MIS 5170

Operating System Security

Week 7

Windows Firewalls

Fox School of Business
TEMPLE UNIVERSITY®

Tonight's Plan

- ❑ Questions from Last Week
- ❑ Firewalls
- ❑ Review Quiz Questions
- ❑ Review for 1st test
- ❑ Assignment 3 Overview
- ❑ Spring Break
- ❑ Test 1

Questions From Last Week

- 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)

- Any additional questions?

Firewalls

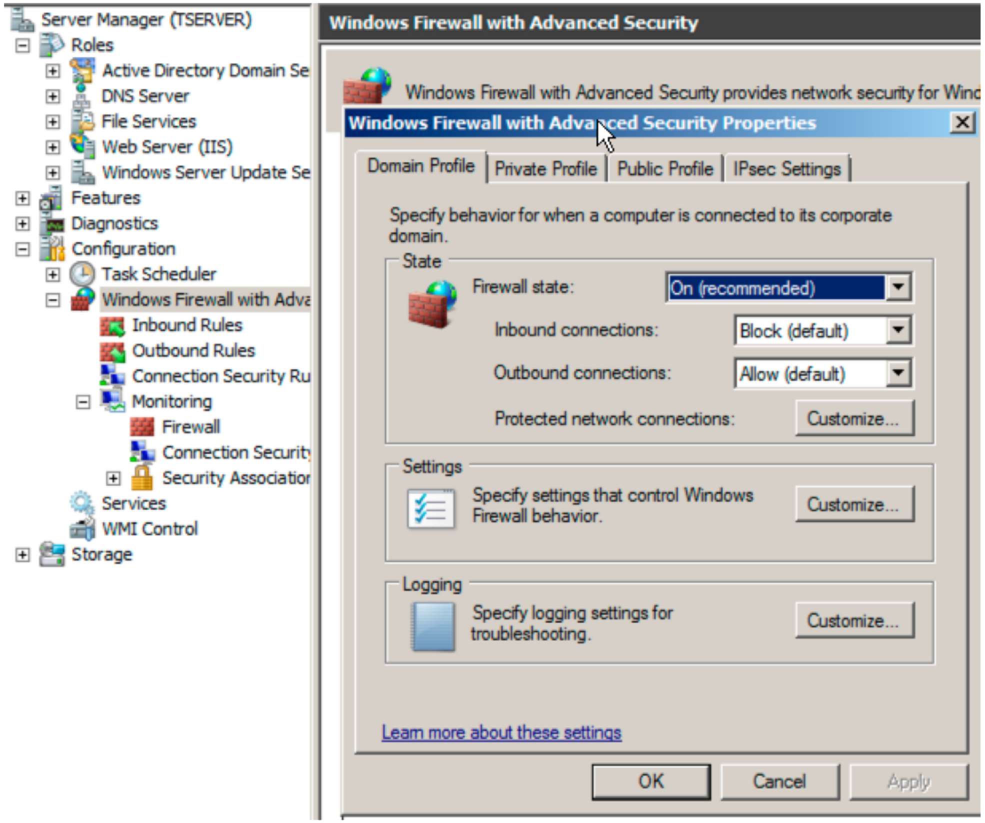
- ❑ What is a firewall?
- ❑ How do we configure it on Windows?

Firewalls (cont)

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

Firewalls (cont)

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



Server Manager (TSERVER)
- Roles
  - Active Directory Domain Se
  - DNS Server
  - File Services
  - Web Server (IIS)
  - Windows Server Update Se
- Features
- Diagnostics
- Configuration
  - Task Scheduler
  - Windows Firewall with Adva
    - Inbound Rules
    - Outbound Rules
    - Connection Security Ru
    - Monitoring
      - Firewall
      - Connection Security
      - Security Associatior
  - Services
  - WMI Control
- Storage

Windows Firewall with Advanced Security

Windows Firewall with Advanced Security provides network security for Winc

Windows Firewall with Advanced Security Properties

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Firewall behavior. Customize...

