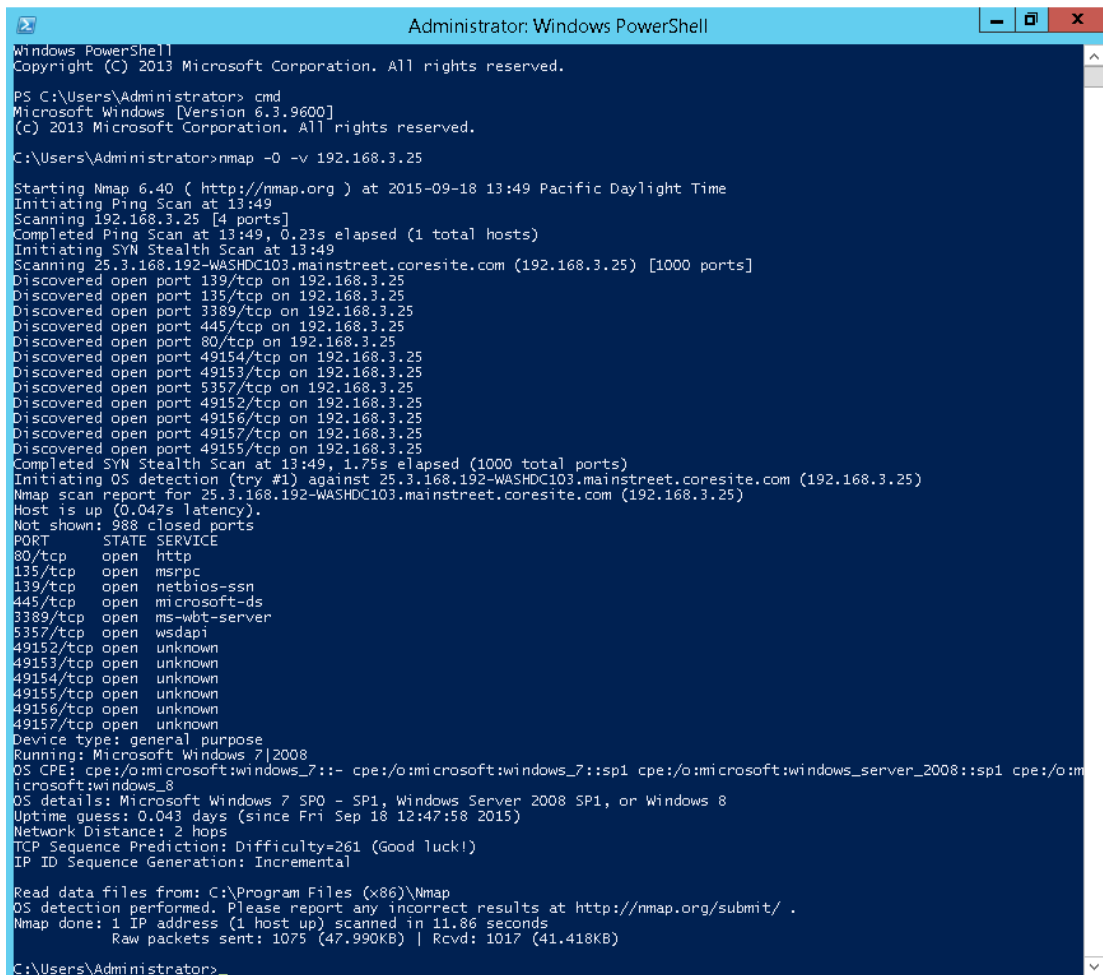


# Lab Report

## 1. Nmap -O -v 192.168.3.25



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cmd
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

