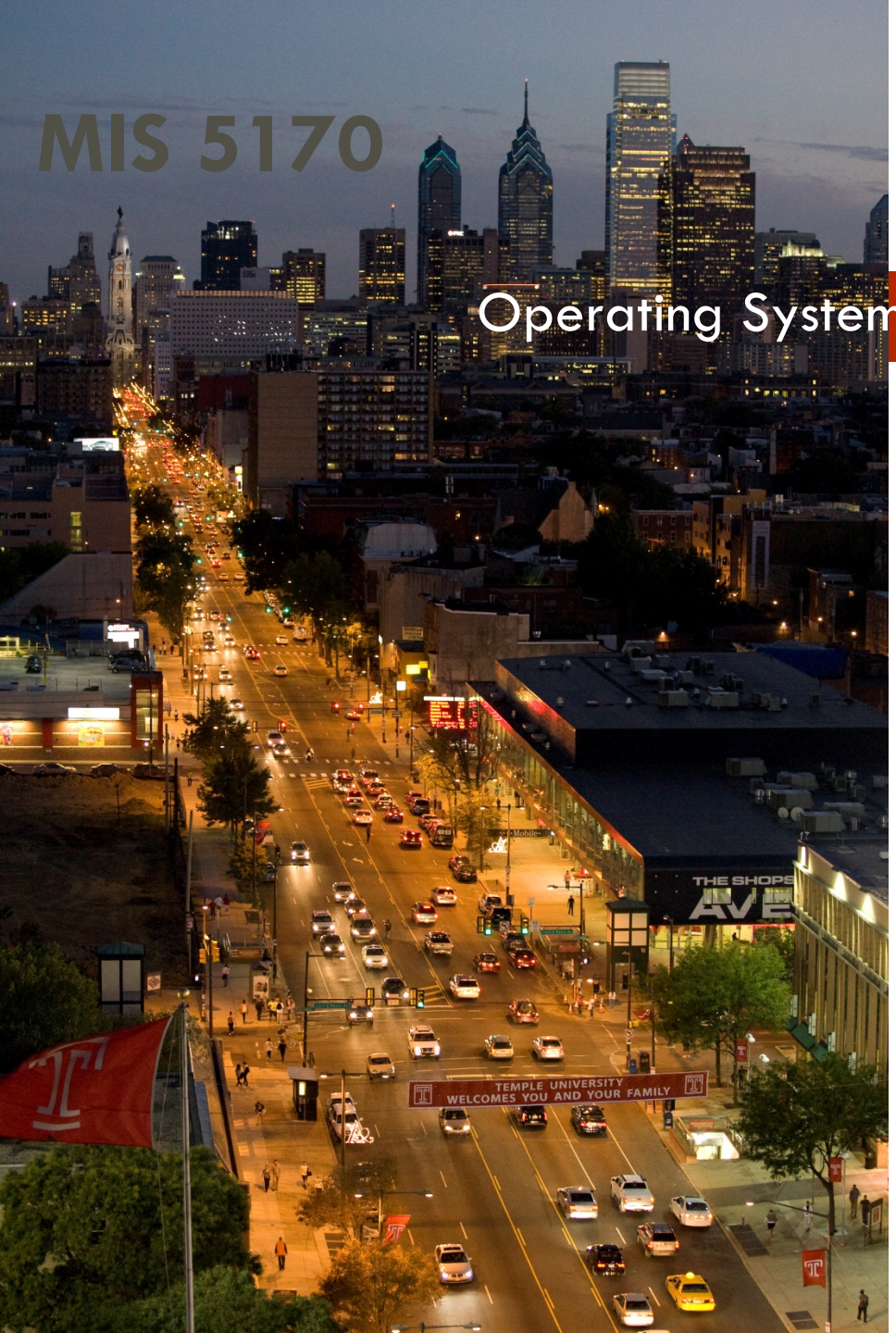


Operating System Security

Week 8

Windows Logging

Fox School of Business
TEMPLE UNIVERSITY®

Tonight's Plan

- Questions from Last Week
- Review on-line posts
- In The News
- Logging
- Assignment 3 Due Mar 24th
- Next Week
- Quiz
- Spring Break

Questions From Last Week

- Any Questions from last week?
- Test 1; review from Blackboard results – Week 7.

Column **Test 1 (Test)**

COLUMN DETAILS

Column	Test 1 (Test)
Points Possible	250
Description	

STATISTICS

Count	19
Minimum Value	190.00
Maximum Value	250.00
Range	60.00
Average	231.58
Median	230.00
Standard Deviation	14.60
Variance	213.30

STATUS DISTRIBUTION

Null	0
In Progress	0
Needs Grading	0
Exempt	0

GRADE DISTRIBUTION

Greater than 100	0
90 - 100	14
80 - 89	4
70 - 79	1
60 - 69	0
50 - 59	0
40 - 49	0
30 - 39	0
20 - 29	0
10 - 19	0
0 - 9	0
Less than 0	0

Questions From Last Week (cont)

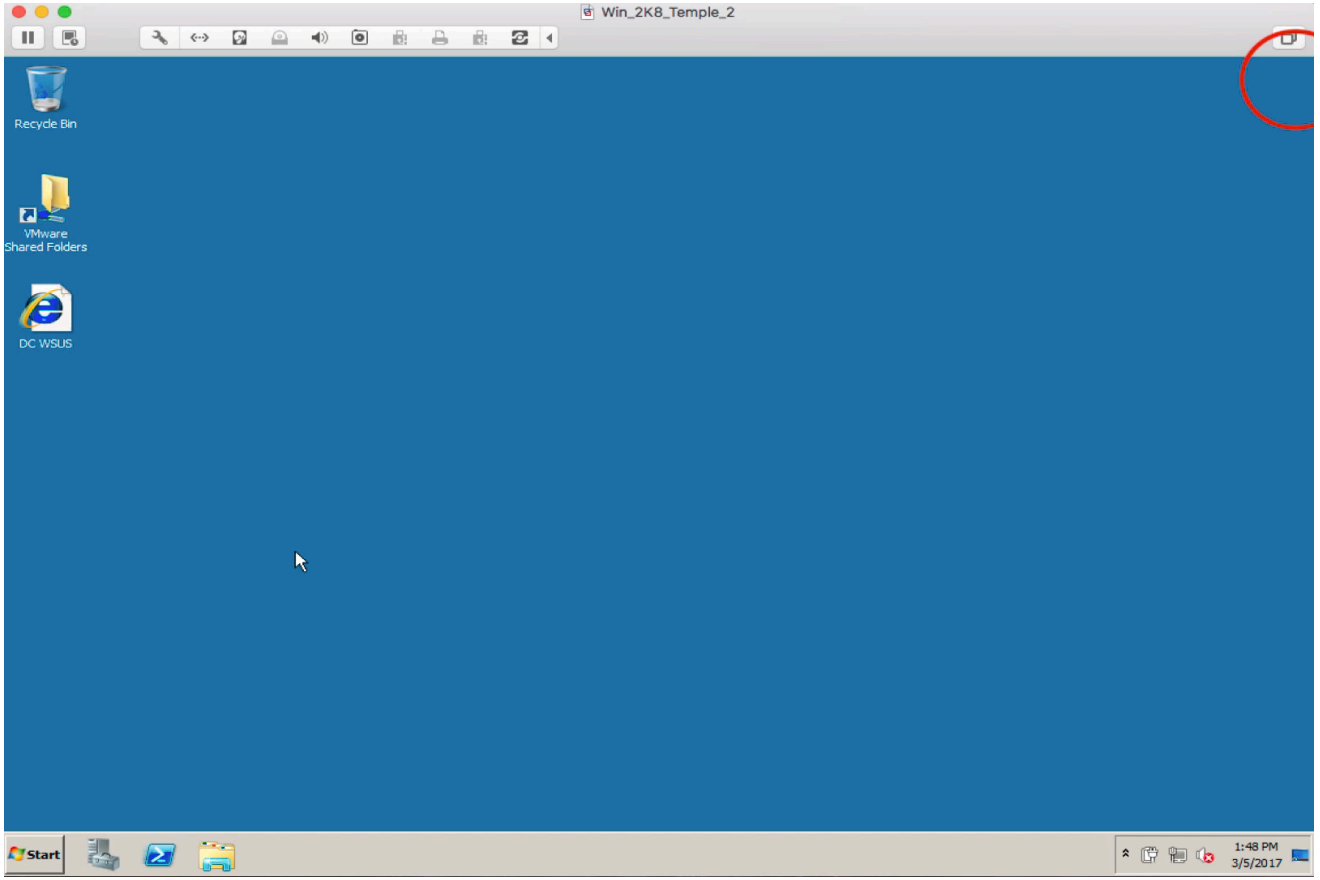
- Any additional questions?

