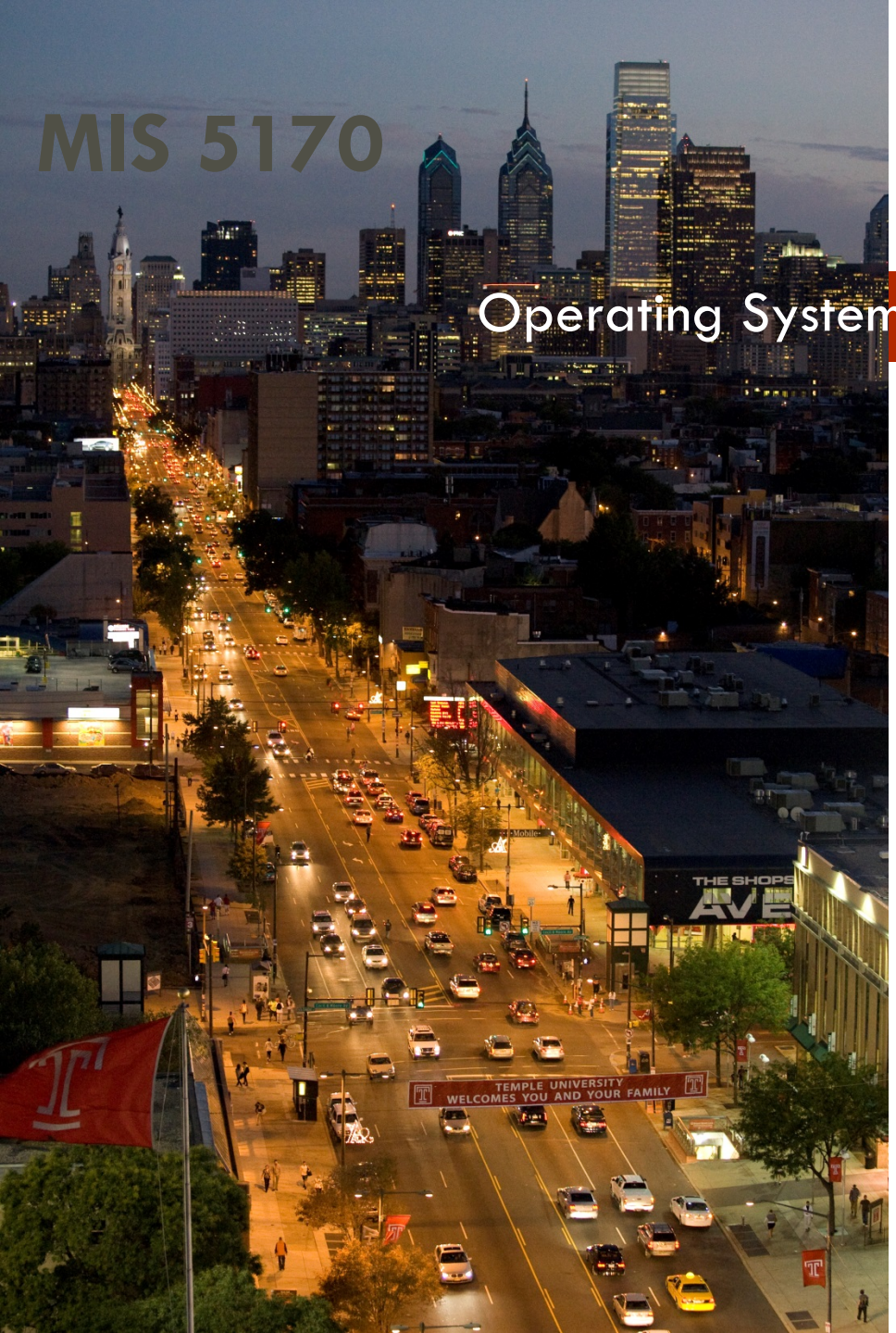


Operating System Security

Week 6

Windows Antivirus

Fox School of Business
TEMPLE UNIVERSITY®

Tonight's Plan

- Questions from Last Week
- Review on-line posts
- In The News
- Malware/Spyware
- Detection tools
- Antivirus
- Sniffers
- Assignment 3 Overview
- Next Week
- Quiz

Questions From Last Week

- 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.

Questions From Last Week (cont)

- Any additional questions?

