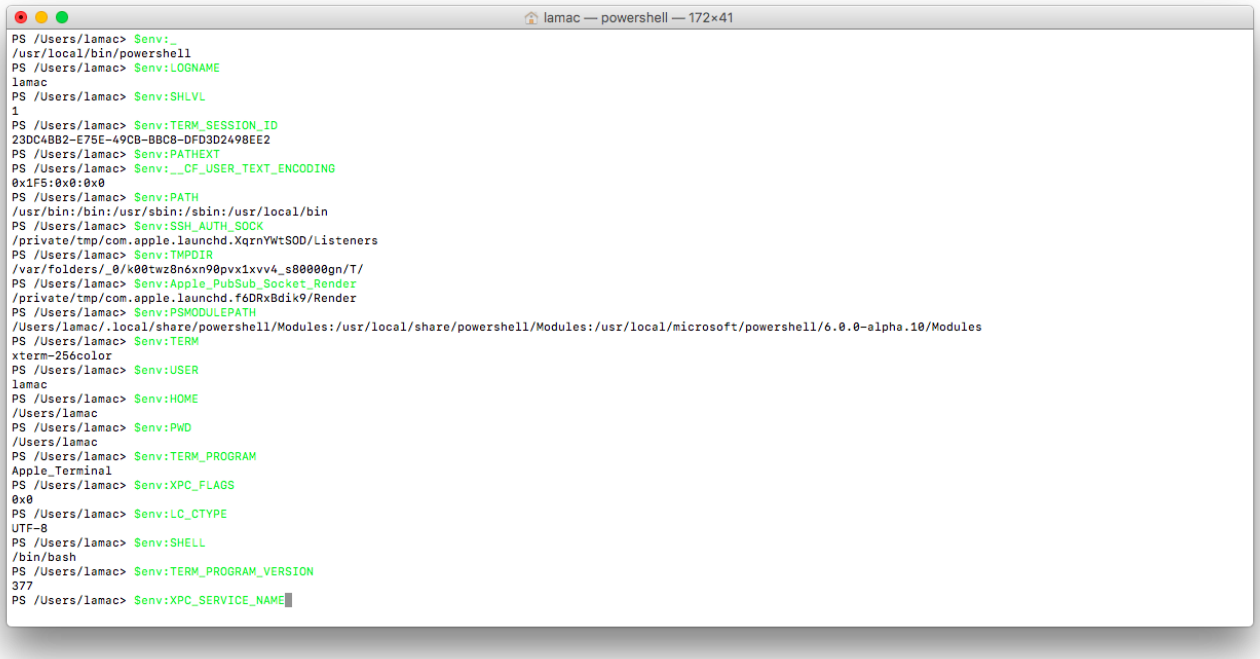
Windows Post Exploitation Cmdlets Execution (PowerShell)

Presence

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

System

[crayon-6a9d5f4859135262922495/]



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/]

Persistance

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/]