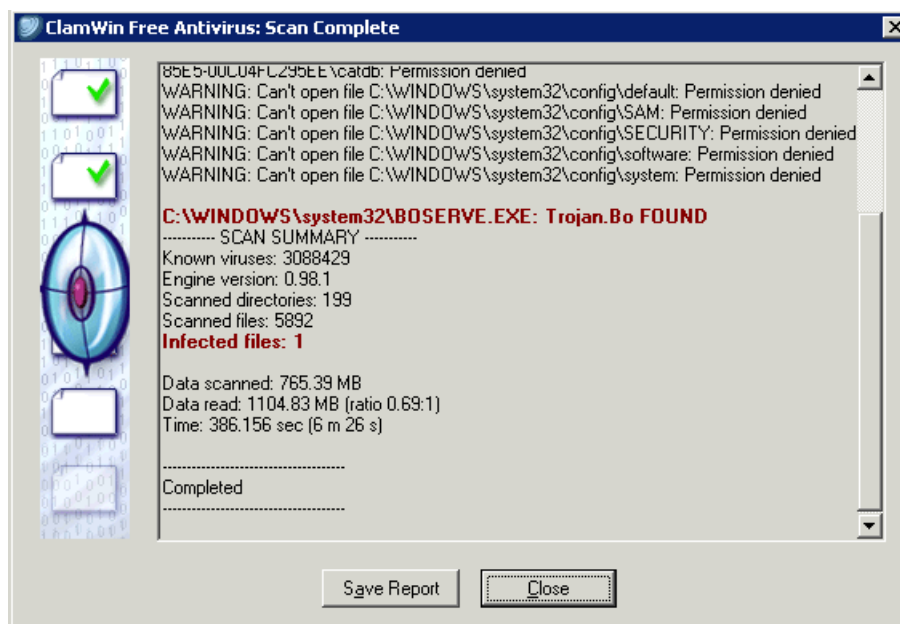
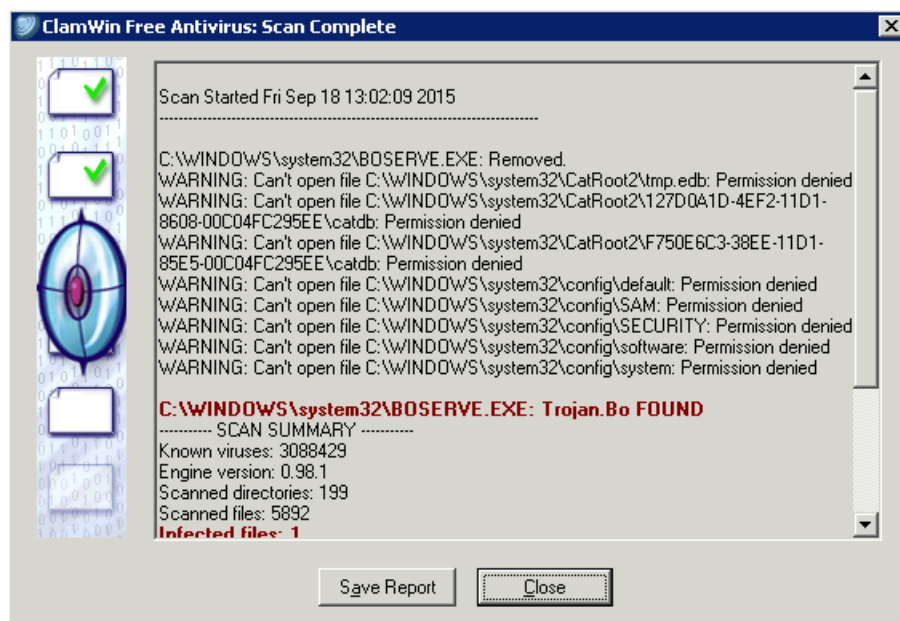
C:\Users\Administrator>nmap -O -v 192.168.3.25

