MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Aug. 27, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

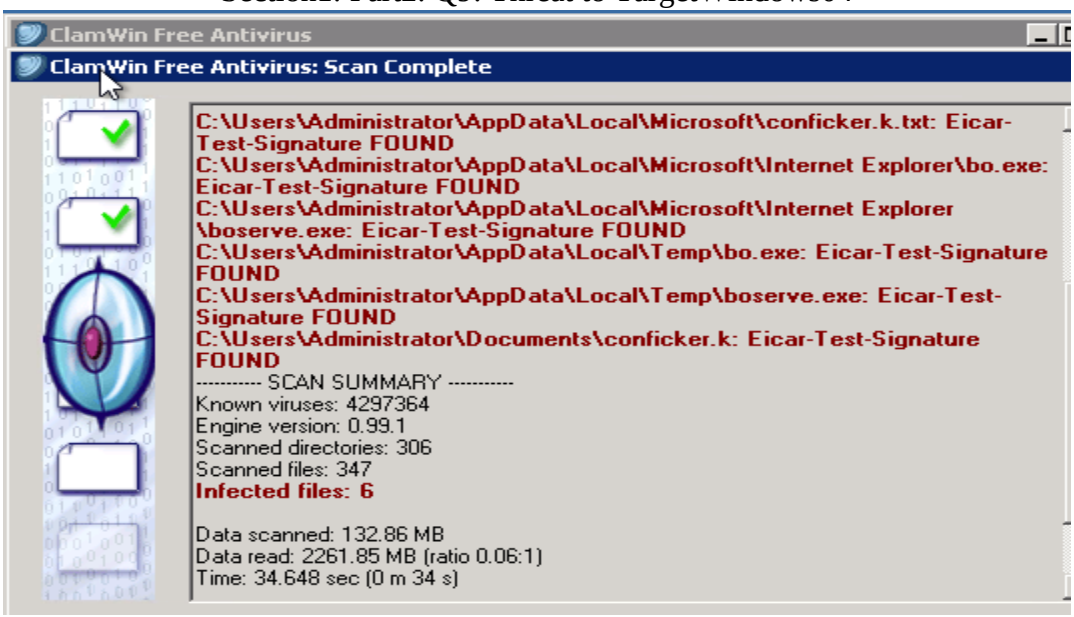
LAB REPORT FILE (LAB1)

SECTION 1

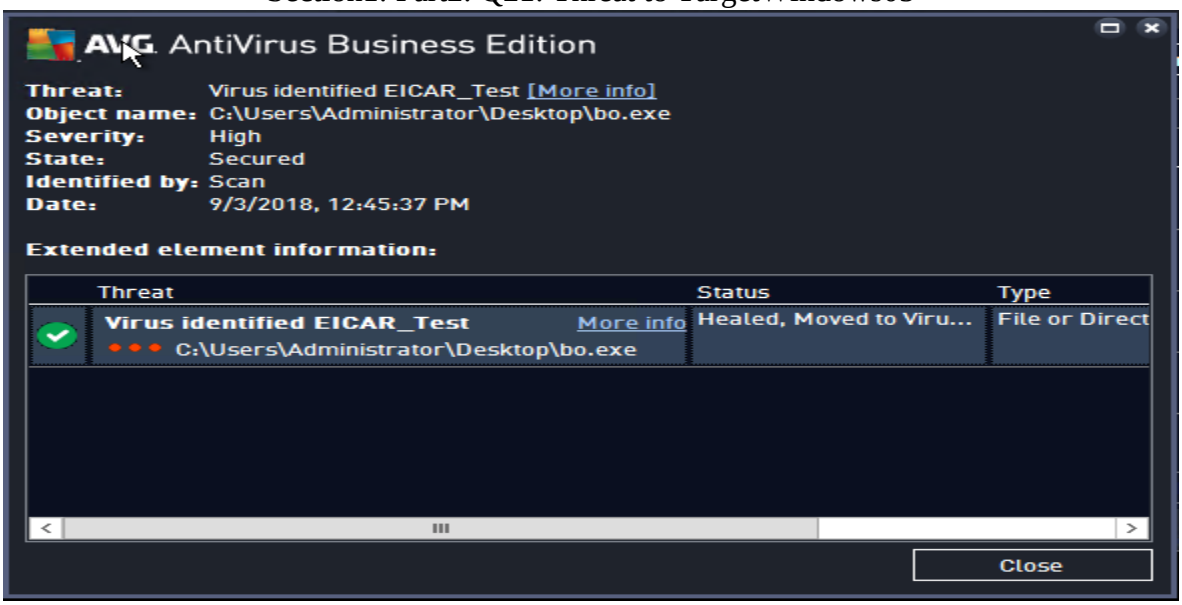
Section1: Part1: Q3: Nmap OS scan for 100.16.16.50

```
C:\Users\Administrator>nmap -O -v 100.16.16.50

Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-03 12:02 Pacific Daylight Time
Initiating ARP Ping Scan at 12:02
Scanning 100.16.16.50 [1 port]
Completed ARP Ping Scan at 12:02, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:02
Completed Parallel DNS resolution of 1 host. at 12:02, 16.52s elapsed
Initiating SYN Stealth Scan at 12:02
Scanning 100.16.16.50 [1000 ports]
Discovered open port 445/tcp on 100.16.16.50
Discovered open port 3389/tcp on 100.16.16.50
Discovered open port 22/tcp on 100.16.16.50
Discovered open port 139/tcp on 100.16.16.50
Discovered open port 135/tcp on 100.16.16.50
Discovered open port 1027/tcp on 100.16.16.50
Completed SYN Stealth Scan at 12:02, 1.17s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.16.16.50
Nmap scan report for 100.16.16.50
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1027/tcp open  IIS
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A6:B0:8D (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
```

