Lab #3 – Secure Configuration & Management

Outcomes

CIS Controls:

- CIS Control 4: Secure Configuration of Enterprise Assets and Software
- CIS Control 5: Account Management
- CIS Control 6: Access Control Management
- CIS Control 15: Service Provider Management

IT&C Learning Outcomes:

1. History & Context
4. Practicum
6. Security for Technical and Non-technical Personnel

Students will be able to:

- Identify best practices in setup of enterprise assets and software configurations
- Explain how the above-mentioned best management practices contribute to minimizing organizational and operational risk
- Identify best practices in account setup and management in a Windows system environment, as well as best practices that are general to all environments (Windows, Mac, Linux, other)
- Identify general procedures in securing a Windows AD environment, as well as implementing a basic Domain Controller.

Background

With the abundance of technology used in businesses today, the first line of defense is using technology that is configured properly. Now, saying that is much easier than implementing it 100%. Mitigating risk earlier on is always preferable to making it up down the road, and is typically more costly, in terms of time, money or other resources.

Secure configuration requires an understanding of how to configure the technology you are working on to begin with. Often the best documentation of how to configure technology will include where and when to make security minded decisions. Having a perspective on where those junctions occur is what we are striving for in this lab. Typically, the earlier you can implement security decisions into the configuration of your services, the better.

Although we cannot teach you how to configure everything securely in one lab, the principles included and discussed are applicable across many mediums. Look to trusted online resources, such as the ones listed under the References for additional training.

It is **highly recommended** that you read the sections of the CIS controls document found in learning suite, pages 28- 36, 57-59 of the PDF. (17-25, 46-48 of the actual document)

Activity

To submit: Give **2-5** sentences of well thought out responses.

1. **Windows Authentication**
    a. Explore Windows and Windows Authentication methods through the following TryHackMe Rooms. Complete both rooms and include screenshots of 100% completion in your writeup.
        i. https://tryhackme.com/room/windowsfundamentals3xzx
        (NOTE: on Task 8: Bitlocker, the Microsoft docs don't have the exact phrase it's looking for. Try putting "USB" at the beginning of your answer.)

        ii. https://tryhackme.com/room/bypassinguac

2. **Security Controls**

a) Write a definition and implementation example of how Role-Based Access Control follows the principle of Least Privilege

Role-Based Access Control (RBAC) is a security mechanism that restricts system access to authorized users based on their roles within an organization. Each role is assigned specific permissions that define what actions the user can perform. This ensures that users only have the access necessary to perform their job function (**Principle of Least Privilege (PoLP)**, which states that individuals should have the minimum level of access necessary to complete their tasks.)

Implementation Example: In a company using a cloud infrastructure, the following roles can be defined:

- **Administrator:** Has full control over all resources.
- **Developer:** Can deploy and manage applications but cannot modify network configurations.
- **Auditor:** Has read-only access to logs and configurations for monitoring purposes.

b) Remember the generic types of security controls we discussed in the Cyber Intro Lecture? Using the two guides below, identify three examples of where they introduce security controls and identify the type of control it is (try to identify at least 2 different types). Now suggest a new security control in a type that you didn't already identify for one of the two services below.
   a. https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-22-04
   b. https://www.digitalocean.com/community/tutorials/how-to-install-suricata-on-ubuntu-20-04

Administrative Controls: Policies, procedures, and training.

Technical (Logical) Controls: Software and hardware mechanisms like firewalls, encryption, and authentication.

New control:
Physical Controls**:** Security mechanisms like locks, surveillance, and access badges.

c) Imagine you are a manager of a security team within a small company. Your company uses LastPass as a password management solution. Given its recent events, your CISO wants to hear whether should continue with that service. Please write descriptive enough that this could be sent in an email to the CISO.
   a. Research and present two reasons for and against
      i. This website is a good place to start, but look for more sources of information: https://www.tomsguide.com/computing/password-managers/millions-stolen-from-lastpass-users-in-massive-hack-attack-what-you-need-to-know

b. If your recommendation is to replace it, provide an alternative solution with pros/cons for that new service

Dear Manager,

In light of recent developments concerning LastPass, I have conducted an analysis to determine whether we should continue utilizing their services. Below are the findings, including arguments both for and against maintaining our current subscription.

Arguments in Favor of Continuing with LastPass:
Established Reputation and Feature Set: LastPass has been a prominent player in the password management industry, offering a comprehensive suite of features such as password generation, secure storage, and cross-platform synchronization. These tools have historically enhanced our organization's security posture and user convenience.

Arguments Against Continuing with LastPass:

Security Breaches and Data Compromise: In 2022, LastPass experienced significant security breaches where unauthorized parties accessed and exfiltrated sensitive data, including customer vault backups. This led to subsequent attacks, with reports indicating that hackers utilized the stolen data to misappropriate funds from users' cryptocurrency accounts.

Alternative Solution: Bitwarden

Considering the above points, it may be good to explore alternative password management solutions. One such option is Bitwarden.