Starting Nmap 6.40 ( http://nmap.org ) at 2015-09-18 13:49 Pacific Daylight Time
Initiating Ping Scan at 13:49
Scanning 192.168.3.25 [4 ports]
Completed Ping Scan at 13:49, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:49
Scanning 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25) [1000 ports]
Discovered open port 139/tcp on 192.168.3.25
Discovered open port 135/tcp on 192.168.3.25
Discovered open port 3389/tcp on 192.168.3.25
Discovered open port 445/tcp on 192.168.3.25
Discovered open port 80/tcp on 192.168.3.25
Discovered open port 49154/tcp on 192.168.3.25
Discovered open port 49153/tcp on 192.168.3.25
Discovered open port 5357/tcp on 192.168.3.25
Discovered open port 49152/tcp on 192.168.3.25
Discovered open port 49156/tcp on 192.168.3.25
Discovered open port 49157/tcp on 192.168.3.25
Discovered open port 49155/tcp on 192.168.3.25
Completed SYN Stealth Scan at 13:49, 1.75s elapsed (1000 total ports)
Initiating OS detection (try #1) against 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25)
Nmap scan report for 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25)
Host is up (0.047s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Uptime guess: 0.043 days (since Fri Sep 18 12:47:58 2015)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental

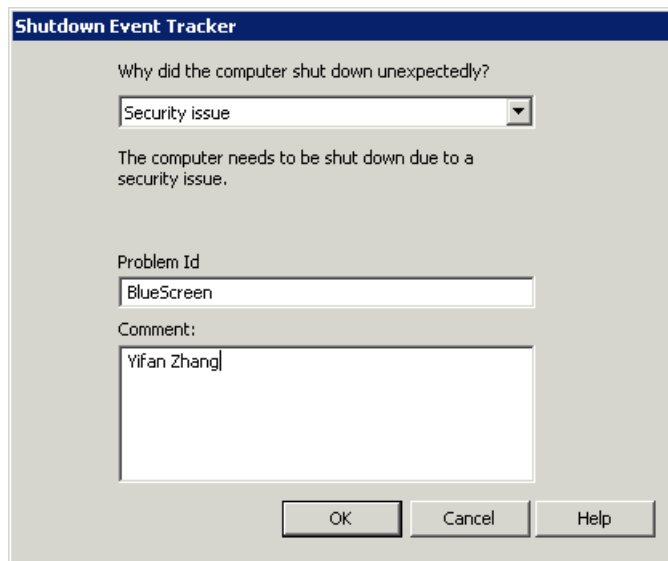
Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds
Raw packets sent: 1075 (47.990KB) | Rcvd: 1017 (41.418KB)

C:\Users\Administrator>
```

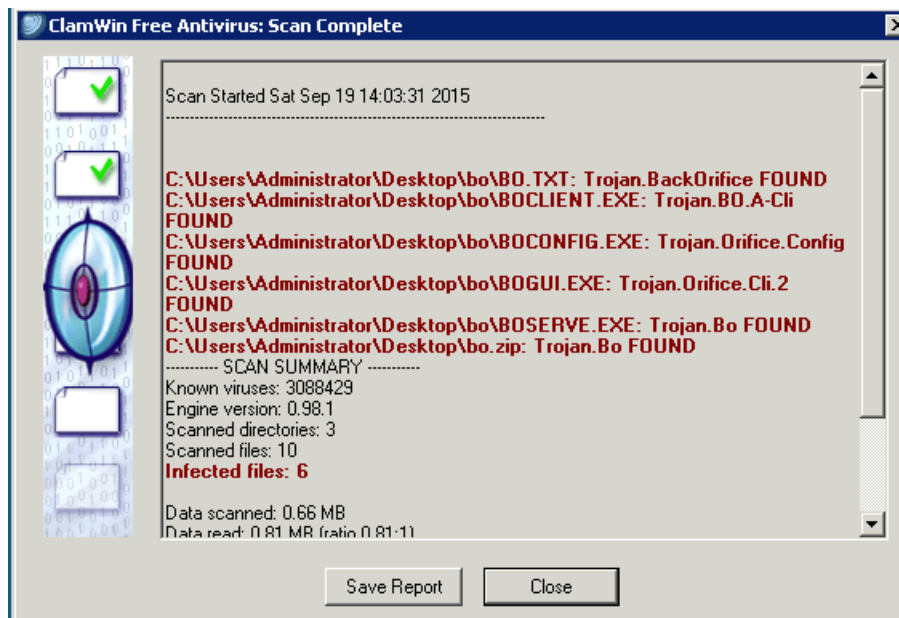
## 2. ClamWin system32 folder scan result

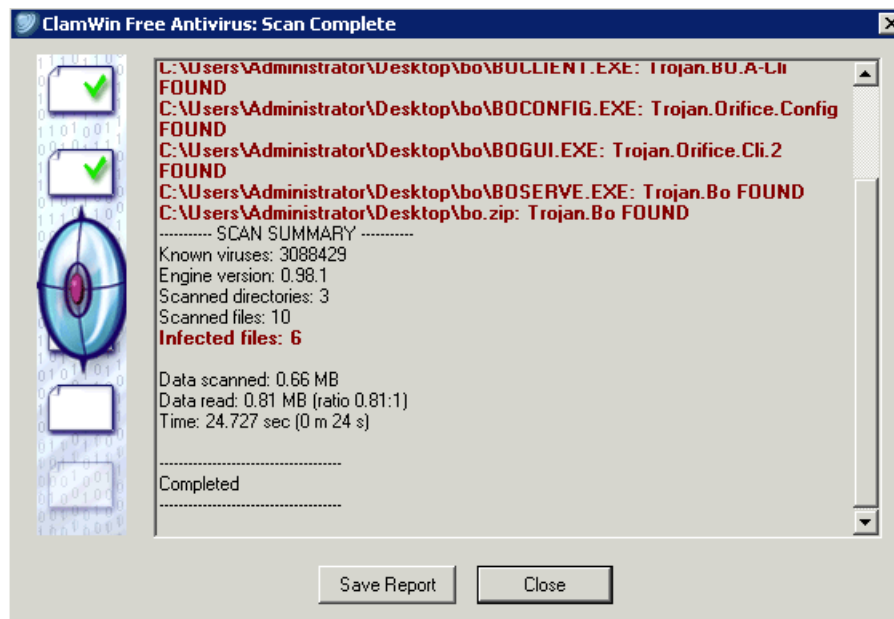


### 3. Shutdown Event Tracker



### 4. ClamWin desktop folder scan result





## 5. Nmap scan results and the reduced attack surface

### 5.1 Nmap -O -v 10.20.100.50

Before applying Firewall

