**IT 204: LAB 1**

**WINDOWS SECURITY CONFIGURATION**

**DR. MICHAEL J. SIMKO**

Table of Contents

[Objectives 2](#_Toc106624002)

[Duration 3](#_Toc106624003)

[Setup 3](#_Toc106624004)

[Logging into the VLABs Environment 3](#_Toc106624005)

[Deliverables 5](#_Toc106624006)

[Expectations 5](#_Toc106624007)

[Credentials 5](#_Toc106624008)

[WINDOWS SERVER SECURITY CONFIGURATION (SERVER HARDENING) 6](#_Toc106624009)

[Validate Network Settings 6](#_Toc106624010)

[Validate System Date and Time 8](#_Toc106624011)

[Validate Update & Patching Settings 9](#_Toc106624012)

[Audit Network Sharing 9](#_Toc106624013)

[Audit Scheduled Tasks 11](#_Toc106624014)

[Audit tasks in Task Manager 12](#_Toc106624015)

[Review Programs & Features 13](#_Toc106624016)

[PowerShell Method 13](#_Toc106624017)

[Graphical User Interface Method 14](#_Toc106624018)

[Audit Groups & Users 15](#_Toc106624019)

[Modifying User Account Control Settings 15](#_Toc106624020)

[Review Services 16](#_Toc106624021)

[Review Disk Management 17](#_Toc106624022)

[Audit Windows Firewall 18](#_Toc106624023)

[Command Prompt Method 18](#_Toc106624024)

[PowerShell Method 21](#_Toc106624025)

[Graphical User Interface Method 21](#_Toc106624026)

[EternalBlue 23](#_Toc106624027)

[Exercise 23](#_Toc106624028)

# **Objectives**

* Defend Servers from attack using technical, administrative and physical control measures.
* Integrate secure network configuration best practices to ensure a diverse layered defense.
* Enforce basic Windows Server Hardening techniques.
* Utilize both PowerShell and Graphical User Interfaces to audit, validate & review Windows Server settings.

# **Duration**

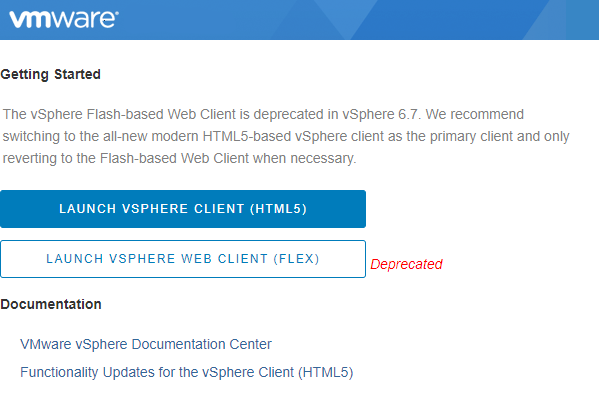
This lab will take approximately an hour and a half. It may require additional time if you run into issues and must troubleshoot. This lab is meant to provide you basic hardening techniques. There is not nearly enough time in the course to cover all hardening techniques.

# **Setup**

* 1 Microsoft Windows Server 2012 VM
* 1 Kali Linux VM.

## **Logging into the VLABs Environment**

1. Type in the URL: https://vlabs.walshcollege.edu/
2. You will receive a notification like so:



1. Click Launch VShpere Client (HTML5)

Next, you will be prompted for your Walsh User Name and Password.

Graphical user interface, application

Description automatically generated

1. In User name **ENTER** **academic\yourusername**, **ENTER** **your password** in Password, and click **Login**

When logged in, you will be brought to the main vmware vSphere Web Client screen.

By default, hosts and clusters  is normally selected.

1. Select **VMs and Templates**. 

You should now see the IT204 folder.

1. Expand the folder to view your personal folder and access your student VMs.
2. Find your **SRVR2012 VM**, right click it and select **Power on** to turn it on.

# **Deliverables**

* All deliverables should be submitted in Moodle as Microsoft Word Documents.
* Format: FirstnameLastname.docx with **ALL COMPLETED STEPS** including full screen captures and 2-3 sentences explaining what was accomplished within each step.

# **Expectations**

Example of a screen shot:

Graphical user interface

Description automatically generated

Example Narrative below screen shot:

This is a screenshot depicting the date and time I captured activity on my VM. The date and time should be visible in each screenshot with each task performed. This ensures screen shots of completed tasks were not taken from Google, YouTube or elsewhere. I will know for certain the lab was completed by you within the allotted time frame.

