## LESSON: Introduction to Windows Client

**Before you Begin**

This is the first module in the Microsoft Security Administration course. Please note that there is a Windows Client Installation activity that you will be expected to demonstrate using your own instance of a virtual machine. The students are simply observing your demonstration. The demonstration is not performed using the TDX Arena. This demonstration also provides you with the opportunity to speak at a high level concerning the use of virtual technology. For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed:

* 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.
* Ensure learners are given opportunities for breaks throughout the lesson. The pacing guide below provides recommended breaks. However, there are additional breaks added in the slide deck, please use them if needed.
* 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.

### Summary

In this lesson, learners will gain a thorough understanding of Microsoft Windows operating systems, spanning over 35 years of evolution and their pivotal role in modern cybersecurity. They will understand the distinctions between client and server OSs, navigate user-friendly installations, and harness tools like Event Viewer and Device Manager for effective system analysis, troubleshooting, and hardware management. The lesson will equip learners with essential commands vital for cybersecurity practices and delve into user and group account creation, emphasizing secure access provisioning and permissions assignment. By exploring security applications like BitLocker and UAC, learners will discover techniques to prevent unauthorized access and protect sensitive information. The lesson culminates with an exploration of Windows Security features, including firewall and network protection, empowering learners with practical strategies to mitigate vulnerabilities and uphold client OS security, thus fostering a solid foundation for a successful cybersecurity career.

