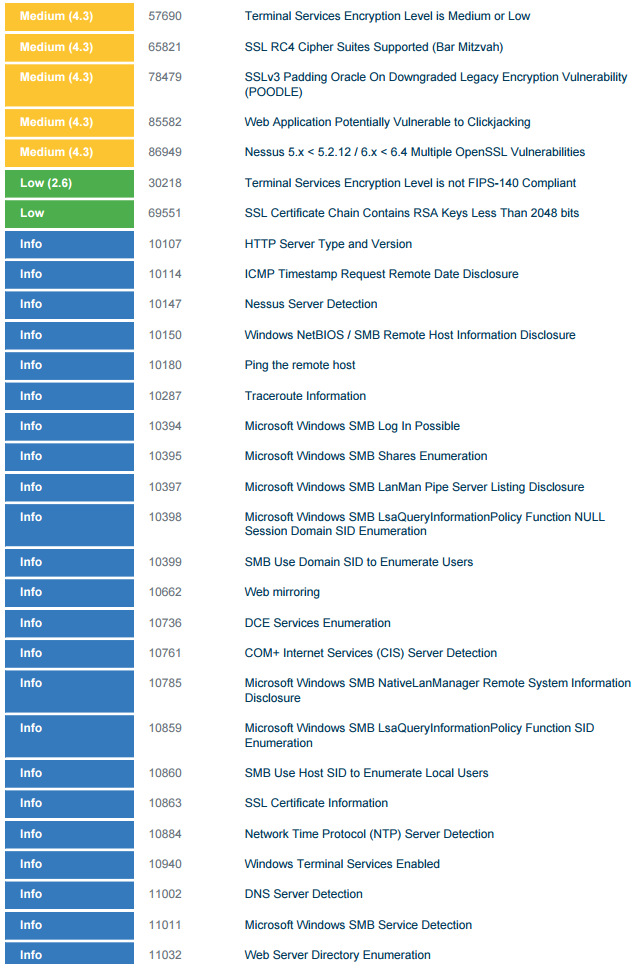
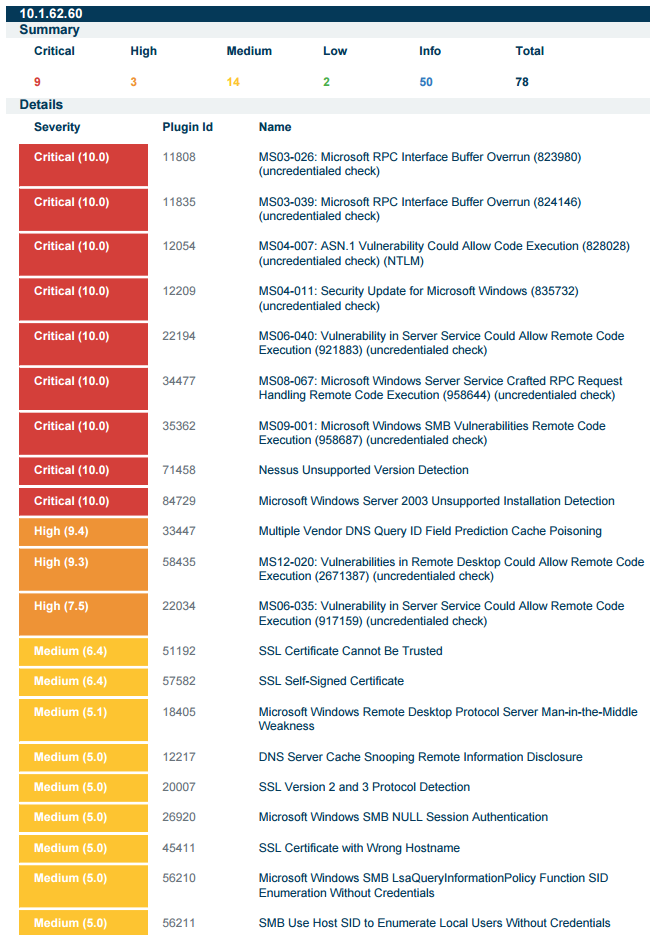
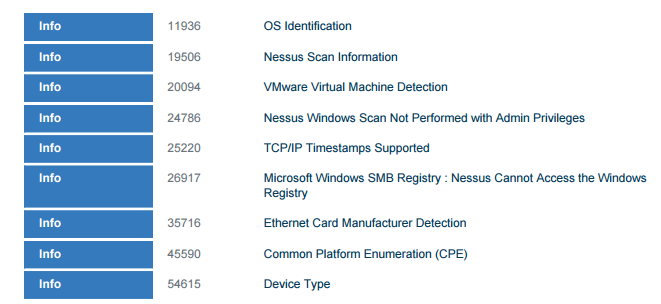
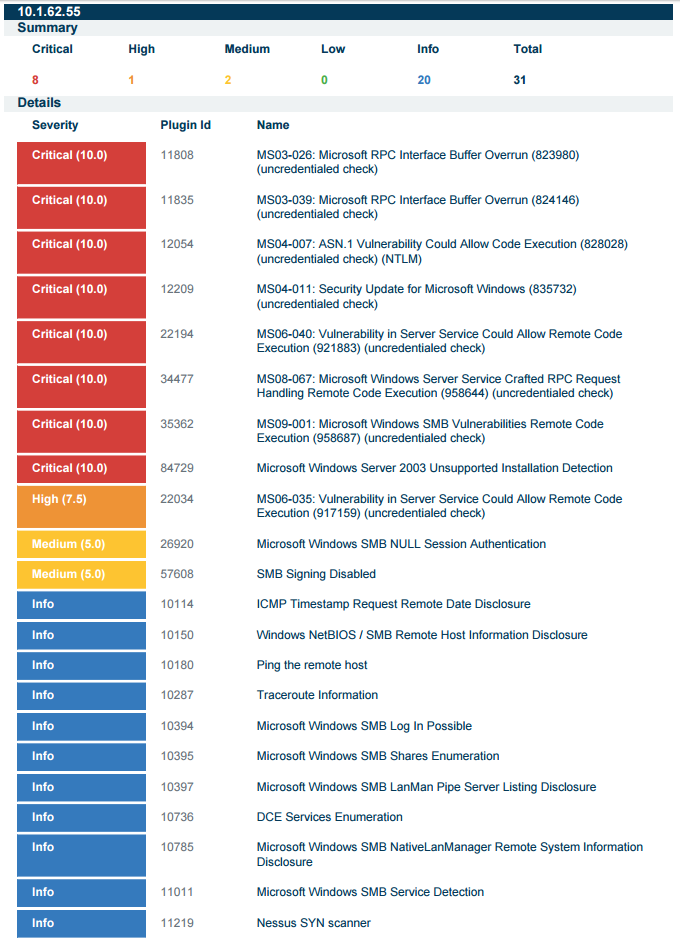
**5353/udp open|filtered zeroconf**

