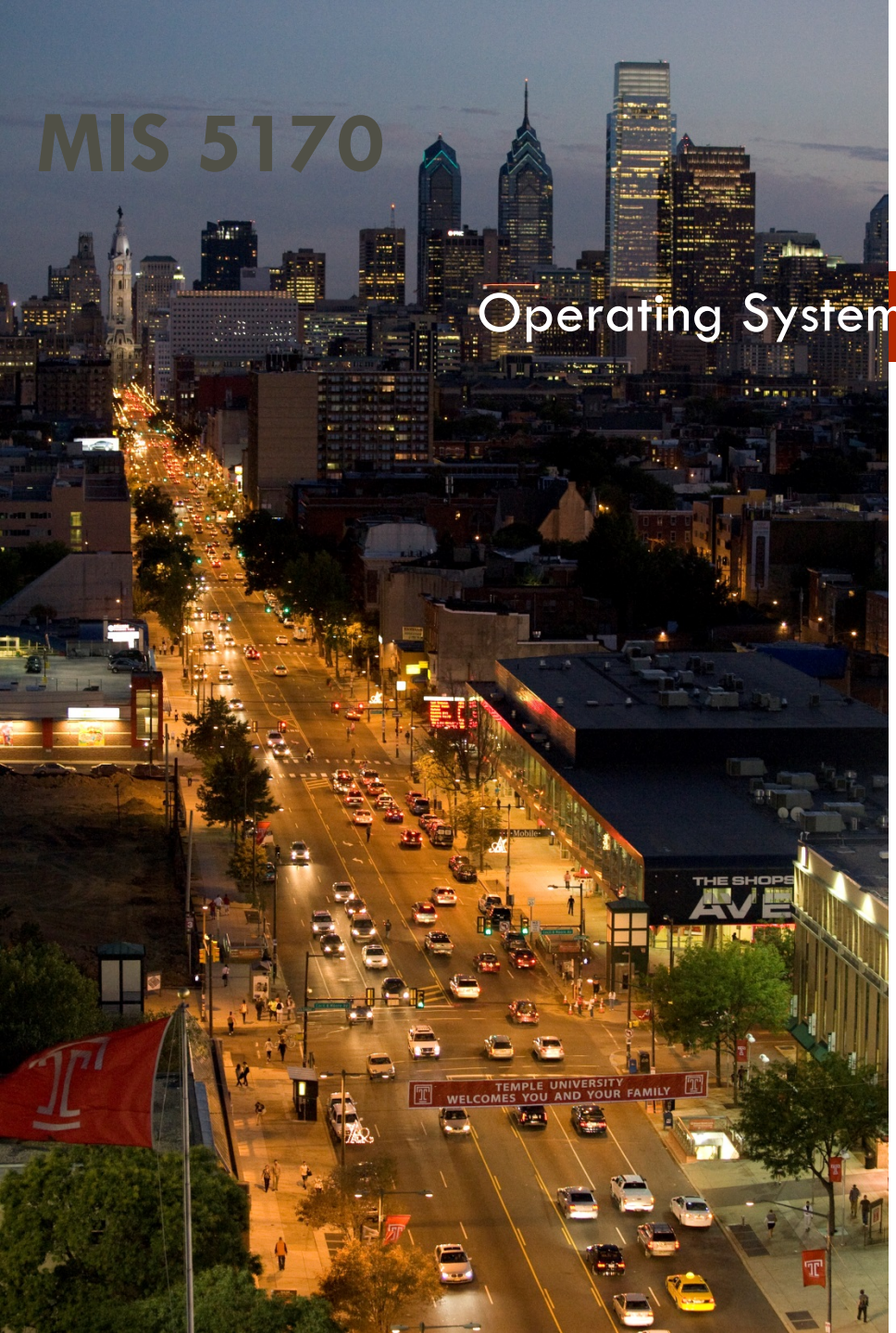


Operating System Security

Week 5

Windows Patching

Fox School of Business
TEMPLE UNIVERSITY

Tonight's Plan

- Questions from Last Week
- Review on-line posts
- In The News
- Patching
- Vulnerability Scanning and Remediation
- Setup of Switches
- Free Group Working Sessions
- Assignment 2 Review
- Next Week
- Quiz

Questions From Last Week

- 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.

