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

1 meterpreter > run windows/gather/arp\_scanner RHOSTS=192.168.1.110‐120 THREADS=20

2

3 [\*] Running module against VM\_2003X86

4 [\*] ARP Scanning 192.168.1.110‐120

5 [+] IP: 192.168.1.115 MAC 00:0c:29:af:ce:cc (VMware, Inc.)

6 [+] 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

1 meterpreter > run windows/gather/enum\_ad\_computers

二十七：基于windows/gather/enum\_computers发现域中存活主机

1 meterpreter > run windows/gather/enum\_computers 2

3 [\*] Running module against VM\_2003X86

4 [‐] 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

1 meterpreter > run windows/gather/enum\_domain

二十九：基于windows/gather/enum\_domains 发现域中存活主机

1 meterpreter > run windows/gather/enum\_domains 2

3 [\*] Enumerating DCs for WORKGROUP

4 [‐] 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

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