Introduction

In this we will learn how to enumerate the network after compromisig a machine. We use PowerView, Blood Hound tools to enumerate an understand.

Tools

PowerView

Its a tool in PowerTools by PowerShellEmpire

https://github.com/PowerShellEmpire/PowerTools.git

Usage:

```
. .\PowerView.ps1
```

`Get-Domain` → Info about the network Domain
`Get-DomainController`
`Get-DomainPolicy`
`(Get-DomainPolicy)."system access"`
`Get-NetUser | select cn,description,account name`
`Get-UserProperty` → Displays all user properties we can use
`Get-UserProperty -Properties pwdlastset`
`Get-UserProperty -Properties logoncount`
`Get-UserProperty -Properties badpwdcount` → Wrong passwords
`Get-NetComputer` → Displays all computers
`Get-NetComputer -FullData` ——→ Full Data too much info
`Get-NetComputer -FullData | select OperatingSystem`
`Get-NetGroup` → All groups including BuiltIn
`Get-NetGroup -GroupName "Domain Admins"`
`Get-NetGroup -GroupName *admin*` → Displays all types of admins
`Get-NetGPO` → Shows all group policies

`Invoke-ShareFinder` → Displays all the SMB shares in the network
`Invoke-ShareFinder | select displayname, whenchanged` → Increases verbosity

Blood Hound

Installation

1. `sudo apt install bloodhound`

2. https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1

About

→ It runs on a tool called neo4j
→ Default Credentials: neo4j:neo4j
→ This tool is just used to visualise data which was gathered by Invoke-BloodHound tool

Usage

Starting

Linux

Command: `neo4j console`
→ This Starts the database for BloodHound.
Command: `bloodhound`
→ This runs the BloodHound instance.

Windows

→ Here we are collecting information of the domain
→ For that we should first run the script sharphound

Command: `. .\path\to\SharpHound.ps1`

Enumerating

Windows

Command:`Invoke-BloodHound`
→ This creates all files by collecting the info about the domain

Parameters:
`-CollectionMethod All`→ Collects all data
`-Domain domain_name.local` → Name of the domain
`-ZipFileName file_name.zip`→ Creates the zip file of gathered data.