```

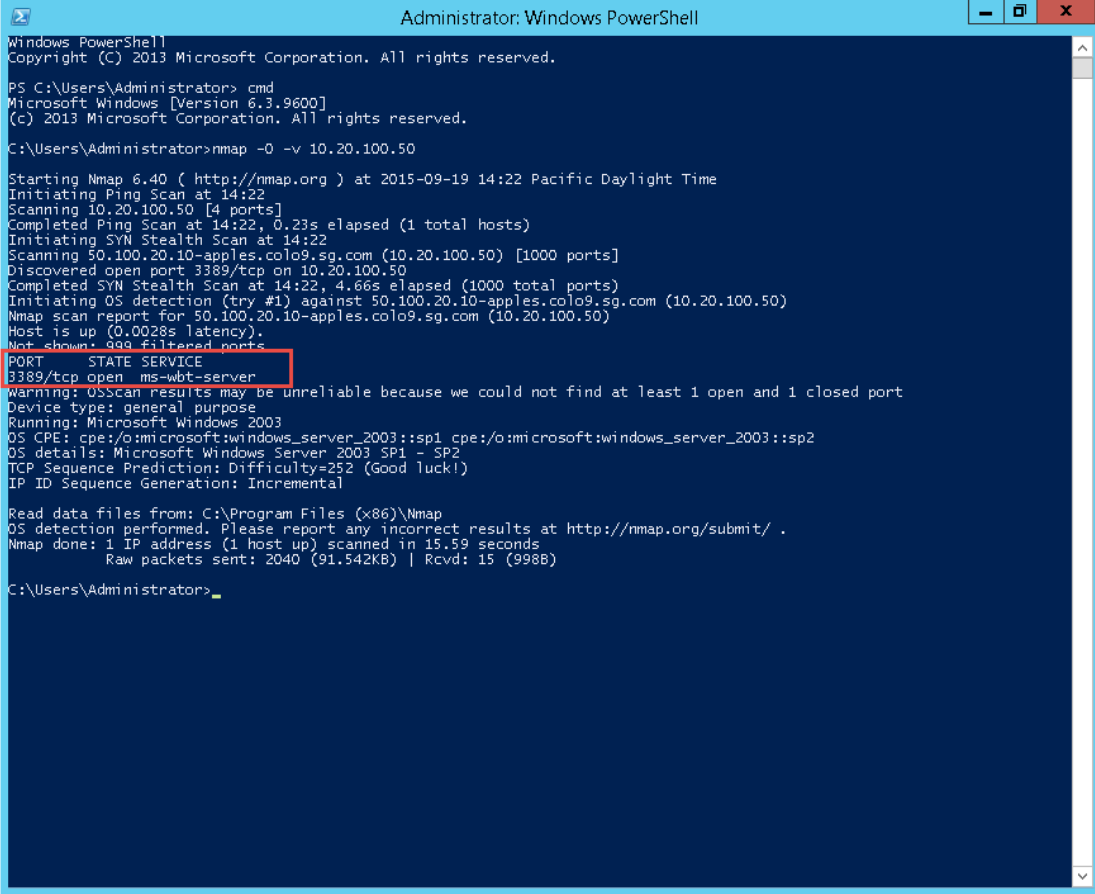
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> nmap -O -v 10.20.100.50