Review on-line posts

- Review on-line videos
  - Install Telnet services on Windows Server
  - Install Telnet client on Windows Desktop
  - Enable FW logging on Windows Server
  - Enable firewall rule for telnet on Windows Server
  - Trace telnet traffic to Windows Server
  - Create IPSec Rule
  - Verify IPSec Rule

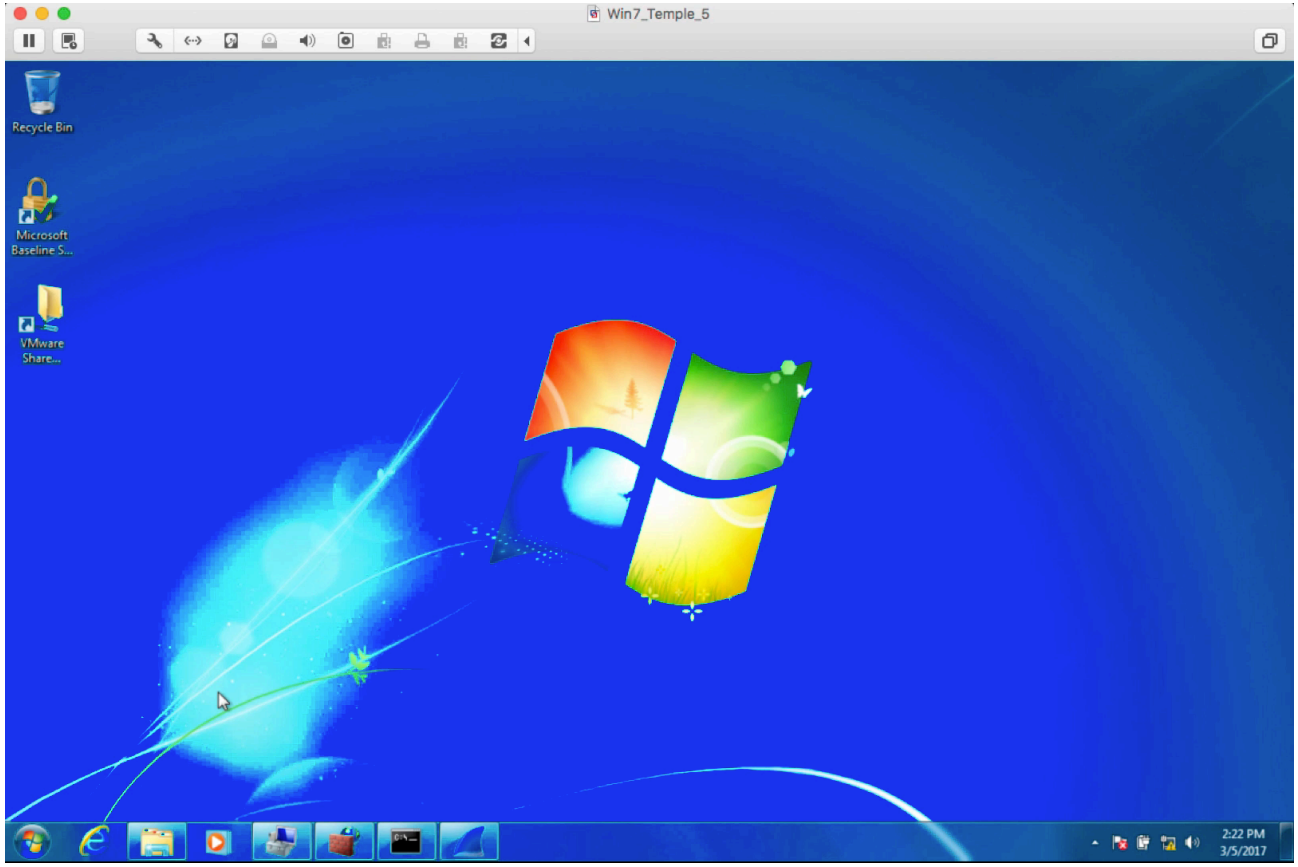
Review on-line posts (cont)

