PRE-COMPETITION:

<https://www.cvedetails.com/vendor/26/Microsoft.html>

Use this link to find out more about the specific windows you are using and what CVE’s it could have. Specify OS and version, then find the build and sort through the CVEs.

START COMPETITION:

**How to remove SMBv1 and replace with SMB2 via PowerShell**

**After doing the top command on the screenshot, replace the 2 with 1 and replace true with false.**

A screenshot of a computer program

AI-generated content may be incorrect.

Windows 8.1, Windows 10, and Windows 11: Add or Remove Programs method:

1. In Control Panel, select Programs and Features.
2. Under Control Panel Home, select Turn Windows features on or off to open the Windows Features box.
3. In the Windows Features box, scroll down the list, clear the check box for SMB 1.0/CIFS File Sharing Support and select OK.

After Windows applies the change, on the confirmation page, select Restart now

Install SimpleWall from Softonix

Disable the telemetry service if it is unnecessary to send data to Microsoft OR find where the telemetry data is.

\*disable\* Services > Connected user experience and telemetry > disable.

\*find\* admin PowerShell > cd back to the C drive > cd ProgramData\Microsoft\Diagnosis\ > then ls what’s in the file > delete anything scary or **cat** any file to view contents.

Disable unused Networking Devices. First check which network adapter you’re using.

PowerShell > Get-NetAdapter > Look at Interface description, that is what you’re using.

Control panel > system and security > system > device manager > network manager > disable the unused network and update network driver that you are using.

Protecting Local DNS

C:\Windows\System32\Drivers\etc\hosts to check your dns. Look in the non # areas and see if anyone changed something.

Mitigating Address Resolution Protocol Attack

PowerShell > arp -a

The table contains MAC addresses in the middle and IP addresses in the left. If the table includes a MAC mapped to two IPs, you are probably susceptible to an ARP poisoning attack.

To clear the ARP cache and prevent the attack, issue the command arp -d.

Safe App Installation

Only allow installation of applications from the Microsoft Store on your computer.

Go to Setting > Select Apps and Features and then select The Microsoft Store only.

AppLocker

Allows users to block specific executables, scripts, and installers from execution through a set of rules.

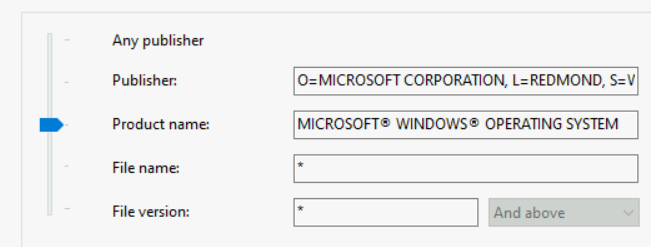
Local group policy editor > windows settings > security settings > application control policies > applocker > configure rule enforcement > check if executable rules is checkbox configured and the dropdown is enforce rules. (if it is not, then some red teamer has privileges).

Click on executable rules and review what is there. If you want to add a new allow/deny rule-

Right click executable rules > create a new rule > go through process of allow or deny who > click the specific file or program you want. \*You can even customize how far you want to protect. Figure 1-1 you can select a specific file or program, figure 1-2 shows you can go back further.\*

A screenshot of a computer program

Description automatically generated1-1

1-2

Check windows defender antivirus scan. Make sure nothing is ! and everything is configured right.

Check virus and & threat protection settings and check exclusions to make sure nothing malicious is excluded.

**BEFORE DOING THE NEXT STEP, CONFIRM IF THERE IS BITLOCKER:** PowerShell 🡪 manage-bde -status 🡪 check protection status (if it says **PROTECTION ON, DO NOT DO OFFLINE SCAN)**

FULL OFFLINE SCAN

Virus & threat protection 🡪 scan options 🡪 offline scan # this will take up to 15 minutes so make sure you don’t have impending injects,

Disable Macros on all Microsoft office-based applications

1. Select the **File** tab and choose **Options**.
2. Select **Trust Center**, and then choose **Trust Center Settings**.
3. In the **Trust Center**, select **Macro Settings**.

4. **Disable all macros with notification**    Macros are disabled, but security alerts appear if there are macros present.

Also check if macros is available from the developer tab. To access developer tab:

On the File tab, choose Options to open the Options dialog box.

Choose Customize Ribbon on the left side of the dialog box.

and then select the Developer check box.

Choose OK.

Splunk search - Identifying Internal hosts and services for lateral movement (Splunk, Sysmon native)

It should be noted that when a host/ port/ service scan is performed from a compromised machine, a single machine makes multiple calls to other hosts in the network to identify live hosts and services. This can be detected using the following query:

sourcetype='firewall\_logs' dest\_ip = 'internal\_subnet' | stats dc(dest\_port) as pcount by src\_ip | where pcount >5

[Analytics | MITRE Cyber Analytics Repository](https://car.mitre.org/analytics/)

Scripts for splunk/zeek or even Sysmon to use.