Section1: Part2: Q9: Threat to TargetWindows04



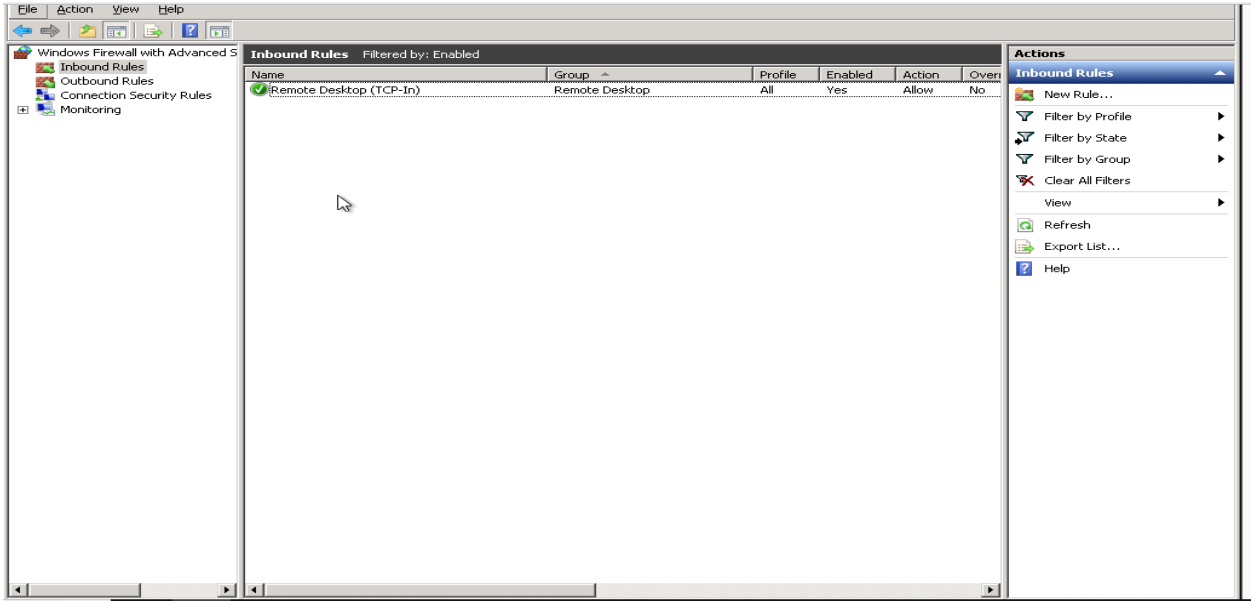
Section1: Part2: Q21: Threat to TargetWindows05



Section1: Part3: Q25: Nmap scan for TargetVulnerable01 and Reduced attack surface

```
C:\Users\Administrator>nmap -O -v 100.16.16.50

Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-03 13:01 Pacific Daylight Time
Initiating ARP Ping Scan at 13:01
Scanning 100.16.16.50 [1 port]
Completed ARP Ping Scan at 13:01, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:01
Completed Parallel DNS resolution of 1 host. at 13:02, 16.50s elapsed
Initiating SYN Stealth Scan at 13:02
Scanning 100.16.16.50 [1000 ports]
Discovered open port 3389/tcp on 100.16.16.50
Completed SYN Stealth Scan at 13:02, 4.99s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.16.16.50
Nmap scan report for 100.16.16.50
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A6:B0:8D (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2003|2008
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_ser
ver_2008::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2008 E
nterprise SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.50 seconds
           Raw packets sent: 2036 (91.374KB) | Rcvd: 14 (954B)

C:\Users\Administrator>
```

Section1: Part4: Q6: Enabled Inbound Rule on Windows 2008



Section1: Part4: Q24: Nmap scan for TargetVulnerable04 and Reduced attack surface

Administrator: Command Prompt

```
Completed Parallel DNS resolution of 1 host. at 13:26, 16.56s elapsed
Initiating SYN Stealth Scan at 13:26
Scanning 100.20.9.25 [1000 ports]
Discovered open port 3389/tcp on 100.20.9.25
Completed SYN Stealth Scan at 13:26, 4.99s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.20.9.25
Retrying OS detection (try #2) against 100.20.9.25
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
Nmap scan report for 100.20.9.25
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A6:49:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|printer|broadband router|router|firewall
Running (JUST GUESSING): Motorola embedded (92%), Konica Minolta embedded (86%), D-Link embedded (86%), Adtran embedded
(85%), ZyXEL ZyNOS 3.X (85%)
OS CPE: cpe:/h:motorola:rfs_6000 cpe:/h:konicaminolta:1600f cpe:/h:dlink:di-808hv cpe:/h:adtran:total_access_904 cpe:/o:
zyxel:zynos:3.62
Aggressive OS guesses: Motorola RFS 6000 wireless switch (92%), Konica Minolta 1600f printer (86%), D-Link DI-808HV rout
er (86%), Adtran Total Access 904 router (85%), ZyXEL ZyWALL 2 firewall or Prestige 660HW-61 ADSL router (ZyNOS 3.62) (8
5%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.67 seconds
           Raw packets sent: 2076 (95.036KB) | Rcvd: 22 (1.432KB)

C:\Users\Administrator>
```

