专注APT攻击与防御

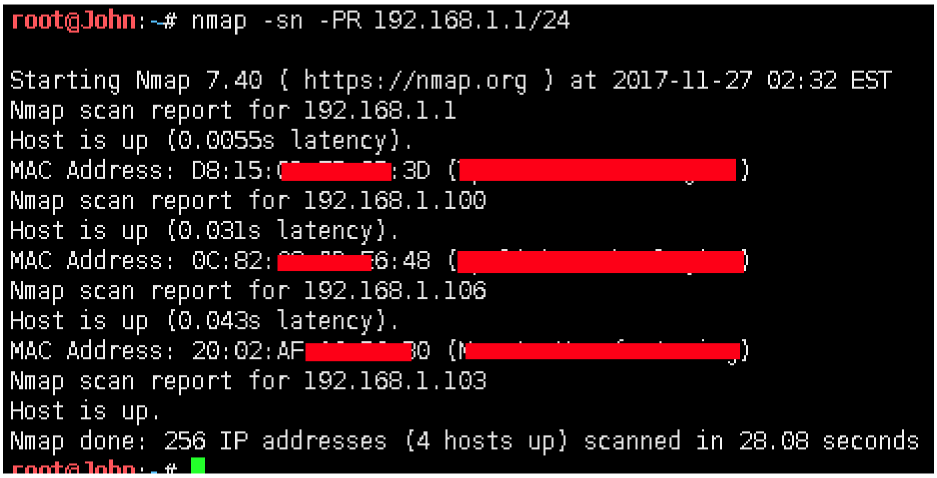
https://micropoor.blogspot.com/

## ARP简介：

ARP,通过解析网路层地址来找寻数据链路层地址的一个在网络协议包中极其重要的网络传输协议。根据IP地址获取物理地址的一个TCP/IP协议。主机发送信息时将包含目标IP地址的ARP请求广播到网络上的所有主机，并接收返回消息，以此确定目标的物理地址

## 1.nmap扫描

**root@John:~**# nmap -sn -PR 192.168.1.1/24



```
root@John:~# nmap -sn -PR 192.168.1.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-11-27 02:32 EST
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
MAC Address: D8:15:[redacted]:3D ([redacted])
Nmap scan report for 192.168.1.100
Host is up (0.031s latency).
MAC Address: 0C:82:[redacted]6:48 ([redacted])
Nmap scan report for 192.168.1.106
Host is up (0.043s latency).
MAC Address: 20:02:AF[redacted]0 ([redacted])
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.08 seconds
root@John:~# 
```

## 2.msf扫描

msf > use  auxiliary/scanner/discovery/arp_sweep

msf auxiliary(**arp_sweep**) > show options

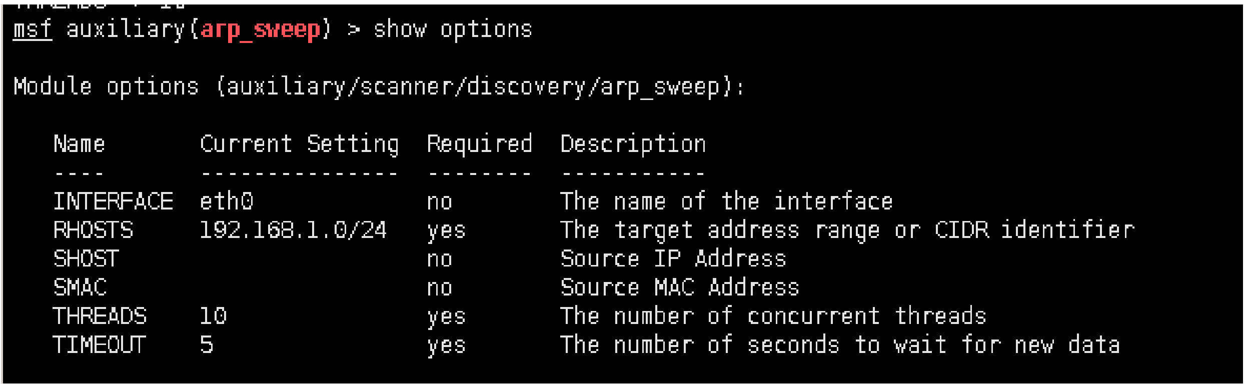
Module options (auxiliary/scanner/discovery/arp_sweep):

