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：

```
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 Utility
 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 Applications Scanner
 auxiliary/gather/enum_dns normal No DNS Record Scanner and Enumerator
 ....
 auxiliary/scanner/winrm/winrm_cmd normal Yes WinRM Command Runner
 auxiliary/scanner/winrm/winrm_login normal Yes WinRM Login Utility
 auxiliary/scanner/winrm/winrm_wql normal Yes WinRM WQL Query Runner
 auxiliary/scanner/wproxy/att_open_proxy 2017-08-31 normal Yes Open WAN-to-LAN proxy on AT&T routers
 auxiliary/scanner/wsdd/wsdd_query normal Yes WS-Discovery Information Discovery
 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/afp/afp_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

```
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)
```

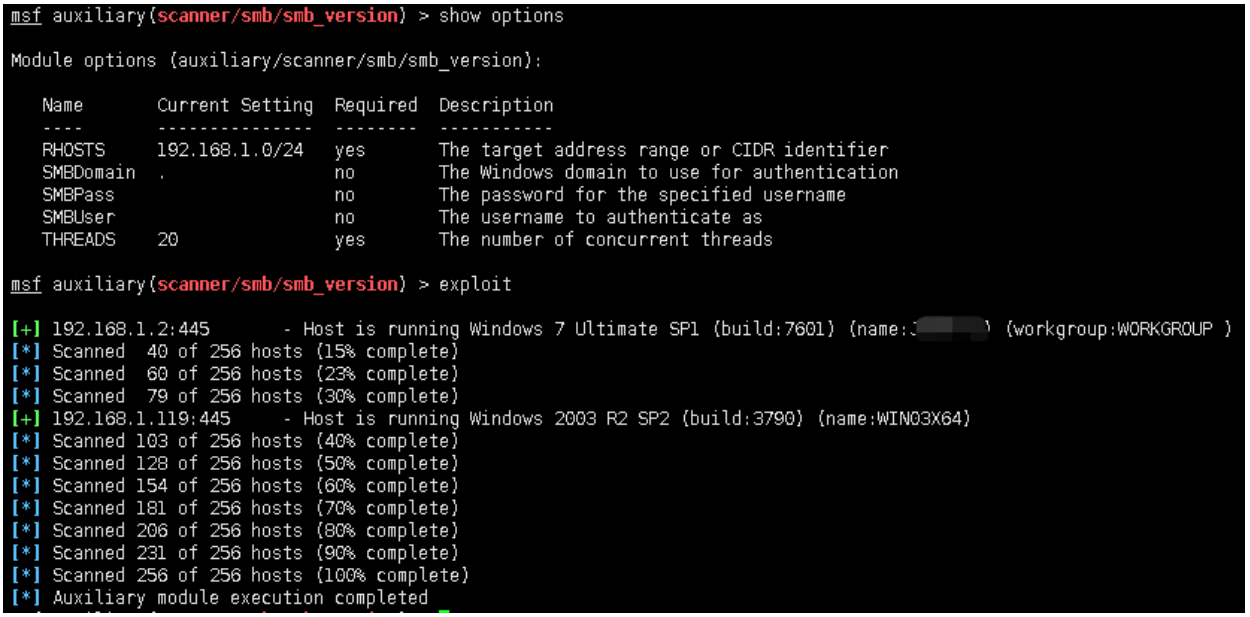
```
[*] Scanned 63 of 256 hosts (24% complete)
[*] Scanned 82 of 256 hosts (32% complete)
[*] Scanned 103 of 256 hosts (40% complete)
[+] 192.168.1.119:80 Microsoft-IIS/6.0 ( Powered by ASP.NET )
[*] Scanned 129 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 182 of 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

```