- Install Telnet services on Windows Server



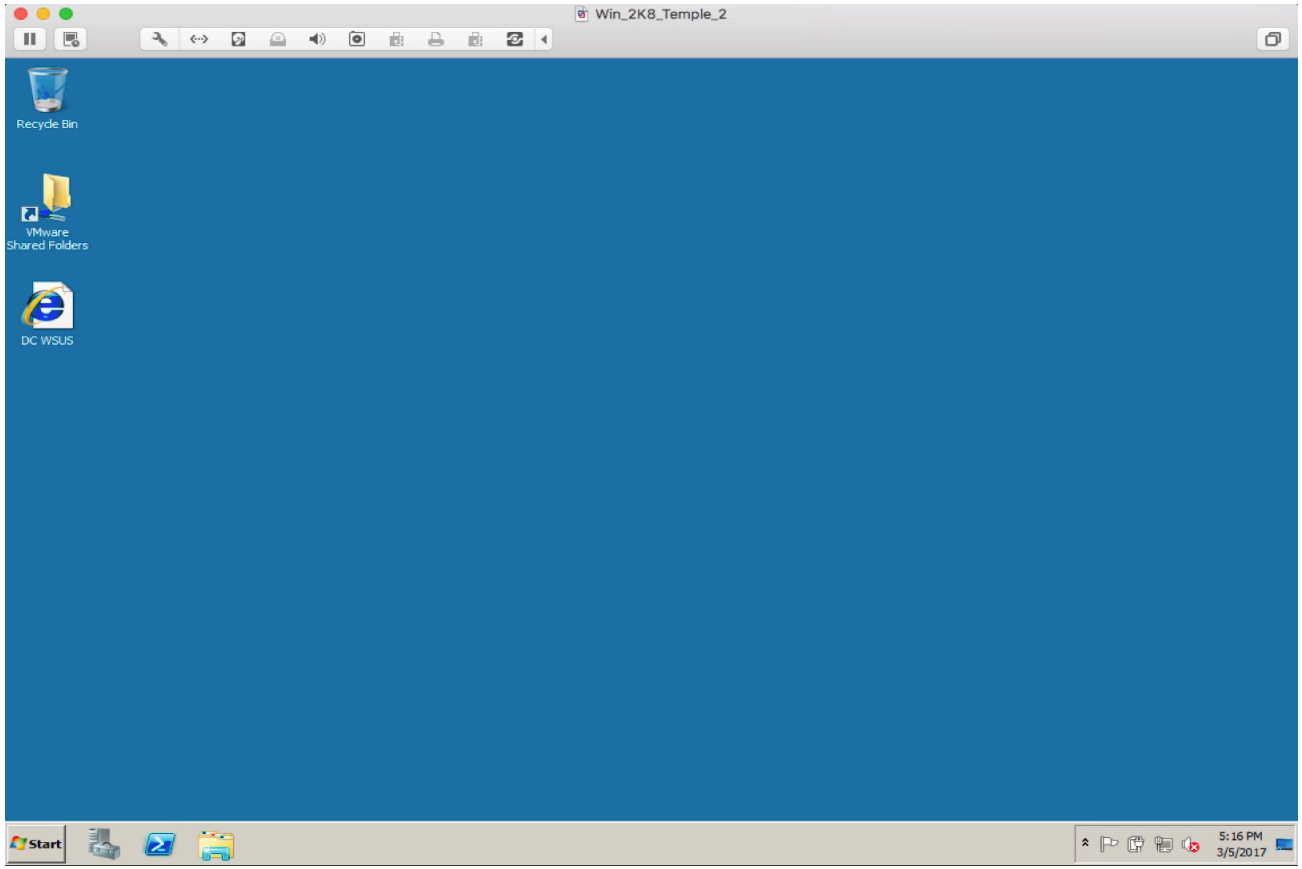
Review on-line posts (cont)

- Install Telnet client on Windows Desktop



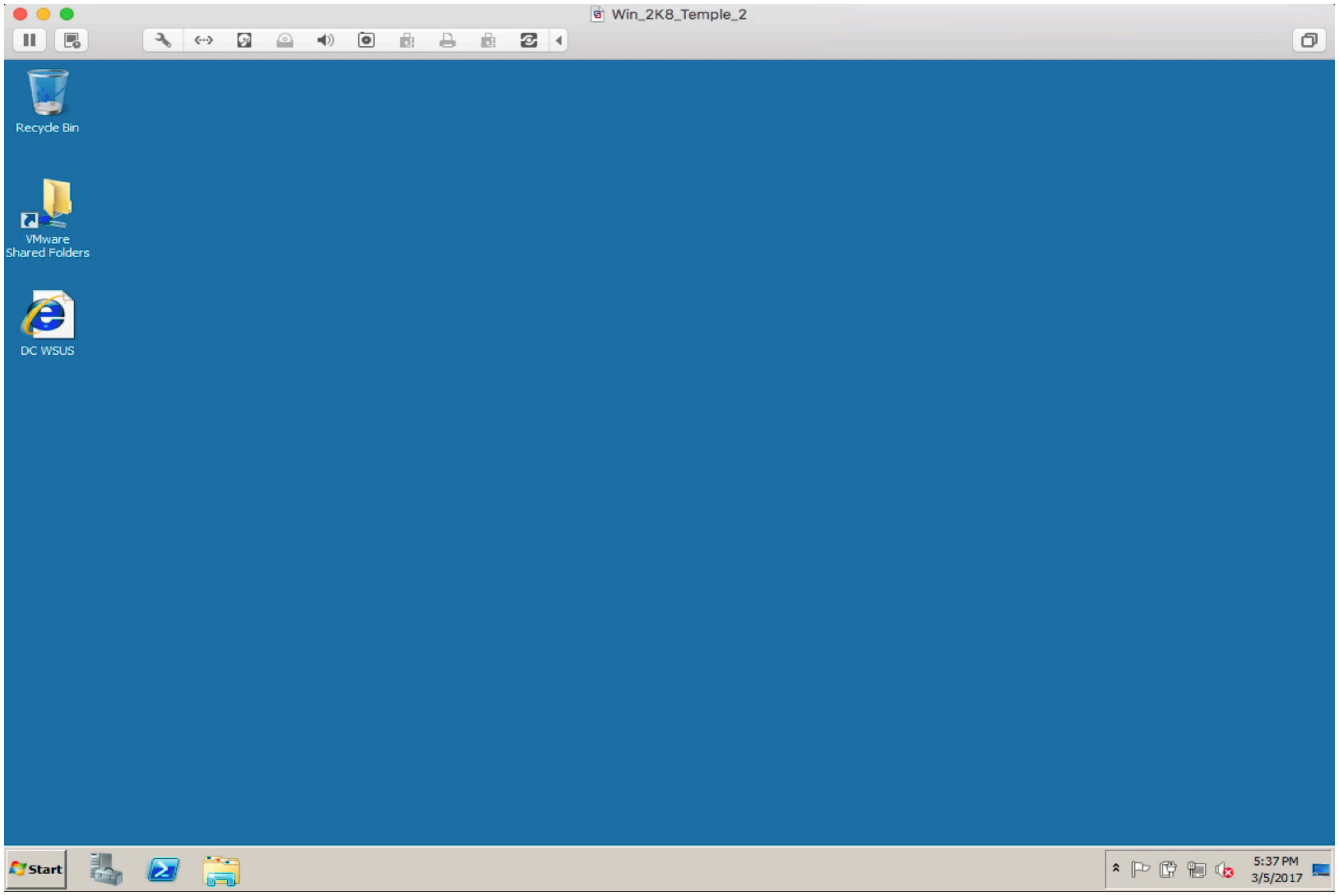
Review on-line posts (cont)