### Objectives

* Differentiate between a Windows client and server.
* Identify different Windows OS versions.
* Describe the uses of the Control Panel, Windows Firewall, Windows Device Manager, and Windows Event Viewer.
* Explain the use of the CMD to interact with the Windows OS.
* Identify the basic commands used in the CMD.
* Group a set of user characteristics into appropriate user types.
* Compare and contrast user security needs and permissions within a Windows Client environment.
* Differentiate between the different Windows users and groups.
* Identify the CMD commands used for creating or adding users and groups.
* Understand the steps that can be taken to secure the client.
* Apply the CIA triad to cybersecurity design and implementation.
* Identify the different applications within Windows Security.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Introduction to Windows Client | * Introduce learners to the importance of Windows client and the impact it has in Microsoft security administration. |
| 5 min | **Real World Scenario:**  Introduction to Windows Client | * 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. |
| 40 min | **Cyber Uncovered:**  Windows Environment | * Explain the difference between a client operating system and a server operating system. * Discuss how client OSs are used by consumers for daily tasks, while server OSs offer clients various services. * Provide a brief history of Microsoft Windows versions. * Highlight the availability of Windows in both client and server versions. * Discuss the popularity of Windows 10 as the most widely used version. * Discuss the release of Windows 11 and the importance of cybersecurity in newer versions. * Explain the challenges businesses may face when upgrading to a new OS version. * Emphasize the cybersecurity risks associated with using outdated OS versions. * Present the market share statistics for different desktop Windows versions. * Highlight the dominance of Windows 10 and the decreasing usage of Windows 7. * Provide a step-by-step guide for installing Windows, including downloading the ISO file and following the installation procedure. * Emphasize the importance of hardware requirements and user setup during the installation process. * **Note: Demonstrate** the installation process using your local virtual machine. The installation process is lengthy so you may want to continue the lesson and return to the installation process from time to time. * 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. |
| 5 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:**  Client Configuration | * Explain the importance of configuring Windows client based on company needs and security requirements. * Emphasize the need to restrict access to certain folders and applications for end users. * Discuss the Control Panel folder and its applications, as well as how they are used for system changes. * Highlight the security risks associated with uneducated users making system changes. * Explain the role of Windows Firewall in controlling system access. * Present the Windows System settings and their differences across versions. * Explain how these settings relate to technical specifications and domain environments. * Introduce the Administrative Tools folder and the applications it contains for conducting administrative operations. * Discuss specific tools like Event Viewer and Local Security Policy and their potential impact. * Explain the purpose of Device Manager in managing hardware components. * Present the functions of Event Viewer and Network Center. * Emphasize the vulnerability of internal parts and the importance of maintaining their integrity. * Highlight the need to prioritize end users' job needs while ensuring efficiency and effectiveness. * 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. |
| 5 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:**  Introduction to the CMD | * Explain the direct interaction with the Windows OS through the CMD. * Emphasize its role in troubleshooting, creating/modifying folders, files, and users. * Discuss the use of CMD for quick and efficient folder/file creation and manipulation. * Present essential commands, such as cd, dir, copy, move, mkdir, and rmdir. * Explain the navigation within CMD using the cd command. * Describe absolute and relative path navigation examples. * Discuss the dir command for listing directories and providing file details. * Explain the displayed information, such as file dates and sizes. * Introduce the help feature in CMD for command information. * Explain the usage of the /? flag to display command descriptions. * Present a step-by-step demonstration of CMD commands in action. * Provide examples like changing directories, creating folders, and verifying content. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class to 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:**  Windows Management Commands | * 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, review the results with the learners. Encourage those in the red zone to attend office hours and/or to reach out to the instructors for assistance. |
| 5 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. |
| 30 min | **Cyber Uncovered:**  Users and Group | * Provide an overview of the importance of user and group management in Windows for maintaining system and network security. * Explain the concept of user privilege sets and the role of groups in collective permission assignments. * Emphasize the significance of creating individual user accounts and unique group accounts for specific teams or roles within the organization. * Describe the process of assigning permissions to group accounts instead of directly to user accounts to streamline management and ensure flexibility. * Highlight the benefits of this approach, such as simplified user transitions and reduced chances of retaining unnecessary or outdated permissions. * Introduce essential Windows groups, such as Administrators, Users, and Guests, detailing their respective access levels and purposes. * Explain the concept of group accounts and their role in sharing network resources, such as files, folders, and applications, among multiple users. * Demonstrate the process of creating and managing group accounts, emphasizing the efficient delegation of rights and permissions within a single group. * Guide learners to locating user and group settings within the Computer Management tool, showcasing its interface and functionalities. * Explain the distinction between local users and groups, highlighting their relevance for individual machines and local network use. * Provide step-by-step instructions for creating local users and groups using both GUI and CMD methods, detailing the advantages of each approach. * Demonstrate the utilization of the net.exe utility for user and group command processing in CMD. * Introduce the "Switch user" option in Windows, enabling one user to replace another while remaining logged into the system. * Describe how to access the "Switch user" option via the Start menu, facilitating seamless user transitions. * 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. |
| 5 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:**  Windows Client Security | * Introduce the concept of the client computer as the frontline for potential security breaches and phishing attacks. * Emphasize the critical role of administrators in mitigating vulnerabilities and safeguarding client systems. * Explain how users pose a significant security risk due to unpredictable actions. * Highlight the administrator's responsibility in implementing preventative measures to enhance client system security. * Detail the two common methods for securing client systems: Utilizing Windows Update for timely patches and implementing regular backups for data restoration. * Introduce the CIA triad model (Confidentiality, Integrity, Availability) as a framework for holistic cybersecurity considerations. * Break down each element of the triad and its relevance to client system security. * Explain how Confidentiality ensures sensitive data remains protected from unauthorized access. * Describe Integrity as maintaining data accuracy and trustworthiness. * Define Availability in the context of data accessibility and server uptime. * Explore BitLocker's role in encrypting drives and files for data protection in case of theft or unauthorized access. * Discuss User Account Control (UAC) as a tool for limiting application execution based on user privileges. * Highlight the evolution of Windows Defender to Windows Security, detailing its applications for virus protection, firewall and network security, application and browser protection, and local device security. * Stress the importance of regularly updating the Windows OS for bug fixes and security enhancements. * Emphasize the significance of periodic system backups to ensure data preservation and recovery in the event of system failure or data damage. * Provide an overview of key security features, such as BitLocker, for full-drive encryption and User Account Control for application execution limitations. * Illustrate the progression of Windows Defender from Windows 7 to Windows 10, with an emphasis on its real-time protection capabilities. * Detail advanced security features, including Exploit Guard for attack prevention, Application Guard for browser-based exploits, and Advanced Threat Protection for behavior-based threat detection. * Explain the benefits of real-time protection, real-time scans, and cloud-delivered protection in safeguarding client systems. * 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 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. Topics to focus on should include the most common activities performed with regards to client OS management. You can also spend a few minutes discussing how patch management and backups can help secure the overall environment. * You will be able to use the data collected in the pulse check to help with the lesson closure. Remind those learners that reported being in the “red zone” to take advantage of office-hours. * Recommend that the learners ensure they submit all of the assignments on-time to ensure the appropriate credit is provided to them. * Recommend that the students read-ahead and come prepared for the next lesson. * Q&A |
|  | **Additional Time Filler (if needed)** | * Kahoot * Discuss interview prep and questioning * Use breakout rooms for additional lab practice * Continue Real World Scenario Conversation |