```
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

```
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:JOHN-PC) (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

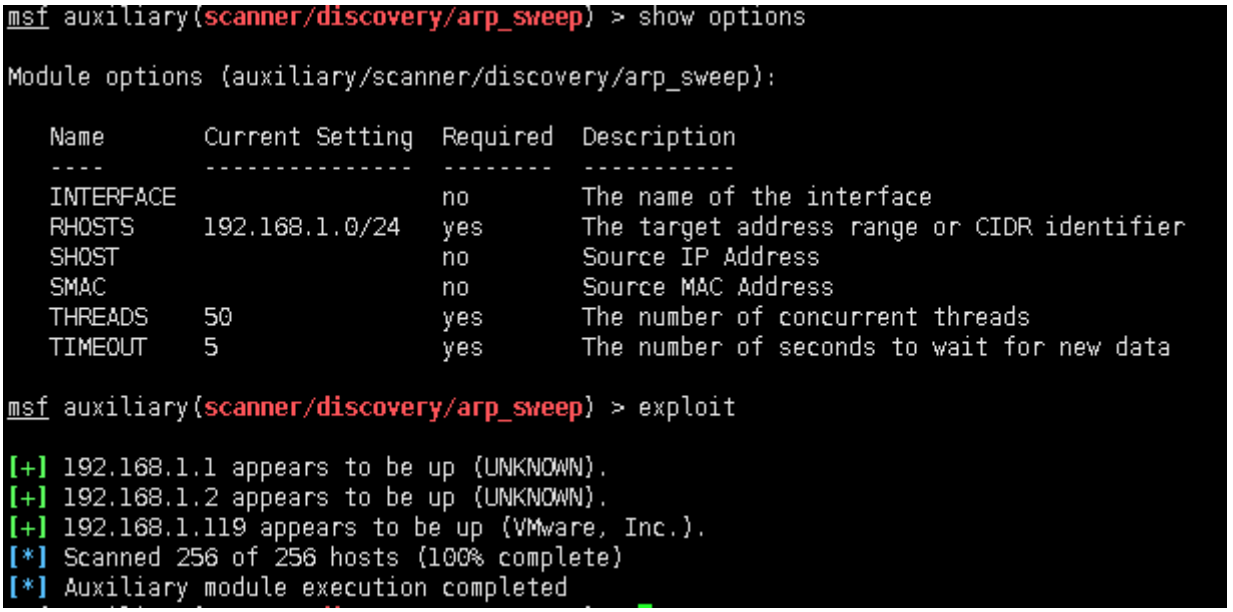
```
msf auxiliary(scanner/ftp/ftp_version) > show options

```

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   FTPPASS  mozilla@example.com  no  The password for the specified usernam
e
   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
```

```
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
```

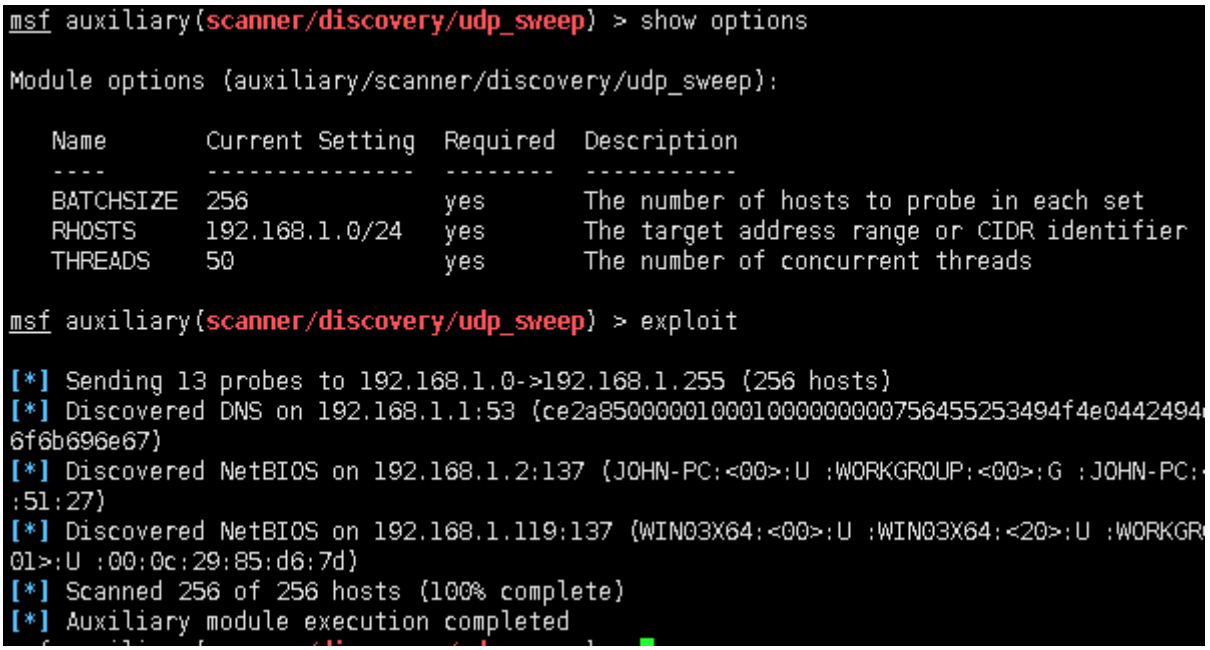
- 四：基于scanner/discovery/arp_sweep发现内网存活主机

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

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

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 INTERFACE 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 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

```
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 (ce2a850000010001000000000756455253494f4e0442494e440000100003c00c0010000300000001001a19737572656c7920796f75206d757374206265206a6f6b696e67)
[*] 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 NetBIOS on 192.168.1.119:137 (WIN03X64:<00>:U :WIN03X64:<20>:U :WORKGROUP:<00>:G :WORKGROUP:<1e>:G :WIN03X64:<03>:U :ADMINISTRATOR:<03>:U :WIN03X64:<01>:U :00:0c:29:85:d6:7d)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```


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 (ce2a850000010001000000000756455253494f4e0442494
6f6b696e67)
[*] 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 :WORKGR
01>:U :00:0c:29:85:d6:7d)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

- Micropoor