Starting Nmap 6.40 ( http://nmap.org ) at 2015-09-18 13:10 Pacific Daylight Time
Initiating Ping Scan at 13:10
Scanning 10.20.100.50 [4 ports]
Completed Ping Scan at 13:10, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:10
Scanning 50.100.20.10-apples.colo9.sg.com (10.20.100.50) [1000 ports]
Discovered open port 445/tcp on 10.20.100.50
Discovered open port 139/tcp on 10.20.100.50
Discovered open port 3389/tcp on 10.20.100.50
Discovered open port 135/tcp on 10.20.100.50
Discovered open port 1026/tcp on 10.20.100.50
Completed SYN Stealth Scan at 13:10, 0.38s elapsed (1000 total ports)
Initiating OS detection (try #1) against 50.100.20.10-apples.colo9.sg.com (10.20.100.50)
Nmap scan report for 50.100.20.10-apples.colo9.sg.com (10.20.100.50)
Host is up (0.0029s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1026/tcp  open  LSA-or-nterm
3389/tcp  open  ms-wbt-server
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=253 (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 http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.58 seconds
Raw packets sent: 1020 (45.570KB) | Rcvd: 1017 (41.254KB)
PS C:\Users\Administrator>
  
```

### After applying Firewall



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cmd
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nmap -O -v 10.20.100.50

Starting Nmap 6.40 ( http://nmap.org ) at 2015-09-19 14:22 Pacific Daylight Time
Initiating Ping Scan at 14:22
Scanning 10.20.100.50 [4 ports]
Completed Ping Scan at 14:22, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:22
Scanning 50.100.20.10-apples.colo9.sg.com (10.20.100.50) [1000 ports]
Discovered open port 3389/tcp on 10.20.100.50
Completed SYN Stealth Scan at 14:22, 4.66s elapsed (1000 total ports)
Initiating OS detection (try #1) against 50.100.20.10-apples.colo9.sg.com (10.20.100.50)
Nmap scan report for 50.100.20.10-apples.colo9.sg.com (10.20.100.50)
Host is up (0.0028s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
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
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 - SP2
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Incremental

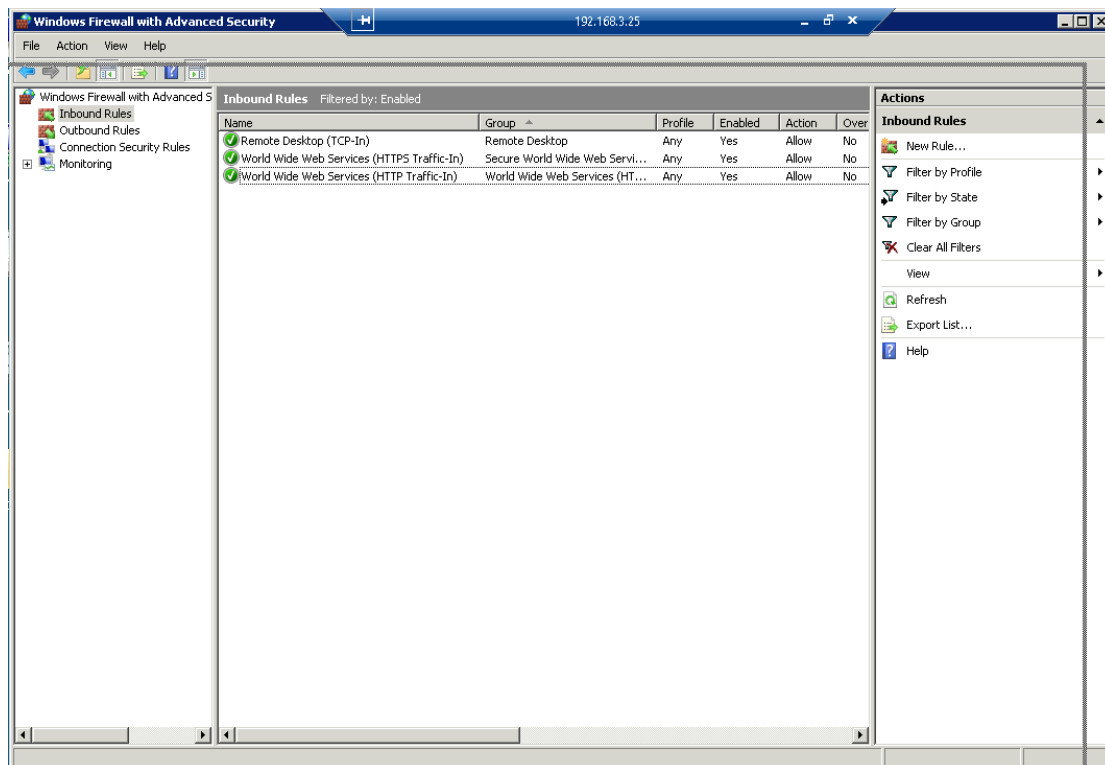
Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.59 seconds
Raw packets sent: 2040 (91.542KB) | Rcvd: 15 (998B)

C:\Users\Administrator>
```

