

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，通风等。

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

192.168.1.119 Windows 2003

MSF的search支持type搜索：

```
1 msf > search scanner type:auxiliary
2
3 Matching Modules
4 =====
5
6 Name Disclosure Date Rank Check Description
7 ---- -
8 auxiliary/admin/appletv/appletv_display_image normal No Apple TV Image Remote Control
9 auxiliary/admin/appletv/appletv_display_video normal No Apple TV Video Remote Control
10 auxiliary/admin/smb/check_dir_file normal Yes SMB Scanner Check File/Directory Utility
11 auxiliary/admin/teradata/teradata_odbc_sql 2018-03-29 normal Yes Teradata ODBC SQL Query Module
12 auxiliary/bnat/bnat_scan normal Yes BNAT Scanner
13 auxiliary/gather/citrix_published_applications normal No Citrix MetaFrame ICA Published Applications Scanner
14 auxiliary/gather/enum_dns normal No DNS Record Scanner and Enumerator
15 ....
16 auxiliary/scanner/winrm/winrm_cmd normal Yes WinRM Command Runner
17 auxiliary/scanner/winrm/winrm_login normal Yes WinRM Login Utility
18 auxiliary/scanner/winrm/winrm_wql normal Yes WinRM WQL Query Runner
19 auxiliary/scanner/wproxy/att_open_proxy 2017-08-31 normal Yes Open WAN-to-LAN proxy on AT&T routers
20 auxiliary/scanner/wsdd/wsdd_query normal Yes WS-Discovery Information Discovery
21 auxiliary/scanner/x11/open_x11 normal Yes X11 No-Auth Scanner
```

```
msf > search scanner type:auxiliary

Matching Modules
=====

Name                                     Disclosure Date Rank  Check Description
-----
auxiliary/admin/appletv/appletv_display_image normal No    Apple TV Image Remote Control
auxiliary/admin/appletv/appletv_display_video normal No    Apple TV Video Remote Control
auxiliary/admin/smb/check_dir_file       normal Yes   SMB Scanner Check File/Directory L
auxiliary/admin/teradata/teradata_odbc_sql 2018-03-29 normal Yes   Teradata ODBC SQL Query Module
auxiliary/bnat/bnat_scan                  normal Yes   BNAT Scanner
auxiliary/gather/citrix_published_applications normal No    Citrix MetaFrame ICA Published App
auxiliary/gather/enum_dns                  normal No    DNS Record Scanner and Enumerator
auxiliary/gather/hp_enum_perfd             normal Yes   HP Operations Manager Perfd Enviro
auxiliary/gather/natpmp_external_address   normal Yes   NAT-PMP External Address Scanner
auxiliary/gather/windows_deployment_services_shares normal Yes   Microsoft Windows Deployment Servi
auxiliary/scanner/acpp/login               normal Yes   Apple Airport ACPP Authentication
auxiliary/scanner/afn/afn_login            normal Yes   Apple Filing Protocol Login Utilit
```

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
- 一：基于scanner/http/http_version发现HTTP服务

```
1 msf auxiliary(scanner/http/http_version) > show options
2
3 Module options (auxiliary/scanner/http/http_version):
4
5 Name Current Setting Required Description
6 ----
7 Proxies no A proxy chain of format type:host:port[,type:host:port]
8 [...]
9 RHOSTS 192.168.1.0/24 yes The target address range or CIDR identifier
10 RPORT 80 yes The target port (TCP)
11 SSL false no Negotiate SSL/TLS for outgoing connections
12 THREADS 20 yes The number of concurrent threads
13 VHOST no HTTP server virtual host
14
15 msf auxiliary(scanner/http/http_version) > exploit
16
17 [+] 192.168.1.1:80
18 [*] Scanned 27 of 256 hosts (10% complete)
```

```

18 [*] Scanned 63 of 256 hosts (24% complete)
19 [*] Scanned 82 of 256 hosts (32% complete)
20 [*] Scanned 103 of 256 hosts (40% complete)
21 [+] 192.168.1.119:80 Microsoft-IIS/6.0 ( Powered by ASP.NET )
22 [*] Scanned 129 of 256 hosts (50% complete)
23 [*] Scanned 154 of 256 hosts (60% complete)
24 [*] Scanned 182 of 256 hosts (71% complete)
25 [*] Scanned 205 of 256 hosts (80% complete)
26 [*] Scanned 231 of 256 hosts (90% complete)
27 [*] Scanned 256 of 256 hosts (100% complete)
28 [*] Auxiliary module execution completed
29

