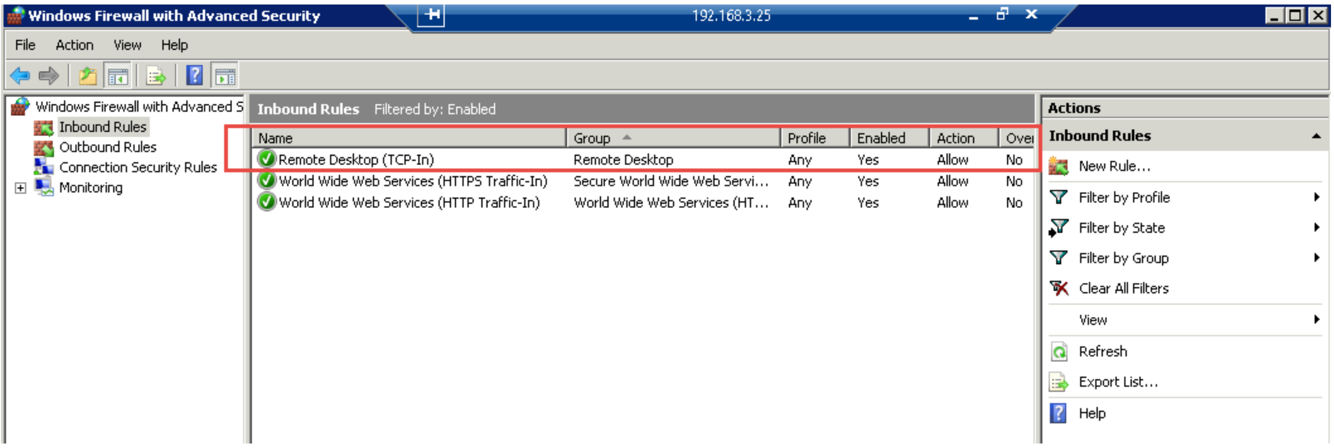
Challenge Lab 11 Report

Question Description:

In previous experiment, we have already disabled all the Inboud rules except **Remote Desktop (TCP-IN)**, **World Wide Web Services (HTTPS Traffic-In)** and **World Wide Web Services (HTTP Traffic-In)** in firewall on remote machine IP 192.168.3.25. And, in this challenge question, we will disable **Remote Desktop (TCP-IN)** and retry **nmap –O –v 192.168.3.25** command to see what happens and what is the difference between previous result and current result.

Answer:

At first, we see that **Remote Desktop (TCP-IN)** is still **enabled**.