- Enable FW logging on Windows Server



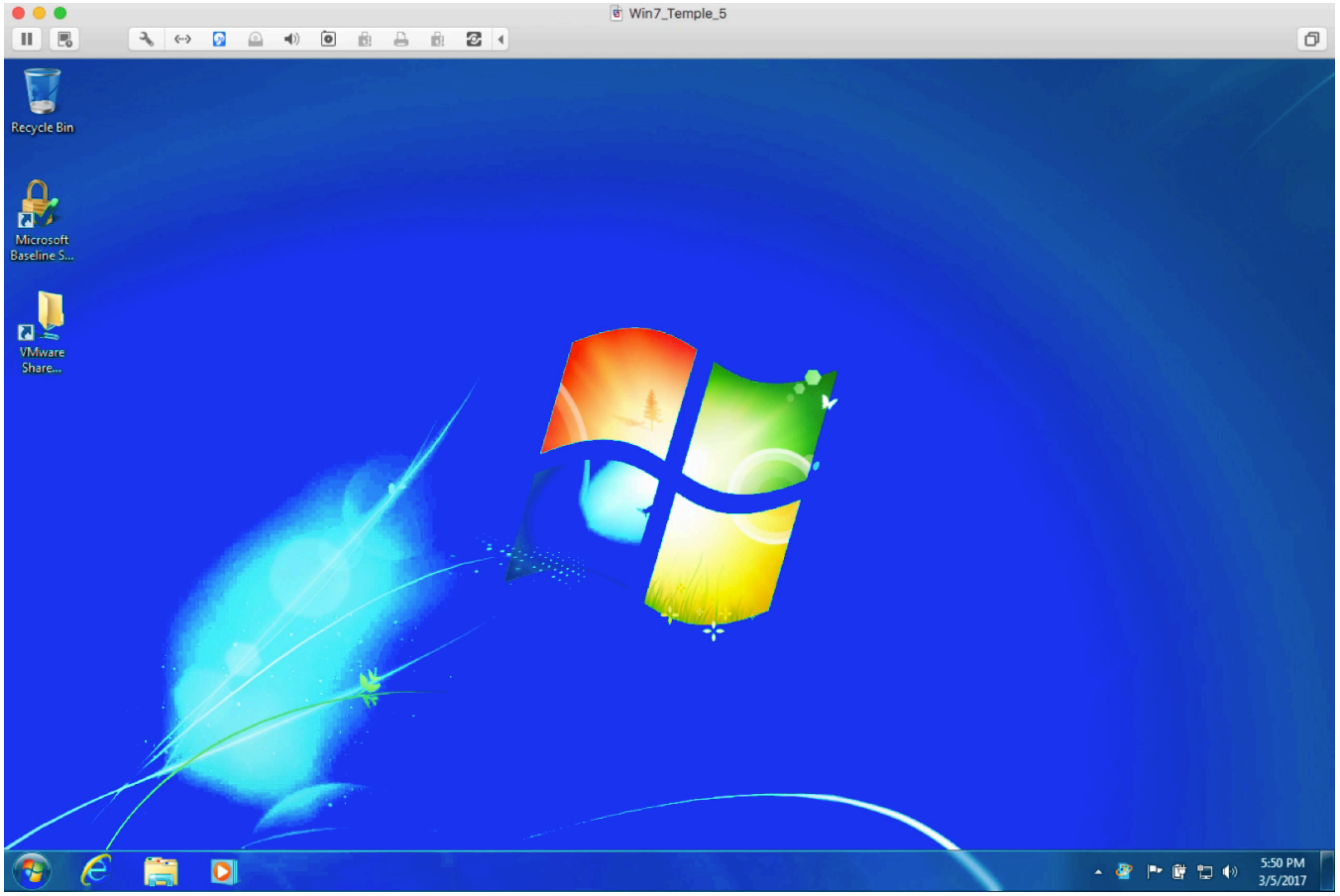
Review on-line posts (cont)

- Enable firewall rule for telnet on Windows Server



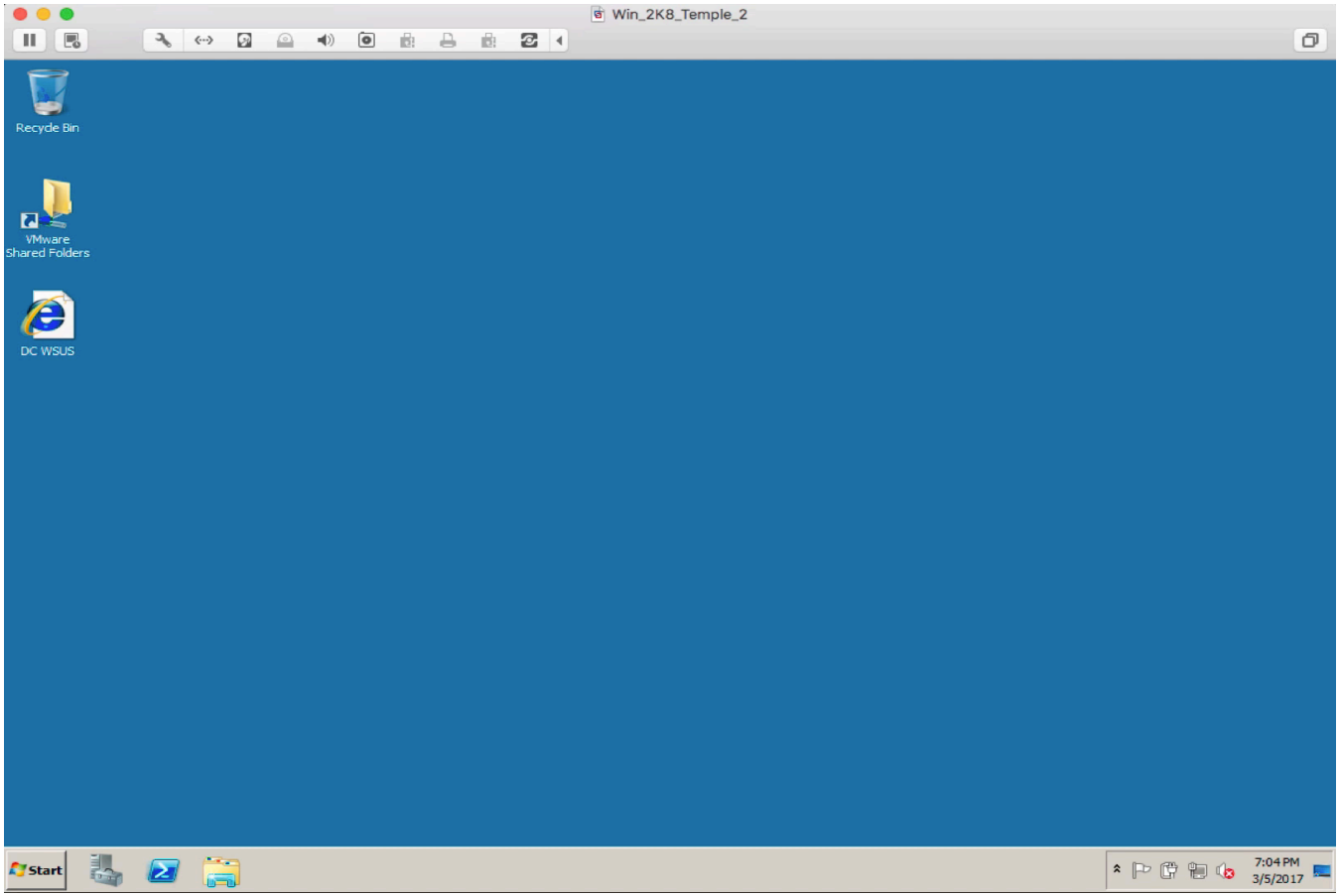
Review on-line posts (cont)