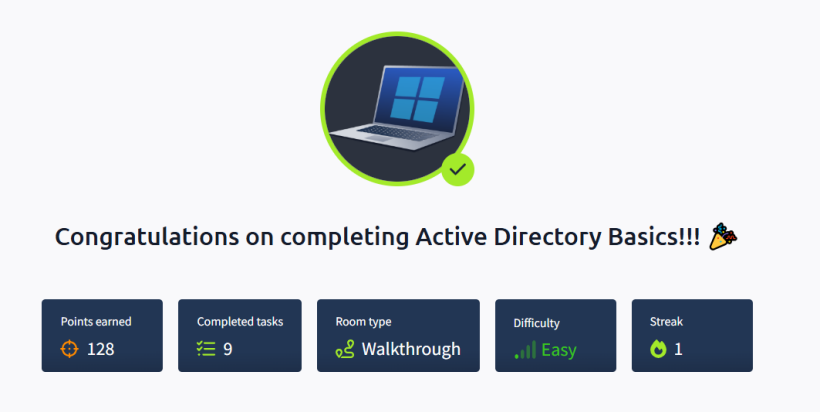
Pros of Bitwarden:

- **Open-Source Transparency:** Bitwarden's open-source nature allows for community scrutiny, ensuring that vulnerabilities can be identified and addressed promptly.
- **Robust Security Features:** It offers end-to-end encryption, zero-knowledge architecture, and supports multi-factor authentication, aligning with industry best practices.

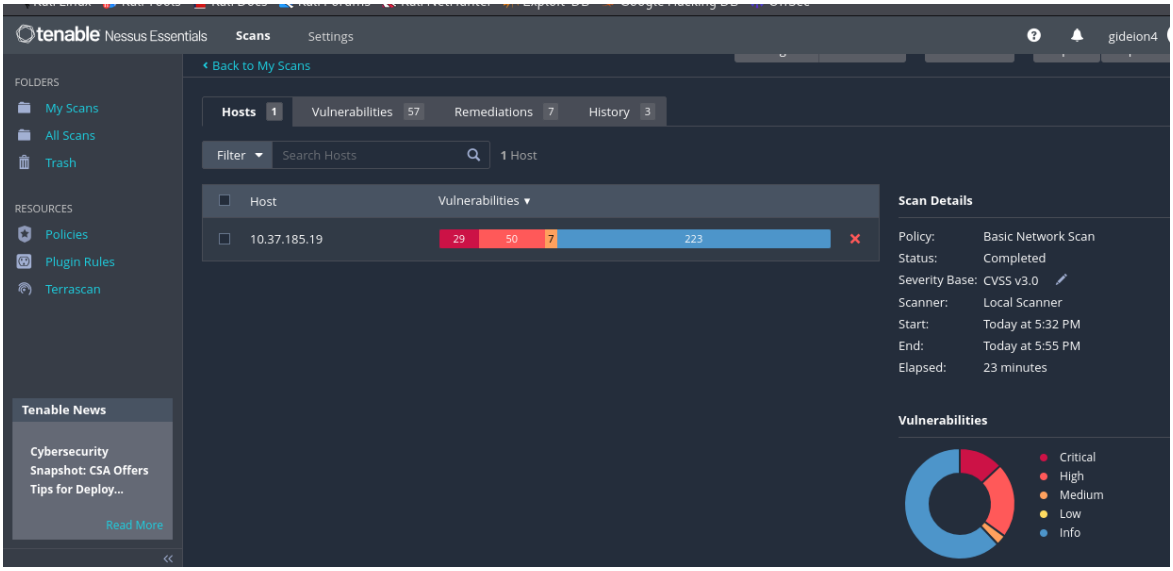
Cons of Bitwarden:

- **User Interface Learning Curve:** Some users may find Bitwarden's interface less intuitive compared to LastPass, potentially requiring additional training and adaptation time.

3. **Active Directory/Group Policy**
    a. Active Directory Preparation: Complete the room below and submit screenshot of 100% completion.
        i. https://tryhackme.com/room/winadbasics



b. Active Directory/Group Policy Activity:
    i. The Active Directory Domain Controller is already set up for you, but it is not configured well and lacks many features that make it secure. Login to your Windows Server 2022 machine with the default credentials Administrator/Password#2!
c. Perform the following baseline security measures
    i. Create a Nessus scanner
        1. Register for a Nessus Activation Code at https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true
        2. Download, extract, and install Nessus on a separate Linux VM in the same network as the Domain Controller you just created (https://www.tenable.com/downloads/nessus)
        3. Run a "Basic Network Scan" against your Domain Controller. Take a screenshot of the results.



a. Make sure you enter your credentials into the "Credentials" tab when configuring your Nessus scan. If

