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。
如有肾囊肿，请定期检查肾囊肿的大小变化。

攻击机： 192.168.1.102 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

第三季主要介绍scanner下的五个模块，辅助发现内网存活主机，分别为：

- auxiliary/scanner/netbios/nbname
- auxiliary/scanner/http/title
- auxiliary/scanner/db2/db2_version
- auxiliary/scanner/portscan/ack
- auxiliary/scanner/portscan/tcp

第四季主要介绍scanner下的五个模块，辅助发现内网存活主机，分别为：

- auxiliary/scanner/portscan/syn
- auxiliary/scanner/portscan/ftpbounce
- auxiliary/scanner/portscan/xmas
- auxiliary/scanner/rdp/rdp_scanner
- auxiliary/scanner/smtp/smtp_version

第五季主要介绍scanner下的三个模块，以及db_nmap辅助发现内网存活主机，分别为：

- auxiliary/scanner/pop3/pop3_version
- auxiliary/scanner/postgres/postgres_version
- auxiliary/scanner/ftp/anonymous
- db_nmap

第六季主要介绍post下的六个模块，辅助发现内网存活主机，分别为：

- windows/gather/arp_scanner
- windows/gather/enum_ad_computers
- windows/gather/enum_computers
- windows/gather/enum_domain
- windows/gather/enum_domains
- windows/gather/enum_ad_user_comments

在实战过程中，许多特殊环境下scanner，db_nmap不能快速符合实战渗透诉求，尤其在域中的主机存活发现，而post下的模块，弥补了该诉求，以便快速了解域中存活主机。

- 二十五：基于windows/gather/arp_scanner发现内网存活主机

```
meterpreter > run windows/gather/arp_scanner RHOSTS=192.168.1.110-120 THREADS=20

[*] Running module against VM_2003X86
[*] ARP Scanning 192.168.1.110-120
[+] IP: 192.168.1.115 MAC 00:0c:29:af:ce:cc (VMware, Inc.)
[+] IP: 192.168.1.119 MAC 00:0c:29:85:d6:7d (VMware, Inc.)
```

```
meterpreter > run windows/gather/arp_scanner RHOSTS=192.168.1.110-120 THREADS=20

[*] Running module against VM_2003X86
[*] ARP Scanning 192.168.1.110-120
[+]     IP: 192.168.1.115 MAC 00:0c:29:af:ce:cc (VMware, Inc.)
[+]     IP: 192.168.1.119 MAC 00:0c:29:85:d6:7d (VMware, Inc.)
```

- 二十六：基于windows/gather/enum_ad_computers发现域中存活主机

```
meterpreter > run windows/gather/enum_ad_computers
```

```
meterpreter > run windows/gather/enum_ad_computers
```

- 二十七：基于windows/gather/enum_computers发现域中存活主机

```
meterpreter > run windows/gather/enum_computers

[*] Running module against VM_2003X86
[-] This host is not part of a domain.
```

```
meterpreter > run windows/gather/enum_computers

[*] Running module against VM_2003X86
[-] This host is not part of a domain.
```

- 二十八：基于windows/gather/enum_domain发现域中存活主机

```
meterpreter > run windows/gather/enum_domain
```

```
meterpreter > run windows/gather/enum_domain
```

- 二十九：基于windows/gather/enum_domains 发现域中存活主机

```
meterpreter > run windows/gather/enum_domains

[*] Enumerating DCs for WORKGROUP
[-] No Domain Controllers found...
```

```
meterpreter > run windows/gather/enum_domains

[*] Enumerating DCs for WORKGROUP
[-] No Domain Controllers found...
```

- 三十：基于windows/gather/enum_ad_user_comments发现域中存活主机

```
1 meterpreter > run windows/gather/enum_ad_user_comments
```

```
meterpreter > run windows/gather/enum_ad_user_comments
```

POST下相关模块如：（列举）不一一介绍

- linux/gather/enum_network
- linux/busybox/enum_hosts
- windows/gather/enum_ad_users
- windows/gather/enum_domain_tokens
- windows/gather/enum_snmp

至此，MSF发现内网存活主机主要模块介绍与使用完毕。

- Micropoor