Logging

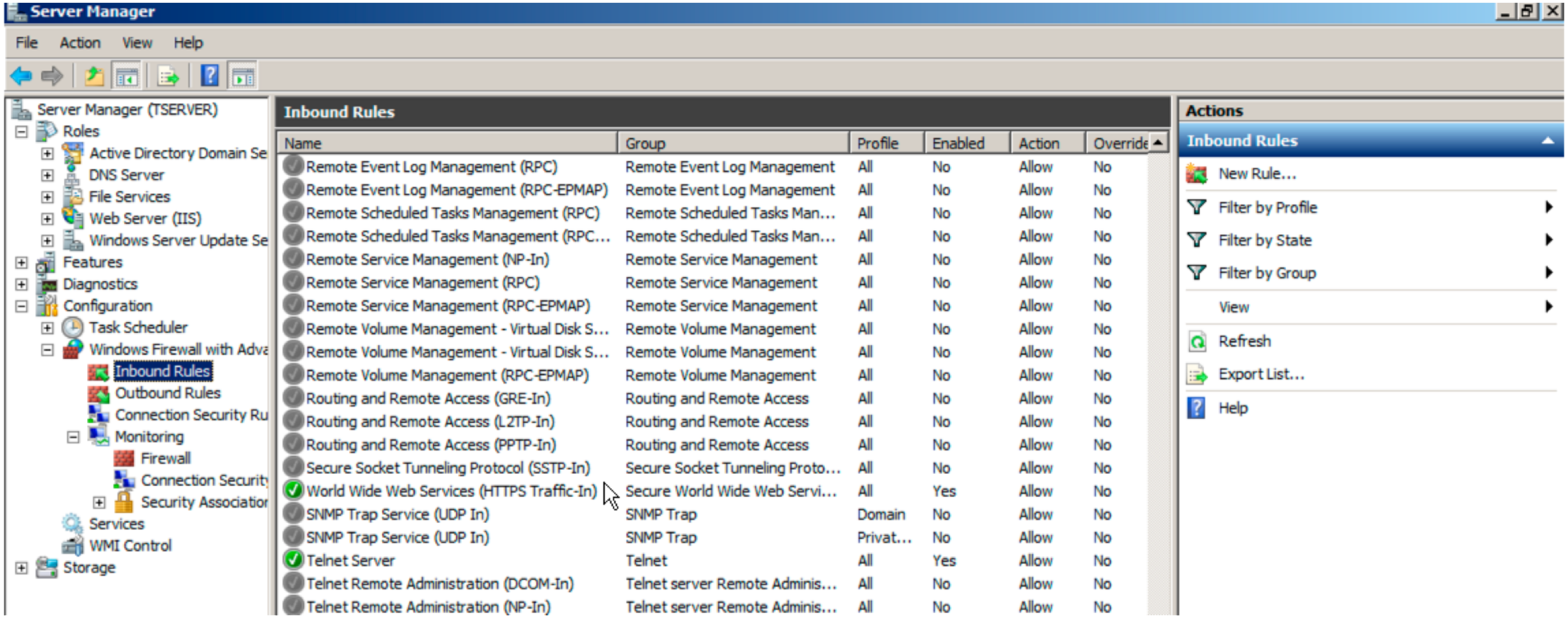
Specify logging settings for troubleshooting. Customize...

Learn more about these settings

OK Cancel Apply

Firewalls (cont)

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

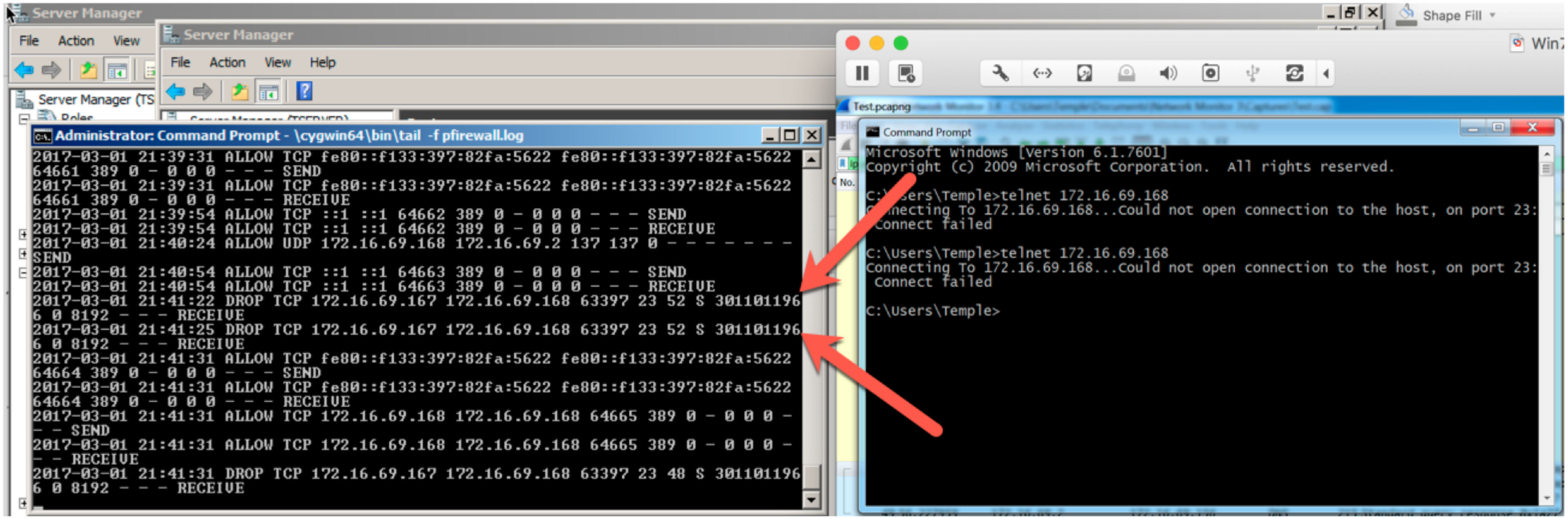


Inbound Rules

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...	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)

- Demo?



