

基于msf

模块：

scanner/smb/smb_version

```
1 msf auxiliary(scanner/smb/smb_version) > show options
2
3 Module options (auxiliary/scanner/smb/smb_version):
4
5 Name Current Setting Required Description
6 ----
7 RHOSTS 192.168.1.0/24 yes The target address range or CIDR identifier
8 SMBDomain . no The Windows domain to use for authentication
9 SMBPass no The password for the specified username
10 SMBUser no The username to authenticate as
11 THREADS 1 yes The number of concurrent threads
12
13 msf auxiliary(scanner/smb/smb_version) > set threads 20
14 threads => 20
15 msf auxiliary(scanner/smb/smb_version) > exploit
16
17 [+] 192.168.1.4:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:XXXXXX) (workgroup:WORKGROUP )
18 [*] Scanned 39 of 256 hosts (15% complete)
19 [*] Scanned 61 of 256 hosts (23% complete)
20 [*] Scanned 81 of 256 hosts (31% complete)
21 [+] 192.168.1.99:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:XXXXXX) (workgroup:WORKGROUP )
22 [+] 192.168.1.119:445 - Host is running Windows 2003 R2 SP2 (build:3790) (name:XXXXXX)
23 [*] Scanned 103 of 256 hosts (40% complete)
24 [*] Scanned 130 of 256 hosts (50% complete)
25 [*] Scanned 154 of 256 hosts (60% complete)
26 [*] Scanned 181 of 256 hosts (70% complete)
27 [*] Scanned 205 of 256 hosts (80% complete)
28 [*] Scanned 232 of 256 hosts (90% complete)
29 [*] Scanned 256 of 256 hosts (100% complete)
```

```
30 [*] Auxiliary module execution completed
```

```
31
```

```
msf auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.0/24  yes       The target address range or CIDR identifier
  SMBDomain .                no        The Windows domain to use for authentication
  SMBPass   .                no        The password for the specified username
  SMBUser   .                no        The username to authenticate as
  THREADS   1                yes       The number of concurrent threads

msf auxiliary(scanner/smb/smb_version) > set threads 20
threads => 20
msf auxiliary(scanner/smb/smb_version) > exploit

[+] 192.168.1.4:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:JOHN-PC) (workgroup:WORKGROUP )
[*] Scanned 39 of 256 hosts (15% complete)
[*] Scanned 61 of 256 hosts (23% complete)
[*] Scanned 81 of 256 hosts (31% complete)
[+] 192.168.1.99:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:JOHN-PC) (workgroup:WORKGROUP )
[+] 192.168.1.119:445 - Host is running Windows 2003 R2 SP2 (build:3790) (name:WIN03X64)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 130 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 181 of 256 hosts (70% complete)
[*] Scanned 205 of 256 hosts (80% complete)
[*] Scanned 232 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

基于cme (参考第九十三课)

```
1 root@John:~# cme smb 192.168.1.0/24
2 SMB 192.168.1.4 445 JOHN-PC [*] Windows 7 Ultimate 7601 Service Pack 1
  x64 (name:JOHN-PC) (domain:JOHN-PC) (signing:False) (SMBv1:True)
3 SMB 192.168.1.99 445 JOHN-PC [*] Windows 7 Ultimate 7601 Service Pack
  1 x64 (name:JOHN-PC) (domain:JOHN-PC) (signing:False) (SMBv1:True)
4 SMB 192.168.1.119 445 WIN03X64 [*] Windows Server 2003 R2 3790 Service
  Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)
```

```
root@John:~# cme smb 192.168.1.0/24
SMB 192.168.1.4 445 JOHN-PC [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:JOHN-PC) (domain:JOHN-PC) (signing:False) (SMBv1:True)
SMB 192.168.1.99 445 JOHN-PC [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:JOHN-PC) (domain:JOHN-PC) (signing:False) (SMBv1:True)
SMB 192.168.1.119 445 WIN03X64 [*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)
```

基于nmap

```
1 root@John:~# nmap -sU -sS --script smb-enum-shares.nse -p 445 192.168.
  1.119
2 Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-29 08:45 EST
3 Nmap scan report for 192.168.1.119
4 Host is up (0.0029s latency).
5
6 PORT STATE SERVICE
7 445/tcp open microsoft-ds
```