# **Credentials**

SERVER 2012 VM

* Username: IT204
* Password: Password12345$

KALI LINUX

* Username: root
* Password: toor

# **WINDOWS SERVER SECURITY CONFIGURATION (SERVER HARDENING)**

## **Validate Network Settings**

1. Right click on the Network Icon  located in the bottom right corner of the screen and select **Open Network and Sharing Center**.

Graphical user interface, text

Description automatically generated

1. Click on **Change adapter settings** located in the upper left corner of the window.

Graphical user interface

Description automatically generated with medium confidence

1. Right click **Ethernet0** and select **Properties**.

Graphical user interface, text, application, chat or text message

Description automatically generated

1. Scroll down and double click **Internet Protocol Version 4 (TCP/IPv4)**.

Graphical user interface, text, application

Description automatically generated

1. Ensure your network adapter is configured to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.   
   **Note:**   
   This is where you would also validate networking information is correct when using Static IP Addresses or actually assign a static IP.

Graphical user interface

Description automatically generated with medium confidence

1. Click **OK** on the **Internet Protocol Version 4 (TCP/IPv4) Properties**.
2. Click **OK** on the **Ethernet0 Properties**.
3. Close out **Network Connections,** and **Network and Sharing Center**.

## **Validate System Date and Time**

We want to ensure time is always accurate for logging and communication.

Right click the **time and date** located in the bottom right corner of the screen.

1. Click **Adjust date/time** when the menu pops up.

Graphical user interface, text, application

Description automatically generated

1. Click the **Internet Time** tab.

Graphical user interface, text, application

Description automatically generated

1. Click **Change settings…**

Graphical user interface, text, application

Description automatically generated

1. Select **time.nist.gov** and click **OK**.

Graphical user interface, text, application, email

Description automatically generated

Why is validating time important?

## **Validate Update & Patching Settings**

1. Click the **Start** icon in the bottom left corner of the screen.
2. Type **Control Panel** and select the control panel icon.
3. Select and a new window will open with (Check for updates, change settings, view update history, restore hidden updates and installed updates).
4. Click **Check for Updates** so your system can search for any applicable updates. **Note:**   
   You may also modify the frequency and schedules of updates by clicking Change settings. It is usually a best practice to NOT have automatic updates on servers, as updates can break systems.

A picture containing timeline

Description automatically generated

1. Install any necessary updates and reboot as applicable.

Why should you not rely on Automatic Updates?

## **Audit Network Sharing**

1. Click the start Icon and type **Windows PowerShell** in the search bar.
2. Right click on **Windows PowerShell** and left click on **Run as Administrator**.
3. Click **yes**.   
   A window will now open. Let’s check for shared folders.
4. Type **net share** and press **ENTER**.

A picture containing text

Description automatically generated

1. Click **Start** and type **file explorer**.
2. Select the Text

   Description automatically generated with medium confidence icon to open it.

What could potentially happen if folders and files are shared? Hint: Think of the CIA triad (confidentiality, integrity and availability).

Let’s compare and contrast what we discovered in PowerShell.

1. Click on Local Disk (C:)
2. Right click on **Windows** and select **Properties**.

Graphical user interface, application

Description automatically generated

1. Select the **Sharing** tab and notice the network path to this folder.   
   If sharing is enabled for the C Drive or Windows folder; this is bad. Network sharing for system folders should never enabled. If sharing is not enabled on your VM, proceed to the next section (Audit Schedule Tasks), but understand how to disable network sharing.

Graphical user interface, text, application, email

Description automatically generated

1. Let’s fix this. Click on **Advanced Sharing**, which will open up a new window.

Graphical user interface, text, application

Description automatically generated

1. Click on **Permissions** to view who has Full Control, Modify and read access. Uncheck each box and click **OK**.

Graphical user interface

Description automatically generated

1. Now uncheck **Share this Folder** and click **OK**.

Graphical user interface, text, application

Description automatically generated

1. Click **Close** to exit out of the **Windows Properties** Box and repeat this process for any other Shared Folders you believe should not be shared.
2. Go back into your PowerShell terminal and type **net share** and **ENTER**.
3. Ensure the share you disabled no longer shows up in PowerShell.