### Explanation:

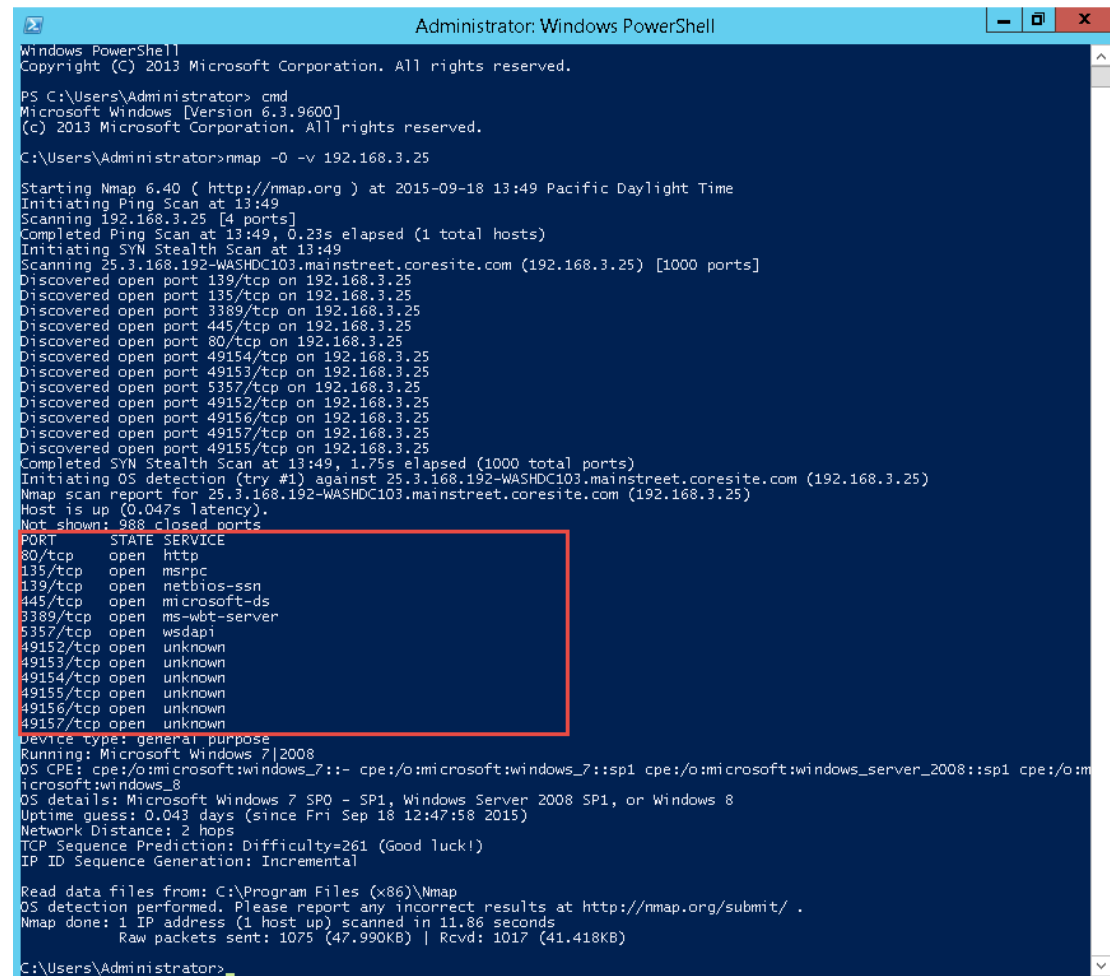
Before we apply the firewall, we could see that there are 5 ports are open for services on machine IP 10.20.100.50. And, after there are only 1 port left. The more ports open for services, the more risky a server is. The reason is that attackers could use these ports to communicate between their local machine and target