Questions From Last Week (cont)

- Any additional questions about the Quiz?

Review On-Line Posts

- Top Posts
  - "Hackers Can Now Steal Data Even From Faraday Cage Air-Gapped Computers"
    - https://thehackernews.com/2018/02/airgap-computer-hacking.html
      - **Shi Yu Dong**
  - February 2018 Adobe Flash Security Update
    - https://helpx.adobe.com/security/products/flash-player/apsb18-03.html
      - Bllaal Williams

Review On-Line Posts (cont)

- Top Posts (cont)
  - iOS 9 Leaked
    - https://www.technewsworld.com/story/85126.html
      - **Matt Roberts**
  - How to convert a VMWare Virtual Machine to run on Hyper-V using MS Converter Utility and PowerShell
    - https://www.microsoft.com/en-us/download/details.aspx?id=42497
      - **Vince Kelly**

Review On-Line Posts (cont)

- Questions about the posts?

In the News

- **Microsoft Patch Tuesday, February 2018 Edition**
  - Microsoft Outlook; SANS Internet Storm Center
    - https://krebsonsecurity.com/2018/02/microsoft-patch-tuesday-february-2018-edition/
- **Domain Theft Strands Thousands of Web Sites**
  - a Web services conglomerate that operates more than 100,000 business Web sites
    - https://krebsonsecurity.com/2018/02/domain-theft-strands-thousands-of-web-sites/
- SANS Internet Storm Center
  - https://isc.sans.edu/forums/diary/February+2018+Microsoft+and+Adobe+Patch+Tuesday/23341/

In the News (cont)

- Questions or items anyone has found of interest?
  - Key take aways:

PATCH!

Patching

- Patching
  - Native patching tools
    - Windows Update
    - WSUS
    - SCCM
  - Third-party?

Patching (cont)

- Native patching tools
  - Windows Update
    - Windows Update is a service provided by Microsoft that provides updates for the Microsoft Windows operating system and its installed components, including internet Explorer.
  - WSUS
    - WSUS – Windows Server Update Services is a computer program developed by Microsoft that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment.
  - SCCM
    - SCCM - System Center Configuration Manager is a systems management software product developed by Microsoft for managing large groups of computers.

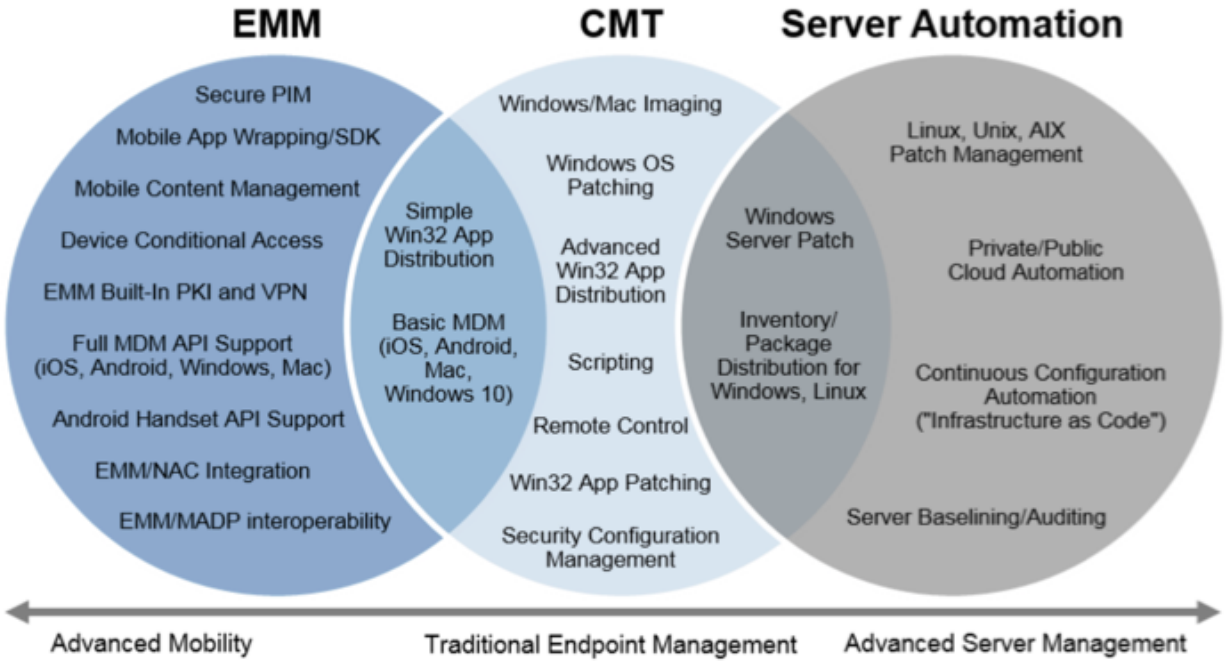
Patching (cont)