- Trace telnet traffic to Windows Server



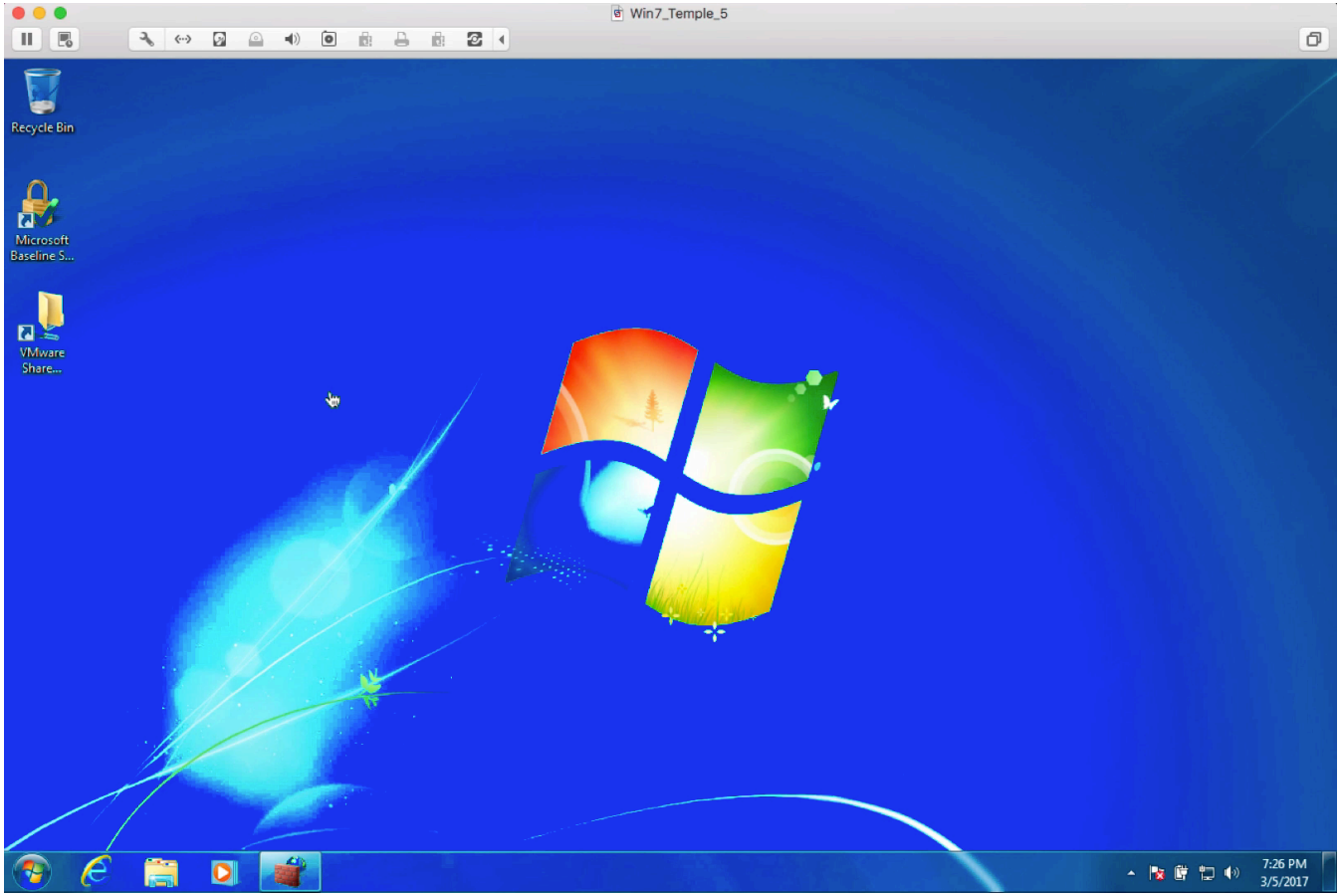
Review on-line posts (cont)

- Create IPSec Rule



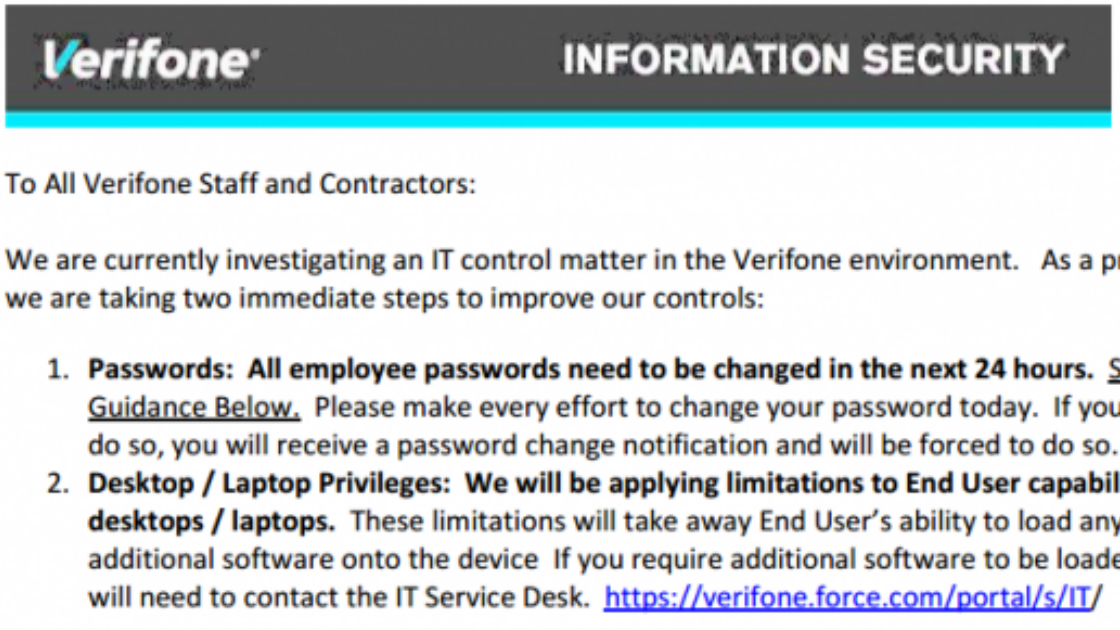
Review on-line posts (cont)

- Verify IPSec Rule



In the News

- Payments Giant Verifone Investigating Breach
  - Verifone's network breach.
    - https://krebsonsecurity.com/2017/03/payments-giant-verifone-investigating-breach/



Verifone INFORMATION SECURITY

To All Verifone Staff and Contractors:

We are currently investigating an IT control matter in the Verifone environment. As a precaution, we are taking two immediate steps to improve our controls:

1. **Passwords: All employee passwords need to be changed in the next 24 hours.** See Guidance Below. Please make every effort to change your password today. If you do not do so, you will receive a password change notification and will be forced to do so.
2. **Desktop / Laptop Privileges: We will be applying limitations to End User capabilities on desktops / laptops.** These limitations will take away End User's ability to load any additional software onto the device If you require additional software to be loaded, you will need to contact the IT Service Desk. https://verifone.force.com/portal/s/IT/

In the News (cont)

Password Policy and Guidance

All passwords must:

1. Be at least 12 characters in length
2. Be original and not have been used by you previously;
3. Contain ALL of the following character groups:

a. English uppercase characters **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**
b. English lowercase characters **a b c d e f g h i j k l m n o p q r s t u v w x y z**
c. Numerals **0 1 2 3 4 5 6 7 8 9**
d. Non-alphanumeric characters **` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : ; " ' < > ? , . /**

Password Guidelines:

- Ransomware for Dummies: Anyone Can Do It
  - Fastest growing cybercrime; encrypt your computer and demand payment to get it back.
    - https://krebsonsecurity.com/2017/03/ransomware-for-dummies-anyone-can-do-it/

In the News (cont)

- Pennsylvania Democratic state senators hit with ransomware attack
  - http://www.techspot.com/news/68391-pennsylvania-democratic-state-senators-hit-ransomware-attack.html

In the News (cont)

- Questions or items anyone has found of interest?

