

专注APT攻击与防御

<https://micropoor.blogspot.com/>

注：请多喝点热水或者凉白开，可预防**肾结石**，**痛风**等。

痛风可伴发肥胖症、高血压病、糖尿病、脂代谢紊乱等多种代谢性疾病。

攻击机： 192.168.1.5 Debian

靶机： 192.168.1.2 Windows 7

192.168.1.115 Windows 2003

192.168.1.119 Windows 2003

第一季主要介绍scanner下的五个模块，辅助发现内网存活主机，分别为：

- auxiliary/scanner/discovery/arp_sweep
- auxiliary/scanner/discovery/udp_sweep
- auxiliary/scanner/ftp/ftp_version
- auxiliary/scanner/http/http_version
- auxiliary/scanner/smb/smb_version

第二季主要介绍scanner下的五个模块，辅助发现内网存活主机，分别为：

- auxiliary/scanner/ssh/ssh_version
- auxiliary/scanner/telnet/telnet_version
- auxiliary/scanner/discovery/udp_probe
- auxiliary/scanner/dns/dns_amp
- auxiliary/scanner/mysql/mysql_version

- **六：**基于auxiliary/scanner/ssh/ssh_version发现SSH服务

```
1 msf auxiliary(scanner/ssh/ssh_version) > show options
2
3 Module options (auxiliary/scanner/ssh/ssh_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  RPORT 22 yes The target port (TCP)
9  THREADS 50 yes The number of concurrent threads
10 TIMEOUT 30 yes Timeout for the SSH probe
11
12 msf auxiliary(scanner/ssh/ssh_version) > exploit
13
14 [+] 192.168.1.5:22 - SSH server version: SSH-2.0-OpenSSH_7.9p1 Debian-
5 ( service.version=7.9p1 openssh.comment=Debian-5 service.vendor=OpenBSD
service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:open
sd:openssh:7.9p1 os.vendor=Debian os.family=Linux os.product=Linux os.cpe
23=cpe:/o:debian:debian_linux:- service.protocol=ssh fingerprint_db=ssh.b
anner )
15 [*] Scanned 52 of 256 hosts (20% complete)
16 [*] Scanned 95 of 256 hosts (37% complete)
17 [*] Scanned 100 of 256 hosts (39% complete)
18 [*] Scanned 103 of 256 hosts (40% complete)
19 [*] Scanned 131 of 256 hosts (51% complete)
20 [*] Scanned 154 of 256 hosts (60% complete)
21 [*] Scanned 180 of 256 hosts (70% complete)
22 [*] Scanned 206 of 256 hosts (80% complete)
23 [*] Scanned 235 of 256 hosts (91% complete)
24 [*] Scanned 256 of 256 hosts (100% complete)
25 [*] Auxiliary module execution completed

```

```

msf auxiliary(scanner/ssh/ssh_version) > show options
Module options (auxiliary/scanner/ssh/ssh_version):
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.1.0/24  yes      The target address range or CIDR identifier
RPORT     22               yes      The target port (TCP)
THREADS   50               yes      The number of concurrent threads
TIMEOUT   30               yes      Timeout for the SSH probe

msf auxiliary(scanner/ssh/ssh_version) > exploit
[+] 192.168.1.5:22 - SSH server version: SSH-2.0-OpenSSH_7.9p1 Debian-5 ( service.version=7.9p1 openssh.c
y=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:7.9p1 os.vendor=Debian os.family=Linux os
service.protocol=ssh fingerprint_db=ssh.banner )
[*] Scanned 52 of 256 hosts (20% complete)
[*] Scanned 95 of 256 hosts (37% complete)
[*] Scanned 100 of 256 hosts (39% complete)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 131 of 256 hosts (51% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 206 of 256 hosts (80% complete)
[*] Scanned 235 of 256 hosts (91% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```

- 七：基于auxiliary/scanner/telnet/telnet_version发现TELNET服务

```

1 msf auxiliary(scanner/telnet/telnet_version) > show options
2
3 Module options (auxiliary/scanner/telnet/telnet_version):
4
5 Name Current Setting Required Description
6 -----
7 PASSWORD no The password for the specified username
8 RHOSTS 192.168.1.119 yes The target address range or CIDR identifier
9 RPORT 23 yes The target port (TCP)
10 THREADS 50 yes The number of concurrent threads
11 TIMEOUT 30 yes Timeout for the Telnet probe
12 USERNAME no The username to authenticate as
13
14 msf auxiliary(scanner/telnet/telnet_version) > exploit
15
16 [+] 192.168.1.119:23 - 192.168.1.119:23 TELNET Welcome to Microsoft Te
lnet Service \x0a\x0a\x0dlogin:
17 [*] Scanned 1 of 1 hosts (100% complete)
18 [*] Auxiliary module execution completed

```