- Native patching tools
  - Let us take a closer look at WSUS
    - Demo

Patching (cont)

- Third-Party
  - As per Gartner:

Figure 2. Client Management Tools Provide Basic Mobile and Server Management



Patching (cont)

- Third-Party as per Gartner (https://www.gartner.com/document/3813664?ref=solrAll&refval=198291204&qid=348a2099becda401875ae3bc4bb8cad9)
  - Microsoft
    - SCCM – Not really third-party.
  - IBM
    - BigFix (formerly IBM Endpoint Manager)
  - Tanium
    - Tanium Core Platform, Patch, Comply, Integrity Monitor, Discover

Patching (cont)

- **Microsoft**
  - Microsoft continues to maintain the largest market share in the CMT market by a wide margin. Microsoft's licensing strategy of offering System Center Configuration Manager (Configuration Manager) as a part of the Core and Enterprise Client Access Licenses is the main driving force behind this. Microsoft also continues to enable a robust and growing ecosystem of certified third-party modules and snap-ins, which integrate with the Configuration Manager console, allowing Microsoft to present a more complete set of capabilities in competitive situations. Over the past several months, Microsoft has generated a substantial amount of interest in its Enterprise Mobility Suite (EMS), due, in large part, to its integration with Configuration Manager. Microsoft also plans to release a major new version of Configuration Manager in the fourth quarter of 2015. Configuration Manager is a good choice for organizations with strong client management skills, especially those running predominantly Microsoft software.
- **STRENGTHS**
  - Configuration Manager's scalability has been proven through many large customers.
  - Microsoft has a large ecosystem of software vendors and service providers that support Configuration Manager, due to its large market share.
- **CAUTIONS**
  - Support for non-Windows PCs is weak. Configuration Manager lacks patch content for most non-Microsoft desktop applications. Organizations must patch most non-Microsoft applications through traditional software distribution or third-party patch management tools.
  - Remote control is frequently supplemented by third-party products, as it lacks advanced security and auditing capabilities offered by third-party remote control tools.

Patching (cont)

- **IBM**
  - IBM BigFix (formerly IBM Endpoint Manager) excels in patch management, multiplatform support and overall scalability. Organizations also frequently use it to manage servers, particularly midsize organizations that prefer a single tool to manage PCs and servers. During the past year, IBM has been heavily focused on more deeply integrating its enterprise mobility solution and lightweight PC management platform, MaaS360, with BigFix, and enhancing its cloud-based device management capabilities. BigFix is a good choice for organizations that are heavily focused on security configuration management (including patching), and those that require strong multiplatform server management in addition to client management, or scalability to support tens of thousands of endpoints. It is not as good a choice for organizations that require simple usability or that lack strong management tool resources.
- **STRENGTHS**
  - The product's endpoint-oriented intelligence and control, along with its relay server architecture, results in a relatively small server footprint to support highly distributed environments.
  - IBM BigFix provides comprehensive out-of-the-box configuration policies and templates.
- **CAUTIONS**
  - Uptake of OS deployment (OSD) remains low, and IBM's track record of supporting it at large scale is unproven.
  - IBM's customers frequently express challenges with support. Client feedback suggests that support for non-Windows management functionality is not as strong as support for Windows-management functions.

