第十七课 MetaSploit扫描指定端口的主机

Author：陈殷

公众号：山丘安全攻防实验室

• auxiliary/scanner/portscan/tcp 可批量扫描指定端口的主机

查找模块

```
msf5 auxiliary(scanner/smb/smb_version) > search portscan/tcp

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

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/portscan/tcp                     normal  Yes    TCP Port Scanner
```

使用模块

```
msf5 auxiliary(scanner/smb/smb_version) > use auxiliary/scanner/portscan/tcp
```

查看选项

```
msf5 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds
```

设置参数

```
msf5 auxiliary(scanner/portscan/tcp) > set rhosts 192.168.0.0-255
rhosts => 192.168.0.0-255
msf5 auxiliary(scanner/portscan/tcp) > set rhosts 192.168.30.0/24
rhosts => 192.168.30.0/24
msf5 auxiliary(scanner/portscan/tcp) > set ports 3389
ports => 3389
msf5 auxiliary(scanner/portscan/tcp) > set threads 50
threads => 50
```

运行

```
msf5 auxiliary(scanner/portscan/tcp) > run

[*] 192.168.30.0-255:      - Scanned  33 of 256 hosts (12% complete)
[*] 192.168.30.0-255:      - Scanned  83 of 256 hosts (32% complete)
[+] 192.168.30.130:        - 192.168.30.130:3389 - TCP OPEN
[*] 192.168.30.0-255:      - Scanned  84 of 256 hosts (32% complete)
[*] 192.168.30.0-255:      - Scanned 125 of 256 hosts (48% complete)
[*] 192.168.30.0-255:      - Scanned 128 of 256 hosts (50% complete)
[*] 192.168.30.0-255:      - Scanned 171 of 256 hosts (66% complete)
[*] 192.168.30.0-255:      - Scanned 183 of 256 hosts (71% complete)
[*] 192.168.30.0-255:      - Scanned 217 of 256 hosts (84% complete)
[*] 192.168.30.0-255:      - Scanned 231 of 256 hosts (90% complete)
[*] 192.168.30.0-255:      - Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

扫描完成

文章作者：陈殷

文章出处：山丘安全攻防实验室