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   RHOSTS                      yes       The target address range or CIDR identifier
   SHOST                       no        Source IP Address
   SMAC                        no        Source MAC Address
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    5                yes       The number of seconds to wait for new data
```

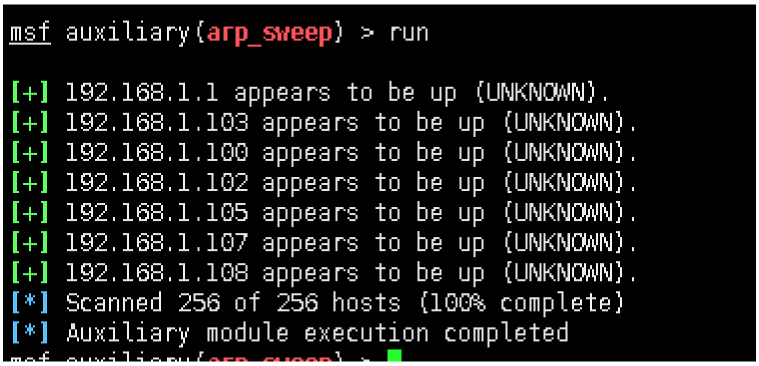
msf auxiliary(**arp_sweep**) > set RHOSTS 192.168.1.0/24

RHOSTS => 192.168.1.0/24

msf auxiliary(arp_sweep) > set THREADS 10



