Living-Off-The-Land Lab

Table of contents

List of Figures

List of Tables

1. Lab Objective

- Demonstrate attacks using native Windows tools (PowerShell, WMI).
- Perform file-less execution to bypass antivirus.
- Harvest system credentials safely in a lab environment.

2. Tools

Tool	***Purpose***
PowerShell	Execute fileless attacks in memory
WMI	Enumerate users and harvest credentials
Windows VM	Target system for simulation (IP: 192.168.1.38)

Table 2.1 Shows Tools

3. Lab Execution

Step 1: Fileless PowerShell Execution

Encode a PowerShell command

```
$command = 'Get-Process'
$bytes = [System.Text.Encoding]::Unicode.GetBytes($command)
$encoded = [Convert]::ToBase64String($bytes)
```

Execute encoded command (fileless)

```
powershell.exe -NoProfile -ExecutionPolicy Bypass -EncodedCommand $encoded
```

Observation: Processes listed without creating any files on disk. AV bypassed in lab simulation.

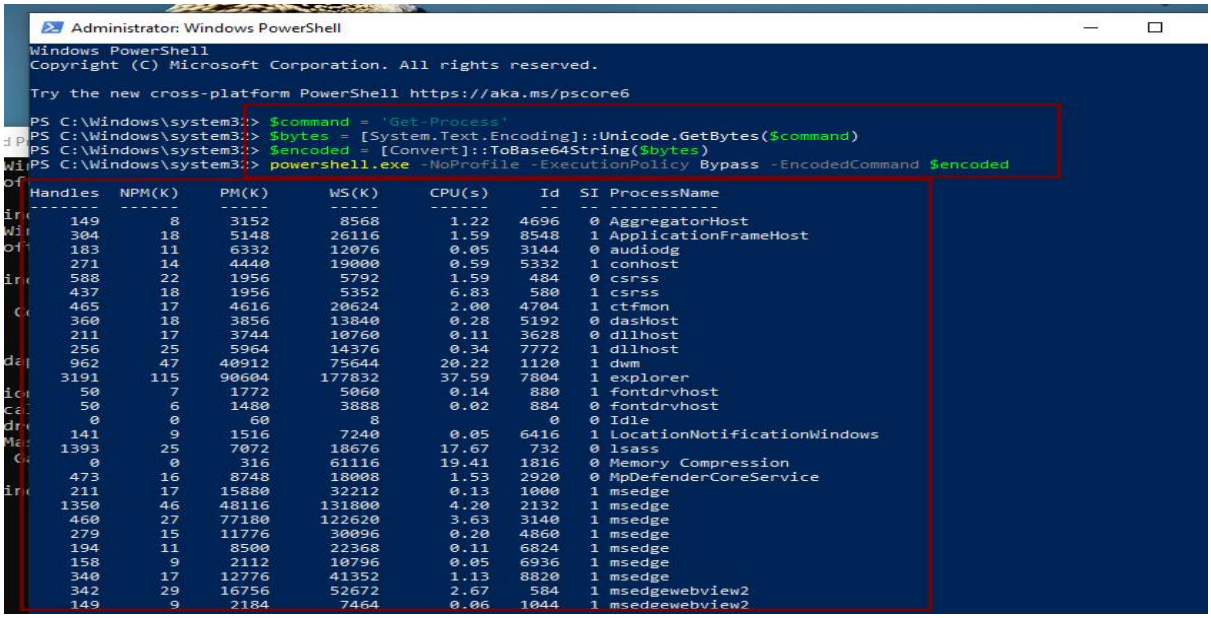

Figure 3.1 Shows AV bypassed and all process listed

Step 2: Credential Harvesting via WMI

List Local Users

Get-WmiObject Win32_UserAccount -Filter "LocalAccount='True'"

