## LESSON: Security Policies and Authentication

**Before you Begin**

As a reminder, this is the final module that you will review with your students. At the end of the lesson, ensure you set aside a few minutes to allow students to complete the final survey. Ensure that you also remind students to complete all of the assigned tasks to receive proper credit. 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 comprehensive understanding of privileged and non-privileged accounts and how organizations can strike a balance between user access and Windows environment security. They will grasp the significance of password policies in maintaining secure accounts, controlling network and system resource access, and protecting against cyberthreats. By establishing robust password practices, learners will discover how organizations can bolster their security stance and thwart various forms of cyberattacks. The lesson delves into the pivotal role of local security policies in maintaining account security, fortified communication, and overall Windows environment security. Learners will master the art of configuring these policies effectively to enforce strong password regulations, manage user access, secure network communications, and safeguard systems from potential threats. The session also highlights the importance of physical access and system data security while emphasizing the benefits of employing NTLMv2 and Kerberos authentication methods to enhance security and mitigate authentication-related risks. By understanding the Kerberos authentication process and the role of the Key Distribution Center, learners will grasp how this method ensures secure user authentication and access control. Lastly, learners will explore strategies for mitigating risks related to PtT attacks through regular system updates and patching.

### Objectives

* Explain the difference between privileged and non-privileged accounts in a Windows environment.
* Summarize the importance of password policies in maintaining secure accounts and controlling access to network and system resources.
* Describe the effect of local security policies on account functionality and communication in a Windows environment.
* Explain the importance of security maintenance in reducing the attack surface of a system.
* Differentiate between physical access security and system data security.
* Describe the purpose of NTLM authentication.
* Explain the concept of pass-the-hash (PtH) attacks and their potential impact on NTLM.
* Explain the purpose of Kerberos authentication and identify its components, including KDC, TGT, and TGS.
* Describe the process of Kerberos authentication and how it is used in a Windows domain environment.
* Identify the risks associated with pass-the-ticket (PtT) attacks and their potential impact on Kerberos authentication.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Security Policies and Authentication | * Introduce learners to the importance of Security Policies and Authentication in Microsoft Security. |
| 5 min | **Real World Scenario:**  Security Policies and Authentication | * 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. |
| 20 min | **Cyber Uncovered:**  Account Security Policies | * Explain the distinction between privileged and non-privileged accounts based on access levels and permissions in a Windows environment. * Emphasize that privileged accounts possess elevated privileges for critical system operations, while non-privileged accounts have restricted permissions for regular tasks. * Introduce Administrator accounts, Service accounts, and Domain Admin accounts as examples of privileged accounts. * Detail the extensive administrative access and control these accounts hold over the system, applications, and network resources. * Highlight the significance of proper management and security practices for these accounts to mitigate potential security risks. * Explain the process of disabling administrator accounts using both Active Directory Users and Computers in a domain environment and Edit Local Users and Groups in a local environment. * Describe the importance of using privileged accounts instead of administrator accounts. * Emphasize the need to grant privileged account access to authorized users only. * Explain how privileged accounts are added to the Administrators or Domain Admins group. * Present the advantages of non-privileged accounts, such as reduced attack surface, adherence to the principle of least privilege (PoLP), and implementation of a defense-in-depth strategy. * Describe how the segregation of administrative functions and everyday tasks enhances overall security posture. * Stress the importance of careful management and monitoring of privileged accounts due to their potential impact on security. * Introduce best practices like strong password policies, multi-factor authentication, privileged account activity monitoring, and regular privilege access reviews. * Highlight the critical role of password policies in maintaining secure accounts and controlling access to resources. * Explain how password policies enforce strong and unique passwords to reduce unauthorized access risks and deter attackers. * Discuss how password policies link user actions to individual accounts, aligning with the principle of least privilege. * Differentiate password requirements for domain environments and independent stations, emphasizing security needs. * Clarify the connection between password policies and compliance with industry regulations like GDPR and HIPAA. * Stress the educational aspect of password policies in promoting secure practices and user awareness. * Suggest additional security measures like multi-factor authentication and password managers to enhance policy effectiveness. * Define the account lockout policy and its purpose in defending against brute-force attacks. * Explain how the policy determines the number of login attempts before an account is locked and optional time limits. * Detail the significance of frequent account lockouts as indicators of suspicious or malicious activity. * Emphasize how organizations can analyze account lockout events to identify and respond to potential security incidents. * Mention industry regulations like PCI DSS and SOX that require account lockout policies. * Highlight how implementing such policies demonstrates proactive data protection and regulatory compliance. |
