

MIS 5170

Operating System Security

Week 7

Windows Firewalls

Tonight's Plan

2

- ❑ Questions from Last Week
- ❑ Review on-line posts
- ❑ In The News – Will post On-Line
- ❑ Firewalls
- ❑ Review Quiz Questions
- ❑ Review for 1st test
- ❑ Assignment 3 Overview
- ❑ Next Week
- ❑ Test 1

Questions From Last Week

3

- ❑ Any Questions from last week?
- ❑ Quiz; review from Blackboard results – Week 6.
- ❑ SCCM
 - ❑ Remember that SCCM is a way of patching large numbers of computers.

Questions From Last Week (cont)

4

- Any additional questions?

In the News

5

- ❑ More on Bluetooth Ingenico Overlay Skimmers
 - ❑ Remember that if you can touch it; it has a greater chance of being compromised.
 - <https://krebsonsecurity.com/2017/02/more-on-bluetooth-ingenico-overlay-skimmers/>
- ❑ iPhone Robbers Try to iPhish Victims
 - ❑ Physical and virtual robbery of a iPhone owner.
 - <https://krebsonsecurity.com/2017/02/iphone-robbers-try-to-iphish-victims/>
- ❑ My own story in the past week
 - ❑ Your Microsoft License is expiring.



In the News (cont)

6

- ❑ Questions or items anyone has found of interest?

Firewalls

7

- ❑ What is a firewall?
- ❑ How do we configure it on Windows?

Firewalls (cont)

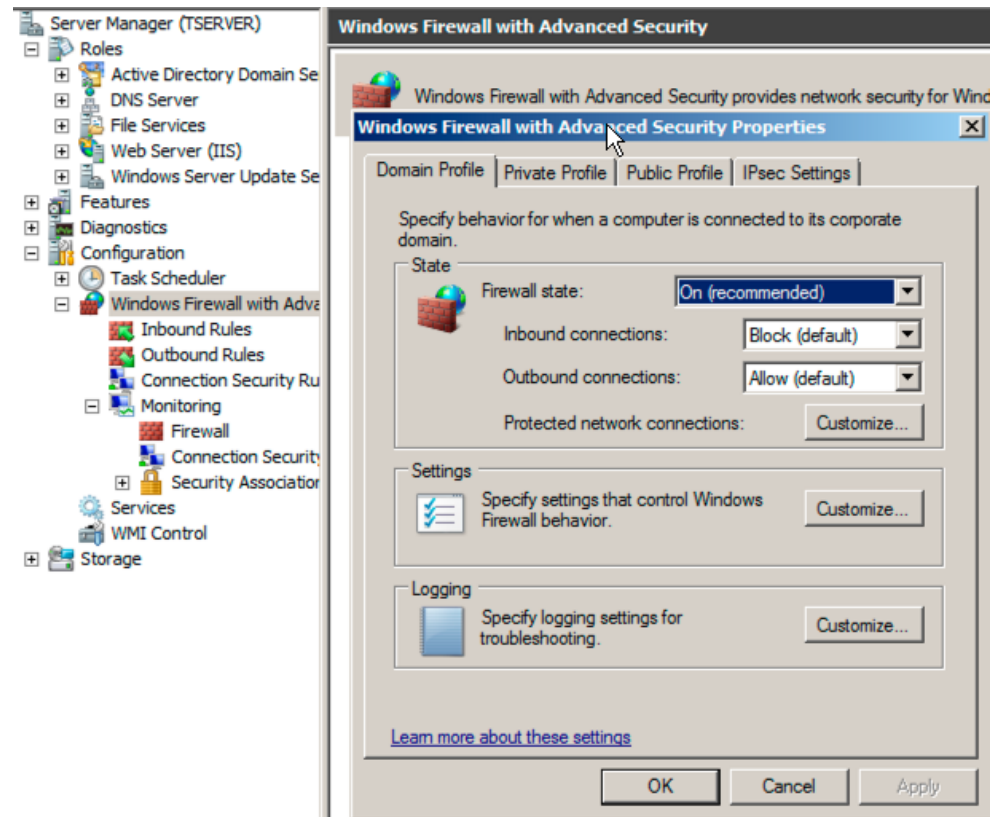
8

- ❑ What is a firewall?
 - ❑ A firewall network security system that monitors and controls the incoming and outgoing network traffic.

