Report: Living-Off-The-Land Lab

Objective

Execute attacks using native tools, harvest credentials.
Use PowerShell for fileless execution.
Perform file-less execution to bypass antivirus.

Tool Used:

Powershell, WMI, Windows

Lab Execution

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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> $command = 'Get-Process'
PS C:\WINDOWS\system32> $bytes = [System.Text.Encoding]::Unicode.GetBytes($command)
PS C:\WINDOWS\system32> $encoded = [Convert]::ToBase64String($bytes)
PS C:\WINDOWS\system32> powershell.exe -NoProfile -ExecutionPolicy Bypass -EncodedCommand$encoded
-EncodedCommand$encoded : The term '-EncodedCommand$encoded' is not recognized as the name of a cmdlet, function,
script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
At line:1 char:1
+ -EncodedCommand$encoded
+ ~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (-EncodedCommand$encoded:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\WINDOWS\system32> powershell.exe -NoProfile -ExecutionPolicy Bypass -EncodedCommand $encoded

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    261      17    10016       5236       6.19   4872   0 AdjustService
    182      11     3112       3784       0.91   8160   0 AggregatorHost
    792      52    86416      18400      97.53  12076   1 ApCent
    738      32    69156      28856       2.17  17488   1 ApplicationFrameHost
    164      10     2044       1148       0.02  19948   1 AppVShNotify
    586      19    15992      14464     126.14   3784   0 audiodg
    396      38   242176     193340       7.86   1560   1 chrome
   1136     100   713108     204084   1,179.08   1976   1 chrome
    301      29    53916      28536       4.42   2172   1 chrome
    288      26    42128      44940      46.38   2760   1 chrome
    303      29    65972      66000      18.42   6116   1 chrome
    256      25    20920      48844       0.06   7720   1 chrome
    300      30    70812      52768      34.77   8180   1 chrome
    382      43   245176     254112      89.05   8200   1 chrome
    306      29    59436      59044      16.00   9588   1 chrome
    333      31    54784      77720       5.47  11416   1 chrome
    317      32    61540      61040     420.39  11988   1 chrome
    574      59   291364     262560      54.95  16164   1 chrome
    289      24    20312      20640       0.66  17268   1 chrome
    362      29    55940      76160      12.14  17680   1 chrome
    527      49    39688      57824     159.94  18400   1 chrome
    341      11     2460       2468       0.34  18576   1 chrome
   3147     144   323768     386232   1,164.25  18760   1 chrome
    289      24    22448      19356       0.45  19232   1 chrome
    224      16    11520       8656       3.22  19360   1 chrome
    265      18     9736       7748      11.73  19988   1 chrome
    689      32    64392       6796       1.41  20424   1 chrome
    437      37   270936     344280      10.38  21032   1 chrome
    289      24    19224      14920       0.36  21400   1 chrome
    535      50   290012     315272     133.48  21884   1 chrome
    283      26    39376      27076       2.11  22660   1 chrome
    498      50   297260     337672      33.11  22832   1 chrome
    288      29   156480     192572       2.44  22976   1 chrome
    327      29    39684      61696       9.16  23016   1 chrome
    275      26    36220      30332       5.42  23312   1 chrome
    312      25    35080      34760       0.41  23728   1 chrome
    364      25    40144      91860       0.53  24228   1 chrome
    347      34    61112     140480       1.58  25628   1 chrome
    229      21    15348      34240       0.06  25856   1 chrome
    282      16     3092      22492       0.41  11276   1 conhost
    568      30    59500       4736       0.73   8980   1 CrossDeviceResume
   1281     127    79196      75228     233.56   5944   1 CrossDeviceService
    728      27     2520       2580       3.81    912   0 csrss
   1035      43     4564       2884      66.78   1072   1 csrss
    642      22    10252      14504      18.63  12956   1 ctfmon
    333      20     7836      12676       0.36  20904   1 DataExchangeHost
   1176      54   125352      87512      78.97  14392   1 Discord
    201      13    10800       2552       0.05  15416   1 Discord
    819      47   418024     220168   5,012.78  15520   1 Discord
    389      23    17076      19112      16.34  15540   1 Discord
   1493     123   732264     616728   3,745.63  16420   1 Discord
    283      17    13240       8840       4.11  17024   1 Discord
    224      13     2988       8344       0.11   1368   1 dllhost
    221      12     2792       8488       0.13   7792   1 dllhost
    228      13     2764       8028       0.19  19608   1 dllhost
   2075     103   545652     110020   2,263.23   1800   1 dwm
    584      34    19988       6564       5.02   4880   0 EasyTuneEngineService
   6927     180   389744     270900     507.92   9084   1 explorer
     43      11     4464       4804       0.81   1408   1 fontdrvhost
     43       7     1748        540       0.00   1416   0 fontdrvhost
    799      20    21948      32720     947.92   9644   1 FxSound
    784      29    21260      17380      21.27   7256   0 gamingservices
    301      14    12132       1428       0.08   7248   0 gamingservicesnet
```

Fig 1.1 AV bypassed, and all process listed

Credential Harvesting via WMI

List Local Users.