```

msf auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
Name      Current Setting  Required  Description
-----
PASSWORD  no               no       The password for the specified username
RHOSTS    192.168.1.119   yes      The target address range or CIDR identifier
RPORT     23              yes      The target port (TCP)
THREADS   50              yes      The number of concurrent threads
TIMEOUT   30              yes      Timeout for the Telnet probe
USERNAME  no              no       The username to authenticate as

msf auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.1.119:23 - 192.168.1.119:23 TELNET Welcome to Microsoft Telnet Service \x0a\x0a\x0dlogin:
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

- 八：基于scanner/discovery/udp_probe发现内网存活主机

```

1 msf auxiliary(scanner/discovery/udp_probe) > show options
2
3 Module options (auxiliary/scanner/discovery/udp_probe):
4
5 Name Current Setting Required Description
6 -----
7 CHOST no The local client address

```

```

8  RHOSTS 192.168.1.0/24 yes The target address range or CIDR identifier
9  THREADS 50 yes The number of concurrent threads
10
11 msf auxiliary(scanner/discovery/udp_probe) > exploit
12
13 [+] Discovered NetBIOS on 192.168.1.2:137 (JOHN-PC:<00>:U :WORKGROUP:
<00>:G :JOHN-PC:<20>:U :WORKGROUP:<1e>:G :WORKGROUP:<1d>:U :__MSBROWSE__
<01>:G :4c:cc:6a:e3:51:27)
14 [+] Discovered DNS on 192.168.1.1:53 (de778500000100010000000007564552
53494f4e0442494e440000100003c00c0010000300000001001a19737572656c7920796f:
5206d757374206265206a6f6b696e67)
15 [*] Scanned 43 of 256 hosts (16% complete)
16 [*] Scanned 52 of 256 hosts (20% complete)
17 [*] Scanned 89 of 256 hosts (34% complete)
18 [+] Discovered NetBIOS on 192.168.1.119:137 (WIN03X64:<00>:U :WIN03X6
4:<20>:U :WORKGROUP:<00>:G :WORKGROUP:<1e>:G :WIN03X64:<03>:U :ADMINISTR
TOR:<03>:U :WIN03X64:<01>:U :00:0c:29:85:d6:7d)
19 [*] Scanned 103 of 256 hosts (40% complete)
20 [*] Scanned 140 of 256 hosts (54% complete)
21 [*] Scanned 163 of 256 hosts (63% complete)
22 [*] Scanned 184 of 256 hosts (71% complete)
23 [*] Scanned 212 of 256 hosts (82% complete)
24 [*] Scanned 231 of 256 hosts (90% complete)
25 [*] Scanned 256 of 256 hosts (100% complete)
26 [*] Auxiliary module execution completed

```

```

msf auxiliary(scanner/discovery/udp_probe) > show options
Module options (auxiliary/scanner/discovery/udp_probe):
  Name      Current Setting  Required  Description
  ----      -
  CHOST     192.168.1.0/24  no        The local client address
  RHOSTS    192.168.1.0/24  yes       The target address range or CIDR identifier
  THREADS   50               yes       The number of concurrent threads

msf auxiliary(scanner/discovery/udp_probe) > exploit
[+] Discovered NetBIOS on 192.168.1.2:137 (JOHN-PC:<00>:U :WORKGROUP:<00>:G :JOHN-PC:<20>:U :WORKGROUP:<
1e>:G :WORKGROUP:<1d>:U :__MSBROWSE__<01>:G :4c:cc:6a:e3:51:27)
[+] Discovered DNS on 192.168.1.1:53 (de77850000010001000000000756455253494f4e0442494e440000100003c00c00
6f6b696e67)
[*] Scanned 43 of 256 hosts (16% complete)
[*] Scanned 52 of 256 hosts (20% complete)
[*] Scanned 89 of 256 hosts (34% complete)
[+] Discovered NetBIOS on 192.168.1.119:137 (WIN03X64:<00>:U :WIN03X64:<20>:U :WORKGROUP:<00>:G :WORKGR
01>:U :00:0c:29:85:d6:7d)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 140 of 256 hosts (54% complete)
[*] Scanned 163 of 256 hosts (63% complete)
[*] Scanned 184 of 256 hosts (71% complete)
[*] Scanned 212 of 256 hosts (82% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```

- 九：基于auxiliary/scanner/dns/dns_amp发现内网存活主机