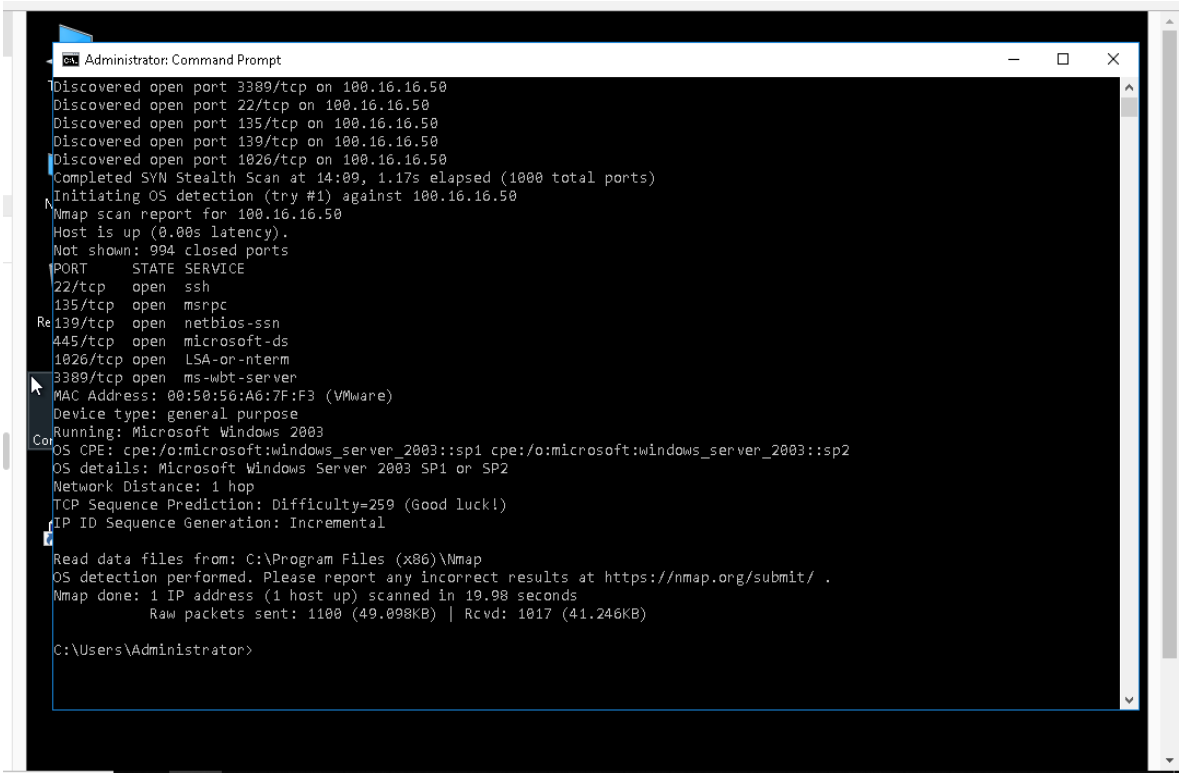
SECTION 2

Section2:Part1: Q8: Decoy IP Address Screen Capture

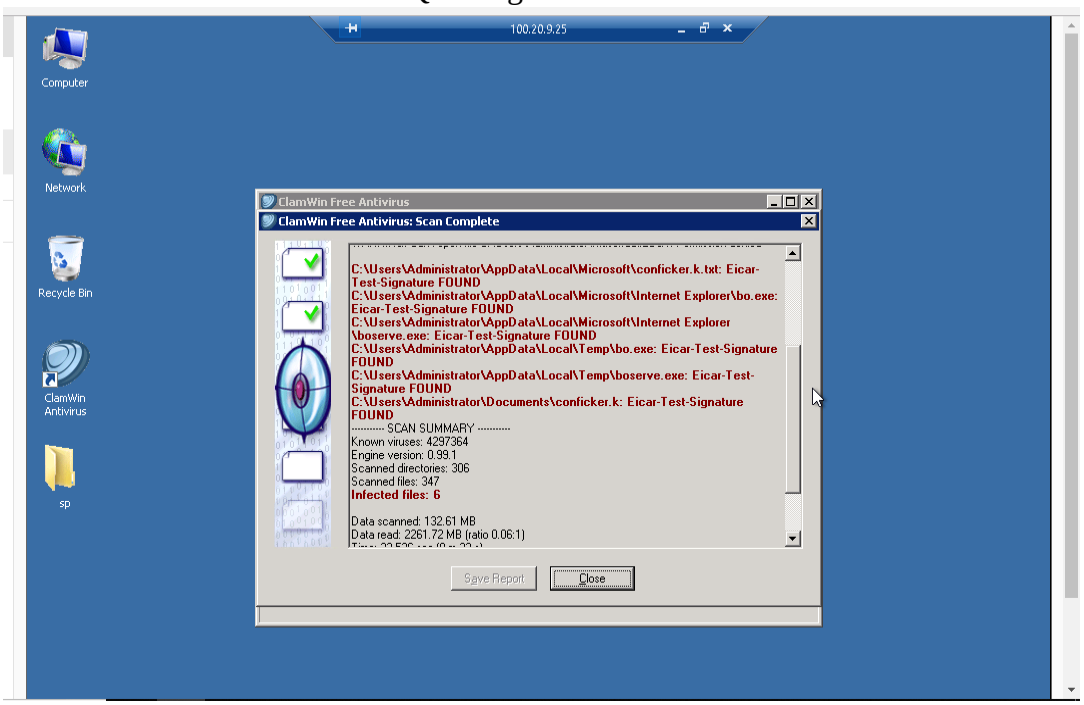
100.30.10.238 - PuTTY

```
Using username "root".
Linux cisco 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
Last login: Fri Aug 11 10:33:16 2017
root@cisco:~# tcpdump  -i eth0 port 80 -w georgeboakye_capture_s2
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
^C12 packets captured
12 packets received by filter
0 packets dropped by kernel
root@cisco:~# tcpdump -r georgeboakye_capture_s2
reading from file georgeboakye_capture_s2, link-type EN10MB (Ethernet)
14:01:36.944221 IP 100.30.10.2.65274 > 100.30.10.238.http: Flags [S], seq 263554
8970, win 1024, options [mss 1460], length 0
14:01:36.944332 IP 100.30.10.238.http > 100.30.10.2.65274: Flags [S.], seq 26200
64438, ack 2635548971, win 14600, options [mss 1460], length 0
14:01:36.944373 IP 88.77.66.44.65274 > 100.30.10.238.http: Flags [S], seq 263554
8970, win 1024, options [mss 1460], length 0
14:01:36.944816 IP 33.22.11.1.65274 > 100.30.10.238.http: Flags [S], seq 2635548
970, win 1024, options [mss 1460], length 0
14:01:36.944845 IP 95.85.75.65.65274 > 100.30.10.238.http: Flags [S], seq 263554
8970, win 1024, options [mss 1460], length 0
14:01:36.944910 IP 100.30.10.2.65274 > 100.30.10.238.http: Flags [R], seq 263554
8971, win 0, length 0
14:02:07.380855 IP 88.77.66.44.47365 > 100.30.10.238.http: Flags [S], seq 112783
2444, win 1024, options [mss 1460], length 0
14:02:07.381000 IP 33.22.11.1.47365 > 100.30.10.238.http: Flags [S], seq 1127832
444, win 1024, options [mss 1460], length 0
14:02:07.381037 IP 100.30.10.2.47365 > 100.30.10.238.http: Flags [S], seq 112783
2444, win 1024, options [mss 1460], length 0
14:02:07.381062 IP 100.30.10.238.http > 100.30.10.2.47365: Flags [S.], seq 54858
4454, ack 1127832445, win 14600, options [mss 1460], length 0
14:02:07.381092 IP 95.85.75.65.47365 > 100.30.10.238.http: Flags [S], seq 112783
2444, win 1024, options [mss 1460], length 0
14:02:07.381391 IP 100.30.10.2.47365 > 100.30.10.238.http: Flags [R], seq 112783
2445, win 0, length 0
root@cisco:~#
```

