**NECCDC 2021 – Windows Systems**

**Pace University - BergCyberSec**

**[INITIAL TASKS]**

Things that can be done when disconnected from the internet. This will be done in conjunction with initial manual threat hunting.

Elevate Powershell to administrator level.

Start-Process Powershell -Verb runAs

Powershell Command Stream

Dependent on the Windows DOMAIN CONTROLER. Powershell Module Logging and Script Block Logging both need to be enabled. Powershell must also be listed in the modules.

Computer Configuration > Administrative Templates > Windows Components > Windows Powershell

Module Logging: Enable

Options: Show…

Microsoft.Powershell.\*

PowerShell Script Block Logging: Enable

* Log Script Block Invocation Start / Stop Events

ALL WINDOWS COMPUTERS need to update their group policies in Powershell after the Domain controller changes the previous policies.. But will need to wait for Azure to follow through on pushing the update to each device.

gpupdate

**[POST CONNECTION]**

Tasks that can be done once the network firewall reconnects to the internet.

Installs the Wazuh Agent. Be sure to add the ip address of the wazuh server in both instanced, between ‘ ’

**Wazuh Agent Installation Windows**

Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.0.3-1.msi -OutFile wazuh-agent.msi; ./wazuh-agent.msi /q WAZUH\_MANAGER='wazuh\_server\_ip\_address' WAZUH\_REGISTRATION\_SERVER='wazuh\_server\_ip\_address'

(New-object System.Net.webclient).downloadfile("https://packages.wazuh.com/4.x/windows/wazuh-agent-4.0.3-1.msi","wazuh-agent.msi")

msiexec.exe "./wazuh-agent.msi" /q WAZUH\_MANAGER='192.168.50.26' WAZUH\_REGISTRATION\_SERVER='192.168.50.26'

(New-object System.Net.webclient).downloadfile("https://packages.wazuh.com/4.x/windows/wazuh-agent-4.0.3-1.msi","wazuh-agent.msi"); .\wazuh-agent.msi /q WAZUH\_MANAGER="192.168.50.26" WAZUH\_REGISTRATION\_SERVER="192.168.50.26"