```
1 msf auxiliary(scanner/dns/dns_amp) > show options
2
3 Module options (auxiliary/scanner/dns/dns_amp):
4
5 Name Current Setting Required Description
6 -----
7 BATCHSIZE 256 yes The number of hosts to probe in each set
8 DOMAINNAME isc.org yes Domain to use for the DNS request
9 FILTER no The filter string for capturing traffic
10 INTERFACE no The name of the interface
11 PCAPFILE no The name of the PCAP capture file to process
12 QUERYTYPE ANY yes Query type(A, NS, SOA, MX, TXT, AAAA, RRSIG,
13 DNSKEY, ANY)
14 RHOSTS 192.168.1.0/24 yes The target address range or CIDR identifier
15 RPORT 53 yes The target port (UDP)
16 SNAPLEN 65535 yes The number of bytes to capture
17 THREADS 50 yes The number of concurrent threads
18 TIMEOUT 500 yes The number of seconds to wait for new data
19
20 msf auxiliary(scanner/dns/dns_amp) > exploit
21 [*] Sending DNS probes to 192.168.1.0->192.168.1.255 (256 hosts)
22 [*] Sending 67 bytes to each host using the IN ANY isc.org request
23 [+] 192.168.1.1:53 - Response is 530 bytes [7.91x Amplification]
24 [*] Scanned 256 of 256 hosts (100% complete)
25 [*] Auxiliary module execution completed
```

```

msf auxiliary(scanner/dns/dns_amp) > show options

Module options (auxiliary/scanner/dns/dns_amp):

  Name      Current Setting  Required  Description
  ----      -
  BATCHSIZE 256              yes       The number of hosts to probe in each set
  DOMAINNAME isc.org          yes       Domain to use for the DNS request
  FILTER     no               no        The filter string for capturing traffic
  INTERFACE  no               no        The name of the interface
  PCAPFILE   no               no        The name of the PCAP capture file to process
  QUERYTYPE  ANY              yes       Query type(A, NS, SOA, MX, TXT, AAAA, RRSIG, DNSKEY, ANY)
  RHOSTS     192.168.1.0/24  yes       The target address range or CIDR identifier
  RPORT      53               yes       The target port (UDP)
  SNAPLEN   65535            yes       The number of bytes to capture
  THREADS    50               yes       The number of concurrent threads
  TIMEOUT    500              yes       The number of seconds to wait for new data

msf auxiliary(scanner/dns/dns_amp) > exploit

[*] Sending DNS probes to 192.168.1.0->192.168.1.255 (256 hosts)
[*] Sending 67 bytes to each host using the IN ANY isc.org request
[+] 192.168.1.1:53 - Response is 530 bytes [7.91x Amplification]
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```

- 十：基于auxiliary/scanner/mysql/mysql_version发现mysql服务

```

1 msf auxiliary(scanner/mysql/mysql_version) > show options
2
3 Module options (auxiliary/scanner/mysql/mysql_version):
4
5 Name Current Setting Required Description
6 ---- -
7 RHOSTS 192.168.1.115 yes The target address range or CIDR identifier
8 RPORT 3306 yes The target port (TCP)
9 THREADS 50 yes The number of concurrent threads
10
11 msf auxiliary(scanner/mysql/mysql_version) > exploit
12
13 [+] 192.168.1.115:3306 - 192.168.1.115:3306 is running MySQL 5.1.52-community (protocol 10)
14 [*] Scanned 1 of 1 hosts (100% complete)
15 [*] Auxiliary module execution completed

```

```
msf auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.115   yes       The target address range or CIDR identifier
  RPORT     3306             yes       The target port (TCP)
  THREADS   50               yes       The number of concurrent threads

msf auxiliary(scanner/mysql/mysql_version) > exploit

[+] 192.168.1.115:3306 - 192.168.1.115:3306 is running MySQL 5.1.52-community (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Micropoor