| 20 min | **Lab:**  User Password Policies | * 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 | **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:**  Local Security Policies | * Explain the significance of local security policies in controlling access, privileges, and security settings on a Windows system. * Introduce the key aspects that local security policies govern, including password requirements, account lockouts, and user permissions. * Describe how local security policies dictate password attributes like length, complexity, and expiration. * Explain how policies control the number of failed login attempts before an account is locked out to prevent unauthorized access. * Discuss how local security policies help administrators configure privileges and permissions for user accounts. * Emphasize the importance of assigning appropriate access levels based on roles and responsibilities. * Present the security options offered by local security policies to enhance the overall security of the Windows OS. * Outline settings related to password storage, user authentication, interactive logon, and device security. * Introduce software restriction policies as a form of local security policy controlling application execution on Windows systems. * Explain how these policies permit or restrict the launch of specific applications based on various criteria. * Highlight the need for careful configuration of local security policies to strike a balance between strong security and user usability. * Discuss the potential issues of overly restrictive or weak policies and their impact on system functionality. * Explain that organizations should establish local security policies aligned with their unique security needs, industry standards, and best practices. * Provide a detailed guide for configuring local security policies. * Stress the importance of testing policies after configuration to ensure they function as intended. * Emphasize the importance of monitoring user behavior, network activity, and system access to validate policy effectiveness. * Clarify that local security policies only apply to individual systems, while Group Policy Objects (GPOs) can affect multiple systems in a domain environment. * Warn against incorrect policy configurations that could impact system functionality or security. * Stress the need for periodic review and the updating of local security policies to adapt to changing security requirements and emerging threats. * Introduce other important policies, such as renaming the administrator account and not displaying the last username. * Emphasize their roles in enhancing system security. * Be prepared to discuss the implications 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. |
| 20 min | **Lab:**  Handling Local Security Policies | * 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 | **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:**  Additional Security Measures | * Define security maintenance as the ongoing process of monitoring and addressing security issues that could jeopardize an organization's safety. * Highlight key areas of security maintenance, including service management, user management, and software updates. * Explain the significance of disabling or uninstalling unused services to prevent potential security threats. * Discuss the risk of unauthorized or hijacked services and how they can compromise system integrity. * Emphasize the importance of disabling or deleting inactive user accounts to reduce the attack surface. * Explain how maintaining user accounts can minimize potential vulnerabilities. * Stress the importance of installing Microsoft's latest service packs, hot fixes, and updates to address known security vulnerabilities. * Highlight how timely updates contribute to a more secure system. * Explain the concept of an attack surface and how reducing it is vital for minimizing vulnerabilities. * Explain how security maintenance directly contributes to reducing the attack surface and enhancing system security. * Describe strategies for reducing the attack surface, including applying security patches, vulnerability assessments, secure configuration practices, monitoring, and user education. * Present physical access security as a strategy to protect physical assets and infrastructure. * Explain the purpose of implementing measures like locked doors, access control systems, and barriers to prevent unauthorized access. * Emphasize the goals of physical access security, such as preventing theft, vandalism, and unauthorized entry. * Explain how physical security measures contribute to overall organizational safety. * Detail the importance of protecting BIOS access with a password to prevent unauthorized changes. * Explain the necessity of disabling automatic administrative logon to the recovery console for enhanced security. * Describe the significance of