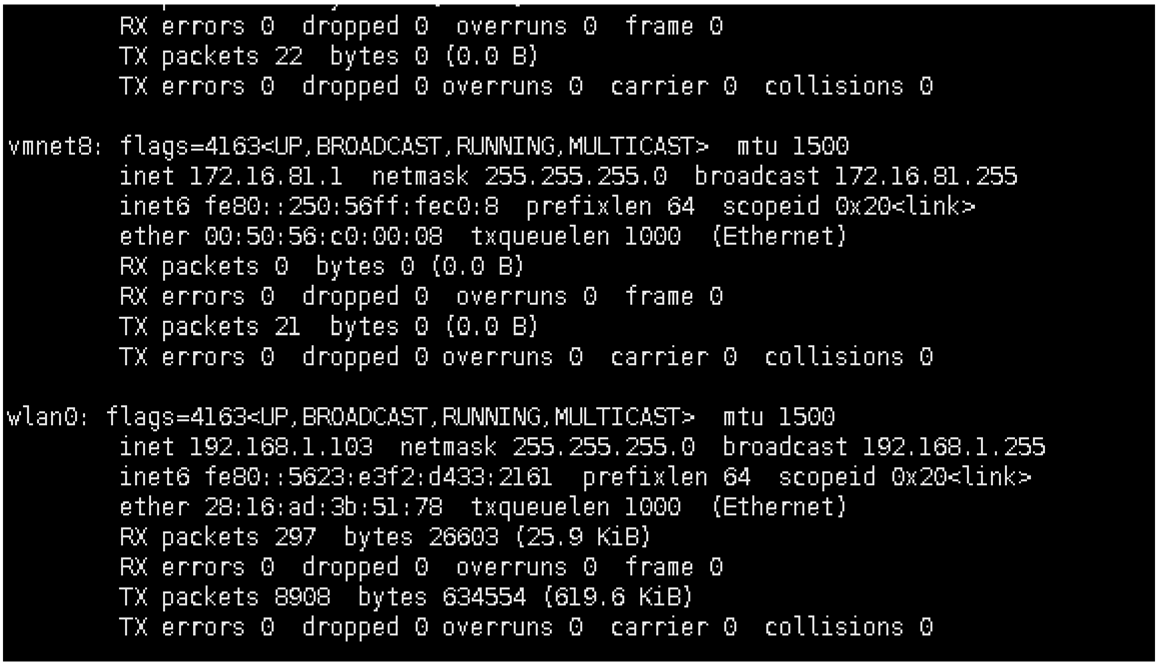
```
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE  eth0             no        The name of the interface
   RHOSTS     192.168.1.0/24   yes       The target address range or CIDR identifier
   SHOST                       no        Source IP Address
   SMAC                        no        Source MAC Address
   THREADS    10               yes       The number of concurrent threads
   TIMEOUT    5                yes       The number of seconds to wait for new data
```



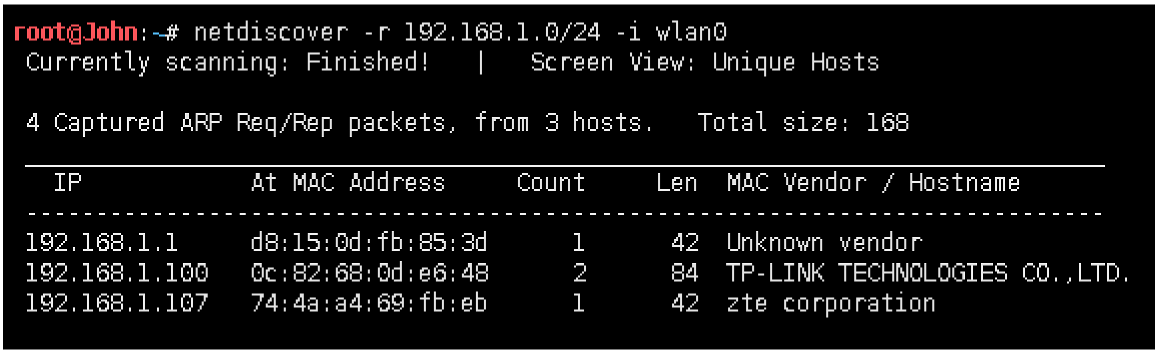
```
msf auxiliary(arp_sweep) > run

