【AD】【列舉】SharpHound

https://github.com/puckiestyle/powershell/blob/master/SharpHound.ps1

SharpHound 有幾種不同的格式可用。我們可以自己編譯它，使用已經編譯好的可執行文件，或者將其用作 PowerShell 腳本。在我們的情況下，我們將使用位於 CLIENT75 的 C:\Tools 中的 PowerShell 腳本。首先，讓我們打開一個 PowerShell 窗口並將腳本載入內存：

```
PS C:\Tools> Import-Module .\Sharphound.ps1
```

SharpHound 已經載入，現在我們可以開始收集域數據。然而，為了運行 SharpHound，我們首先必須運行 Invoke-BloodHound。這並不直觀，因為在這個階段我們只運行 SharpHound。讓我們調用 Get-Help 來了解有關此命令的更多信息。

```
PS C:\Tools> Get-Help Invoke-BloodHound
```

```
PS C:\Tools> Get-Help Invoke-BloodHound

NAME
    Invoke-BloodHound

SYNOPSIS
    Runs the BloodHound C# Ingestor using reflection. The assembly is stored in
this file.


SYNTAX
    Invoke-BloodHound [-CollectionMethod <String[]>] [-Domain <String>] [-
SearchForest] [-Stealth] [-LdapFilter <String>] [-DistinguishedName
    <String>] [-ComputerFile <String>] [-OutputDirectory <String>] [-
OutputPrefix <String>] [-CacheName <String>] [-MemCache] [-RebuildCache]
    [-RandomFilenames] [-ZipFilename <String>] [-NoZip] [-ZipPassword <String>]
[-TrackComputerCalls] [-PrettyPrint] [-LdapUsername <String>]
    [-LdapPassword <String>] [-DomainController <String>] [-LdapPort <Int32>]
[-SecureLdap] [-DisableCertVerification] [-DisableSigning]
    [-SkipPortCheck] [-PortCheckTimeout <Int32>] [-SkipPasswordCheck] [-
ExcludeDCs] [-Throttle <Int32>] [-Jitter <Int32>] [-Threads <Int32>]
    [-SkipRegistryLoggedOn] [-OverrideUsername <String>] [-RealDNSName
<String>] [-CollectAllProperties] [-Loop] [-LoopDuration <String>]
    [-LoopInterval <String>] [-StatusInterval <Int32>] [-Verbosity <Int32>] [-
Help] [-Version] [<CommonParameters>]


DESCRIPTION
    Using reflection and assembly.load, load the compiled BloodHound C#
ingestor into memory
    and run it without touching disk. Parameters are converted to the
equivalent CLI arguments
    for the SharpHound executable and passed in via reflection. The appropriate
function
    calls are made in order to ensure that assembly dependencies are loaded
properly.


RELATED LINKS

REMARKS
    To see the examples, type: "get-help Invoke-BloodHound -examples".
    For more information, type: "get-help Invoke-BloodHound -detailed".
    For technical information, type: "get-help Invoke-BloodHound -full".
```

我們將從 -CollectionMethod 開始，該參數描述了各種收集方法。在我們的情況下，我們將嘗試收集所有數據，這將執行除了本地組策略之外的所有收集方法。

默認情況下，SharpHound 將以 JSON 文件的形式收集數據並自動將其壓縮為 ZIP 文件。這使我們能夠輕鬆將文件傳輸到稍後的 Kali Linux。我們將保存這個輸出文件到桌面上，帶有如下的 "corp audit" 前綴：

Invoke-BloodHound -CollectionMethod All -OutputDirectory C:\Users\stephanie\Desktop\ -OutputPrefix "corp audit"

```
PS C:\Tools> Invoke-BloodHound -CollectionMethod All -OutputDirectory
C:\Users\stephanie\Desktop\ -OutputPrefix "corp audit"
```

請注意，數據收集可能需要一些時間才能完成，這取決於我們正在列舉的環境的大小。讓我們檢查 SharpHound 的輸出：

```
2022-10-12T09:20:22.3688459-07:00|INFORMATION|This version of SharpHound is
compatible with the 4.2 Release of BloodHound
2022-10-12T09:20:22.5909898-07:00|INFORMATION|Resolved Collection Methods:
Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container,
RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-10-12T09:20:22.6383624-07:00|INFORMATION|Initializing SharpHound at 9:20
AM on 10/12/2022
2022-10-12T09:20:22.9661022-07:00|INFORMATION|Flags: Group, LocalAdmin,
GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps,
DCOM, SPNTargets, PSRemote
2022-10-12T09:20:23.3881009-07:00|INFORMATION|Beginning LDAP search for
corp.com
2022-10-12T09:20:23.4975127-07:00|INFORMATION|Producer has finished, closing
LDAP channel
2022-10-12T09:20:23.4975127-07:00|INFORMATION|LDAP channel closed, waiting for
consumers
2022-10-12T09:20:53.6398934-07:00|INFORMATION|Status: 0 objects finished (+0
0)/s -- Using 96 MB RAM
2022-10-12T09:21:13.6762695-07:00|INFORMATION|Consumers finished, closing
output channel
2022-10-12T09:21:13.7396906-07:00|INFORMATION|Output channel closed, waiting
for output task to complete
Closing writers
2022-10-12T09:21:13.8983935-07:00|INFORMATION|Status: 106 objects finished
(+106 2.12)/s -- Using 104 MB RAM
2022-10-12T09:21:13.8983935-07:00|INFORMATION|Enumeration finished in
00:00:50.5065909
2022-10-12T09:21:14.0094454-07:00|INFORMATION|Saving cache with stats: 66 ID to
type mappings.
 68 name to SID mappings.
 2 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2022-10-12T09:21:14.0255279-07:00|INFORMATION|SharpHound Enumeration Completed
at 9:21 AM on 10/12/2022! Happy Graphing!
```

根據清單 78 中的輸出，我們總共掃描了 106 個對象。這顯然會根據域中存在多少對象和會話而變化。

在這種情況下，SharpHound 實際上是從 stephanie 使用者那裡對域進行了一個快照，我們應該能夠分析使用者帳戶有權訪問的所有內容。收集的數據存儲在我們桌面上的 ZIP 文件中：

```
PS C:\Tools> ls C:\Users\stephanie\Desktop\

    Directory: C:\Users\stephanie\Desktop

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/27/2022  11:00 PM          12680 corp
audit_20220927230019_BloodHound.zip
-a----         9/27/2022  11:00 PM           9734
MTk2MmZkNjItY2IyNC00MWMzLTk5YzMtM2E1ZDcwYThkMzRl.bin
```

⏲修訂版本 #2
★由 treeman 建立於 12 ⍰Q⍰G⍰⍰ 2023 01:16:52
✎由 treeman 更新於 3 ⍰G⍰⍰ 2024 13:05:44