Post-Compromise Enumeration

Index:

Powerview

Requirements:

https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView

Enumeration:

- Load up a command prompt and cd into Downloads

  ```
  powershell -ep bypass

  -ep is ExecutionPolicy (Stops us from executing scripts)
  bypass - bypass :)
  ```

- Load PowerView

  ```
  . .\Powerview.ps1
  ```

- Fundamental Commands

```
Get-NetDomain
//Returns information about the domain

Get-NetDomainController
// Returns Information about DC

Get-DomainPolicy
// Returns Domain Policies such as Kerberos Policy, System Access,
Version, Registry Values

(Get-DomainPolicy)."system access"
// Returns Policies about System Access

Get-NetUser
// Returns all the users

Get-NetUser | select cn
// Returns all the usernames
```

```
Get-UserProperty
// Returns the properties that a user might have

Get-UserProperty -Properties pwdlastset
// Returns the property value of pwdlastset

Get-UserProperty -Properties logoncount
// If some accounts are logged in 0 or less number of times, it may be a
honeypot account!

Get-NetComputer -FullData
// Returns list of all the computers (with Full Data)

Get-NetGroup
// Returns all the groups in the domain

Get-NetGroup -GroupName *admin*
// Returns the groups having "admin" in their name

Get-NetGroupMember -GroupName "Domain Admins"
// Returns the members of the group "Domain Admins"

Invoke-ShareFinder
// Returns all the SMB Shares in the network
// You can see what files are being shared and where they're being shared

Get-NetGPO
// Returns all the group policies
```

Bloodhound

Bloodhound is a tool which downloads the data of Active Directory and Visualize the data in a graph!

Setup:

- Install Bloodhound

  ```
  apt install bloodhound
  ```

- Bloodhound runs on neo4j
- We need to change our default credentials

  ```
  localhost:7474
  ```

Enumeration:

- Open Bloodhound

  ```
  bloodhound
  ```

- Shaprhound Github and Run on Windows 10 E https://github.com/BloodHoundAD/BloodHound/blob/master/Collectors/SharpHound.ps1
- Run Commands

  ```
  Invoke-Bloodhound -CollectionMethod All -Domain MARVEL.local -ZipFileName file.zip
  ```

- Get that Data into Parrot Machine
- Upload Data into Bloodhound
- Enumerate!