[+] 192.168.1.1 appears to be up (UNKNOWN).
[+] 192.168.1.103 appears to be up (UNKNOWN).
[+] 192.168.1.100 appears to be up (UNKNOWN).
[+] 192.168.1.102 appears to be up (UNKNOWN).
[+] 192.168.1.105 appears to be up (UNKNOWN).
[+] 192.168.1.107 appears to be up (UNKNOWN).
[+] 192.168.1.108 appears to be up (UNKNOWN).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(arp_sweep) >
```

## 3.netdiscover

**root@John:~**# netdiscover -r 192.168.1.0/24 -i wlan0



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.81.1  netmask 255.255.255.0  broadcast 172.16.81.255
        inet6 fe80::250:56ff:fec0:8  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:08  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.103  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::5623:e3f2:d433:2161  prefixlen 64  scopeid 0x20<link>
        ether 28:16:ad:3b:51:78  txqueuelen 1000  (Ethernet)
        RX packets 297  bytes 26603 (25.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8908  bytes 634554 (619.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



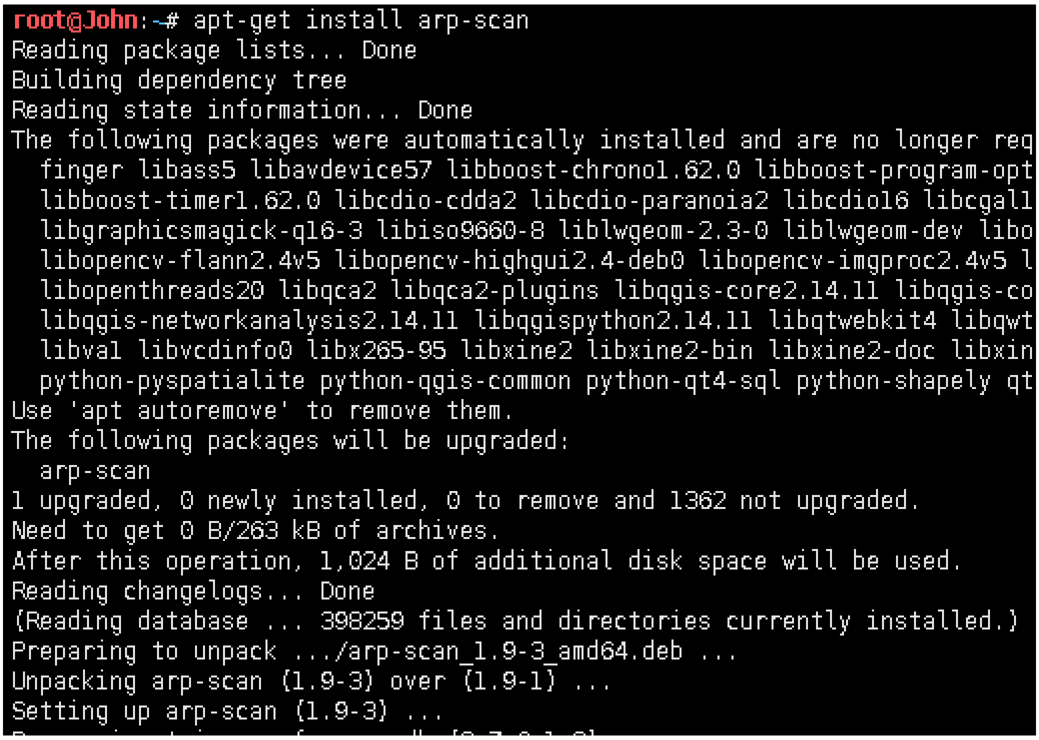
```
root@John:~# netdiscover -r 192.168.1.0/24 -i wlan0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 168
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     d8:15:0d:fb:85:3d      1      42  Unknown vendor
 192.168.1.100   0c:82:68:0d:e6:48      2      84  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.1.107   74:4a:a4:69:fb:eb      1      42  zte corporation