server. The most common exploit is to send tremendous data through these open channels.

## 5.2 Enabled Inbound Rules



### 5.3 Nmap -O -v 192.168.3.25

Before applying firewall



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cmd
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

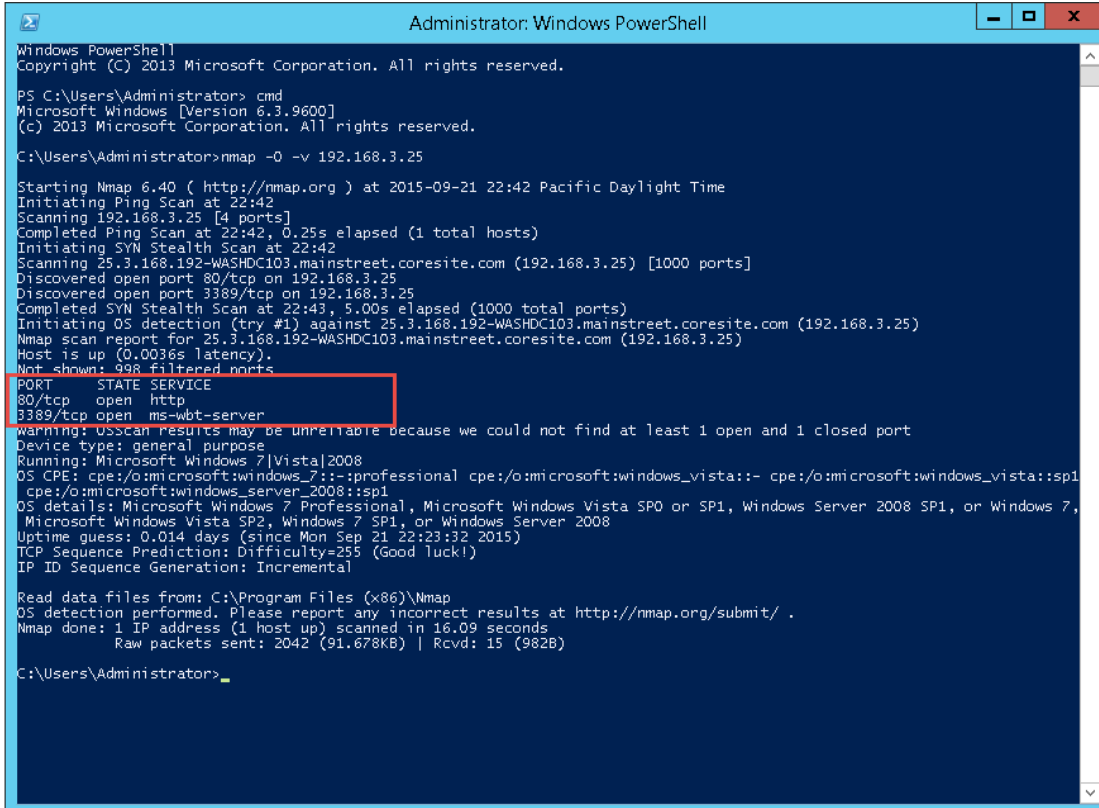
C:\Users\Administrator>nmap -O -v 192.168.3.25