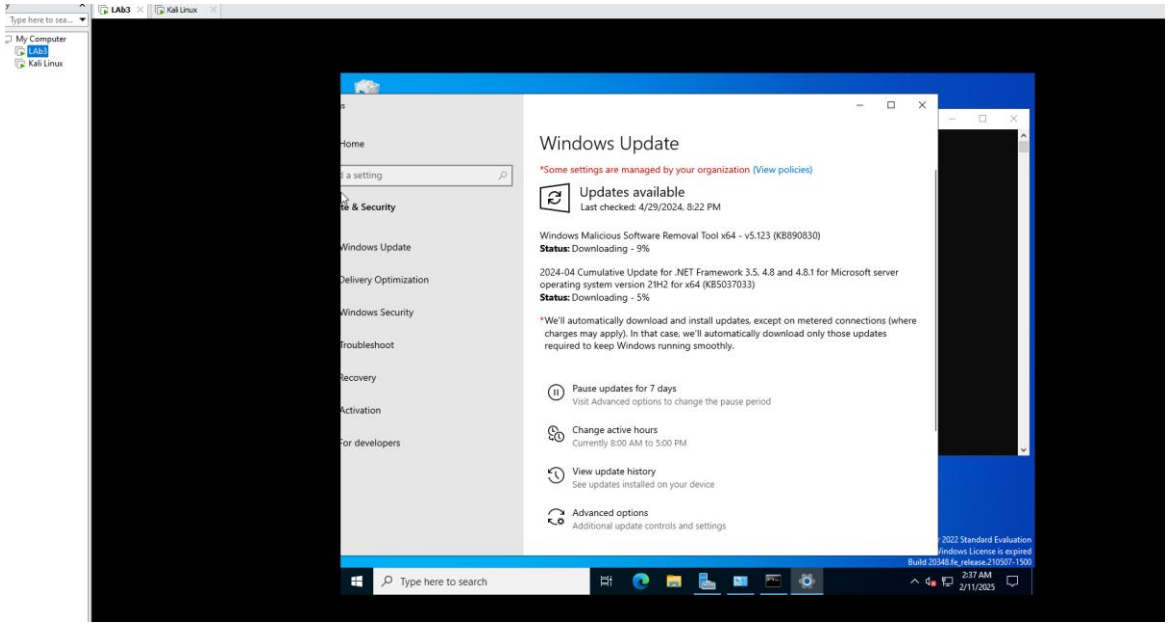
you do not do this, no critical issues will be found and you will not receive full credit for this scan.

i. Authentication Method: Password
ii. Username: Administrator
iii. Password: Password#2!
iv. Domain: ITC366LAB3FUN

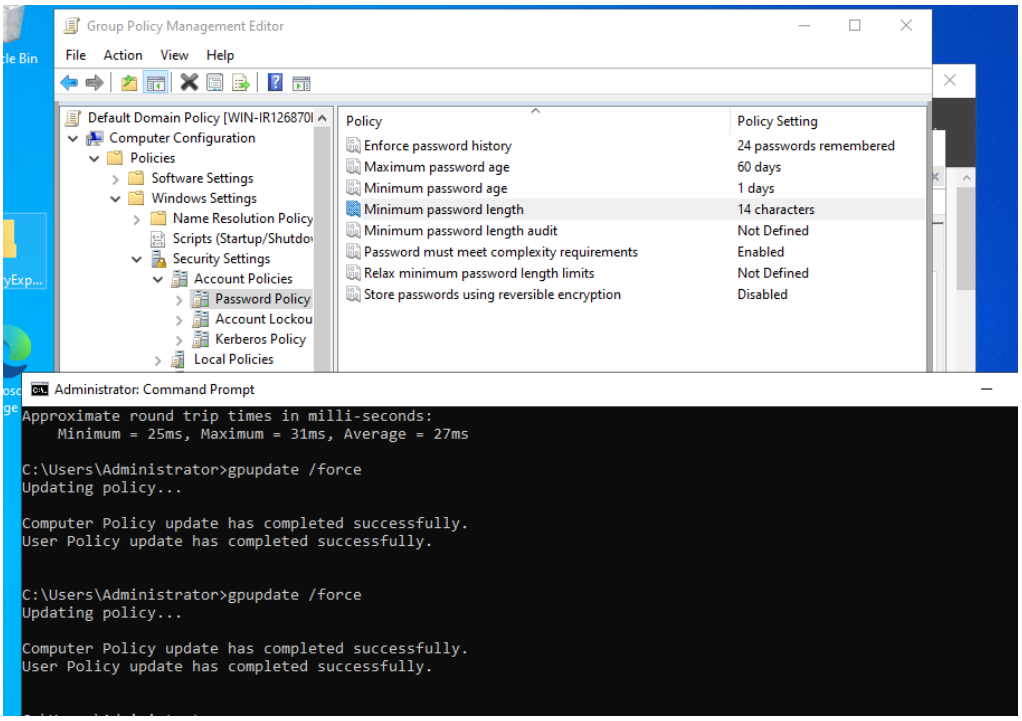
b. Make sure you are scanning all ports and not only common ports

ii. Harden the Domain Controller (provide a screenshot for each of these steps)