```

## 4.arp-scan（linux）

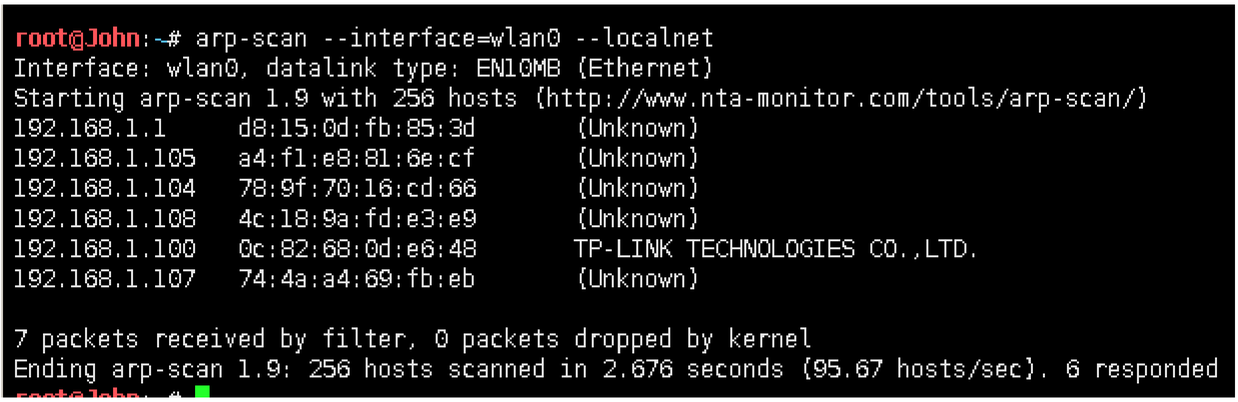
**(推荐)**速度与快捷

项目地址：https://linux.die.net/man/1/arp-scan

arp-scan没有内置kali，需要下载安装。



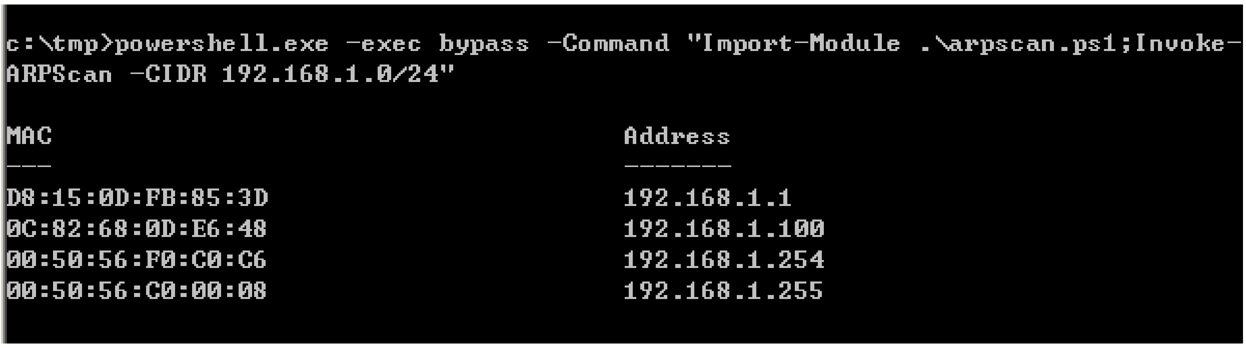
```
root@John:~# apt-get install arp-scan
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer req
  finger libass5 libavdevice57 libboost-chrono1.62.0 libboost-program-opt
  libboost-timer1.62.0 libcdio-cdda2 libcdio-paranoia2 libcdio16 libcgal1
  libgraphicsmagick-q16-3 libiso9660-8 liblwgeom-2.3-0 liblwgeom-dev libo
  libopencv-flann2.4v5 libopencv-highgui2.4-deb0 libopencv-imgproc2.4v5 l
  libopenthreads20 libqca2 libqca2-plugins libqgis-core2.14.11 libqgis-co
  libqgis-networkanalysis2.14.11 libqgispython2.14.11 libqtwebkit4 libqwt
  libval libvcdinfo0 libx265-95 libxine2 libxine2-bin libxine2-doc libxin
  python-pyspatialite python-qgis-common python-qt4-sql python-shapely qt
Use 'apt autoremove' to remove them.
The following packages will be upgraded:
  arp-scan
1 upgraded, 0 newly installed, 0 to remove and 1362 not upgraded.
Need to get 0 B/263 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Reading changelogs... Done
(Reading database ... 398259 files and directories currently installed.)
Preparing to unpack .../arp-scan_1.9-3_amd64.deb ...
Unpacking arp-scan (1.9-3) over (1.9-1) ...
Setting up arp-scan (1.9-3) ...
```