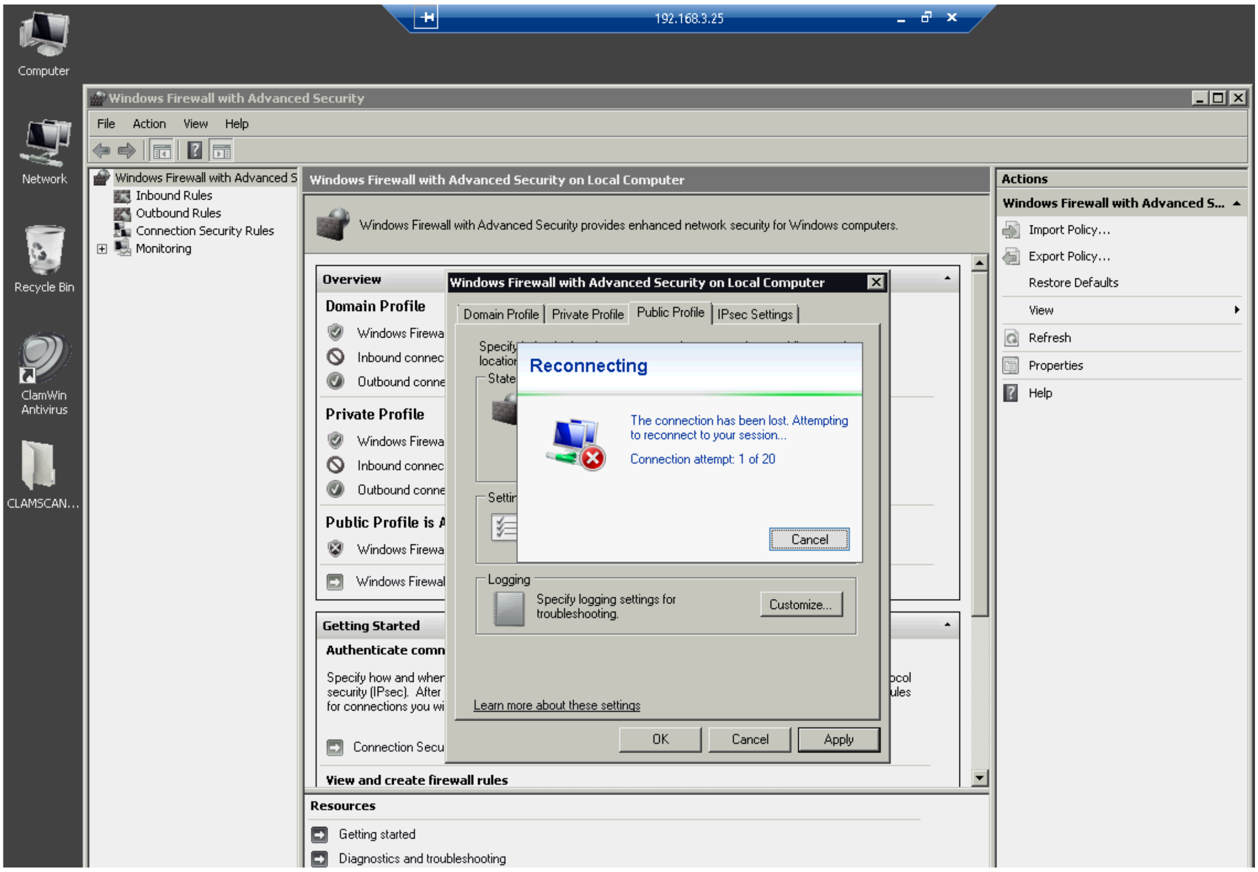


Inbound Rules Filtered by: Enabled

Name	Group	Profile	Enabled	Action	Over
✓ Remote Desktop (TCP-In)	Remote Desktop	Any	Yes	Allow	No
✓ World Wide Web Services (HTTPS Traffic-In)	Secure World Wide Web Servi...	Any	Yes	Allow	No
✓ World Wide Web Services (HTTP Traffic-In)	World Wide Web Services (HT...	Any	Yes	Allow	No

‘

After we disable the **Remote Desktop (TCP-IN)**, the remote connection between Vworkstation and machine 192.168.3.25 becomes unavailable anymore. The reason is pretty clear that when we disable the Inbound rule in firewall, we just block the channel that used for communication between two machines. The result of following picture shows the user’s remote desktop request is declined by remote server due to the firewall settings.



Windows Firewall with Advanced Security provides enhanced network security for Windows computers.

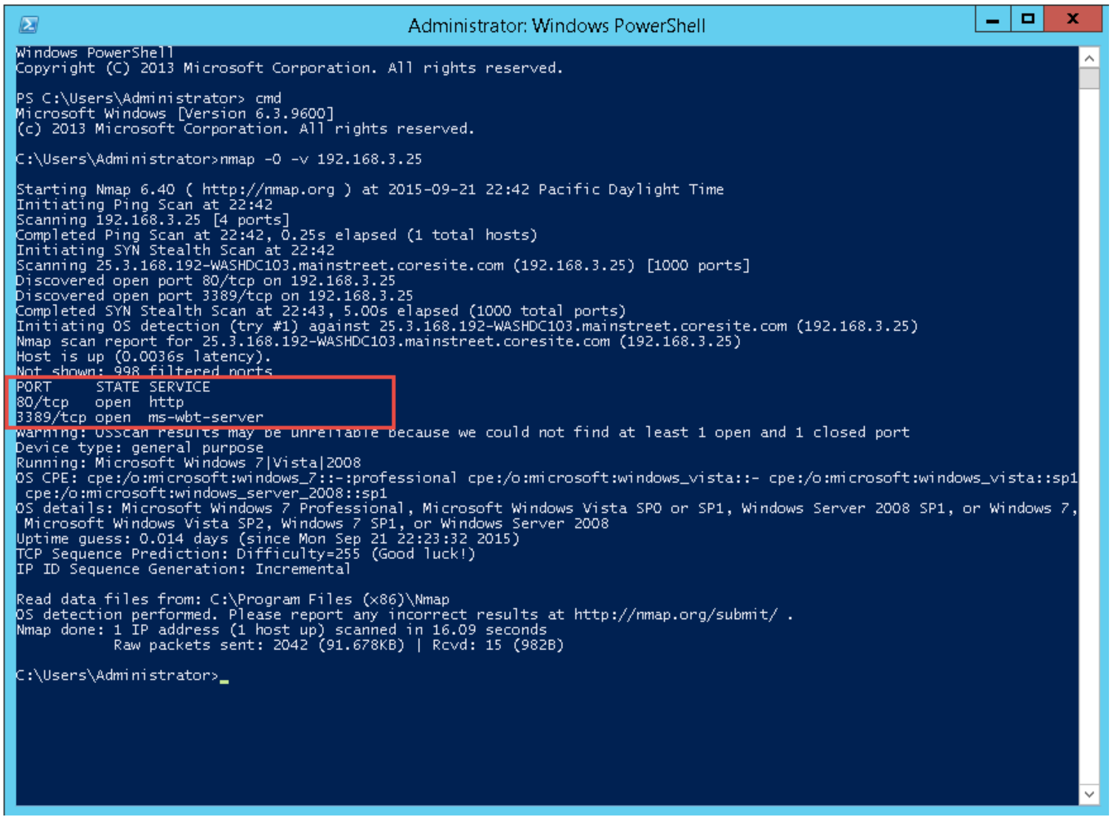
Specify how and wher security (IPsec). After for connections you wi