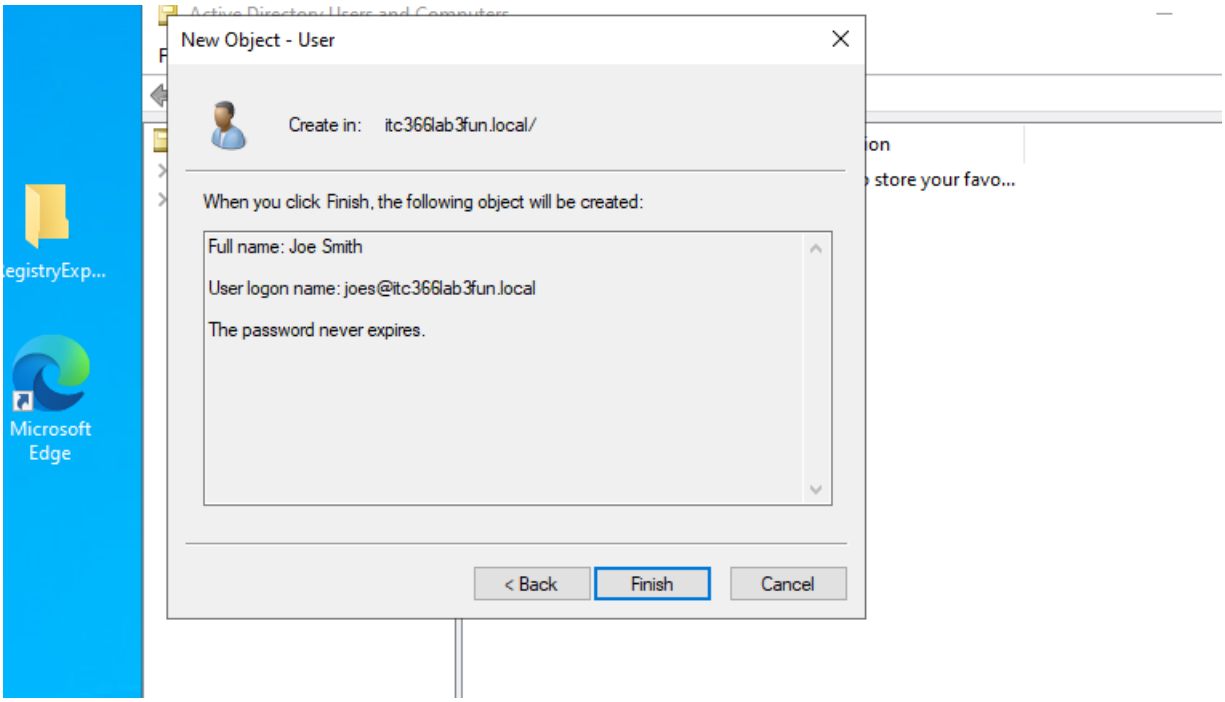
1. Perform windows Updates (make sure the Domain Controller can access the Internet using NAT on the host machine)