```
root@John:~# arp-scan --interface=wlan0 --localnet
Interface: wlan0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.1     d8:15:0d:fb:85:3d       (Unknown)
192.168.1.105   a4:f1:e8:81:6e:cf       (Unknown)
192.168.1.104   78:9f:70:16:cd:66       (Unknown)
192.168.1.108   4c:18:9a:fd:e3:e9       (Unknown)
192.168.1.100   0c:82:68:0d:e6:48       TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.107   74:4a:a4:69:fb:eb       (Unknown)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.676 seconds (95.67 hosts/sec). 6 responded
```

## 5.Powershell

c:\tmp>powershell.exe -exec bypass -Command "Import-Module .\arpscan.ps1;Invoke-
ARPScan -CIDR 192.168.1.0/24"

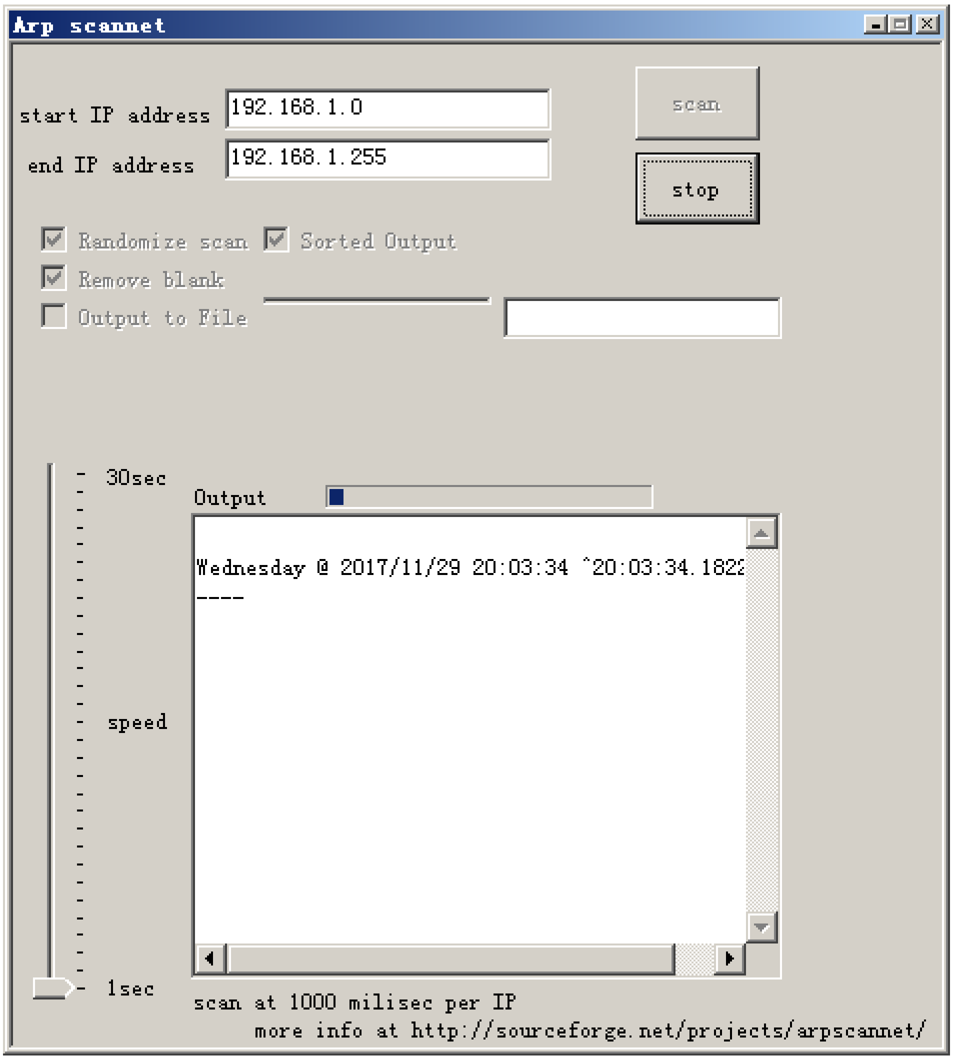