```
PS C:\WINDOWS\system32> Get-WmiObject Win32_UserAccount -Filter "LocalAccount='True'"


AccountType : 512
Caption     : DESKTOP-4V2J8CB\Administrator
Domain      : DESKTOP-4V2J8CB
SID         : S-1-5-21-3029045385-181532478-1101399575-500
FullName    :
Name        : Administrator

AccountType : 512
Caption     : DESKTOP-4V2J8CB\Ajay Pratap Singh
Domain      : DESKTOP-4V2J8CB
SID         : S-1-5-21-3029045385-181532478-1101399575-1000
FullName    : Ajay Pratap Singh
Name        : Ajay Pratap Singh

AccountType : 512
Caption     : DESKTOP-4V2J8CB\DefaultAccount
Domain      : DESKTOP-4V2J8CB
SID         : S-1-5-21-3029045385-181532478-1101399575-503
FullName    :
Name        : DefaultAccount

AccountType : 512
Caption     : DESKTOP-4V2J8CB\Guest
Domain      : DESKTOP-4V2J8CB
SID         : S-1-5-21-3029045385-181532478-1101399575-501
FullName    :
Name        : Guest

AccountType : 512
Caption     : DESKTOP-4V2J8CB\WDAGUtilityAccount
Domain      : DESKTOP-4V2J8CB
SID         : S-1-5-21-3029045385-181532478-1101399575-504
FullName    :
Name        : WDAGUtilityAccount
```

Fig 1.2 All local users on system

Show current Logged-In User

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

UserName
--------
DESKTOP-4V2J8CB\Ajay Pratap Singh
```

Fig 1.3 Current Users

Simulated Credential Extraction.

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

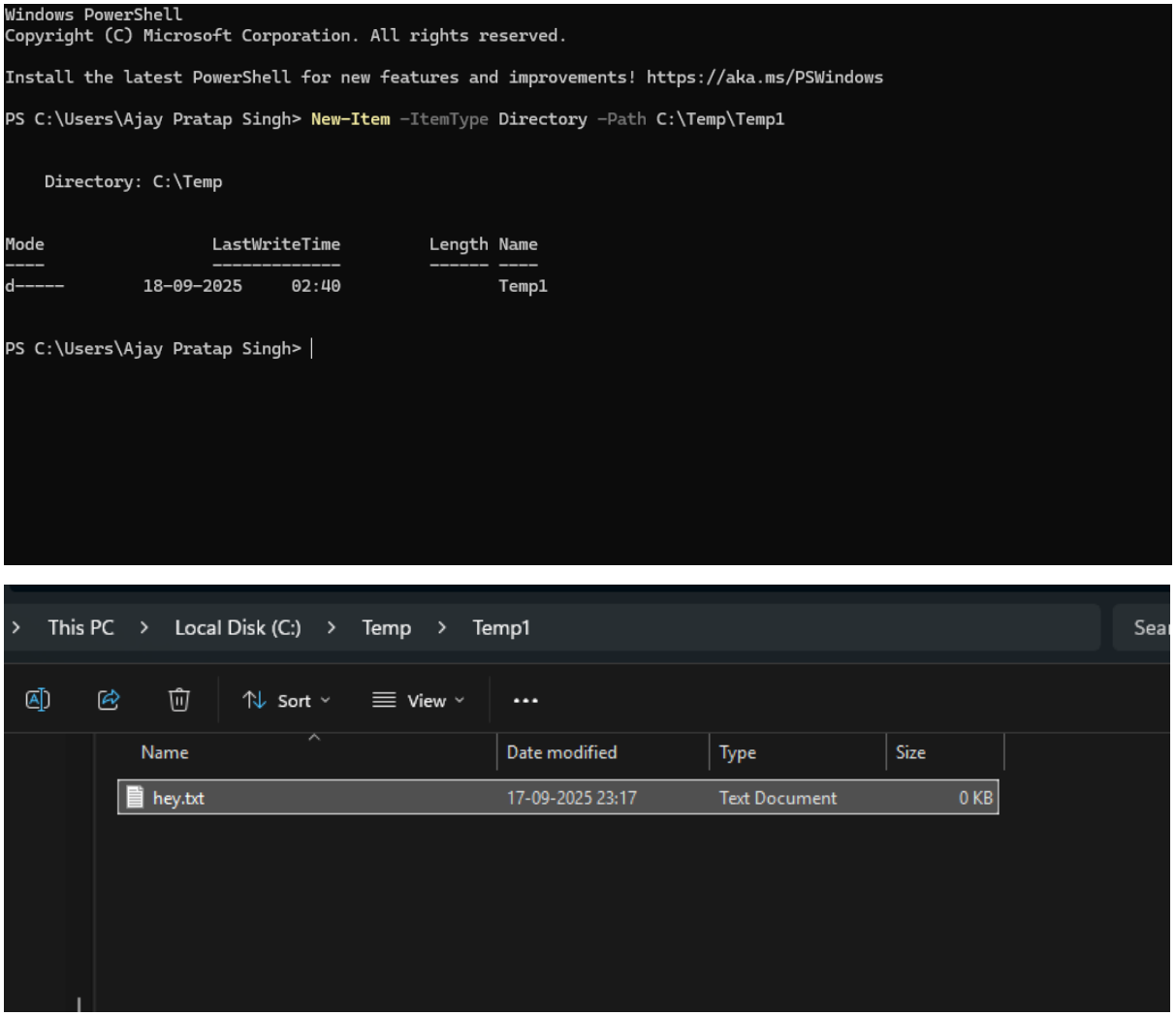

Fig 1.4 Harvesting Credentials

Cleanup

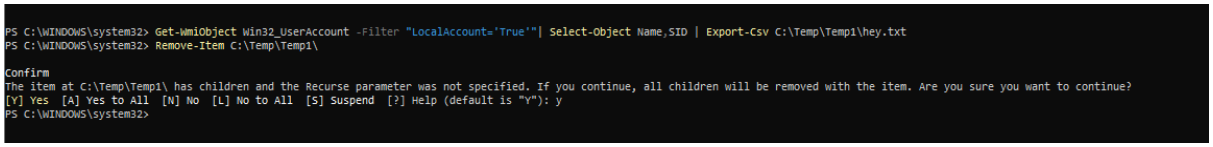

Fig 1.5 Cleaning Up of exported files

Lab Logs

Tool	Action
Powershell	Fileless execution
WMI	Credential harvest