Starting Nmap 6.40 ( http://nmap.org ) at 2015-09-18 13:49 Pacific Daylight Time
Initiating Ping Scan at 13:49
Scanning 192.168.3.25 [4 ports]
Completed Ping Scan at 13:49, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:49
Scanning 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25) [1000 ports]
Discovered open port 139/tcp on 192.168.3.25
Discovered open port 135/tcp on 192.168.3.25
Discovered open port 3389/tcp on 192.168.3.25
Discovered open port 445/tcp on 192.168.3.25
Discovered open port 80/tcp on 192.168.3.25
Discovered open port 49154/tcp on 192.168.3.25
Discovered open port 49153/tcp on 192.168.3.25
Discovered open port 5357/tcp on 192.168.3.25
Discovered open port 49152/tcp on 192.168.3.25
Discovered open port 49156/tcp on 192.168.3.25
Discovered open port 49157/tcp on 192.168.3.25
Discovered open port 49155/tcp on 192.168.3.25
Completed SYN Stealth Scan at 13:49, 1.75s elapsed (1000 total ports)
Initiating OS detection (try #1) against 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25)
Nmap scan report for 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25)
Host is up (0.047s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdaapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Uptime guess: 0.043 days (since Fri Sep 18 12:47:58 2015)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (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 http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds
Raw packets sent: 1075 (47.990KB) | Rcvd: 1017 (41.418KB)

C:\Users\Administrator>
```

### After applying Firewall



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cmd
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator> nmap -O -v 192.168.3.25

Starting Nmap 6.40 ( http://nmap.org ) at 2015-09-21 22:42 Pacific Daylight Time
Initiating Ping Scan at 22:42
Scanning 192.168.3.25 [4 ports]
Completed Ping Scan at 22:42, 0.25s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:42
Scanning 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25) [1000 ports]
Discovered open port 80/tcp on 192.168.3.25
Discovered open port 3389/tcp on 192.168.3.25
Completed SYN Stealth Scan at 22:43, 5.00s elapsed (1000 total ports)
Initiating OS detection (try #1) against 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25)
Nmap scan report for 25.3.168.192-WASHDC103.mainstreet.coresite.com (192.168.3.25)
Host is up (0.0036s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
3389/tcp   open  ms-wbt-server
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 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7,
Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 0.014 days (since Mon Sep 21 22:23:32 2015)
TCP Sequence Prediction: Difficulty=255 (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 http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.09 seconds
Raw packets sent: 2042 (91.678KB) | Rcvd: 15 (982B)

C:\Users\Administrator>
```

### Explanation:

Same as the previous analysis in section 5.1, the firewall blocked the majority ports existing on machine IP 192.168.3.25. And, this action could reduce a lot of the hacking risks because hackers could utilize these open ports to implement an attack to targets. For example, some hackers could use DDos or DoS technique to attack these ports, which makes the services are not available to end user. However, using this way to harden system has an obvious side-effect that when service ports are blocked, both normal user and hackers could not use it any more. Thus, a more wise way to do that is to refine the filtering rules instead of disable them all.