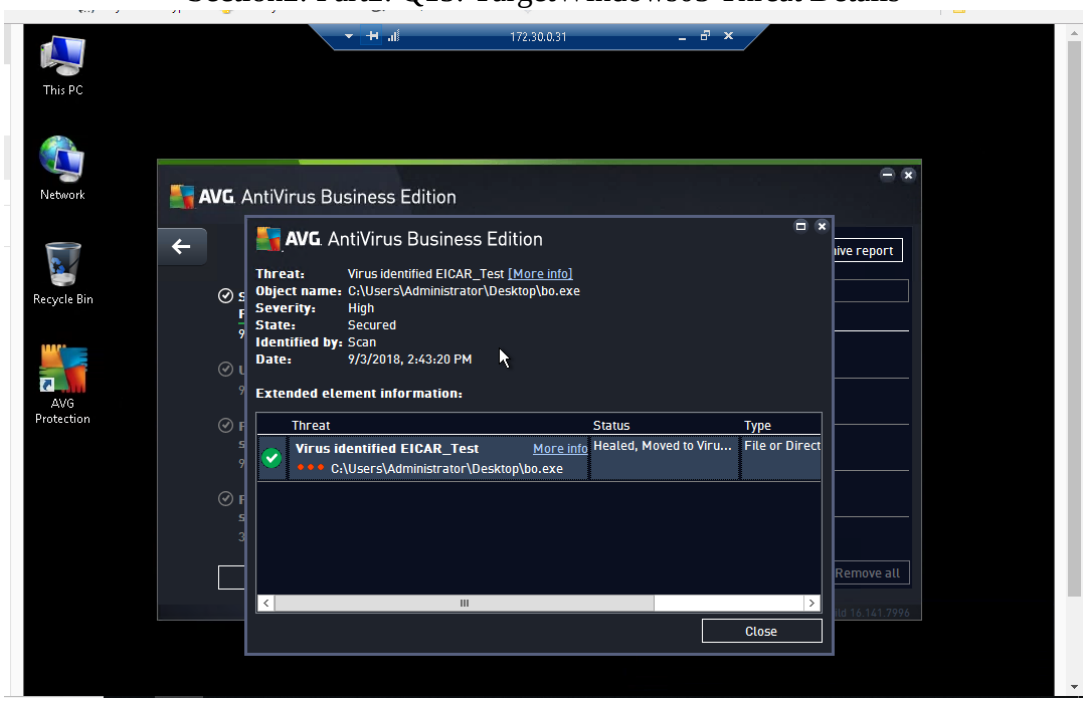
Section2: Part1: Q12: TargetVulnerable01 Nmap OS scan



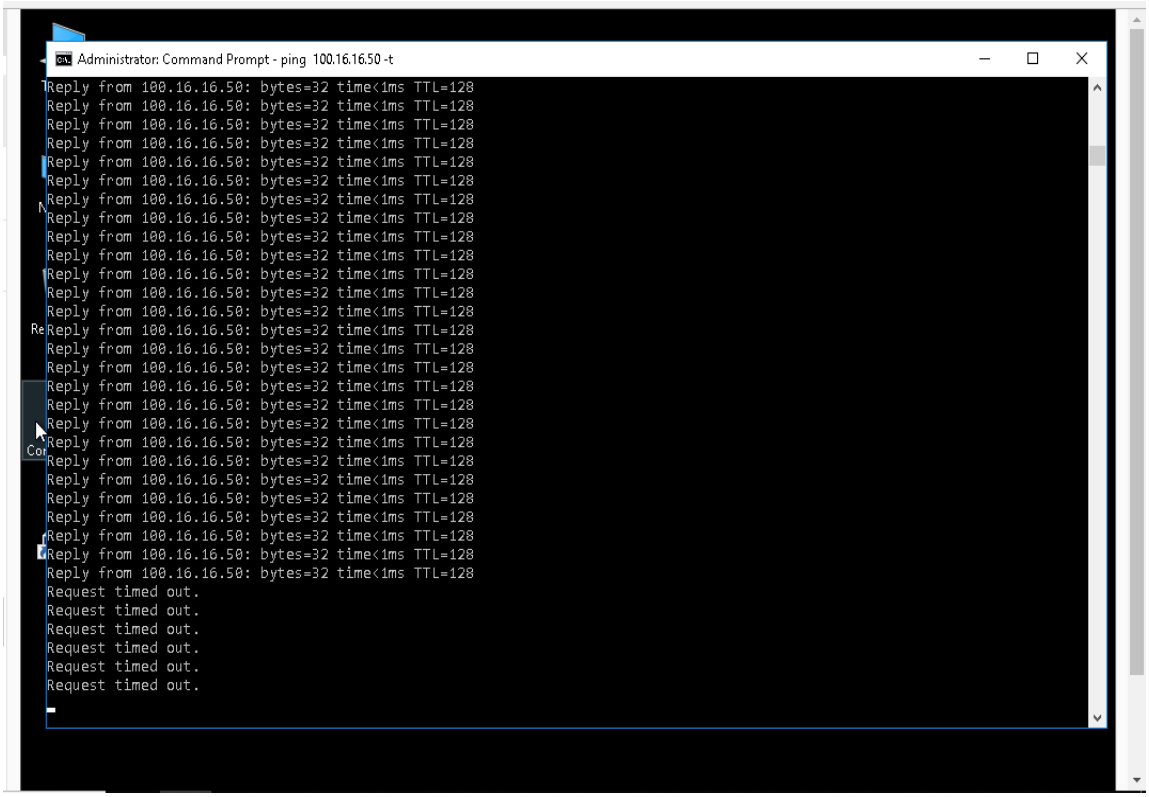
Section2: Part2: Q8: TargetWindows04 Threat Details



