【SMB】enum4linux

```
$ enum4linux -a -o 192.168.202.13



 ========================================( Target Information
)=========================================

Target ..... 192.168.202.13
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.202.13
)============================


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Information for 192.168.202.13
)================================

Looking up status of 192.168.202.13
        SAMBA          <00> -         B <ACTIVE>  Workstation Service
        SAMBA          <03> -         B <ACTIVE>  Messenger Service
        SAMBA          <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP      <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP      <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==================================( Session Check on 192.168.202.13
)==================================


[+] Server 192.168.202.13 allows sessions using username '', password ''


 ================================( Getting domain SID for 192.168.202.13
)================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==================================( OS information on 192.168.202.13
)==================================


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.202.13 from srvinfo:
        SAMBA          Wk Sv PrQ Unx NT SNT samba server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03
```

```
 ========================================( Users on 192.168.202.13
)========================================

Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value $users in print at ./enum4linux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 988.

 ================================( Share Enumeration on 192.168.202.13
)================================

smbXcli_negprot_smb1_done: No compatible protocol selected by server.

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        files           Disk      Flag: OS{861316807af111601f7db90f63ab6e3d}
        IPC$            IPC       IPC Service (samba server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.202.13

//192.168.202.13/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.202.13/files  Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//192.168.202.13/IPC$   Mapping: N/A Listing: N/A Writing: N/A
```

```
root@kali:~# enum4linux -h
enum4linux v0.8.9 ( http :// labs . portcullis . co . uk / application / enum4linux / )
Copyright (C) 2011 Mark Lowe ( mrl@portcullis-security.com )
簡單的封裝了在samba套件中的工具，以提供類似的enum.exe功能（以前從www.bindview.com）。為了方便起見，也增加了一些附加功能，例如RID循環。
用法: ./enum4linux.pl [選項] ip位址
列舉選項：
    -U 取得使用者列表
    -M 取得機器清單*
    -S 取得共享列表
    -P 取得密碼策略訊息
    -G 取得群組和成員列表
    -d 詳述適用於-U和-S
    -u user 使用者指定要使用的使用者名稱（預設""）
    -p pass 指定要使用的密碼（預設為""）
以下選項是enum.exe未實現的: -L, -N, -D, -f
其他選項:
   -a 做所有簡單枚舉（-U -S -G -P -r -o -n -i），如果您沒有提供任何其他選項，請啟用此選項
   -h 顯示此說明訊息並退出
   -r 透過RID循環列舉用戶
   -R range RID範圍要列舉（預設值：500-550,1000-1050，隱含-r）
   -K n 繼續搜尋RID，直到n個連續的RID與使用者名稱不對應，Impies RID範圍結束於999999.對DC有用
   -l 透過LDAP 389 / TCP取得一些（有限的）資訊（僅適用於DN）
   -s 檔案暴力猜測共享名稱
   -k user 遠端系統上存在的使用者（預設值：administrator，guest，krbtgt，domain admins，root，bin，none）
           用於取得sid與“lookupsid known_username”
           使用逗號嘗試幾個用戶：“-k admin，user1，user2”
   -o 取得作業系統資訊
   -i 取得印表機訊息
   -w wrkg 手動指定工作組（通常自動找到）
   -n 做一個nmblookup（類似nbtstat）
   -v 詳細輸出，顯示正在運行的完整命令（net，rpcclient等）
RID循環應從Windows（或Samba）主機中提取一個使用者列表，其中限制匿名設定為1（Windows NT和2000）或啟用「網路存取：允許匿名SID /名
```

稱轉換」（XP，2003）。

注意：Samba伺服器通常似乎有RID在範圍3000-3050。

修訂版本 #1
★由 treeman 建立於 7 ﷺ 2023 23:27:45
由 treeman 更新於 7 ﷺ 2024 19:30:26