preventing unauthorized booting from external media to safeguard against potential threats. * Define system data security and its focus on preserving the confidentiality, integrity, and availability of digital information. * Highlight security measures such as user authentication, data encryption, firewalls, intrusion detection systems, secure protocols, and regular backups. * Explain EFS (Encryption File System) and BitLocker Drive Encryption as methods for safeguarding data at the file and drive levels. * Emphasize the importance of choosing appropriate encryption techniques based on security needs. * Discuss the importance of planning and managing shared resources on the network with proper access permissions. * Highlight the risks of poorly managed shared resources and how they can lead to data exposure. * Be prepared to discuss the implications 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. |
| 20 min | **Lab:**  Audit Policies | * 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. |
| 20 min | **Cyber Uncovered:**  New Technology LAN Manager (NTLM) Authentication | * Begin the lesson by explaining that NTLM (NT LAN Manager) authentication is a legacy authentication protocol used in Windows operating systems. Its purpose is to authenticate users and establish a secure connection between a client and server in a Windows domain environment. * Emphasize that while NTLM has been widely used in the past, it has limitations and security vulnerabilities compared to more modern authentication protocols like NTLMv2 and Kerberos. * Present the key purposes of NTLM authentication, highlighting its importance in user authentication, enabling single sign-on, providing security through encryption, and ensuring compatibility with older systems. * Introduce NTLMv2 as an enhanced version of the NTLM authentication protocol used in Windows operating systems. * Explain that NTLMv2 was introduced to address security vulnerabilities and provide stronger authentication mechanisms. * Present the key purposes of NTLMv2 authentication, focusing on enhanced security features, protection against pass-the-hash attacks, extended authentication options, improved compatibility, and compliance with security standards. * Discuss each purpose in detail, explaining how NTLMv2 incorporates stronger security measures, prevents pass-the-hash attacks, supports additional authentication methods, maintains compatibility with legacy systems, and adheres to security standards. * Explain how PtH attacks involve gaining access to the hash representation of a user's password stored on a compromised system and using the stolen hash to authenticate and gain unauthorized access to other systems or resources within the network. * Highlight the weaknesses of NTLM hashes, the reusability of stolen password hashes, and the lack of mutual authentication as key factors contributing to the risks associated with PtH attacks. * Present various strategies and security measures to mitigate PtH attacks and enhance NTLM authentication security. * Discuss implementing stronger authentication protocols like Kerberos, enforcing complex and unique passwords, implementing multi-factor authentication (MFA), regularly patching and updating systems, monitoring and detecting suspicious activities, and educating users about the risks of credential theft. * Be prepared to discuss the implications 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:**  Kerberos Authentication | * Explain that Kerberos authentication is a network authentication protocol used to securely authenticate users, verify their identities, and control access to network resources. * Highlight the importance of strong authentication and protection against security threats in network environments. * Introduce the Key Distribution Center (KDC) as a central component alongside the authentication server (AS) and the ticket granting server (TGS). * Explain the Ticket Granting Ticket (TGT) and its role in user authentication. * Describe the Ticket Granting Service (TGS) and its responsibility in issuing service tickets. * Present the steps of Kerberos authentication: Authentication, ticket request, service ticket issuance, and service access. * Emphasize the secure and efficient nature of Kerberos authentication in network environments. * Introduce pass-the-ticket (PtT) attacks and their connection to Kerberos authentication. * Explain that PtT attacks involve the theft and misuse of Kerberos tickets. * Highlight the risks and impact of PtT attacks, including unauthorized access, lateral movement, and prolonged access. * Discuss mitigation strategies to strengthen Kerberos authentication security. * Mention the importance of regular patching and updates, strong security practices, monitoring network traffic, and implementing multi-factor authentication. * Emphasize the need to review and revoke unnecessary privileges and tickets. * Be prepared to discuss the implications 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. Review with the students how security policies and auditing can be used to protect the endpoints and users as well as having the ability to review security events for later analysis. * 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 |
| 5 min | **End-of-Course Survey** | * Allocate 5 minutes to facilitate the completion of the End-of-Course Survey. * Encourage learners to provide honest and constructive feedback about their learning experience. |
|  | **Additional Time Filler (if needed)** | * Kahoot * Discuss interview prep and questioning * Use breakout rooms for additional lab practice * Continue Real World Scenario Conversation |