**Nmap done: 256 IP addresses (21 hosts up) scanned in 1299.83 seconds**

**root@Kali-Cannell:~#**

* + DO NOT compromise any of the machines. This is an information-gathering mission.
* Vulnerability Assessment of the two other computers you selected.

**Nessus:**



**Nmap scan report for 10.1.62.50**

**Host is up (0.00011s latency).**

**Not shown: 1990 closed ports**

**PORT STATE SERVICE**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**3372/tcp open msdtc**

**137/udp open netbios-ns**

**138/udp open|filtered netbios-dgm**

**445/udp open|filtered microsoft-ds**

**500/udp open|filtered isakmp**

**1029/udp open solid-mux**

**MAC Address: 00:50:56:97:17:17 (VMware)**

**Nmap scan report for 10.1.62.50**

**Host is up (0.000092s latency).**

**Not shown: 989 closed ports**

**PORT STATE SERVICE**

**21/tcp open ftp**

**25/tcp open smtp**

**80/tcp open http**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**443/tcp open https**

**445/tcp open microsoft-ds**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**1027/tcp open IIS**

**3372/tcp open msdtc**

**MAC Address: 00:50:56:97:17:17 (VMware)**

**Device type: general purpose**

**Running: Microsoft Windows 2000|XP|Me**

**OS CPE: cpe:/o:microsoft:windows\_2000::- cpe:/o:microsoft:windows\_2000::sp2 cpe:/o:microsoft:windows\_2000::sp4 cpe:/o:microsoft:windows\_xp::- cpe:/o:microsoft:windows\_xp::sp1 cpe:/o:microsoft:windows\_me**

**OS details: Microsoft Windows 2000 SP0/SP2/SP4 or Windows XP SP0/SP1, Microsoft Windows 2000 SP1, Microsoft Windows 2000 SP2, Microsoft Windows Millennium Edition (Me)**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.55**

**Host is up (0.000094s latency).**

**Not shown: 995 closed ports**

**PORT STATE SERVICE**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**MAC Address: 00:50:56:97:32:87 (VMware)**

**Device type: general purpose**

**Running: Microsoft Windows XP|2003**

**OS CPE: cpe:/o:microsoft:windows\_xp::sp2:professional cpe:/o:microsoft:windows\_server\_2003**

**OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003**

**Network Distance: 1 hop**

**Nmap scan report for 10.1.62.60**

**Host is up (0.00012s latency).**

**Not shown: 980 closed ports**

**PORT STATE SERVICE**

**21/tcp open ftp**

**53/tcp open domain**

**80/tcp open http**

**88/tcp open kerberos-sec**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**389/tcp open ldap**

**445/tcp open microsoft-ds**

**464/tcp open kpasswd5**

**593/tcp open http-rpc-epmap**

**636/tcp open ldapssl**

**1025/tcp open NFS-or-IIS**

**1026/tcp open LSA-or-nterm**

**1028/tcp open unknown**

**1040/tcp open netsaint**

**1041/tcp open danf-ak2**

**1051/tcp open optima-vnet**

**3268/tcp open globalcatLDAP**

**3269/tcp open globalcatLDAPssl**

**3389/tcp open ms-wbt-server**

**MAC Address: 00:50:56:97:1D:04 (VMware)**

**Device type: general purpose**

**Running: Microsoft Windows XP|2003**

**OS CPE: cpe:/o:microsoft:windows\_xp cpe:/o:microsoft:windows\_server\_2003**

**OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003**

**Network Distance: 1 hop**

* Appendix - containing a report from the tool(s) you used to perform your VA, if your tool produces a standard report. If the tool does not produce a report, then that needs to be noted along with the tool you used, and a summary of what information was produced.

I will attach the Nessus report when I submit the assignment, and all my NMAP notes. I also used Wireshark so I will attach my packet capture.

**NOTE:** Each of you has been given two VMs. One was created with Kali Linux, the other was created with Windows Server 2012 Standard.