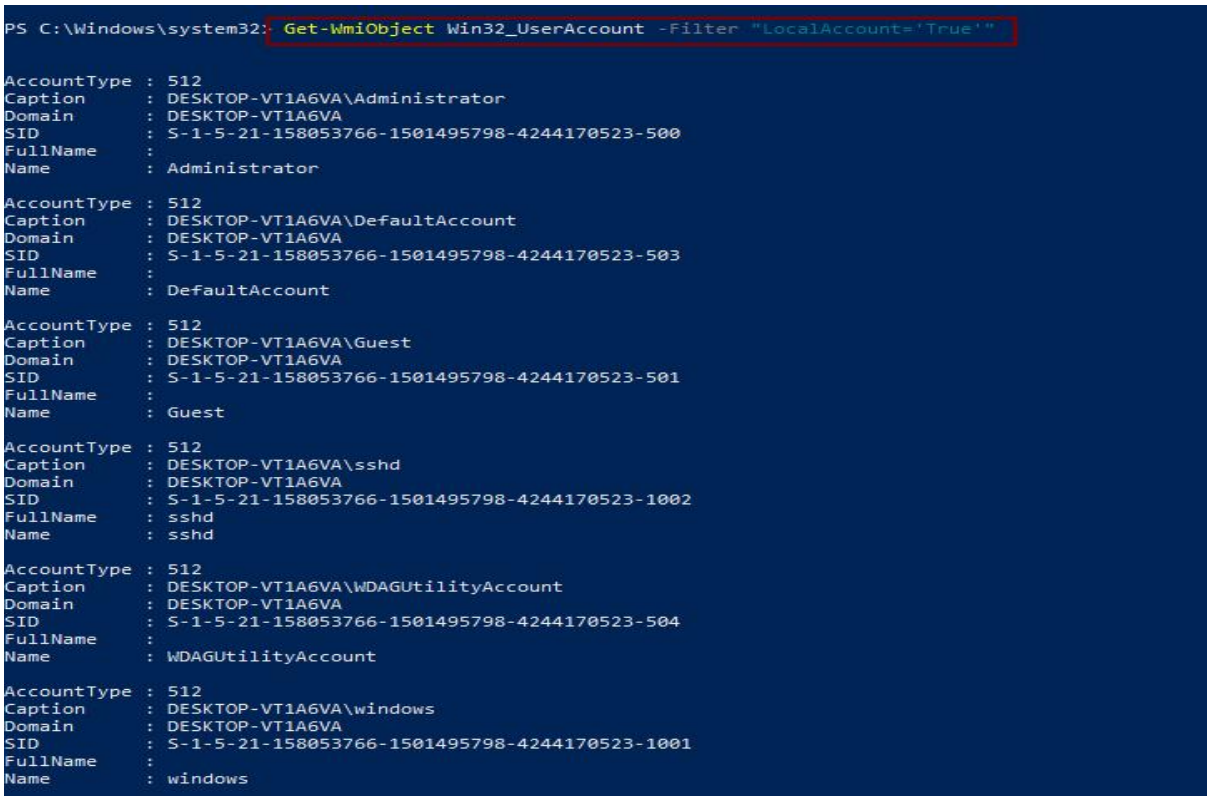

Figure 3.2 Shows all local users on system

Step 3: Show Current Logged-In User

Get-WmiObject -Class Win32_ComputerSystem | Select-Object UserName

```
PS C:\Windows\system32> Get-WmiObject -Class Win32_ComputerSystem | Select-Object UserName

UserName
--------
DESKTOP-VT1A6VA\windows
```

Figure 3.3 Shows current user

Step 4: Simulated Credential Extraction

Get-WmiObject Win32_UserAccount -Filter "LocalAccount='True'" | Select-Object Name,SID | Export-Csv C:\Lab\UserList.csv

Observation: Local user accounts exported safely, simulating credential harvesting.