Firewalls (cont)

9

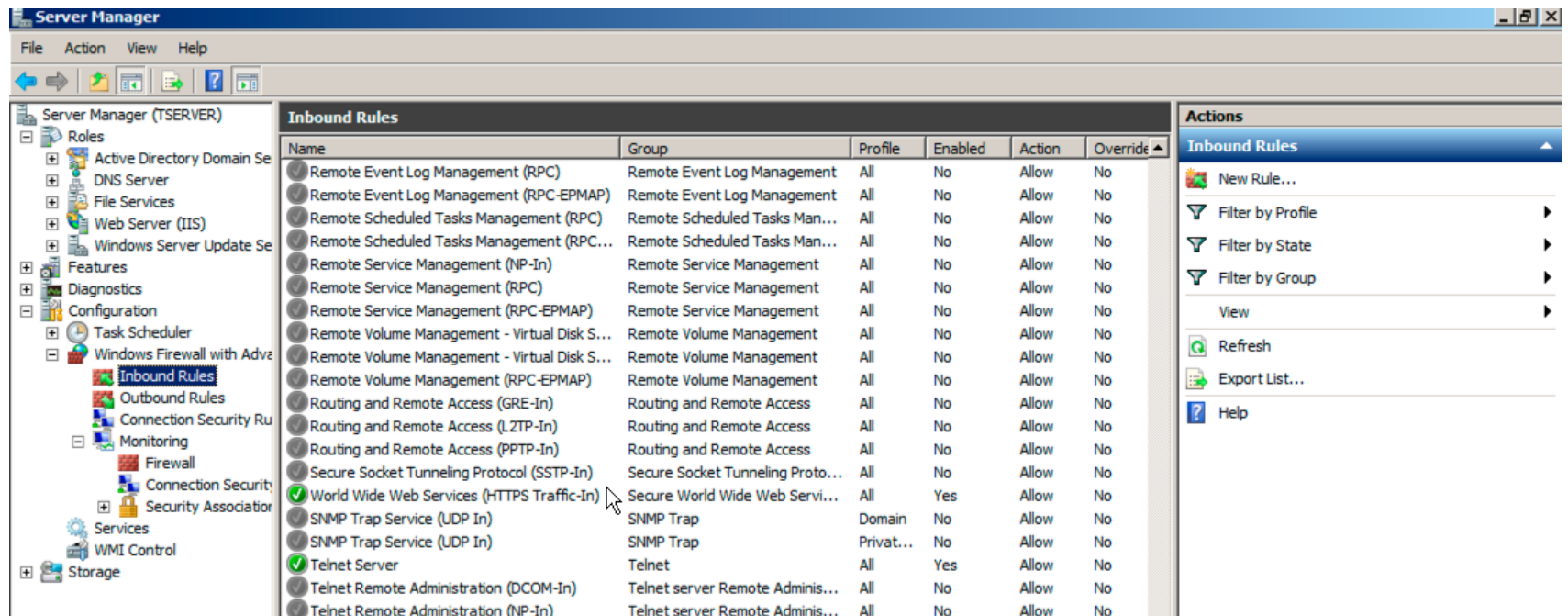
- How do we configure it on Windows?
 - ▣ Turn on Logging:



Firewalls (cont)

10

- ❑ Install Telnet
 - ❑ Add the Telnet Client and Server under Features
- ❑ Create a rule to allow Telnet