Logging

- What is logging?
- Why is it important?
- How can it help us secure our operating systems?
- How do we enable logging on Windows?
- What do we do with it once it is enabled?

Logging (cont)

- What is logging?
  - Logging is 'enabling' in an operating system the function of writing activities to a file or logging facility.
    - In Windows that facility is the 'Event Viewer'
    - They are stored in files under %windir%\system32\winevt\Logs
      - In the format of either .evt or .evtx
        - .evt prior to Windows 2008 & Windows 7
      - You need 'Event Viewer' to read them

Logging (cont)

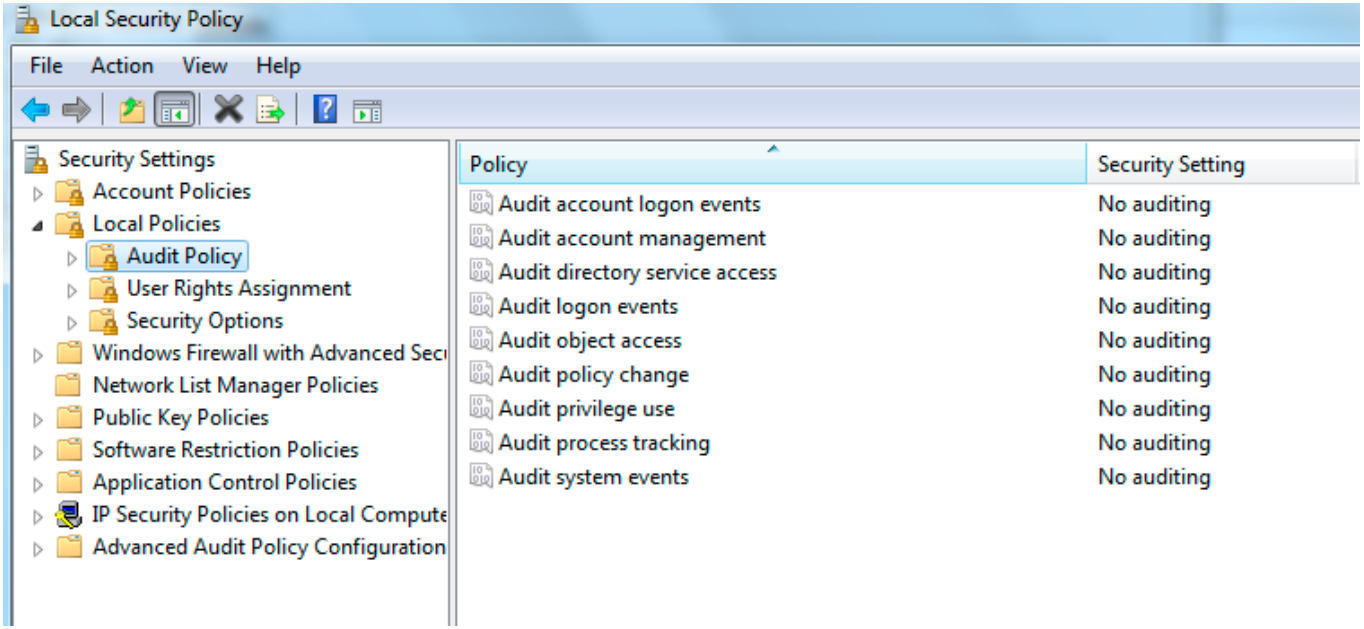
- Why is it important?
  - Without logs you will not be able to see what is in your environment
  - Remember you will be attacked and someone will get in
    - Without logs you will not be able to see that attack and foot hold
  - Prevention is what we all want, but detection is an important part securing our operating systems
  - Also logging gives us the data on what additional things we need to 'lock down' in our operating systems

Logging (cont)

- How can it help us secure our operating systems?
  - As the last slide stated:
    - Tells us what items users and process are using to get in
    - Watch the trends and work on the 80%
      - Remove the ways process or users are getting in that are not needed or wanted
  - Tells us what is going right
    - Failures are those things we have locked down correctly
    - Failures are thoes things we might not want locked down
      - Remember our Denies in the firewall logs

Logging (cont)

- How do we enable logging on Windows?
  - Local Security Policy
  - Windows Group Policy