Review On-Line Posts

- Top Posts
  - New EU Privacy Law May Weaken Security
    - The European Union's General Data Protection Regulation (GDPR)
      - **Jason A Lindsley**
  - **Article: Microsoft Patch Tuesday, February 2018 Edition**
    - **Sev Shirozian**
      - **"After all, getting down to zero vulnerabilities on your network is impossible. However your vulnerability management program should use tools like this to reduce attack vectors by addressing the critical and high vulnerabilities first, especially in the DMZ or public facing servers."**

Review On-Line Posts (cont)

- Hosting a DC on Cloud…
  - "This is a bad idea for many reasons"
    - Frederic D Rohrer
- Questions about the posts?

In the News

- Article: Domain Theft Strands Thousands of Web Sites
  - Three domains belonging to Newtek Business Services Corp. [NASDAQ:NEWT]
    - https://krebsonsecurity.com/2018/02/domain-theft-strands-thousands-of-web-sites/
- February Updates from Adobe, Microsoft
  - Windows (SMB) could let attackers crash Windows 8.1, and Windows 10 systems, as well as server equivalents of those platforms.
    - https://krebsonsecurity.com/2017/02/february-updates-from-adobe-microsoft/

The smartest option is probably to ditch the program once and for all and significantly increase the security of your system in the process. An extremely powerful and buggy program that binds itself to the browser, Flash is a favorite target of attackers and malware. For some ideas about how to hobble or do without Flash (as well as slightly less radical solutions) check out A Month Without Adobe Flash Player.

In the News (cont)

- New EU Privacy Law May Weaken Security
  - The European Union's General Data Protection Regulation (GDPR)
    - https://krebsonsecurity.com/2018/02/new-eu-privacy-law-may-weaken-security/

In the News (cont – Last Year)

On Feb. 2, the **CERT Coordination Center** at **Carnegie Mellon University** warned that an unpatched bug in a core file-sharing component of Windows (SMB) could let attackers crash Windows 8.1, and Windows 10 systems, as well as server equivalents of those platforms. CERT warned that exploit code for the flaw was already available online.

- What does it mean about "as well as server equivalents of those platforms."?
  - OS releases; code streams are released as desktop – server code.
    - For Example: Windows 7 – Server 2008
- Questions or items anyone has found of interest?

Malware/Spyware

- What is Malware/Spyware?
- How can you get Malware/Spyware on your system?
- How can you remove them if you do get hit?

Malware/Spyware (cont)

- What is Malware?
  - Malware is a class of software that has been created to either damage or track specific information about a user's activities back to the creator of that software.
    - Malware is the main class of software, which includes: Viruses, spyware, adware, nagware, trojans, worms and more.
  - Spyware may log activity and send it back to the creator for the creator's specific purpose.
  - Viruses similar to a human virus it tries to get into a computer and spread to other neighboring computers.

Malware/Spyware (cont)

- How can you get Malware on your system?
  - Drive-by's – a term know as I can't infect the site you visit, but I can place an ad on that site to infect your system.
    - Ad's on Bing, google, CNN, etc
  - Pop-up Ad's
  - Downloads/Installs from not the vendors sites
  - Boot-sector; more likely to be a found USB key; or shared USB key.
  - Etc
  - Can you name any?

Malware/Spyware (cont)

- How can you remove them if you do get hit?
  - Vendor products
    - Malicious Removal Tool
  - Third-Party (lots in this space)
    - MalwareBytes
      - One of the first ones I've used
    - Symantec
    - McAfee
  - We will not go into infecting any systems, but lots of tools.
    - Remember the writer of the software may have tested against these products so they might not work.
    - Second; time is money and these tools might be a trojan horse looking for users with higher privledges…

Malware/Spyware (cont)

- We will not go into infecting any systems, but lots of tools. (cont)
  - Lots of companies have a crush and re-load policy to prevent the spread of 'Trojan' and malware.
- Questions?