Note: If you did ever want to enable folder/file sharing you would access the same menu and options pertaining to the specific folder. I understand sometimes this is necessary for organizational requirements, however, double check you are only sharing with those who require a need to know.

## **Audit Scheduled Tasks**

1. Click the Start Icon and type **Windows PowerShell** in the search bar.
2. Right click on **Windows PowerShell** and click on **Run as Administrator**.
3. Click **Yes**. The PS window will open.
4. Type **schtasks** and press **ENTER**.   
   You will receive an output similar to this:

Text, timeline

Description automatically generated

What exactly are you seeing here?

## **Audit tasks in Task Manager**

1. Click the **Start** icon and type **Task Manager**.
2. Click on the Text

   Description automatically generated with medium confidence icon.
3. If your task manager does not have detailed processes, click **More details** to expand the list.



1. Review each of the processes.
2. To kill a process, select it and click **End task**.

I know you are all probably familiar with this function and capability but be sure to check tasks frequently for suspicious activity.

## **Review Programs & Features**

### **PowerShell Method**

1. Click the **Start** icon and type **Windows PowerShell** in the search bar.
2. Right click on **Windows PowerShell** and click on **Run as Administrator**.
3. Click **Yes**.   
   A window will now open.
4. Type **Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\\* and press ENTER.   
   This will generate a list of all 64 bit programs currently installed.**
5. **Review each to ensure nothing is suspicious.   
   You will receive an output similar to this:**

Text

Description automatically generated

1. You can export the list of installed programs to a text file by adding the following after the command above:   
   **| Format-Table –AutoSize > C:\Users\IT204\Desktop\ProgramsPS.txt**   
   and pressing **ENTER**.

**Note: This is the general method to output anything to a text file in PowerShell.**

### **Graphical User Interface Method**

1. **Click Start and type Control Panel.**
2. **Click on the**  **icon.**
3. **Click Programs and Features.**

Graphical user interface, text, application

Description automatically generated

1. **Click on a program to select it (usually a program you want to remove).   
   Note:   
   This is for awareness purposes. You may or may not want to remove any programs within the virtual environment but it is best practice to remove any unnecessary programs the server does not require. I am sure many of you know how to uninstall a program, but when auditing your devices at work; ensure there is no unauthorized software or programs not required for work purposes.**
2. **Click Uninstall/Change to initiate removal of the program.**

## **Audit Groups & Users**

### **Modifying User Account Control Settings**

1. Click **Star**t and type **control panel** in the search bar.
2. Click on Control Panel
3. Click **System and Security**

Graphical user interface, text

Description automatically generated

1. Click **Change User Account Control Settings**.



1. Click on and drag the bar up and down to view different security options specific to user account control.
2. When you are finished reading what each does, drag the bar to **Always notify me when** and click **OK** to complete the change.
3. Now click **User Accounts** on the left side of the same window.

Graphical user interface, text, application

Description automatically generated with medium confidence

1. Select **User Accounts** again.

Diagram

Description automatically generated with low confidence

1. Audit any un-needed accounts or modify user account settings here. There are several other ways to review user accounts as well but for the purpose of this lab; we will just address this method.

## **Review Services**

1. Click the **Start** icon and type **Task Manager**.
2. Click on the Text

   Description automatically generated with low confidence icon.
3. Click on **Task Scheduler (Local)** and scroll to view preconfigured tasks.   
   Do you notice anything odd?

Graphical user interface, text

Description automatically generated

1. Double click the task that appears to be malicious and click **Delete** on the right side of the screen to remove it.
2. When prompted whether or not you want to remove it, click **Yes**.

Graphical user interface, text, application

Description automatically generated

## **Review Disk Management**

1. Click **Start** in the bottom right corner, type Create, **and format hard disk partitions**.
2. Click on the Text

   Description automatically generated icon to open up the **Disk Management** window.   
   You will see a window similar to this:

Graphical user interface, text, application, email

Description automatically generated

This is where you can format additional hard drives or create new partitions. You would want to ensure there are no unauthorized partitions present here that could house malicious content.

## **Audit Windows Firewall**

### **Command Prompt Method**

1. Click the **Start** icon and type **cmd.exe** in the search bar.
2. Right click on **Command Prompt** and click on **Run as Administrator**.

