

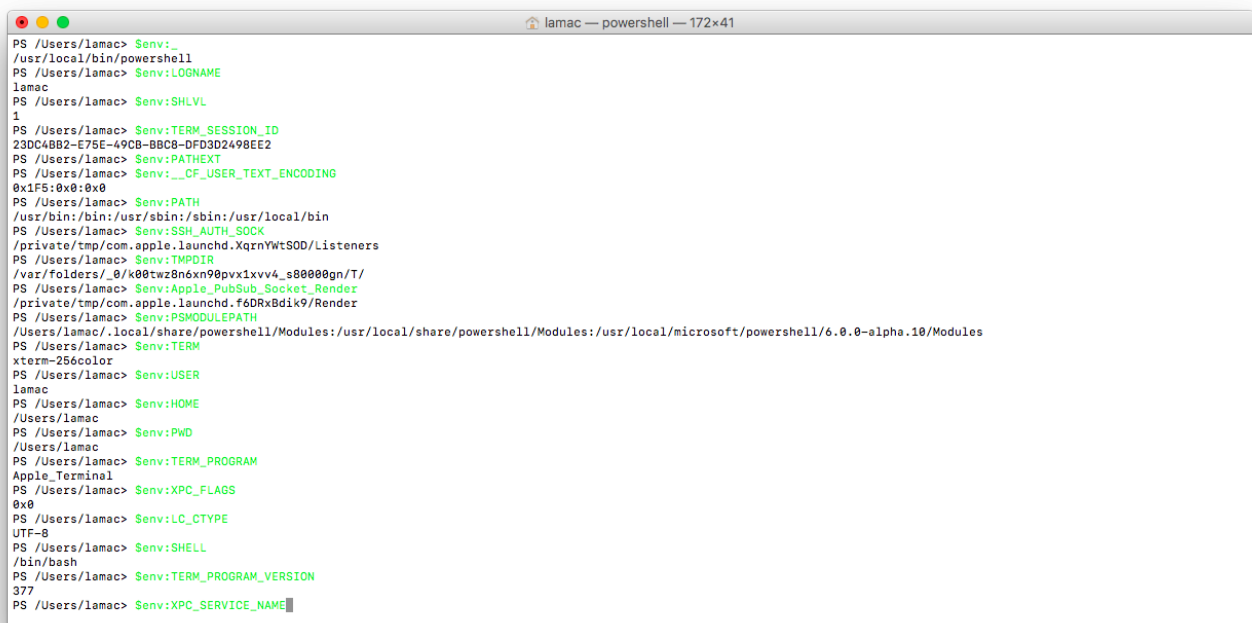
Windows Post Exploitation Cmdlets (PowerShell)

Presence

This section focuses on information gathering about the victim host and the network that it's attached to.

System

[crayon-6a9d5f4859135262922495/]

A screenshot of a PowerShell terminal window titled 'lamac — powershell — 172x41'. The terminal shows a series of 'PS /Users/lamac> Senv:...' commands and their outputs, which are system environment variables and paths. The outputs include: 'usr/local/bin/powershell', 'LOGNAME lamac', 'SHLVL 1', 'TERM_SESSION_ID 23DC48B2-E75E-49CB-BBC8-DFD3D2498EE2', 'PATHTEXT', 'CF_USER_TEXT_ENCODING 0x1F5:0x0:0x0', 'PATH /usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin', 'SSH_AUTH_SOCK /private/tmp/com.apple.launchd.XqrnYwTSOD/Listeners', 'TMPDIR /var/folders/_0/k00twz8n6xn90pvx1xvv4_s80000gn/T/', 'Apple_PubSub_Socket_Render /private/tmp/com.apple.launchd.f6DRxBdik9/Render', 'PSMODULEPATH /Users/lamac/.local/share/powershell/Modules:/usr/local/share/powershell/Modules:/usr/local/microsoft/powershell/6.0.0-alpha.10/Modules', 'TERM xterm-256color', 'USER lamac', 'HOME /Users/lamac', 'PWD /Users/lamac', 'TERM_PROGRAM Apple_Terminal', 'XPC_FLAGS 0x0', 'LC_CTYPE UTF-8', 'SHELL /bin/bash', 'TERM_PROGRAM_VERSION 377', and 'XPC_SERVICE_NAME'.

```
PS /Users/lamac> Senv:
/usr/local/bin/powershell
PS /Users/lamac> Senv:LOGNAME
lamac
PS /Users/lamac> Senv:SHLVL
1
PS /Users/lamac> Senv:TERM_SESSION_ID
23DC48B2-E75E-49CB-BBC8-DFD3D2498EE2
PS /Users/lamac> Senv:PATHTEXT
PS /Users/lamac> Senv:___CF_USER_TEXT_ENCODING
0x1F5:0x0:0x0
PS /Users/lamac> Senv:PATH
/usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin
PS /Users/lamac> Senv:SSH_AUTH_SOCK
/private/tmp/com.apple.launchd.XqrnYwTSOD/Listeners
PS /Users/lamac> Senv:TMPDIR
/var/folders/_0/k00twz8n6xn90pvx1xvv4_s80000gn/T/
PS /Users/lamac> Senv:Apple_PubSub_Socket_Render
/private/tmp/com.apple.launchd.f6DRxBdik9/Render
PS /Users/lamac> Senv:PSMODULEPATH
/Users/lamac/.local/share/powershell/Modules:/usr/local/share/powershell/Modules:/usr/local/microsoft/powershell/6.0.0-alpha.10/Modules
PS /Users/lamac> Senv:TERM
xterm-256color
PS /Users/lamac> Senv:USER
lamac
PS /Users/lamac> Senv:HOME
/Users/lamac
PS /Users/lamac> Senv:PWD
/Users/lamac
PS /Users/lamac> Senv:TERM_PROGRAM
Apple_Terminal
PS /Users/lamac> Senv:XPC_FLAGS
0x0
PS /Users/lamac> Senv:LC_CTYPE
UTF-8
PS /Users/lamac> Senv:SHELL
/bin/bash
PS /Users/lamac> Senv:TERM_PROGRAM_VERSION
377
PS /Users/lamac> Senv:XPC_SERVICE_NAME
```

WMI

[crayon-6a9d5f485913f885122966/]

Networking

[crayon-6a9d5f4859141171433086/]

Users

[crayon-6a9d5f4859149478185170/]

Configs

[crayon-6a9d5f485914d602039276/]

Finding important files

[crayon-6a9d5f485914f722177107/]

Files to pull

[crayon-6a9d5f4859150316955584/]

Remote system access

[crayon-6a9d5f4859152792224017/]

Software

[crayon-6a9d5f4859154179618489/]

AutoStart directories

[crayon-6a9d5f4859157680390018/]

Persistence

This section focuses on gaining a foothold to regain, or re-obtain access to a system through means of authentication, backdoors, etc..

Download

[crayon-6a9d5f4859159702148856/]

Compress or expand ZIP archive

[crayon-6a9d5f485915a855417117/]

Reg command exit

[crayon-6a9d5f485915c801467807/]

Deleting logs

[crayon-6a9d5f485915d276425790/]

Uninstalling software «Antivirus»

[crayon-6a9d5f485915f318069656/]

Invasive or altering commands

[crayon-6a9d5f4859161717159132/]