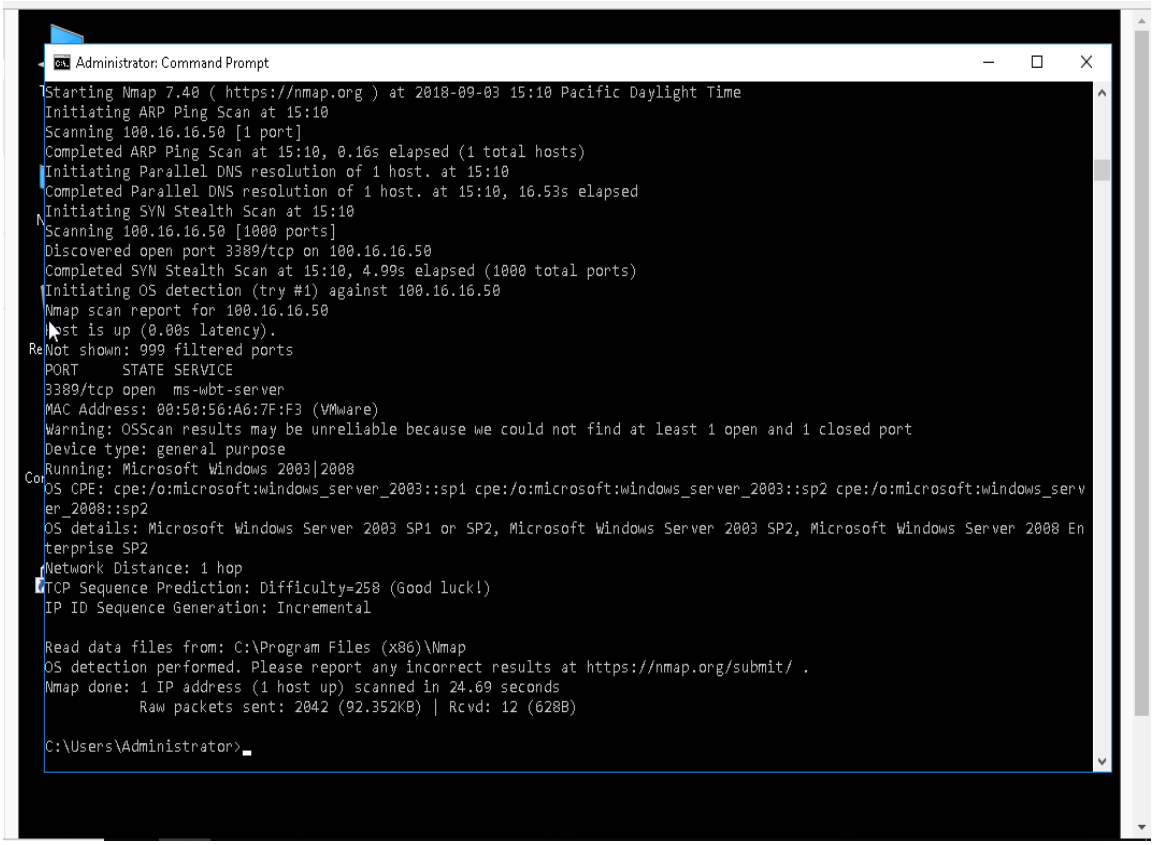
Section2: Part2: Q15: TargetWindows05 Threat Details



Section2: Part3: Q20: Timedout Ping of TargetVulnerable01



Section2: Part3: Q28: TargetVulnerable01 New Nmap OS scan

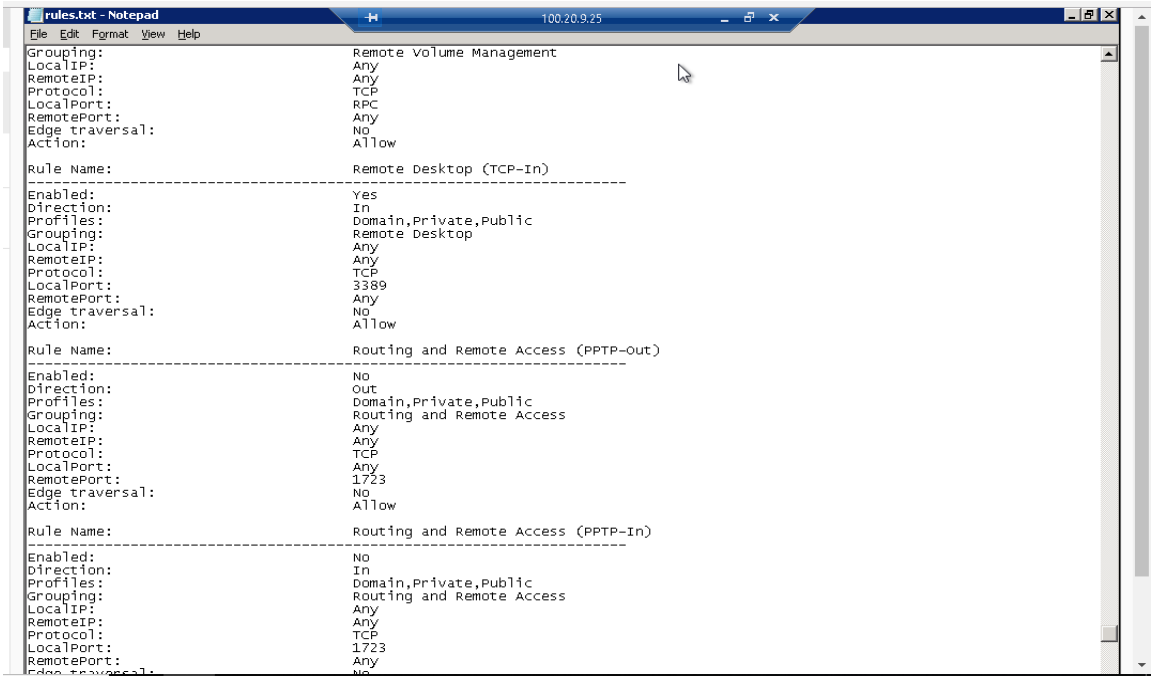


```
Administrator: Command Prompt
Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-03 15:10 Pacific Daylight Time
Initiating ARP Ping Scan at 15:10
Scanning 100.16.16.50 [1 port]
Completed ARP Ping Scan at 15:10, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:10
Completed Parallel DNS resolution of 1 host. at 15:10, 16.53s elapsed
Initiating SYN Stealth Scan at 15:10
Scanning 100.16.16.50 [1000 ports]
Discovered open port 3389/tcp on 100.16.16.50
Completed SYN Stealth Scan at 15:10, 4.99s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.16.16.50
Nmap scan report for 100.16.16.50
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A6:7F:F3 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2003|2008
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_serv
er_2008::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2008 En
terprise SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.69 seconds
           Raw packets sent: 2042 (92.352KB) | Rcvd: 12 (628B)

C:\Users\Administrator>
```