**Download and use Recuva if there are critical files that are linked to services.**

Using event viewer

TO find “execute a remote command” ID 4104:

Event viewer > applications and service logs > PowerShell > operational > filter for event id 4104

Check properties on actions tab while looking at a specific log to see these

A screenshot of a computer

Description automatically generatedMake sure it’s logging.

[Get-WinEvent (Microsoft.PowerShell.Diagnostics) - PowerShell | Microsoft Learn](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent?view=powershell-7.4&viewFallbackFrom=powershell-7.1)

Using PowerShell to view events

\*Example 9, pipe | Measure-Object at the end of the command to get a count of them all\*

To check for a specific user and their activities such as logging on:

**Get-WinEvent -LogName Security -FilterXPath '\*/EventData/Data[@Name="TargetUserName"]=" "'**

Fill in that second “” with the name.. example would be

**Get-WinEvent -LogName Security -FilterXPath '\*/EventData/Data[@Name="TargetUserName"]="Kenny"'**

To check for activities based on IDs:

**Get-WinEvent -LogName Security -FilterXPath ' \*/System/EventID= '**

Example: **Get-WinEvent -LogName Security -FilterXPath ' \*/System/EventID=4720'**

ID list: (this list can be used for event viewer as well)

4720 – user account was created

4726 – user account was deleted

4722 - user account was enabled

4738 - user account was changed

4724 - An attempt was made to reset an account's password

4798 - A user's local group membership was enumerated

4625 – an account failed to log on

4624 – an account successfully logged on

4648 - A logon was attempted using explicit credentials.

4776 - The computer attempted to validate the credentials

4697 - Attempt to install a service

7045 – New Service installed

4688 - A new process has been created.

4698 - A scheduled task was created.

4699 - A scheduled task was deleted.

4700 - A scheduled task was enabled.

4701 - A scheduled task was disabled.

4702 - A scheduled task was updated.

**400 – PowerShell downgrade attack.**

[Appendix L - Events to Monitor | Microsoft Learn](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor)

Full list of IDs

[www.myeventlog.com](http://www.myeventlog.com)

**can search specific event IDs**

Some events will not be generated by default, and certain features will need to be enabled/configured on the endpoint, such as PowerShell logging. This feature can be enabled via

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell

Local Computer Policy > Computer Configuration > Administrative Templates > System > Audit Process Creation (this one is to generate ID 4688)

TO CYA on all event IDs, do this

In the Group Policy Editor, go to “Computer Configuration” > “Windows Settings” > “Security Settings” > “Advanced Audit Policy Configuration” > “Audit Policies” > have EVERYTHING become success and failure.

[0d42b-windowsloggingcheatsheet\_ver\_oct\_2016.pdf](https://igorsec.blog/wp-content/uploads/2023/08/0d42b-windowsloggingcheatsheet_ver_oct_2016.pdf)

WINDOWS LOGGING CHEAT SHEET - Win 7 thru Win 2012

[SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing](https://github.com/SwiftOnSecurity/sysmon-config)

Using SYSMON the right way

\*Metasploit will use mainly port 4444, sometimes 5555.

To filter if something is coming from Metasploit: use PowerShell

Get-WinEvent -Path <Path to Log> -FilterXPath '\*/System/EventID=3 and \*/EventData/Data[@Name="DestinationPort"] and \*/EventData/Data=4444'

Example:

PS C:\Windows\system32> Get-WinEvent -Path C:\Users\THM-Analyst\Desktop\Scenarios\Practice\Filtering.evtx -FilterXPath '\*/EventData/Data[@Name="DestinationPort"] and \*/EventData/Data=4444'

To detect Mimikatz/LSASS behavior

Get-WinEvent -Path <Path to Log> -FilterXPath '\*/System/EventID=10 and \*/EventData/Data[@Name="TargetImage"] and \*/EventData/Data="C:\Windows\system32\lsass.exe"'

For hunting common back ports to find C2 servers:

Get-WinEvent -Path <Path to Log> -FilterXPath '\*/System/EventID=3 and \*/EventData/Data[@Name="DestinationPort"] and \*/EventData/Data=<Port>'

Detecting evasion:

Get-WinEvent -Path <Path to Log> -FilterXPath '\*/System/EventID=8'

Using SysInternals: download the suite from https://learn.microsoft.com/en-us/sysinternals/downloads/

To find where a file was downloaded, use streams from PowerShell.

A blue screen with white text

Description automatically generated

Then use notepad to display in text form and add the data stream you found.

EX: notepad file.txt:ads.txt.

Use resmon to get more detailed information on what’s running

Use tcpview to get a better version of task manager.

Use whois or Talos intelligence through the browser to the ISP/Organization to the remote IP.

[The Ultimate Guide to Procmon](https://adamtheautomator.com/procmon/)

Use this to filter and find processes.

Handle: This handy command-line utility will show you what files are open by which processes, and much more.

PsLoggedOn: Show users logged on to a system

BgInfo: It automatically displays relevant information about a Windows computer on the desktop's background, such as the computer name, IP address, service pack version, and more.

These two pictures below can help check in depth performance issues. (Task manager will only be brief.)

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.