Clase 3  
LOL -> “Living of the Land”

Comportamiento del adversario

* Reconocimiento interno
* Uso de PowerShell
* Actividades de proxy no específicosficas
* Uso de la interfaz de linea de comandos
* Agente de usuario HTTP
* Servidor de comando y control
* Uso de la tunelizacion DNS
* Uso de Web Shell
* Preparacion de datos

Pwd -> Es el path

netstat ->

Net-stat | out-file C: \User\User\Net-stat.txt ->

tasklist | out-file C: \User\User\tasklist.txt

tasklist /FI “PIN eq ###”

Get-history | -> La barra te ayuda a sacar un parceo del de un documento

Get-history para obtener el historial de códigos ↳ get-history | out-file C:/Logs

…Hackertarget.com/server-info/ -> Ver información de una IP

…cybercrime-tracker.net -> lugar lleno de direcciones IP -> Ciber ataques -> Lugar donde se puede hacer muchos ataques

…port.tools -> sirve para

VPN -> (Virtual Private Networking) ↳ Proxy -> Anonimo, pero se puede hacer un tracer hasta llegar a la IP

A screenshot of a computer program

AI-generated content may be incorrect.

Si estan “open” puede que se este robando información -> Facil de atacar Si estan “filtered” el hacker puede estar robando información -> Medio de atacar

Si esta “close” no configurado -> Dificil de atacar  Aca podemos ver que de esta IP tiene varios status donde podemos ser atacados o atacar

A screenshot of a computer program

AI-generated content may be incorrect.