Section2:Part3: Q29: Comparing results of 2 scans of TargetVulnerable01

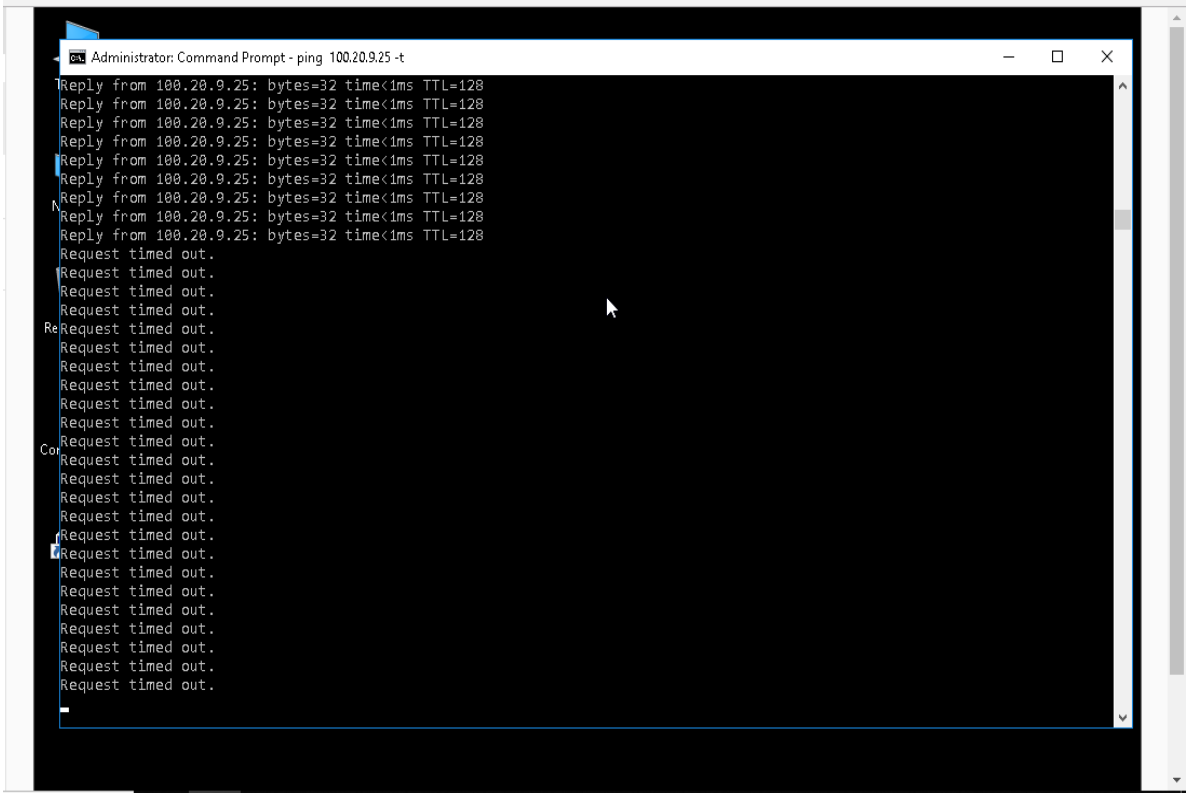
The Nmap scan against TargetVulnerable01 (IP: 100.16.16.50) revealed 6 open ports (22-SSH, 135-MSRP, 139-NetBIOS, 445-SMB, 1025-NFS/IIS, and 3389-RDP) that could've been used for exploit. After hardening, the system only has the RDP port (3389) open just to allow for remote login. The hardening was made through the configuration of the host-based firewall on the Windows 2003 (IP: 100.16.16.50) system. The configuration involved utilizing the network shell (netsh) command and disabling the unneeded services in TargetVulnerable01.