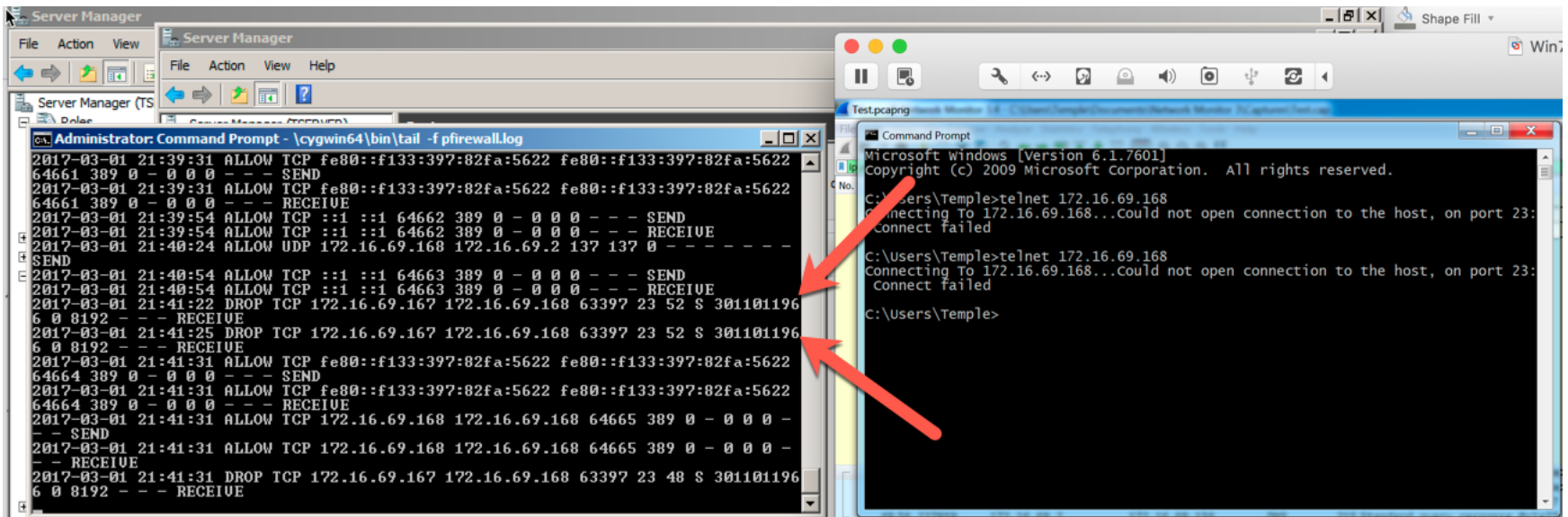
The screenshot shows the Windows Server Manager interface. The left-hand navigation pane is expanded to 'Features', and 'Inbound Rules' is selected. The main pane displays a table of inbound firewall rules. The 'Telnet Server' rule is highlighted with a green checkmark in the 'Enabled' column, indicating it is active. Other rules include Remote Event Log Management, Remote Service Management, and various Routing and Remote Access rules.

Name	Group	Profile	Enabled	Action	Override
Remote Event Log Management (RPC)	Remote Event Log Management	All	No	Allow	No
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Management	All	No	Allow	No
Remote Scheduled Tasks Management (RPC)	Remote Scheduled Tasks Man...	All	No	Allow	No
Remote Scheduled Tasks Management (RPC-EPMA...)	Remote Scheduled Tasks Man...	All	No	Allow	No
Remote Service Management (NP-In)	Remote Service Management	All	No	Allow	No
Remote Service Management (RPC)	Remote Service Management	All	No	Allow	No
Remote Service Management (RPC-EPMAP)	Remote Service Management	All	No	Allow	No
Remote Volume Management - Virtual Disk S...	Remote Volume Management	All	No	Allow	No
Remote Volume Management - Virtual Disk S...	Remote Volume Management	All	No	Allow	No
Remote Volume Management (RPC-EPMAP)	Remote Volume Management	All	No	Allow	No
Routing and Remote Access (GRE-In)	Routing and Remote Access	All	No	Allow	No
Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No
Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow	No
Secure Socket Tunneling Protocol (SSTP-In)	Secure Socket Tunneling Proto...	All	No	Allow	No
World Wide Web Services (HTTPS Traffic-In)	Secure World Wide Web Servi...	All	Yes	Allow	No
SNMP Trap Service (UDP In)	SNMP Trap	Domain	No	Allow	No
SNMP Trap Service (UDP In)	SNMP Trap	Privat...	No	Allow	No
Telnet Server	Telnet	All	Yes	Allow	No
Telnet Remote Administration (DCOM-In)	Telnet server Remote Adminis...	All	No	Allow	No
Telnet Remote Administration (NP-In)	Telnet server Remote Adminis...	All	No	Allow	No