```
c:\tmp>powershell.exe -exec bypass -Command "Import-Module .\arpscan.ps1;Invoke-
ARPScan -CIDR 192.168.1.0/24"

MAC                                       Address
---                                       -------
D8:15:0D:FB:85:3D                         192.168.1.1
0C:82:68:0D:E6:48                         192.168.1.100
00:50:56:F0:C0:C6                         192.168.1.254
00:50:56:C0:00:08                         192.168.1.255
```

## 6.arp scannet

项目地址：

https://sourceforge.net/projects/arpscannet/files/arpscannet/arpscannet%200.4/



start IP address 192.168.1.0

end IP address 192.168.1.255

☑ Randomize scan ☑ Sorted Output

☑ Remove blank

□ Output to File

```
Wednesday @ 2017/11/29 20:03:34 ^20:03:34.1822
----
```

scan at 1000 milisec per IP

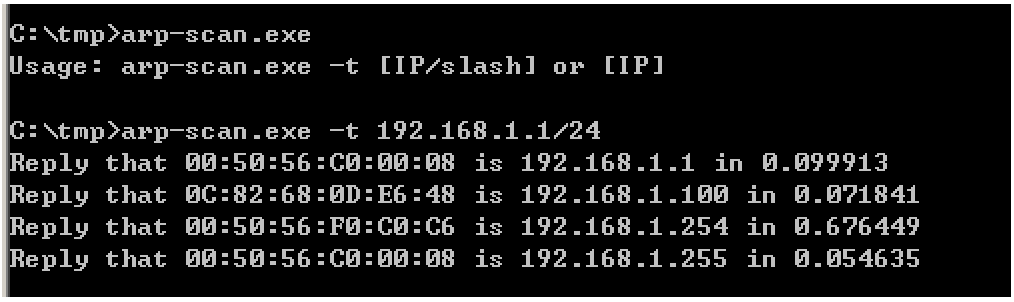
more info at http://sourceforge.net/projects/arpscannet/

## 7.arp-scan（windows）

(推荐)速度与快捷

arp-scan.exe -t 192.168.1.1/24

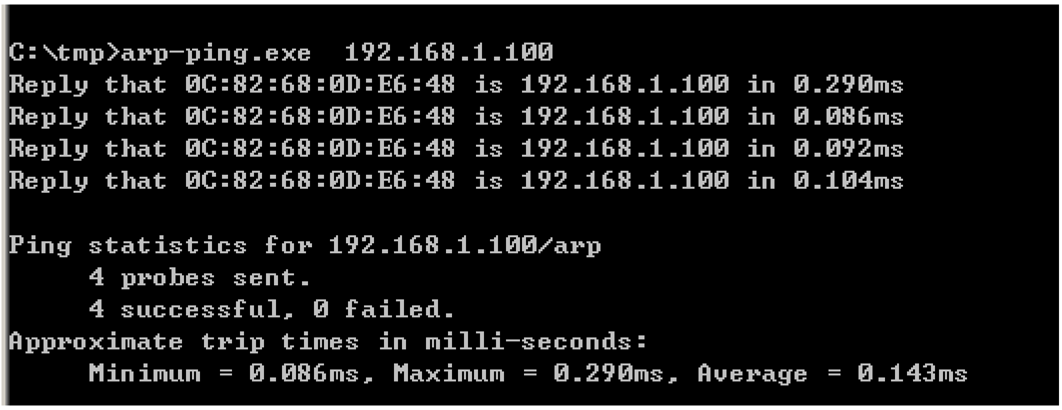
项目地址：https://github.com/QbsuranAlang/arp-scan-windows-/tree/master/arp-scan（非官方）



```
C:\tmp>arp-scan.exe
Usage: arp-scan.exe -t [IP/slash] or [IP]

C:\tmp>arp-scan.exe -t 192.168.1.1/24
Reply that 00:50:56:C0:00:08 is 192.168.1.1 in 0.099913
Reply that 0C:82:68:0D:E6:48 is 192.168.1.100 in 0.071841
Reply that 00:50:56:F0:C0:C6 is 192.168.1.254 in 0.676449
Reply that 00:50:56:C0:00:08 is 192.168.1.255 in 0.054635
```

## 8.arp-ping.exe

arp-ping.exe  192.168.1.100



```
C:\tmp>arp-ping.exe  192.168.1.100
Reply that 0C:82:68:0D:E6:48 is 192.168.1.100 in 0.290ms
Reply that 0C:82:68:0D:E6:48 is 192.168.1.100 in 0.086ms
Reply that 0C:82:68:0D:E6:48 is 192.168.1.100 in 0.092ms
Reply that 0C:82:68:0D:E6:48 is 192.168.1.100 in 0.104ms

Ping statistics for 192.168.1.100/arp
     4 probes sent.
     4 successful, 0 failed.
Approximate trip times in milli-seconds:
     Minimum = 0.086ms, Maximum = 0.290ms, Average = 0.143ms
```

## 9.其他

如cain的arp发现，一些开源py，pl脚本等，不一一介绍。

## 附录：

以上非内置文件网盘位置。**后门自查**。

链接：https://pan.baidu.com/s/1boYuraJ 密码：58wf

- Micropoor