Graphical user interface, application

Description automatically generated

1. Click **yes**.   
   A window will now open.
2. Type **netsh advfirewall show all state** and press **ENTER**.   
   This command will let you know the status of various Firewall Profiles. Typically, you should see each state indicated as ON. If they are not on, you may want to turn them on.

Text

Description automatically generated

1. To turn Firewall Profiles on and off type **netsh advfirewall set allprofiles state on and press ENTER.   
   You can swap allprofiles with the specific profile you want as well. Let’s try it.**
2. **Type netsh advfirewall set domainprofile state off and press ENTER.**
3. **Now turn it back on.**
4. Let’s check out Firewall Rules. Type **netsh advfirewall firewall show rule name= all** and press **ENTER**.   
   You can scroll to view various firewall rules. Note: You can also output to a text file for review as we learned in previous labs.

A picture containing text

Description automatically generated

1. If you want to filter results, you can type:   
   **netsh advfirewall firewall show rule dir=in name= all** and press **ENTER**.   
   In this case we are viewing inbound rules.

Let’s do the same for outbound.

1. Type **netsh advfirewall firewall show rule dir=out name= all** and press **ENTER**.
2. Type **netsh advfirewall firewall add rule name=PingNo dir=in protocol=icmpv4 action=block and press ENTER.   
   This will configure a firewall rule to block any other systems from pinging our host.**

Text

Description automatically generated

1. **To block a specific IP Address, type netsh advfirewall firewall add rule name=NotoKali dir=in interface=any action=block remoteip=<insert your kali host IP here> and press ENTER.**



1. **Now type netsh advfirewall firewall add rule name=NotoKali dir=out interface=any action=block remoteip=<insert your kali host IP here> and press ENTER.**



1. **Log into your Kali VM, and attempt to ping your Microsoft Windows Server 2012 IP Address.**

**Let’s configure logging on our Firewall for dropped connections.**

1. **Type netsh advfirewall set allprofiles logging droppedconnections enable and press ENTER.**



1. **To verify your rules were successfully created, type netsh advfirewall firewall show rule name=PingNo and press ENTER.**
2. **Repeat the same command above to verify your NotoKali firewall rule.**

Text

Description automatically generated

### **PowerShell Method**

1. Type **Set-NetFirewallProfile –Profile Domain,Public,Private –Enabled False** and **ENTER** to turn the Firewall off.
2. To view Firewall state, type **Get-NetFirewallProfile** and press **ENTER**. You should see each profile is set to false.
3. Type the same command with **True** at the end to turn on the firewall.
4. Repeat the command for viewing the current state to verify each profile is now set to true.

### **Graphical User Interface Method**

1. Click **Start**.
2. Type **Windows Firewall with Advanced Security**.
3. Click on the icon when it populates.

A window will open.

1. To enable Firewall profiles, click **Windows Firewall Properties**.

Graphical user interface, text, application, chat or text message

Description automatically generated

You can navigate through Profiles by clicking each tab on the top part of the menu (**Domain Profile, Private Profile, & Public Profile**).

1. Ensure each is set to **On (recommended)** and click **OK** when complete.

Graphical user interface, application

Description automatically generated

1. Click **Inbound Rules** on the left side of the screen to modify existing rules or add new rule(s).

Graphical user interface, text

Description automatically generated

1. Click **Outbound Rules** on the left side of the screen to modify existing rules or add new rules.

Text

Description automatically generated with low confidence

Navigate through existing rules to become familiar with standard configurations.   
When you are finished, close out of the **Windows Firewall with Advanced Security** window.

## **EternalBlue**

The WannaCry Ransomware attack wreaked havoc on many organizations through the duration of the year 2017. This type of ransomware exploits vulnerabilities in SMBv1.

1. Click the start Icon and type **Windows PowerShell** in the search bar.
2. Right click on **Windows PowerShell** and click on **Run as Administrator**.
3. Click **yes**.   
   A window will now open.
4. Type **Get-WindowsFeature FS-SMB1** and press **ENTER**.   
   What results do you get?
5. Type **Get-SMBServerConfiguration** and press **ENTER**.   
   What did you get here?
6. If you discover **SMBv1** is enabled, research methods to disable the service.

What port is associated with SMBv1?

1. Provide a description of the method you used along with a screen shot proving you disabled it.

## **Exercise**

1. Research on your own **two additional methods** for hardening Microsoft Windows Server 2012.
2. Provide screen shots and step-by-step narrative of additional hardening techniques you stumbled upon and implemented during your research.