Administrator: Command Prompt - \cygwin64\bin\tail -f pfirewall.log

```
2017-03-01 21:39:31 ALLOW TCP fe80::f133:397:82fa:5622 fe80::f133:397:82fa:5622
64661 389 0 - 0 0 0 - - - SEND
2017-03-01 21:39:31 ALLOW TCP fe80::f133:397:82fa:5622 fe80::f133:397:82fa:5622
64661 389 0 - 0 0 0 - - - RECEIVE
2017-03-01 21:39:54 ALLOW TCP ::1 ::1 64662 389 0 - 0 0 0 - - - SEND
2017-03-01 21:39:54 ALLOW TCP ::1 ::1 64662 389 0 - 0 0 0 - - - RECEIVE
2017-03-01 21:40:24 ALLOW UDP 172.16.69.168 172.16.69.2 137 137 0 - - - - - - -
SEND
2017-03-01 21:40:54 ALLOW TCP ::1 ::1 64663 389 0 - 0 0 0 - - - SEND
2017-03-01 21:40:54 ALLOW TCP ::1 ::1 64663 389 0 - 0 0 0 - - - RECEIVE
2017-03-01 21:41:22 DROP TCP 172.16.69.167 172.16.69.168 63397 23 52 S 301101196
6 0 8192 - - - RECEIVE
2017-03-01 21:41:25 DROP TCP 172.16.69.167 172.16.69.168 63397 23 52 S 301101196
6 0 8192 - - - RECEIVE
2017-03-01 21:41:31 ALLOW TCP fe80::f133:397:82fa:5622 fe80::f133:397:82fa:5622
64664 389 0 - 0 0 0 - - - SEND
2017-03-01 21:41:31 ALLOW TCP fe80::f133:397:82fa:5622 fe80::f133:397:82fa:5622
64664 389 0 - 0 0 0 - - - RECEIVE
2017-03-01 21:41:31 ALLOW TCP 172.16.69.168 172.16.69.168 64665 389 0 - 0 0 0 -
- - SEND
2017-03-01 21:41:31 ALLOW TCP 172.16.69.168 172.16.69.168 64665 389 0 - 0 0 0 -
- - RECEIVE
2017-03-01 21:41:31 DROP TCP 172.16.69.167 172.16.69.168 63397 23 48 S 301101196
6 0 8192 - - - RECEIVE
```

Command Prompt

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Temple>telnet 172.16.69.168
Connecting To 172.16.69.168...Could not open connection to the host, on port 23:
 Connect failed

C:\Users\Temple>telnet 172.16.69.168
Connecting To 172.16.69.168...Could not open connection to the host, on port 23:
 Connect failed

C:\Users\Temple>
```

Firewalls (cont)

- Questions?

Quiz Questions Review – Week 3

- 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 3

- Any Questions from last week?
- Quiz; review via Blackboard.
  - We talked about USB keys spreading viruses
    - Home Depot Caulk
  - Primary and Secondary storage
    - What is what; from slides in week 1 (Primary = Memory)
  - Firewalls
    - Controls the address(s) and port(s) to and from
  - IPSec
    - ESP = encryption of everything; AH = Auth Header encryption

Quiz Questions Review – Week 4

- 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

- 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 5

- Any Questions from last week?
- Quiz; review from Blackboard results.
- ACL Precedence
  - Remember that deny with ACL's over-ride allow (all objects)
- Controls to files
  - Remember that files are controlled by file shares and ACL's
- Helpdesk group; does not exist.
  - Remember that we talked about least privilege.
- Microsoft Tier'd model
  - We talked about; key take away keep account and password at the same tier.

Quiz Questions Review – Week 6

- 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 – Week 6

- Any Questions from last week?
- Quiz; review from Blackboard results.
- Base line
  - Remember that a base line is what we want; not what the vendor starts an OS.
- Configuration drift?
  - This is the term used for where we want our baseline vs where it is now; possibly not in a state we want our computers
- 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 (cont)

- Any questions on quiz questions?

Review for Test 1

- Test 1 Review.

Review for Test 1 (cont)

- ❑ Any questions on Test 1 review?

Assignment 3 Overview

- 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 desktop 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 desktop.
  - 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 23rd 11:59pm
  - Late assignments have a 10% penalty per week.

Assignment 3 Overview (cont)

- Questions?

Next Week

- Questions from previous week
- Logging
  - Windows Event Viewer (eventvwr.exe)
  - Paid Products
    - Splunk
- Assignment 3 (Due Mar 23rd)

Test

- We can start Test 1