Section2: Part4: Q7: Remote Desktop Rule in rules.txt



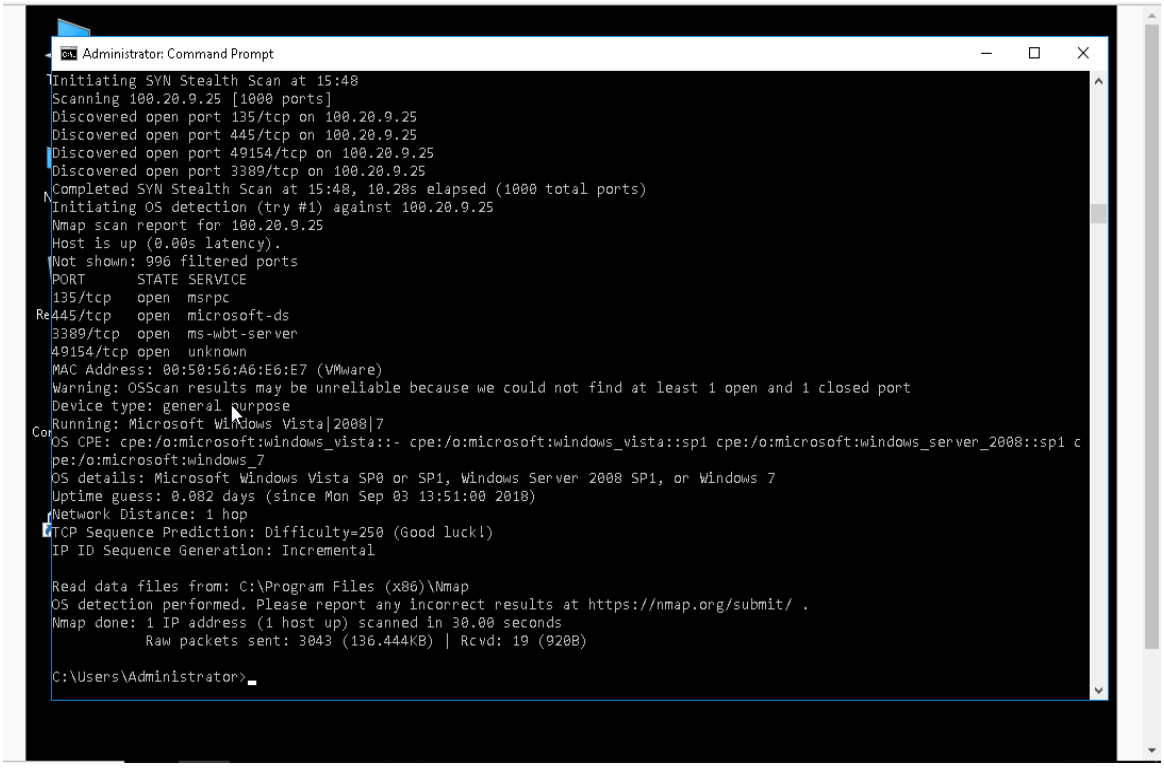
```
Grouping:                           Remote Volume Management
LocalIP:                            Any
RemoteIP:                           Any
Protocol:                           TCP
LocalPort:                          RPC
RemotePort:                         Any
Edge traversal:                     No
Action:                             Allow

Rule Name:                          Remote Desktop (TCP-In)
----------------------------------------------------------------------
Enabled:                            Yes
Direction:                          In
Profiles:                           Domain,Private,Public
Grouping:                           Remote Desktop
LocalIP:                            Any
RemoteIP:                           Any
Protocol:                           TCP
LocalPort:                          3389
RemotePort:                         Any
Edge traversal:                     No
Action:                             Allow

Rule Name:                          Routing and Remote Access (PPTP-Out)
----------------------------------------------------------------------
Enabled:                            No
Direction:                          Out
Profiles:                           Domain,Private,Public
Grouping:                           Routing and Remote Access
LocalIP:                            Any
RemoteIP:                           Any
Protocol:                           TCP
LocalPort:                          Any
RemotePort:                         1723
Edge traversal:                     No
Action:                             Allow

Rule Name:                          Routing and Remote Access (PPTP-In)
----------------------------------------------------------------------
Enabled:                            No
Direction:                          In
Profiles:                           Domain,Private,Public
Grouping:                           Routing and Remote Access
LocalIP:                            Any
RemoteIP:                           Any
Protocol:                           TCP
LocalPort:                          1723
RemotePort:                         Any
```