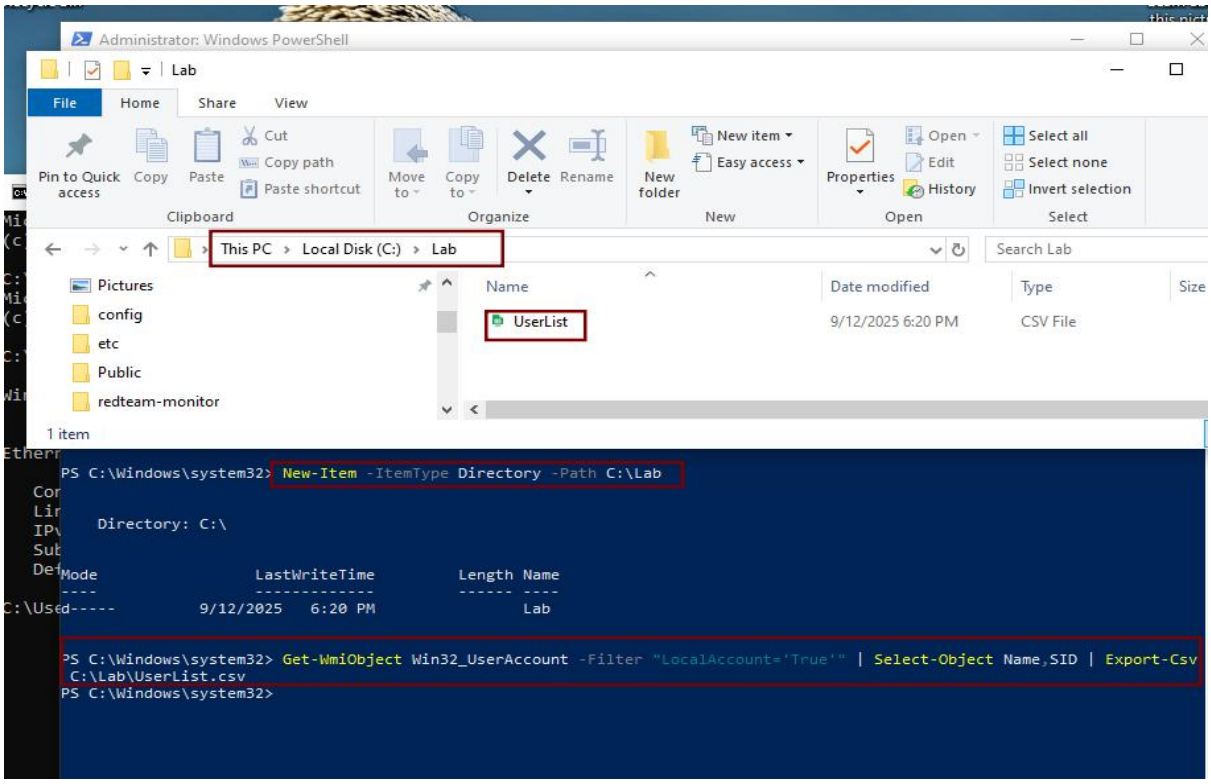

Figure 3.4 Harvesting credentials

Step 5: Cleanup

Remove-Item C:\Lab\UserList.csv

```
PS C:\Windows\system32>
PS C:\Windows\system32> Remove-Item C:\Lab\UserList.csv
PS C:\Windows\system32>
```

Figure 3.5 Shows cleaning up of exported files

4. Lab Logs

Attack ID	*Tool*	*Action*	*Notes*
LID001	PowerShell	Fileless execution	Bypassed AV
LID002	WMI	Credential harvest	Extracted user info (simulated)

Table 4.1 Shows Logs

5. Summary

In the Living-Off-the-Land lab, native Windows tools were leveraged for stealthy attacks. PowerShell enabled file less execution, bypassing antivirus detection, while WMI enumerated and harvested credentials from the system. This demonstrates how attackers can abuse legitimate system tools to perform malicious actions without leaving traces.