0x04-内网渗透之内网扫描

auther：ske

0x00 环境-工具

```
nbtscan       http://www.unixwiz.net/tools/nbtscan.html | http://www.mirrorserv
ms17010       MSF
web扫描       https://github.com/zer0h/httpscan
存活扫描      for /l %i in (1,1,255) do @ping 192.168.1.%i -w 1 -n 1 | find /i "
```

0x01 nbtscan

```
nbtscan 192.168.52.0/24
```

```
C:\Users\Administrator\Desktop>nbtscan.exe 192.168.52.0/24
192.168.52.2    HACK\WINDOWS_SERVER_            SHARING DC
192.168.52.28   HACK\WIN08-WEB                  SHARING
192.168.52.29   HACK\WIN12-IIS                  SHARING
*timeout (normal end of scan)
```

0x02 MS17010

```
MS_17_010_Scan.exe -ip 192.168.52.2 192.168.52.30
```

```
C:\Users\Administrator\Desktop>MS_17_010_Scan.exe -ip 192.168.52.2 192.168.52.30
[-] [192.168.52.2] NOT Found Vuln
[-] [192.168.52.3] Exception: timed out
[-] [192.168.52.4] Exception: timed out
[-] [192.168.52.5] Exception: timed out
[-] [192.168.52.6] Exception: timed out
[-] [192.168.52.7] Exception: timed out
[-] [192.168.52.8] Exception: timed out
[-] [192.168.52.9] Exception: timed out
[-] [192.168.52.10] Exception: timed out
[-] [192.168.52.11] Exception: timed out
[-] [192.168.52.12] Exception: timed out
[-] [192.168.52.13] Exception: timed out
[-] [192.168.52.14] Exception: timed out
[-] [192.168.52.15] Exception: timed out
[-] [192.168.52.16] Exception: timed out
[-] [192.168.52.17] Exception: timed out
[-] [192.168.52.18] Exception: timed out
[-] [192.168.52.19] Exception: timed out
[-] [192.168.52.20] Exception: timed out
[-] [192.168.52.21] Exception: timed out
[-] [192.168.52.22] Exception: timed out
[-] [192.168.52.23] Exception: timed out
[-] [192.168.52.24] Exception: timed out
[-] [192.168.52.25] Exception: timed out
[-] [192.168.52.26] Exception: timed out
[-] [192.168.52.27] Exception: timed out
[+] [192.168.52.28] Found Vuln MS17-010! (Windows Server 2008 R2 Standard 7600)
[-] [192.168.52.29] Exception: [Errno 10054]
```

0x03 web扫描

```
python httpscan.py 203.124.10.0/24
```

```
root@msf:~/httpscan# python httpscan.py 203.124.10.0/24
+----------------+------+--------------------+------------------------------+
|     IP         |Status|       Server       |            Title             |
+----------------+------+--------------------+------------------------------+
|203.124.10.2    |200   |Apache/2.2.34 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.4    |200   |Apache/2.2.17 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.3    |200   |Apache/1.3.41 (Unix)|CLink Office v2               |
+----------------+------+--------------------+------------------------------+
|203.124.10.14   |200   |Apache/2.2.29 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.15   |200   |Apache/2.2.29 (Unix)|CLink Office v2               |
+----------------+------+--------------------+------------------------------+
|203.124.10.16   |200   |Apache/2.2.34 (Unix)|CLink Office v2               |
+----------------+------+--------------------+------------------------------+
|203.124.10.19   |200   |Apache/2.4.23 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.17   |200   |Apache/2.2.34 (Unix)|CLink Office v2               |
+----------------+------+--------------------+------------------------------+
|203.124.10.20   |200   |Apache/2.4.23 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.8    |200   |Apache/2.4.20 (Unix)|DataPort Data Center          |
+----------------+------+--------------------+------------------------------+
|203.124.10.27   |200   |Apache/2.2.22 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.25   |200   |CherryPy/5.1.0      |package repository            |
+----------------+------+--------------------+------------------------------+
|203.124.10.28   |200   |Apache/2.2.22 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.30   |503   |Apache/2.4.23 (Unix)|503 Service Unavailable       |
+----------------+------+--------------------+------------------------------+
|203.124.10.32   |200   |Apache/2.2.22 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
```

```
|203.124.10.190  |200   |Apache/2.2.34 (Unix)|phpMyAdmin                    |
+----------------+------+--------------------+------------------------------+
|203.124.10.192  |500   |Microsoft-IIS/8.5   |執行階段錯誤                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.196  |200   |Apache/2.2.29 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.198  |200   |Apache/2.2.29 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.199  |200   |Apache/2.2.29 (Unix)|CLink Office v2               |
+----------------+------+--------------------+------------------------------+
|203.124.10.200  |200   |Apache/2.2.29 (Unix)|Walton Brown Group: A Full Ser|
+----------------+------+--------------------+------------------------------+
|203.124.10.203  |403   |Microsoft-IIS/8.5   |IIS 8.5 詳細錯誤 - 403.14 - Forbid|
+----------------+------+--------------------+------------------------------+
|203.124.10.205  |200   |Apache/2.2.22 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.208  |403   |Microsoft-IIS/6.0   |Error</title></head><body><hea|
+----------------+------+--------------------+------------------------------+
|203.124.10.209  |403   |Microsoft-IIS/6.0   |Error</title></head><body><hea|
+----------------+------+--------------------+------------------------------+
|203.124.10.210  |200   |Microsoft-IIS/7.5   |IIS7                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.216  |200   |Apache/2.4.23 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.220  |403   |Microsoft-IIS/8.5   |IIS 8.5 詳細錯誤 - 403.14 - Forbid|
+----------------+------+--------------------+------------------------------+
|203.124.10.221  |200   |Apache/2.2.29 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.226  |200   |Microsoft-IIS/7.5   |IIS7                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.227  |403   |Microsoft-IIS/8.5   |IIS 8.5 詳細錯誤 - 403.14 - Forbid|
+----------------+------+--------------------+------------------------------+
|203.124.10.229  |503   |Microsoft-HTTPAPI/2.|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.231  |200   |Apache/2.2.29 (Unix)|None                          |
+----------------+------+--------------------+------------------------------+
|203.124.10.232  |200   |Apache/2.2.29 (Unix)|CLink Office v2               |
```

0x04 存活扫描

```
for /l %i in (1,1,255) do @ping 192.168.1.%i -w 1 -n 1 | find /i "ttl"
```

```
C:\Users\user2\Desktop>for /l %i in (1,1,255) do @ping 192.168.111.%i -w 1 -n 1 | find /i "ttl"
来自 192.168.111.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.111.129 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.111.134 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.111.135 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.111.147 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.111.2 的回复: 字节=32 时间<1ms TTL=128
```