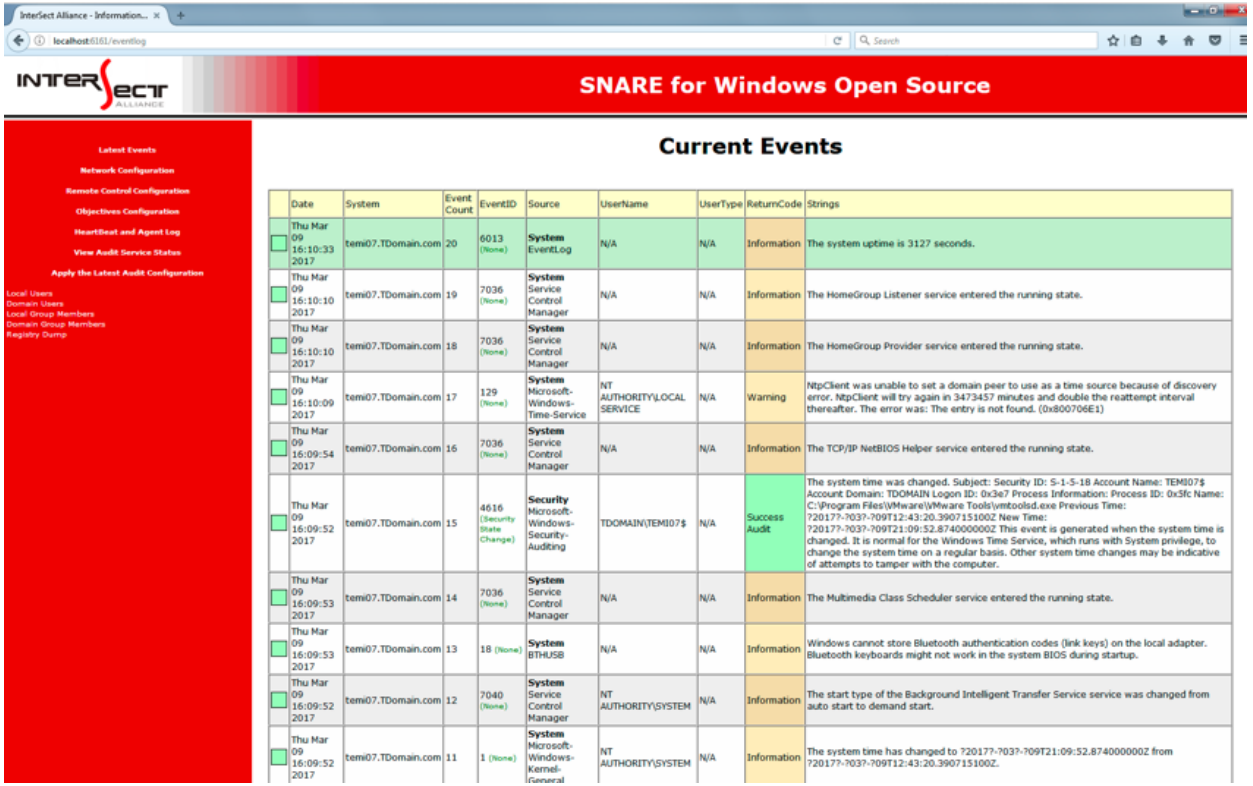


Logging (cont)

- What do we do with it once it is enabled?
  - Get it off the box!!!
  - The main reason you enable logging is to find out if something is going wrong
    - If you don't have the logs because someone deleted them after they got onto you corporate computer. To quote "Does a tree falling in the forest make a sound, if there is no one there to hear it fall?"

Logging (cont)

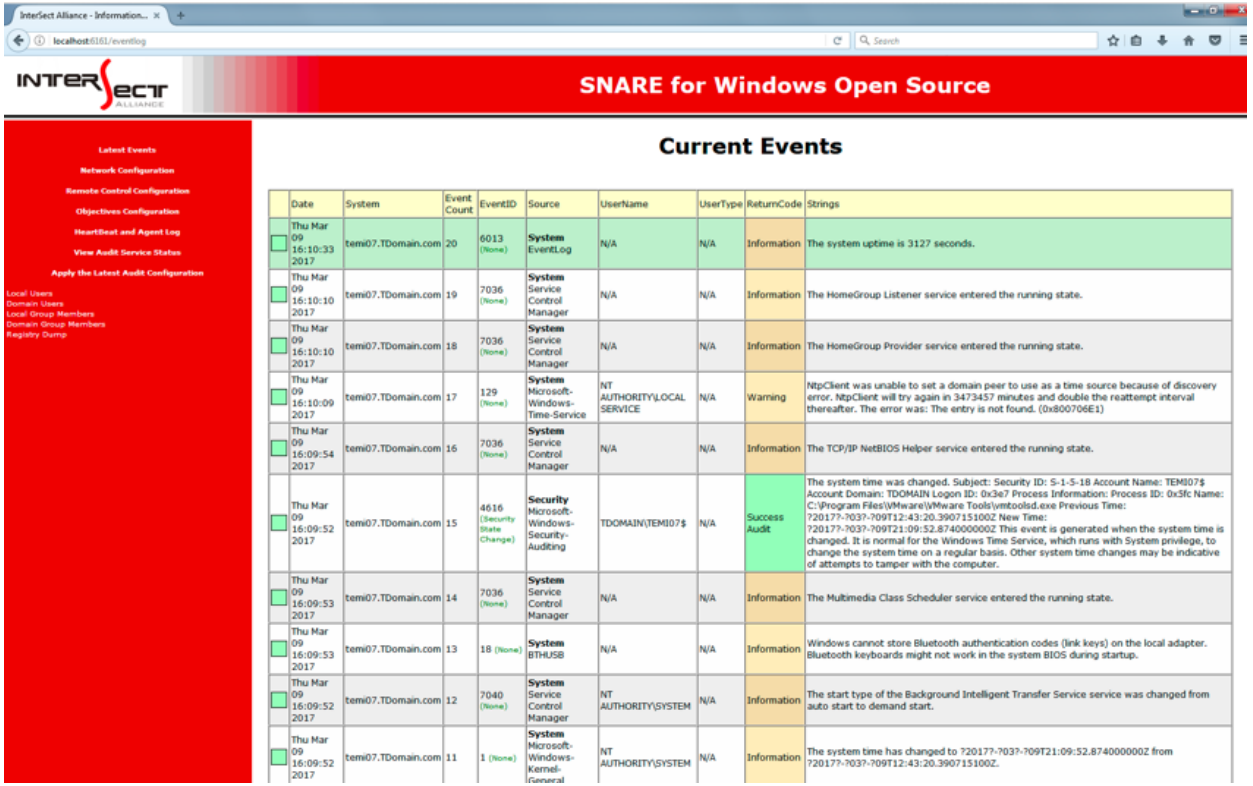
- What do we do with it once it is enabled?
  - Get it off the box!!!
    - SNARE:



	Date	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
	Thu Mar 09 16:10:33 2017	temi07.TDomain.com	20	6013 (None)	System EventLog	N/A	N/A	Information	The system uptime is 3127 seconds.
	Thu Mar 09 16:10:10 2017	temi07.TDomain.com	19	7036 (None)	System Service Control Manager	N/A	N/A	Information	The HomeGroup Listener service entered the running state.
	Thu Mar 09 16:10:10 2017	temi07.TDomain.com	18	7036 (None)	System Service Control Manager	N/A	N/A	Information	The HomeGroup Provider service entered the running state.
	Thu Mar 09 16:10:09 2017	temi07.TDomain.com	17	129 (None)	System Microsoft-Windows-Time-Service	NT AUTHORITY\LOCAL SERVICE	N/A	Warning	NtpClient was unable to set a domain peer to use as a time source because of discovery error. NtpClient will try again in 3473457 minutes and double the reattempt interval thereafter. The error was: The entry is not found. (0x800706E1)
	Thu Mar 09 16:09:54 2017	temi07.TDomain.com	16	7036 (None)	System Service Control Manager	N/A	N/A	Information	The TCP/IP NetBIOS Helper service entered the running state.
	Thu Mar 09 16:09:52 2017	temi07.TDomain.com	15	4616 (Security State Change)	Security Microsoft-Windows-Security-Auditing	TDOMAIN\TEMI07$	N/A	Success Audit	The system time was changed. Subject: Security ID: S-1-5-18 Account Name: TEMI07$ Account Domain: TDOMAIN Logon ID: 0x3e7 Process Information: Process ID: 0x5fc Name: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe Previous Time: ?20177-?03?-?09T12:43:20.390715100Z New Time: ?20177-?03?-?09T21:09:52.874000000Z This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.
	Thu Mar 09 16:09:53 2017	temi07.TDomain.com	14	7036 (None)	System Service Control Manager	N/A	N/A	Information	The Multimedia Class Scheduler service entered the running state.
	Thu Mar 09 16:09:53 2017	temi07.TDomain.com	13	18 (None)	System BTHUSB	N/A	N/A	Information	Windows cannot store Bluetooth authentication codes (link keys) on the local adapter. Bluetooth keyboards might not work in the system BIOS during startup.
	Thu Mar 09 16:09:52 2017	temi07.TDomain.com	12	7040 (None)	System Service Control Manager	NT AUTHORITY\SYSTEM	N/A	Information	The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.
	Thu Mar 09 16:09:52 2017	temi07.TDomain.com	11	1 (None)	System Microsoft-Windows-Kernel-General	NT AUTHORITY\SYSTEM	N/A	Information	The system time has changed to ?20177-?03?-?09T21:09:52.874000000Z from ?20177-?03?-?09T12:43:20.390715100Z.