```

```

msf auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):
  Name      Current Setting  Required  Description
  ----      -
  Proxies   .                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    192.168.1.0/24  yes       The target address range or CIDR identifier
  RPORT     80               yes       The target port (TCP)
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  THREADS   20               yes       The number of concurrent threads
  VHOST     .                no        HTTP server virtual host

msf auxiliary(scanner/http/http_version) > exploit
[+] 192.168.1.1:80
[*] Scanned 27 of 256 hosts (10% complete)
[*] Scanned 63 of 256 hosts (24% complete)
[*] Scanned 82 of 256 hosts (32% complete)
[*] Scanned 103 of 256 hosts (40% complete)
[+] 192.168.1.119:80 Microsoft-IIS/6.0 ( Powered by ASP.NET )
[*] Scanned 129 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 182 of 256 hosts (71% complete)
[*] Scanned 205 of 256 hosts (80% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```

- 二：基于scanner/smb/smb_version发现SMB服务

```

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 20 yes The number of concurrent threads
12
13 msf auxiliary(scanner/smb/smb_version) > exploit
14
15 [+] 192.168.1.2:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:JOHN-PC) (workgroup:WORKGROUP )
16 [*] Scanned 40 of 256 hosts (15% complete)
17 [*] Scanned 60 of 256 hosts (23% complete)
18 [*] Scanned 79 of 256 hosts (30% complete)
19 [+] 192.168.1.119:445 - Host is running Windows 2003 R2 SP2 (build:3790) (name:WIN03X64)
20 [*] Scanned 103 of 256 hosts (40% complete)
21 [*] Scanned 128 of 256 hosts (50% complete)
22 [*] Scanned 154 of 256 hosts (60% complete)
23 [*] Scanned 181 of 256 hosts (70% complete)
24 [*] Scanned 206 of 256 hosts (80% complete)
25 [*] Scanned 231 of 256 hosts (90% complete)
26 [*] Scanned 256 of 256 hosts (100% complete)
27 [*] Auxiliary module execution completed
28

```

```

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   20              yes       The number of concurrent threads

msf auxiliary(scanner/smb/smb_version) > exploit
[+] 192.168.1.2:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name: ) (workgroup:WORKGROUP )
[*] Scanned 40 of 256 hosts (15% complete)
[*] Scanned 60 of 256 hosts (23% complete)
[*] Scanned 79 of 256 hosts (30% complete)
[+] 192.168.1.119:445 - Host is running Windows 2003 R2 SP2 (build:3790) (name:WIN03X64)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 128 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 181 of 256 hosts (70% complete)
[*] Scanned 206 of 256 hosts (80% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```

- 三：基于scanner/ftp/ftp_version发现FTP服务

```

1 msf auxiliary(scanner/ftp/ftp_version) > show options
2

```

```
3 Module options (auxiliary/scanner/ftp/ftp_version):
4
5 Name Current Setting Required Description
6 ----
7 FTPPASS mozilla@example.com no The password for the specified username
8 FTPUSER anonymous no The username to authenticate as
9 RHOSTS 192.168.1.0/24 yes The target address range or CIDR identifier
10 RPORT 21 yes The target port (TCP)
11 THREADS 50 yes The number of concurrent threads
12
13 msf auxiliary(scanner/ftp/ftp_version) > exploit
14
15 [*] Scanned 51 of 256 hosts (19% complete)
16 [*] Scanned 52 of 256 hosts (20% complete)
17 [*] Scanned 100 of 256 hosts (39% complete)
18 [+] 192.168.1.119:21 - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
19 [*] Scanned 103 of 256 hosts (40% complete)
20 [*] Scanned 133 of 256 hosts (51% complete)
21 [*] Scanned 183 of 256 hosts (71% complete)
22 [*] Scanned 197 of 256 hosts (76% complete)
23 [*] Scanned 229 of 256 hosts (89% 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/ftp/ftp_version) > show options

Module options (auxiliary/scanner/ftp/ftp_version):

  Name      Current Setting      Required  Description
  ----      -
  FTPPASS   mozilla@example.com  no        The password for the specified username
  FTPUSER   anonymous             no        The username to authenticate as
  RHOSTS    192.168.1.0/24       yes       The target address range or CIDR identifier
  RPORT     21                   yes       The target port (TCP)
  THREADS   50                   yes       The number of concurrent threads

msf auxiliary(scanner/ftp/ftp_version) > exploit

[*] Scanned 51 of 256 hosts (19% complete)
[*] Scanned 52 of 256 hosts (20% complete)
[*] Scanned 100 of 256 hosts (39% complete)
[+] 192.168.1.119:21 - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 133 of 256 hosts (51% complete)
[*] Scanned 183 of 256 hosts (71% complete)
[*] Scanned 197 of 256 hosts (76% complete)
[*] Scanned 229 of 256 hosts (89% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```

- 四：基于scanner/discovery/arp_sweep发现内网存活主机