Firewalls (cont)

11

□ Demo?



Firewalls (cont)

12

- ❑ Questions?

Quiz Questions Review – Week 3

13

- ❑ Quiz; review from Blackboard results – Week 3.
- ❑ Quiz; review via Blackboard.
- ❑ AH with IPSec; remember it only signs the packet between two computers, not the content
- ❑ Primary and Secondary storage
- ❑ Firewalls are a network device that controls which two computers and on which network ports they can communication. These are different from ports on a switch
- ❑ Switch; Protections for an OS

Quiz Questions Review – Week 4

14

- ❑ Quiz; review from Blackboard results – Week 4.
- ❑ Controls to files
 - ❑ Remember that files are controlled by shares and ACL's
- ❑ Change the account a service runs as.
 - ❑ Remember that modifying all services is under services; the others will be wrong
 - ❑ Remember that deny always takes precedence over allow.
 - ❑ Remember from previous weeks; we create or talk about creating a helpdesk role. This is not a built in item.

Quiz Questions Review – Week 5

15

- ❑ Quiz; review from Blackboard results – Week 5.
- ❑ Group Policy Preferences
 - ❑ Remember that GPO Preferences are what to do if they are not set on a system.
- ❑ Active directory Users and Computers
 - ❑ Remember that there are more things in AD than just users and computers
- ❑ Why Policy Over Preferences
 - ❑ Remember that a policy is enforcement for all users, even ones with local admin access.

Quiz Questions Review – Week 6

16

- ❑ Any Questions from last week?
- ❑ Quiz; review from Blackboard results – Week 6.
- ❑ SCCM
 - ❑ Remember that SCCM is a way of patching large numbers of computers.

Quiz Questions Review (cont)

17

- Any questions on quiz questions?

Review for Test 1

18

- Test 1 Review.

Review for Test 1 (cont)

19

- Any questions on Test 1 review?

Assignment 3 Overview

20

- ❑ Requirements – Same teams members as before.
 - ❑ A report of the CIS baseline built into a GPO
 - Note: there is a report feature for a GPO to where the setting that have been applied can be exported into a report file; that is the report I'm referring to here.
 - Applied to the same DC Windows 7 pair we have been working from assignment 2.
 - ❑ A video from the team as how this improves our security with faces and voices.
 - ❑ Expand upon the GPO that was created in assignment 2 from 20 settings to what the team feels sufficient to secure Windows 7.
 - ❑ This assignment builds to what is presented to the Pen-Testing class for Assignment 4, so the 4th grade is how well the team does in it's selections from the baseline in assignment 3.
- ❑ Due Date: March 9th 11:59pm
 - ❑ Late assignments have a 10% penalty per week.

Assignment 3 Overview (cont)

21

- Questions?

Next Week

22

- ❑ Questions from previous week
- ❑ Logging
 - ❑ Windows Event Viewer (eventvwr.exe)
 - ❑ Paid Products
 - Splunk
- ❑ Assignment 3 (Due Mar 9th)

Quiz

23

- ❑ We can start Test 1