Patching (cont)

- **Modernize Windows 10 Management Using EMM/UEM**
  - The modern management capabilities in Windows 10 present a paradigm shift for organizations that rely on client management tools to manage PCs. I&O leaders managing Windows PCs should extend the use of EMM tools to manage Windows 10 PCs as they mature into UEM suites.
    - https://www.gartner.com/document/3848468?ref=solrAll&refval=198291204&qid=348a2099becda401875ae3bc4bb8cad9
- Market Guide for Client Management Tools
  - CMTs speed patching and reduce the resources required to deploy and update PCs and Macs. Infrastructure and operations leaders should take into account the long-term client and device management trends, as well as the current market dynamics to select the right tool for their needs.
    - https://www.gartner.com/document/3813664?ref=solrAll&refval=198291204&qid=348a2099becda401875ae3bc4bb8cad9

Patching (cont)

- Questions?

Vulnerability Scanning and Remediation

- Tools
  - Native tools
    - MBSA
    - Microsoft Assessments – Payed tools
  - Third-party
    - Qualys
    - OpenVAS

Vulnerability Scanning and Remediation (cont)

- Native tools
  - MBSA – Microsoft Baseline Security Analyzer is a software tool released by Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows.

Vulnerability Scanning and Remediation (cont)

- Third-Party
  - As per Gartner:
    - Last Year

Vulnerability Scanning and Remediation (cont)

- Third-Party
  - As per Gartner:
    - 2017

Vulnerability Scanning and Remediation (cont)

- **Qualys**
  - Qualys, based in Redwood City, California, is a provider of cloud-based security services and offers DAST-as-a-service capabilities. Like the rest of the Qualys' offerings, its Web Application Scanning (WAS) service offering is completely automated and is integrated with the other Qualys services in its Web-based customer portal. A consistent portal, platform, users/roles and workflow is used for WAS as well as its WAF- and Vulnerability Management-as-a-service capabilities. To access internal applications for testing, Qualys uses a physical or virtual appliance to establish secure VPN connectivity. Because of its low cost, in many cases, enterprises using a more expensive competitive offering for their critical applications will supplement with Qualys' scanning for the rest of their application portfolio. Qualys should be considered by any organization looking for basic, automated Web application security testing as a service at an extremely competitive price.
- **STRENGTHS**
  - Qualys offers one of the lowest costs per application scanned of any of the DAST-as-a-service providers, and its WAS business continues to grow significantly year over year.
  - Qualys DAST scanning also scans for the presence of malware on websites.
  - Qualys has introduced progressive scanning, enabling it to pick up scanning where it left off, useful for large sites where scanning can't complete in a given time window.
  - All subscriptions include 24/7 technical support.
  - Qualys has extensive WAF integration, including its own WAF-as-a-service offering.
- **CAUTIONS**
  - Without human augmentation, there are limits as to the types of vulnerabilities that can be discovered using a fully automated approach. Qualys will refer customers to its partners for additional professional services, including having results reviewed by a human.
  - Although Qualys offers basic Web Services Description Language (WSDL) and SOAP Web services fuzzing, it doesn't support the rest of the WS-* standards, nor does it test RESTful application interfaces or test the content within JSON messages.
  - Qualys has no SAST-as-a-service capabilities and no mobile AST capabilities other than testing the Web-services-based interfaces used by the mobile application.
  - Qualys offers no IAST or RASP capabilities.
  - Qualys provides no out-of-the-box trouble ticketing system integration for WAS vulnerabilities discovered, although this is scheduled for 2015.

Vulnerability Scanning and Remediation (cont)

- Questions?

Switch Setup

- Demo

Switch Setup (Cont)

- Questions?

Group Working Sessions

- Who are the groups?

Next Week

- Questions from previous week
- Malware/Spyware
- Detection tools
- Antivirus
- Sniffers
  - NetMon/Microsoft Message Analyzer
  - WireShark
- Assignment 3 Overview (Due Mar 23rd)

Assignment 2 Review

- Requirements – a presentation style document and video to C-Level team on your choices and justification
  - Build a video of what you did with justification.
  - 8 – 10 page power point on the teams recommendation for the baselines items being implemented
  - Create a Windows Domain Controller a type 2 hypervisor.
  - Create a Windows Desktop box connected to the Domain.
  - Apply 20 settings from your baseline via a Group Policy to the Windows Desktop box.
    - Should pick something from CIS baselines
- Due Date: Feb 21nd 11:59 pm

Quiz

- We can start the Quiz