Detection Tools

- Lots of tools in this space; most of them are know as End Point Preventions tools or antivirus.
  - ~~TotalAV~~
  - ~~SCANGuard~~
  - MalwareBytes
  - ~~Norton~~
  - McAfee
  - ~~PCProtect~~
  - KasperskyLab
  - Microsoft (moved up)
  - ~~AVG~~

Detection Tools (cont)

- What is the best detection?
  - Prevention is general the best detections as you can see by the below article.
  - You can also see that they have moved away from writing their own tools or .exe's, etc. in favor of using items that are white-listed
    - What is white-listing – a method of allowing specific programs

The next wave of attacks will be fileless. Advanced attackers have been exploiting script-based attacks for years. Common Windows utilities, such as the command line interface, PowerShell, Pearl, Visual Basic, Nmap and Windows Credential Editor, can be exploited to compromise machines without dropping any executable files, evading all traditional forms of malicious file detection. We are starting to see malware authors experimenting with mass-propagating fileless malware using the same techniques. As a result, EPP buyers should look for vendors that focus on memory exploit protection, script analysis and behavior indicators of compromise. Ultimately, we believe that vendors that focus on detecting behavior indicative of attacker tradecraft (that is, tools, tactics and techniques) will be the most effective.

Detection Tools (cont)

- Questions?

Antivirus

- What is antivirus software?
- How does it help secure your operating system?
- Is Antivirus software dead? As predicted several years ago
- What are some names in this space?
- What is next?

Antivirus (cont)

- What is antivirus software?
  - Antivirus software – now really know as End Point Protection is a software product to prevent well know malicious software from taking hold of a user's computer. Most are base on signatures of these malicious software files other are working to define behavior that are malicious to get ahead of the signature race.

Antivirus (cont)

- How does it help secure your operating system?
  - Defense-in-depth is the primary way it helps; prevent well-know code from being dropped and started on your computer.
  - Another logging method to a central console; gives a SOC notifications of computers on the inside; (got past our IDS/IPS devices and rules) that have either downloaded or tried to download something that was not stopped or quarantined.
    - First system hit
    - Where did it go
    - Can we apply what hit this system to our IDS/IPS devices to stop others from getting hit?

Antivirus (cont)

- Is Antivirus software dead? As predicted several years ago
  - Antivirus is not dead lots or reporting standards still list them on major control documents. From government organization, general security documents, etc
  - Remember defense-in-depth – when you can stop the obvious items from being able to attack your computer.
  - Last weeks Patch Tuesday, there where several AV vendors that had the best prevention to critical vulnerabilities from getting into your environment.

Antivirus (cont)

- What are some names in this space?
  - Top Tier; better know as the magic Quadrant
    - Symantec
    - Sophos
    - Trend Micro
      - Moved out of top right from last graph
        - Kaspersky Lab

Antivirus (cont)

- What is next?

The next wave of attacks will be fileless. Advanced attackers have been exploiting script-based attacks for years. Common Windows utilities, such as the command line interface, PowerShell, Pearl, Visual Basic, Nmap and Windows Credential Editor, can be exploited to compromise machines without dropping any executable files, evading all traditional forms of malicious file detection. We are starting to see malware authors experimenting with mass-propagating fileless malware using the same techniques. As a result, EPP buyers should look for vendors that focus on memory exploit protection, script analysis and behavior indicators of compromise. Ultimately, we believe that vendors that focus on detecting behavior indicative of attacker tradecraft (that is, tools, tactics and techniques) will be the most effective.

- Questions?