```

1 msf auxiliary(scanner/discovery/arp_sweep) > show options
2
3 Module options (auxiliary/scanner/discovery/arp_sweep):
4
5 Name Current Setting Required Description
6 ---- -
7 INTERFACE no The name of the interface
8 RHOSTS 192.168.1.0/24 yes The target address range or CIDR identifier
9 SHOST no Source IP Address
10 SMAC no Source MAC Address
11 THREADS 50 yes The number of concurrent threads
12 TIMEOUT 5 yes The number of seconds to wait for new data
13
14 msf auxiliary(scanner/discovery/arp_sweep) > exploit
15
16 [+] 192.168.1.1 appears to be up (UNKNOWN).
17 [+] 192.168.1.2 appears to be up (UNKNOWN).
18 [+] 192.168.1.119 appears to be up (VMware, Inc.).
19 [*] Scanned 256 of 256 hosts (100% complete)
20 [*] Auxiliary module execution completed
21

```

```
msf auxiliary(scanner/discovery/arp_sweep) > show options
Module options (auxiliary/scanner/discovery/arp_sweep):

  Name      Current Setting  Required  Description
  ----      -
INTERFACE  no               no        The name of the interface
RHOSTS     192.168.1.0/24  yes       The target address range or CIDR identifier
SHOST      no               no        Source IP Address
SMAC       no               no        Source MAC Address
THREADS    50              yes       The number of concurrent threads
TIMEOUT    5               yes       The number of seconds to wait for new data

msf auxiliary(scanner/discovery/arp_sweep) > exploit

[+] 192.168.1.1 appears to be up (UNKNOWN).
[+] 192.168.1.2 appears to be up (UNKNOWN).
[+] 192.168.1.119 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

- 五：基于scanner/discovery/udp_sweep发现内网存活主机

```
1 msf auxiliary(scanner/discovery/udp_sweep) > show options
2
3 Module options (auxiliary/scanner/discovery/udp_sweep):
4
5 Name Current Setting Required Description
6 ---- -
7 BATCHSIZE 256 yes The number of hosts to probe in each set
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_sweep) > exploit
12
13 [*] Sending 13 probes to 192.168.1.0->192.168.1.255 (256 hosts)
14 [*] Discovered DNS on 192.168.1.1:53 (ce2a850000100010000000007564552
53494f4e0442494e440000100003c00c0010000300000001001a19737572656c7920796f7
5206d757374206265206a6f6b696e67)
15 [*] 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)
16 [*] 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)
17 [*] Scanned 256 of 256 hosts (100% complete)
18 [*] Auxiliary module execution completed
19
```

```
msf auxiliary(scanner/discovery/udp_sweep) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  BATCHSIZE 256              yes       The number of hosts to probe in each set
  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_sweep) > exploit

[*] Sending 13 probes to 192.168.1.0->192.168.1.255 (256 hosts)
[*] Discovered DNS on 192.168.1.1:53 (ce2a850000010001000000000756455253494f4e04424946f6b696e67)
[*] Discovered NetBIOS on 192.168.1.2:137 (JOHN-PC:<00>;U :WORKGROUP:<00>;G :JOHN-PC:<51>;27)
[*] Discovered NetBIOS on 192.168.1.119:137 (WIN03X64:<00>;U :WIN03X64:<20>;U :WORKGR01:>;U :00:0c:29:85:d6:7d)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Micropoor