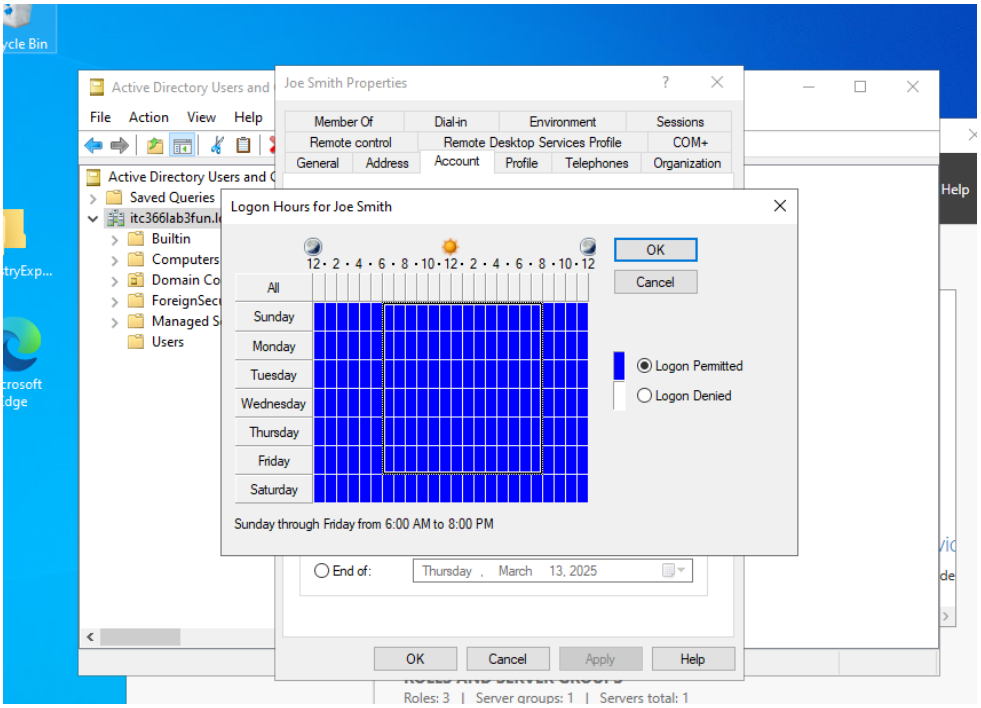


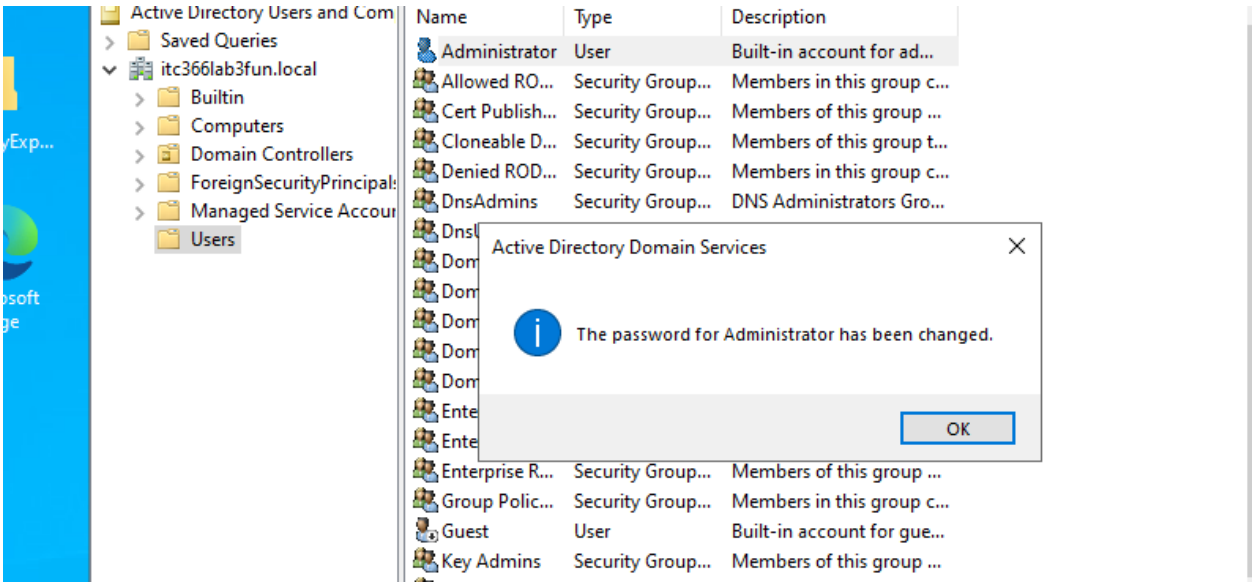
2. Set up a password policy using Group Policy Objects
   a. https://activedirectorypro.com/how-to-configure-a-domain-password-policy/



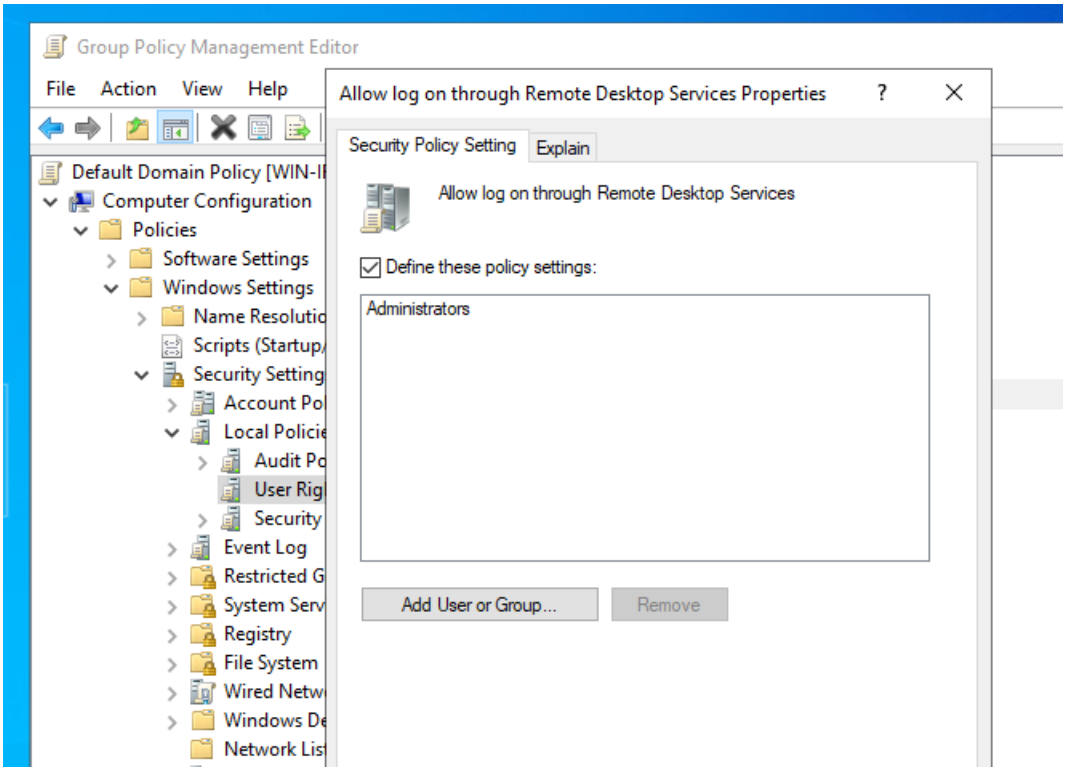
3. Correctly configure users
    a. Create an Active Directory account (not an admin)
    b. Set a secure password
    c. Limit the hours this user can login (access control)
    d. Change the Admin password to something more secure