Sniffers

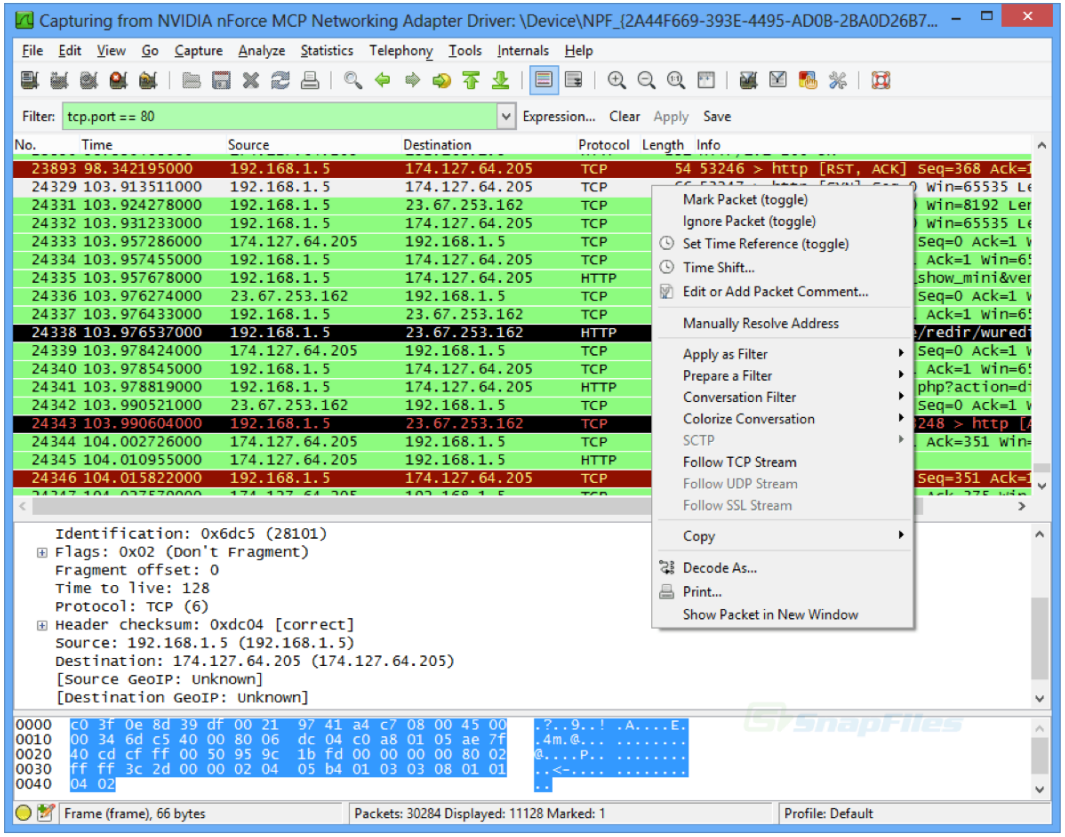
- What is a sniffer/Network Analyzer
- What does it do?
- How can it help us?
- What are some examples?

Sniffers (cont)

- What is a sniffer/Network Analyzer?
  - A network sniffer also know as packet analyzer, protocol analyzer is a computer program or computer hardware that can intercept and log traffic that passes over a digital network to help you diagnose or to isolate captured traffic as needed. Many are now appliances or part of switches and/or firewalls.

Sniffers (cont)

- What does it do?
  - Enables promiscuous mode – a fancy name for turn off MAC Filtering on the network card
  - Record all packets on the network to a circular buffer.
  - Why does a switch make this difficult?



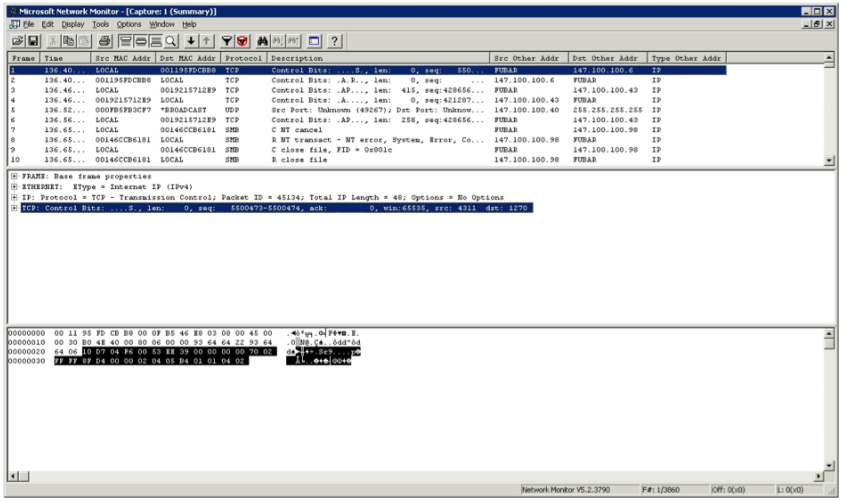
TEMPLE UNIVERSITY

Sniffers (cont)

- How can it help us?
  - Configure firewalls for proper ports in our environment.
  - Troubleshoot network slowness in our environment.
  - Find root-kits on an operating system.
  - Troubleshoot network conversation between two computers.
    - On and on and on…

Sniffers (cont)

- What are some examples?
  - Microsoft NetMon/Message Analyzer
    - Demo
  - WireShark
    - Demo



Sniffers (cont)

- Questions?

Next Week

- Questions from previous week
- Firewalls
  - Host based
    - IPSec
  - Network based
- Review for 1st Test
- Test 1
- Assignment 3 Overview (Due Mar 23rd)

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

Assignment 3 Overview (cont)

- Questions?

Quiz

- The Quiz has been released