Specify logging settings for troubleshooting.

The connection has been lost. Attempting to reconnect to your session...

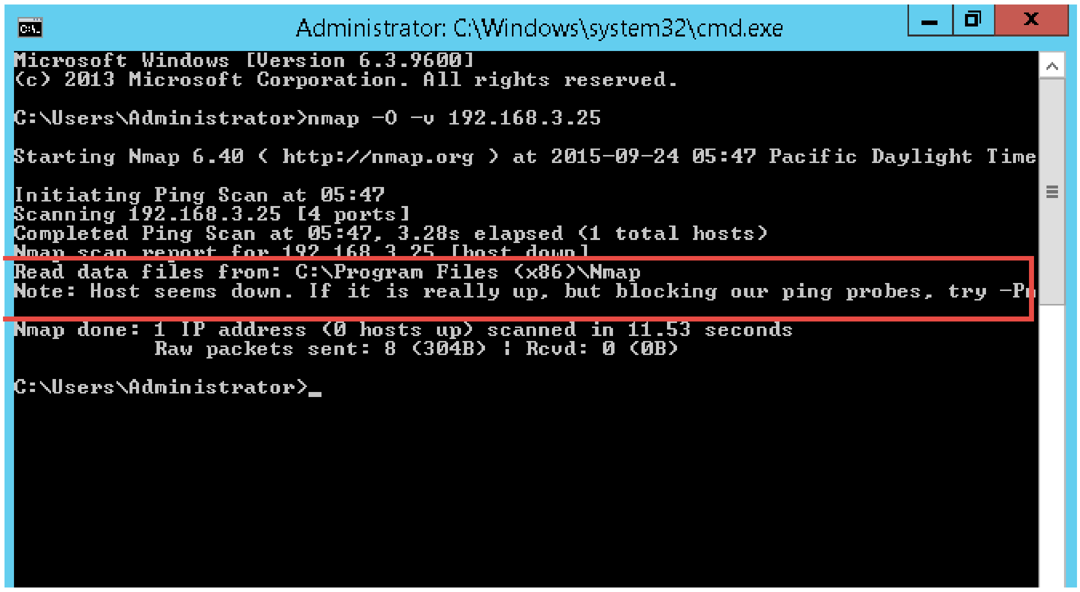
Connection attempt: 1 of 20

At the last step of normal experiment, we get the following result that after applying firewall rules in instruction, we still have two ports that work properly and all other previous alive ports are disappear. The two left ports are **80/tcp** for **http service** and **3389/tcp** for **ms-wbt-server services**



```
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>_
```

After we blocked the **Remote Desktop (TCP-IN)** inbound rules and retried **Nmap –O –v 192.168.3.25**, we found that no any ports can be detected any more. All the ping requests are declined by remote server IP 192.168.3.25.



```
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 2015-09-24 05:47 Pacific Daylight Time

Initiating Ping Scan at 05:47
Scanning 192.168.3.25 [4 ports]
Completed Ping Scan at 05:47, 3.28s elapsed (1 total hosts)
Nmap scan report for 192.168.3.25 [host down]
Read data files from: C:\Program Files (x86)\Nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 11.53 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)

C:\Users\Administrator>_
```