Logging (cont)

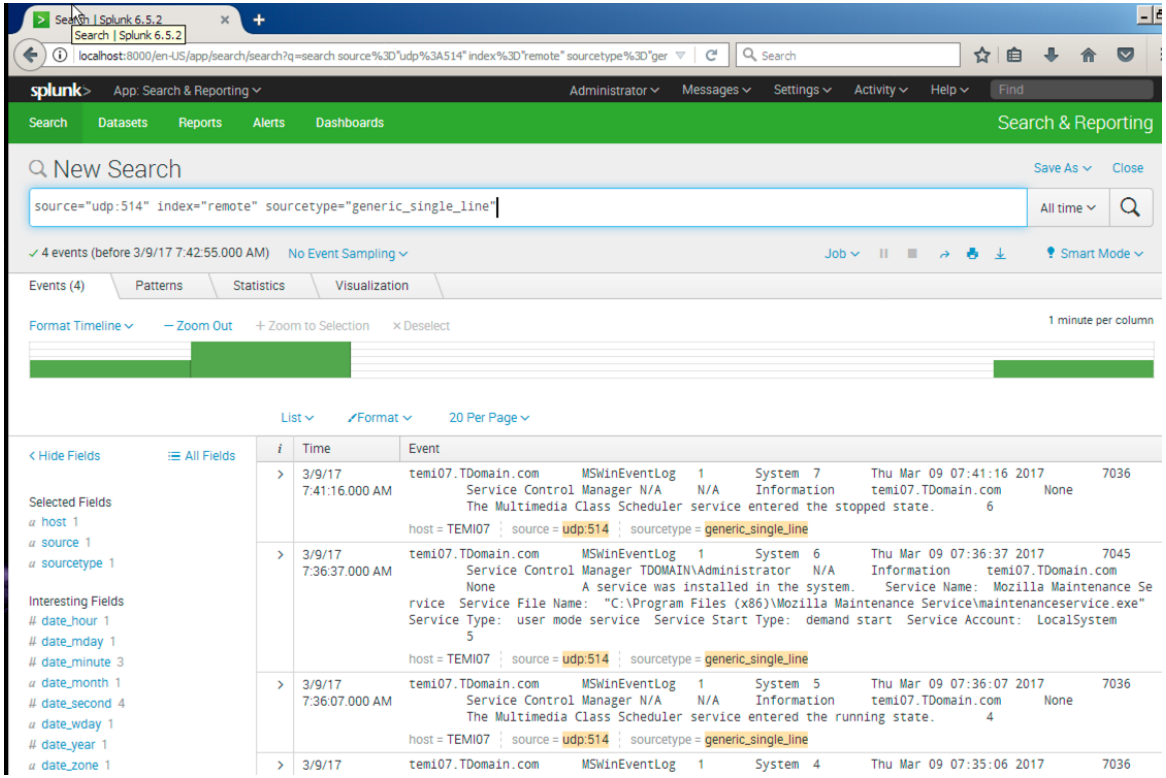
- What do we do with it once it is enabled?
  - Get it off the box!!!
    - SNARE:



	Date	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
	Thu Mar 09 16:10:33 2017	temi07.TDomain.com	20	6013 (None)	System EventLog	N/A	N/A	Information	The system uptime is 3127 seconds.
	Thu Mar 09 16:10:10 2017	temi07.TDomain.com	19	7036 (None)	System Service Control Manager	N/A	N/A	Information	The HomeGroup Listener service entered the running state.
	Thu Mar 09 16:10:10 2017	temi07.TDomain.com	18	7036 (None)	System Service Control Manager	N/A	N/A	Information	The HomeGroup Provider service entered the running state.
	Thu Mar 09 16:10:09 2017	temi07.TDomain.com	17	129 (None)	System Microsoft-Windows-Time-Service	NT AUTHORITY\LOCAL SERVICE	N/A	Warning	NtpClient was unable to set a domain peer to use as a time source because of discovery error. NtpClient will try again in 3473457 minutes and double the reattempt interval thereafter. The error was: The entry is not found. (0x800706E1)
	Thu Mar 09 16:09:54 2017	temi07.TDomain.com	16	7036 (None)	System Service Control Manager	N/A	N/A	Information	The TCP/IP NetBIOS Helper service entered the running state.
	Thu Mar 09 16:09:52 2017	temi07.TDomain.com	15	4616 (Security State Change)	Security Microsoft-Windows-Security-Auditing	TDOMAIN\TEMI07$	N/A	Success Audit	The system time was changed. Subject: Security ID: S-1-5-18 Account Name: TEMI07$ Account Domain: TDOMAIN Logon ID: 0x3e7 Process Information: Process ID: 0x5fc Name: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe Previous Time: ?20177-?03?-?09T12:43:20.390715100Z New Time: ?20177-?03?-?09T21:09:52.874000000Z This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.
	Thu Mar 09 16:09:53 2017	temi07.TDomain.com	14	7036 (None)	System Service Control Manager	N/A	N/A	Information	The Multimedia Class Scheduler service entered the running state.
	Thu Mar 09 16:09:53 2017	temi07.TDomain.com	13	18 (None)	System BTHUSB	N/A	N/A	Information	Windows cannot store Bluetooth authentication codes (link keys) on the local adapter. Bluetooth keyboards might not work in the system BIOS during startup.
	Thu Mar 09 16:09:52 2017	temi07.TDomain.com	12	7040 (None)	System Service Control Manager	NT AUTHORITY\SYSTEM	N/A	Information	The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.
	Thu Mar 09 16:09:52 2017	temi07.TDomain.com	11	1 (None)	System Microsoft-Windows-Kernel-General	NT AUTHORITY\SYSTEM	N/A	Information	The system time has changed to ?20177-?03?-?09T21:09:52.874000000Z from ?20177-?03?-?09T12:43:20.390715100Z.

Logging (cont)

- What do we do with it once it is enabled?
  - Get it off the box!!!



Logging (cont)

- What do we do with it once it is enabled?
  - Get it off the box!!!
  - https://www.gartner.com/document/3406817

Logging (cont)

- Demo

Logging (cont)

- Questions?

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 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 24th 11:59pm
  - Late assignments have a 10% penalty per week.

Assignment 3 Overview (cont)

- Questions?

Next Week

- Spring Break
- Questions from previous week
- Unix/Linux basics
  - Scripting
  - Appropriate permissions
  - Limit services
  - Shares
- Assignment 3 (Due Mar 24th)

Quiz

- We can start the Quiz