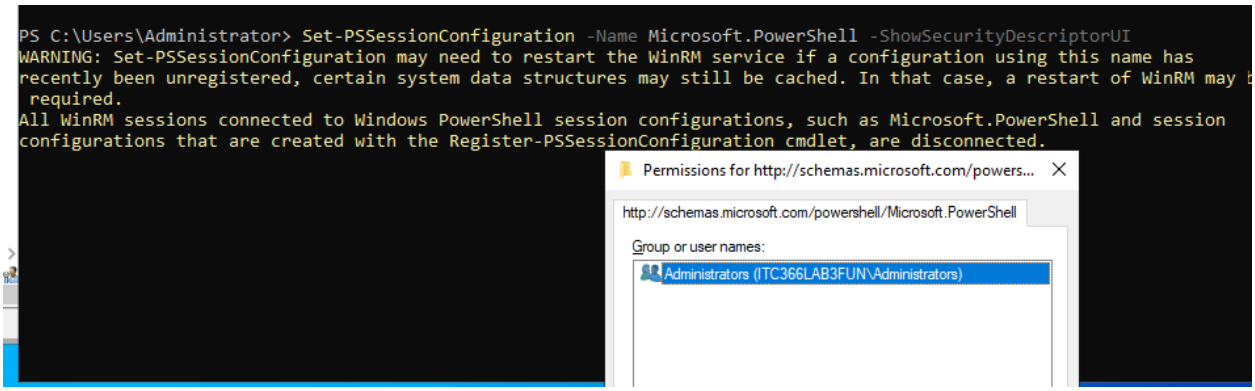




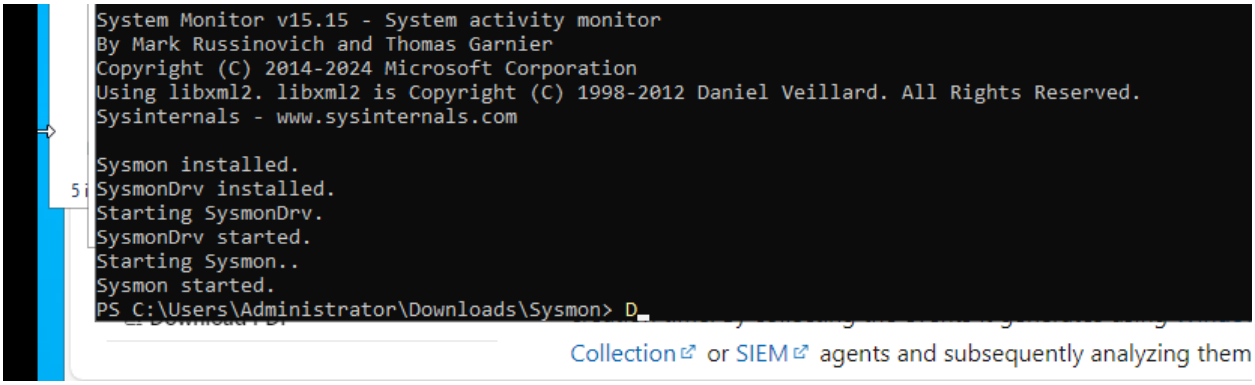


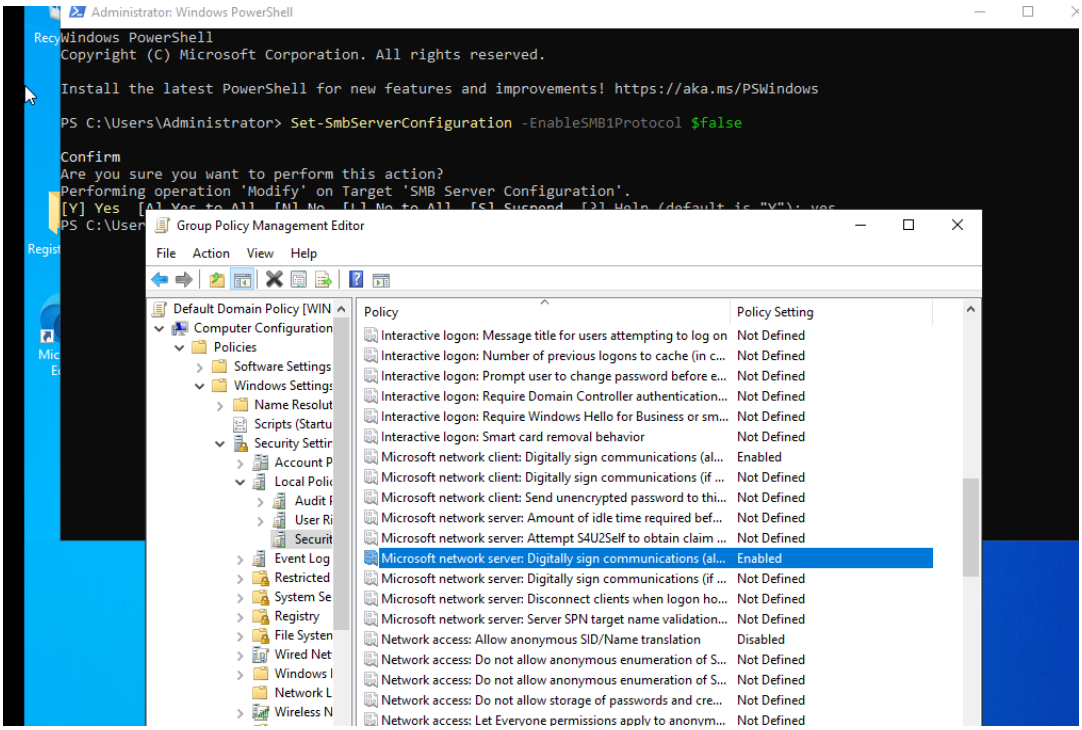
4. Limit RDP and PowerShell to Admins only (you'll need to look this up online to determine the procedures to use)