```
8 445/udp open|filtered microsoft-ds
9 MAC Address: 00:0C:29:85:D6:7D (VMware)
10
11 Host script results:
12 | smb-enum-shares:
13 | account_used: guest
14 | \\192.168.1.119\ADMIN$:
15 | Type: STYPE_DISKTREE_HIDDEN
16 | Comment: \xE8\xBF\x9C\xE7\xA8\x8B\xE7\xAE\xA1\xE7\x90\x86
17 | Anonymous access: <none>
18 | Current user access: <none>
19 | \\192.168.1.119\C$:
20 | Type: STYPE_DISKTREE_HIDDEN
21 | Comment: \xE9\xBB\x98\xE8\xAE\xA4\xE5\x85\xB1\xE4\xBA\xAB
22 | Anonymous access: <none>
23 | Current user access: <none>
24 | \\192.168.1.119\E$:
25 | Type: STYPE_DISKTREE_HIDDEN
26 | Comment: \xE9\xBB\x98\xE8\xAE\xA4\xE5\x85\xB1\xE4\xBA\xAB
27 | Anonymous access: <none>
28 | Current user access: <none>
29 | \\192.168.1.119\IPC$:
30 | Type: STYPE_IPC_HIDDEN
31 | Comment: \xE8\xBF\x9C\xE7\xA8\x8B IPC
32 | Anonymous access: READ
33 | Current user access: READ/WRITE
34 | \\192.168.1.119\share:
35 | Type: STYPE_DISKTREE
36 | Comment:
37 | Anonymous access: <none>
38 | _ Current user access: READ/WRITE
39
40 Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
41
```

```

root@John:~# nmap -sU -sS --script smb-enum-shares.nse -p 445 192.168.1.119
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-29 08:45 EST
Nmap scan report for 192.168.1.119
Host is up (0.0029s latency).

PORT      STATE      SERVICE
445/tcp   open      microsoft-ds
445/udp   open|filtered microsoft-ds
MAC Address: 00:0C:29:85:D6:7D (VMware)

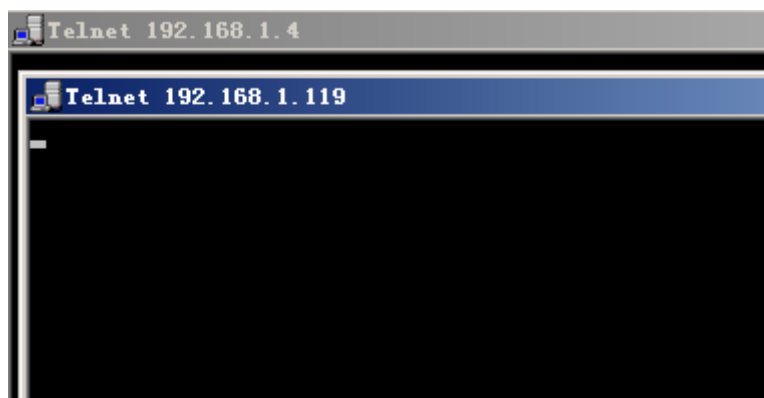
Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.1.119\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: \xE8\xBF\x9C\xE7\xA8\x8B\xE7\xAE\xA1\xE7\x90\x86
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.1.119\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: \xE9\xBB\x98\xE8\xAE\xA4\xE5\x85\xB1\xE4\xBA\xAB
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.1.119\E$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: \xE9\xBB\x98\xE8\xAE\xA4\xE5\x85\xB1\xE4\xBA\xAB
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.1.119\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: \xE8\xBF\x9C\xE7\xA8\x8B IPC
|     Anonymous access: READ
|     Current user access: READ/WRITE
|   \\192.168.1.119\share:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|_

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds

```

基于CMD :

```
1 for /l %a in (1,1,254) do start /min /low telnet 192.168.1.%a 445
```



基于powershell :

一句话扫描 :

单IP :

```
1 445 | %{ echo ((new-object Net.Sockets.TcpClient).Connect("192.168.1.119",$_)) "$_ is open"} 2>$null
```

```
PS C:\Users\John> 445 | %{ echo ((new-object Net.Sockets.TcpClient).Connect("192.168.1.119",$_)) "$_ is open"} 2>$null
445 is open
PS C:\Users\John>
```

多ip :

```
1 1..5 | % { $a = $_; 445 | % {echo ((new-object Net.Sockets.TcpClient).Connect("192.168.1.$a",$_)) "Port $_ is open"} 2>$null}
```

```
PS C:\Users\John> 1..5 | % { $a = $_; 445 | % {echo ((new-object Net.Sockets.TcpClient).Connect("192.168.1.$a",$_)) "Port $_ is open!"} 2>$null}
Port 445 is open!
PS C:\Users\John> _
```

多port , 多IP :

```
1 118..119 | % { $a = $_; write-host "-----"; write-host "192.168.1.$a"; 80,445 | % {echo ((new-object Net.Sockets.TcpClient).Connect("192.168.1.$a",$_)) "Port $_ is open"} 2>$null}
```

```
PS C:\Users\John> 118..119 | % { $a = $_; write-host "-----"; write-host "192.168.1.$a"; 80,445 | % {echo ((new-object Net.Sockets.TcpClient).Connect("192.168.1.$a",$_)) "Port $_ is open"} 2>$null}
-----
192.168.1.118
-----
192.168.1.119
Port 80 is open
Port 445 is open
```

- Micropoor