Section2: Part4: Q17: Timedout Ping of TargetVulnerable04



```
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Reply from 100.20.9.25: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Section2: Part4: Q20: TargetVulnerable04 New Nmap OS scan



SECTION 3

Section3: Part1: Analysis and Discussion

ClamWin identified that the TargetWindows04 machine was infected with the Back Orifice (BO) exploit. Explain how this virus was named and why it can still be dangerous.

Back Orifice (BO) is a rootkit/trojan horse program that attaches itself to emails and allows attacker to monitor and tamper with Windows computers over the Internet without the user detecting the attack. Executing the BO program opens a connection to the internet, allowing the attacker to control the computer by sniffing passwords, recording keystrokes, accessing a desktop's file system, taking screenshots and sending them back to the attacker through remote connection (Ref 1).

The BO malware was coined from the Microsoft's BackOffice product by the hackers group Cult of the Dead Cow (Ref 2)

Section3: Part2: Tools and Commands

Use the internet to identify the netsh command (for both Windows 2003 and Windows 2008 firewalls) that will enable file sharing

Windows 2003

Command
netsh firewall set service FileAndPrint

Windows 2008

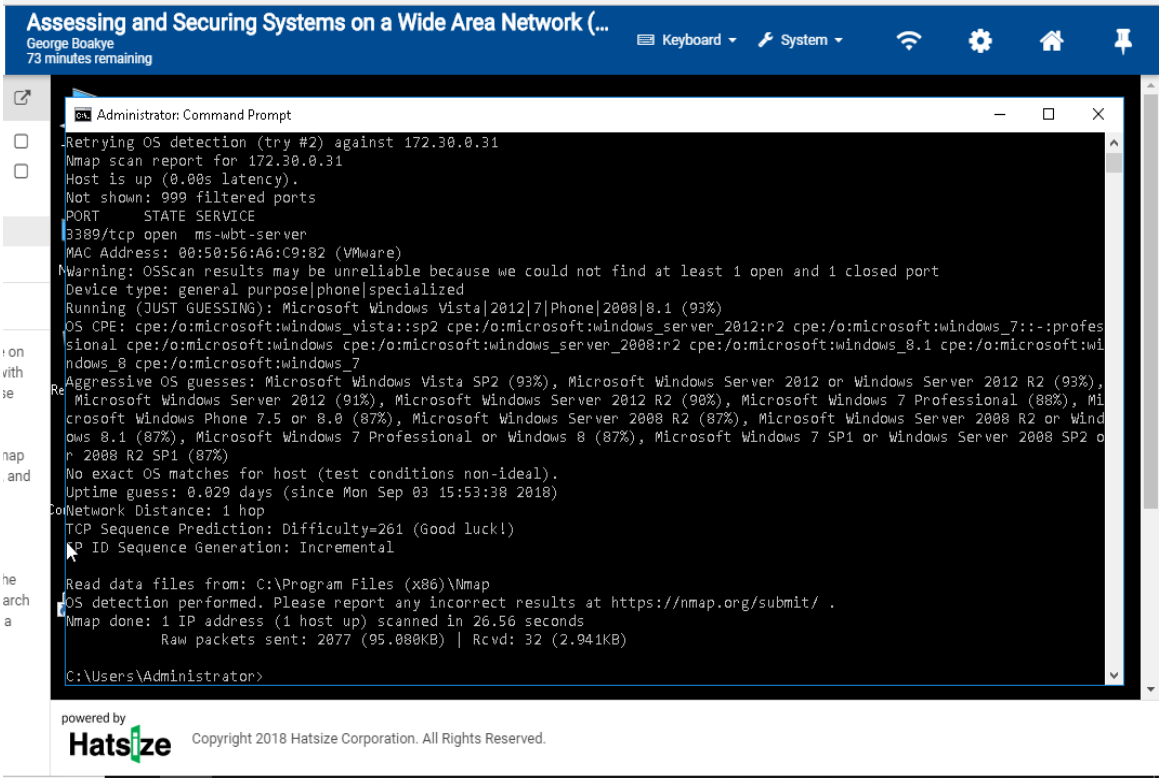
Old Command	New Command
netsh firewall set service FileAndPrint	netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes

Ref. [Microsoft Support]

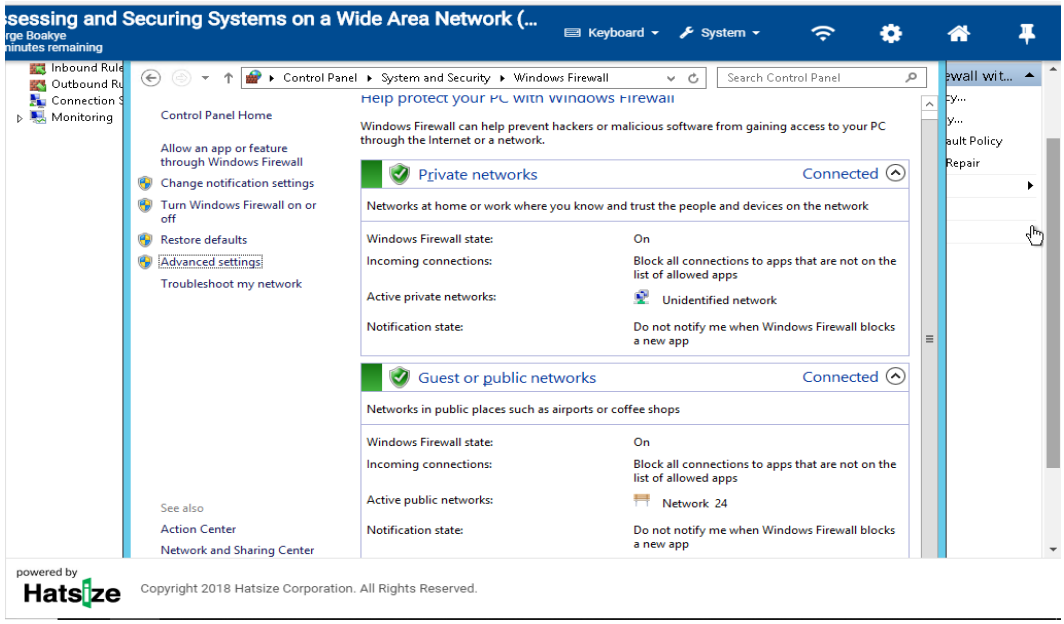
Section3: Part2: Challenge Exercise

1. Hardening TargetWindows05 using Windows Firewall Advanced Security and document with screen captures.

Hardening TargetWondows05 Shot (A)



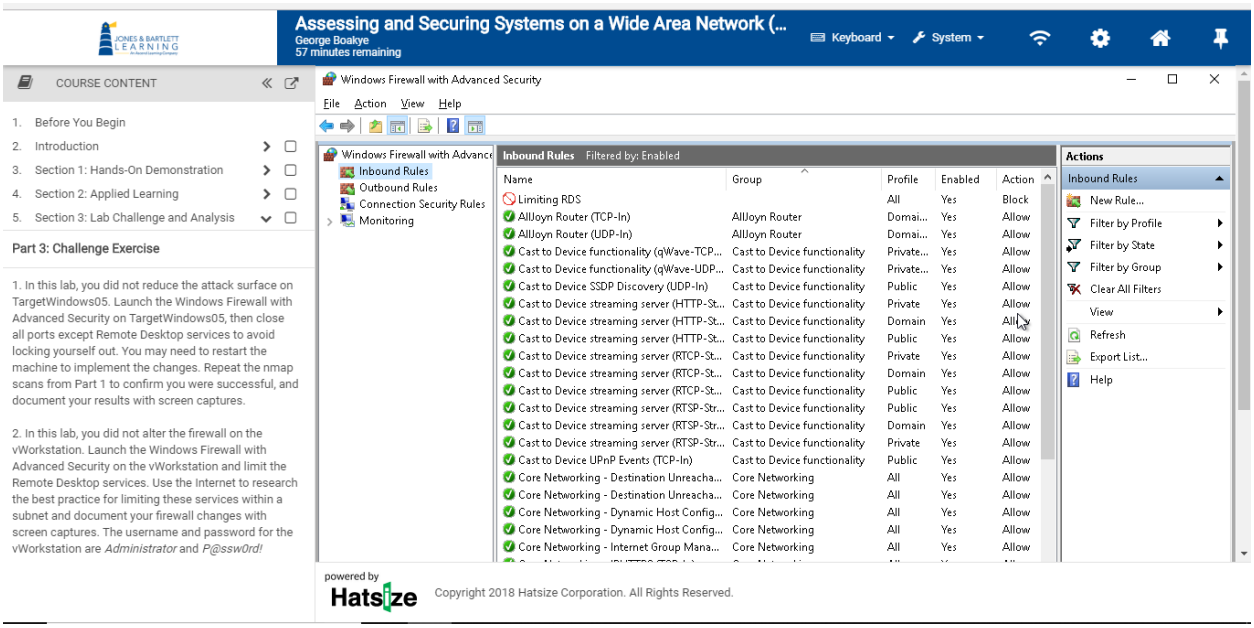
Hardening TargetWondows05 Shot (B)



Section3: Part3: Limiting Remote Desktop Services on the vWorkstation from a different subnet

Section3:Part3: Limiting Remote Desktop Services on the vWorkstation to same subnet

Section3: Part3: Firewall Settings in vWorkstation Window showing “Limiting RDS”



Reference (RDS Settings)