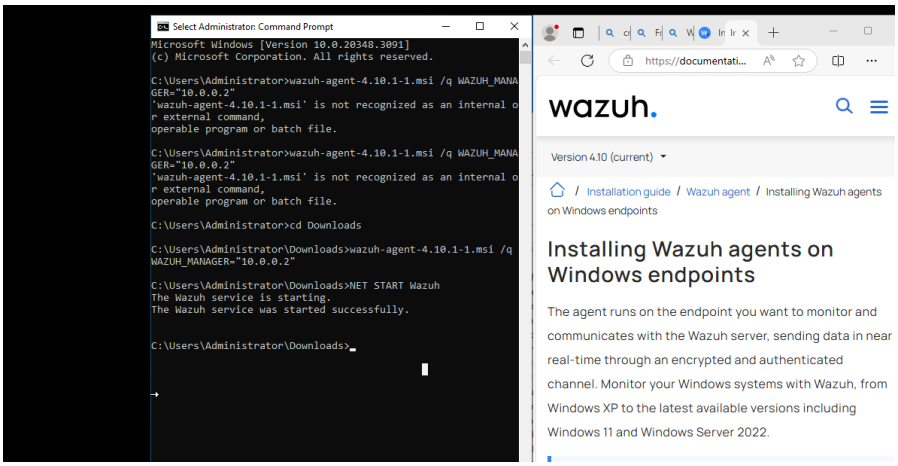




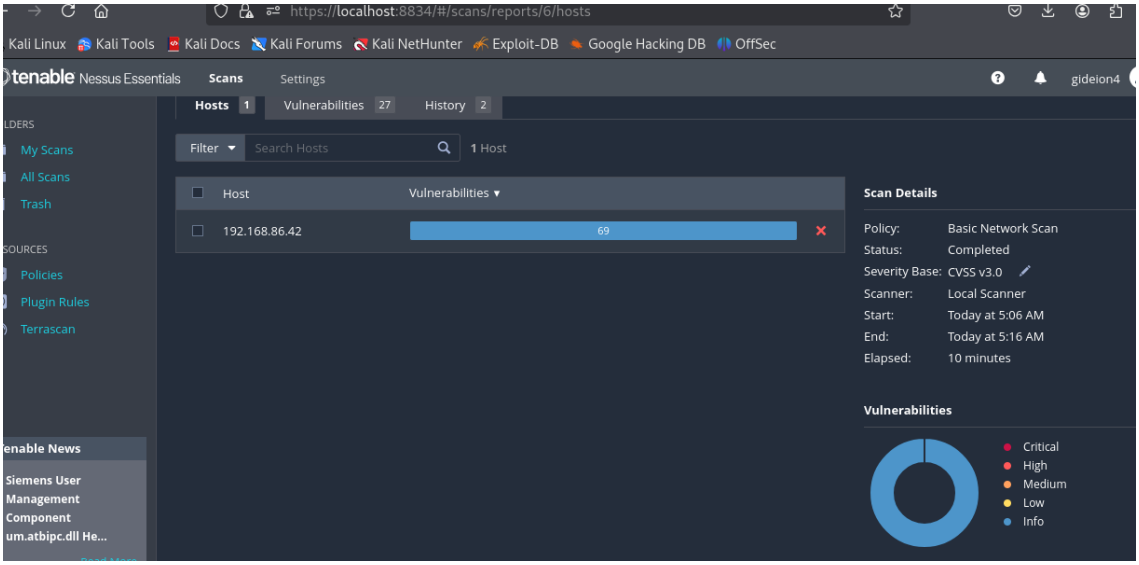
5. There are lots of other things you *should* do to secure a Windows server but are outside the scope of this lab, below are just a few examples
    a. Install Sysmon
    b. Configure the host-based firewall to allow only what is strictly needed
    c. Securely configure SMB
    d. Install an EDR solution


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
PS C:\Users\Administrator\Downloads\Sysmon> D
Collection or SIEM agents and subsequently analyzing them


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Administrator> Set-SmbServerConfiguration -EnableSMB1Protocol $false
Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes
Group Policy Management Editor
File Action View Help
Default Domain Policy [WIN
Computer Configuration
Policies
Software Settings
Windows Settings
Policy
Policy Setting
Interactive logon: Message title for users attempting to log on Not Defined
Interactive logon: Number of previous logons to cache (in c... Not Defined
Interactive logon: Prompt user to change password before e... Not Defined
Interactive logon: Require Domain Controller authentication... Not Defined
Interactive logon: Require Windows Hello for Business or sm... Not Defined
Interactive logon: Smart card removal behavior Not Defined
Microsoft network client: Digitally sign communications (al... Enabled
Microsoft network client: Digitally sign communications (if ... Not Defined
Microsoft network client: Send unencrypted password to thi... Not Defined
Microsoft network server: Amount of idle time required bef... Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim ... Not Defined
Microsoft network server: Digitally sign communications (al... Enabled
Microsoft network server: Digitally sign communications (if ... Not Defined
Microsoft network server: Disconnect clients when logon ho... Not Defined
Microsoft network server: Server SPN target name validation... Not Defined
Network access: Allow anonymous SID/Name translation Disabled
Network access: Do not allow anonymous enumeration of S... Not Defined
Network access: Do not allow anonymous enumeration of S... Not Defined
Network access: Do not allow storage of passwords and cre... Not Defined
Network access: Let Everyone permissions apply to anonym... Not Defined


Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.3091]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>wazuh-agent-4.10.1-1.msi /q WAZUH_MANAGER="10.0.0.2"
'wazuh-agent-4.10.1-1.msi' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>wazuh-agent-4.10.1-1.msi /q WAZUH_MANAGER="10.0.0.2"
'wazuh-agent-4.10.1-1.msi' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>cd Downloads
C:\Users\Administrator\Downloads>wazuh-agent-4.10.1-1.msi /q WAZUH_MANAGER="10.0.0.2"
C:\Users\Administrator\Downloads>NET START Wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.
C:\Users\Administrator\Downloads>
wazuh.
Version 4.10 (current)
Installation guide / Wazuh agent / Installing Wazuh agents on Windows endpoints
Installing Wazuh agents on Windows endpoints
The agent runs on the endpoint you want to monitor and communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel. Monitor your Windows systems with Wazuh, from Windows XP to the latest available versions including Windows 11 and Windows Server 2022.

iii. Run the “Basic Network Scan” again and compare the results with your first scan, take a screenshot



4. **Windows Registry**
   a. A huge part of the Windows structure is the Windows Registry. Please complete the room below and submit a screenshot of 100% completion.
      i. https://tryhackme.com/r/room/windowsforensics1

aboabu

   b. Now, time for some real fun. I would recommend using the application Registry Explorer that is already on the Desktop for this part. Answer the following questions about your machine (hint: paying attention to the TryHackMe room should make this easy).
      i. What is the “EditionID” of your machine?

- Core

      ii. What is the “ComputerName” of the machine?

- GIDZZZ

   c. In your writeup, answer the following questions:
      i. How do registry keys in the Windows Registry relate to security?

The Windows Registry is like a big database that stores important settings and options for the operating system and programs. Some of these settings control how security features work, like user permissions, startup programs, and how the system responds to security threats. If someone can change the wrong registry keys, they could disable security tools, hide malicious software, or give themselves more access than they should have.

ii. Research a few registry keys that a hacker may manipulate.
    1. What is the name of one of the keys of interest to a hacker?

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

    2. Why would a hacker be interested in that key? What would the hacker accomplish by compromising that key?

This key controls which programs start automatically when the computer turns on. A hacker might add their malicious program to this key, so it runs every time the computer starts. This helps the malware stay active on the system without the user noticing, even after a reboot.

5. **Additional Questions**
    1. Why are regular updates important for device security, but particularly for new OS installs?

Regular updates fix security holes that hackers could use to break into your system. When you install a new operating system, it might not have all the latest security patches, making it easier for attackers to exploit known weaknesses. Updates also improve system performance and fix bugs that could cause crashes or other issues.

    2. What basic risk does UAC aim to address?

User Account Control (UAC) helps prevent unauthorized changes to your computer. It stops programs from making changes without your permission, which can protect you from malware that tries to install itself or change system settings without you knowing.

    3. What are the two methods for network authentication on a Windows domain, and why is one of them preferred? (Hint, THM room)

The two methods are NTLM and Kerberos. Kerberos is preferred because it's more secure and efficient. It uses tickets to verify identity instead of constantly sending passwords over the network, which reduces the risk of someone stealing login information.

    4. Share one lesson learned in detail (6-10 sentences) about your experience with Active directory and GPOs. Address how different actions may minimize or increase risk in an environment

One important thing I learned about Active Directory and Group Policy Objects (GPOs) is how powerful they are for controlling user access and system settings across a network. For example, using GPOs, you can force password policies, limit what software users can install, or even lock down desktops to prevent unauthorized changes. This reduces the risk

of users accidentally downloading malware or changing important settings. However, if GPOs are misconfigured, they can open up security holes. For instance, if permissions are too loose, users might gain access to sensitive data they shouldn't see. On the other hand, being too strict could lock users out of necessary tools, causing frustration and work delays. Balancing security with usability is key to managing risks effectively.

Resources

- Additional TryHackMe rooms
  - https://tryhackme.com/room/windowsfundamentals1xbx
  - https://tryhackme.com/room/windowsfundamentals2x0x
- Security Compliance Toolkit
  - https://charbelnemnom.com/microsoft-security-compliance-toolkit/
  - https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10
  - https://www.microsoft.com/en-pk/download/details.aspx?id=55319
- Security Baselines
  - https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines?source=recommendations
- Windows Server Download
  - https://portal.azure.com/#view/Microsoft_Azure_Education/EducationMenuBlade/~/software
- Windows Active Directory
  - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
  - https://rootdse.org/posts/active-directory-lab-setup-forest/
  - https://www.virtualgyanis.com/post/step-by-step-how-to-install-and-configure-domain-controller-on-windows-server-2019
  - https://macrosec.tech/index.php/2021/07/19/building-a-basic-active-directory-lab/
  - https://robertscocca.medium.com/building-an-active-directory-lab-82170dd73fb4
  - https://blog.spookysec.net/ad-lab-1/
- Password Policy
  - https://activedirectorypro.com/how-to-configure-a-domain-password-policy/
- Windows Server Secure Setup Guides
  - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
  - https://petri.com/active-directory-security-5-steps-to-secure-ad/
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf
  - https://www.techtarget.com/searchwindowsserver/tip/Windows-Server-security-hardening-guide-for-admins
  - https://www.upguard.com/blog/the-windows-server-hardening-checklist
- Nessus
  - https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true
  - https://www.tenable.com/downloads/nessus
- Sysmon
  - https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
  - https://syedhasan010.medium.com/sysmon-how-to-setup-configure-and-analyze-the-system-monitors-events-930e9add78d