LESSON: Patch Management

Primer

For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

- Checking with the student to see if they have any questions or need further clarification from any subject from the last class “Endpoint Security”.
- Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
- Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
- For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
- Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
- At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.
- Instructors should manage breaks based on need, considering both timing and duration. You may take a break if you feel the students need it or if a particularly challenging topic has just been covered.
- Remind students to do the discussion post and the weekly checkpoint prior to the next

Summary

In this lesson, learners will grasp the fundamental importance of patch management for maintaining the security and functionality of computer systems, exploring the risks posed by unpatched software, as exemplified by real world incidents like the NHS WannaCry ransomware attack and the Equifax data breach. They will understand the integral role of patch management within comprehensive cybersecurity strategies and how it contributes to reducing vulnerabilities and minimizing the attack surface. Windows Server Update Services (WSUS) is introduced as a central tool for efficiently deploying critical security patches and software updates, with a focus on key components, deployment strategies, and network security maintenance. The lesson will also emphasize the significance of patch approval, deployment, and robust reporting tools provided by WSUS. Additionally, learners will discover the WSUS Offline Update tool's update enhancement capabilities, as well as the role of offline repositories in centralizing software updates and improving network security, especially in organizations with strict security policies and limited internet access. Finally, they will explore the setup, configuration, synchronization, deployment, and maintenance of online and offline repositories for secure and consistent patch management.

Objectives

- Define patch management.
- Illustrate the risks of unpatched software through well-known, real cyberattacks.
- Explain the role of patch management in cybersecurity.
- Recognize Windows Server Update Services (WSUS) as a crucial patch management component.
- Describe Windows Server Update Services (WSUS) components and features
- Identify the different deployment strategies for WSUS.
- Explain the role of WSUS in online patch management.
- Describe how the WSUS Offline Update tool works.
- Summarize the concept and benefits of offline repositories.
- Explain how to set up an offline repository.
- Describe the configuration, synchronization, deployment, and maintenance processes of offline repositories.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
10 min	Questions/Clarifications from last class	● Last Class Highlights ● Address any lingering questions or concerns
5 min	**Lesson Opener:** Patch Management	● Introduce learners to the importance of patch management in cybersecurity.
5 min	**Real World Scenario:** Patch Management	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.

25 min	**Cyber Uncovered:** Introduction to Patch Management	● Begin the lesson by explaining the concept of patch management and its significance in maintaining software updates for computer systems. ● Discuss the various risks associated with unpatched software, including exploitable vulnerabilities, malware and ransomware attacks, and data breaches. ● Provide real world examples, such as the WannaCry ransomware attack on the NHS and the Equifax data breach, to illustrate the consequences of unpatched software vulnerabilities. ● Delve into the specifics of the NHS WannaCry ransomware attack, describing the havoc it caused in terms of locking down critical computer systems, operational chaos in hospitals, and unsecure patient records. ● Explore the Equifax data breach in detail, highlighting the patching oversights, massive data exposure, and the significant reputational and financial repercussions it caused. ● Transition to the role of patch management within a comprehensive cybersecurity strategy, emphasizing its contribution to identifying and mitigating vulnerabilities and reducing the attack surface. ● Explain the concept of a layered defense strategy, pinpointing where patch management fits into this approach. Discuss how it prevents the exploitation of known vulnerabilities and complements other security measures. ● Introduce Windows Server Update Services (WSUS) as a critical component of efficient patch management for organizations. ● Explain its role in providing centralized control over Windows updates. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
10-15 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
20 min	**Cyber Uncovered:** Windows Server Update Services (WSUS)	● Begin the lesson by introducing WSUS (Windows Server Update Services) and its significance in managing software updates for computer systems. ● Cover the key components of WSUS, including the WSUS server, client computers, and update sources, and explain their roles in the update management process. ● Discuss the process of WSUS server synchronization with Microsoft Update to obtain the latest patches and how administrators can approve and deploy these patches to client computers. ● Highlight the detailed reporting tools and monitoring features that WSUS offers, emphasizing their importance in ensuring a secure and up-to-date network.

		● Explore the centralized update management feature of WSUS, explaining how it simplifies the update process for multiple systems from a single server. ● Discuss the concept of customized update approvals and how administrators can approve or decline updates based on their organization's specific needs and requirements. ● Explain the role of reporting and monitoring in WSUS, including the comprehensive reports and monitoring tools that help track update compliance and network health. ● Introduce the different deployment strategies for WSUS, emphasizing the choice between single-server deployment for centralized control and multiple-server deployment for localized control. ● Discuss the benefits and challenges associated with each deployment approach and explain the factors that must be considered when making this decision, such as network size and organizational structure. ● Highlight the importance of WSUS in online patch management, where it serves as the centralized control point for efficiently delivering critical patches and software updates to client computers. ● Describe how administrators employ WSUS for patch approval and deployment, covering aspects like evaluating and approving updates, declining updates to prevent compatibility issues, and deploying updates in stages. ● Explain the concept of granular control in patch management, allowing precise control over the timing and target systems for update deployment while minimizing disruptions. ● Discuss the reporting and monitoring tools within WSUS, focusing on their capabilities to assess the overall health of the system and make informed decisions about update deployment and system security. ● Conclude the lesson by introducing the WSUS Offline Update tool, explaining its purpose in downloading and installing Windows and Office updates on offline computers. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
25 min	**Lab:** WSUS Patch Approval and Deployment	● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. ● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.
5 min	**Pulse Check**	● After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other.

10-15 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.

25 min	**Cyber Uncovered:** Creating an Offline Repository	● Begin the lesson by introducing the concept of an offline repository and its role as a centralized storehouse for software updates and patches, highlighting its significance in maintaining system security without direct internet connectivity.
		● Cover the three essential aspects to consider when creating and managing a WSUS Offline Update repository:
		  ○ Preparation and Initial Download: Guide students through the process of selecting and setting up a dedicated repository machine, downloading the WSUS Offline Update tool and securely transferring initial update files.
		  ○ Configuration and Synchronization: Discuss the configuration and synchronization of offline repositories, emphasizing the importance of targeting specific update versions and languages using the WSUS Offline Update tool.
		  ○ Deployment and Maintenance: Explain how update files are synchronized from an online source to keep the offline repository updated with the latest patches and security updates, and the need for regular maintenance to ensure efficient patch deployment.
		● Dive into the benefits of maintaining an offline repository, such as enhanced network security in environments with limited internet access, greater control over the update process, bandwidth optimization, improved patch management, suitability for organizations with strict security policies, and reduced internet dependency.
		● Create a visual flowchart or diagram for offline repository setup, including steps like selecting and setting up a dedicated repository machine, downloading the WSUS Offline Update tool, and securely transferring initial update files. Encourage students to understand and follow this flowchart.
		● Explain the concept of precise configuration in offline repositories, with a focus on targeting specific update versions and languages using the WSUS Offline Update tool.
		● Discuss the importance of synchronization from an online source, emphasizing the role of consistent synchronization in keeping the repository up to date and prepared for efficient patch deployment, which contributes to network security.
		● Explain the need for periodic synchronizations, documentation, and version control in offline repository deployment and maintenance. Stress the importance of these practices in ensuring a robust and secure offline repository
		● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and

		devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
10-15 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
15 min	**Lesson Closure**	● For this lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. The take-aways discussion should include key concepts such as the importance of patch management in cybersecurity and the risk and impact of unpatch software. Students should review this information prior to moving to the next module. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
N/A	**Additional Time Filler (if needed)**	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation