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

192.168.1.115 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

十六：基于auxiliary/scanner/portscan/syn发现内网存活主机

1 msf auxiliary(scanner/portscan/syn) > show options 2

3 Module options (auxiliary/scanner/portscan/syn): 4

5 Name Current Setting Required Description

6 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

7 BATCHSIZE 256 yes The number of hosts to scan per set

8 DELAY 0 yes The delay between connections, per thread, in millisecond s

9 INTERFACE no The name of the interface

10 JITTER 0 yes The delay jitter factor (maximum value by which to +/‐ D ELAY) in milliseconds.

11 PORTS 445 yes Ports to scan (e.g. 22‐25,80,110‐900)

12 RHOSTS 192.168.1.115 yes The target address range or CIDR identifier

13 SNAPLEN 65535 yes The number of bytes to capture

14 THREADS 50 yes The number of concurrent threads

15 TIMEOUT 500 yes The reply read timeout in milliseconds 16

17 msf auxiliary(scanner/portscan/syn) > exploit 18

19 [+] TCP OPEN 192.168.1.115:445

20 [\*] Scanned 1 of 1 hosts (100% complete)

21 [\*] Auxiliary module execution completed

十七：基于auxiliary/scanner/portscan/ftpbounce发现内网存活主机

1 msf auxiliary(scanner/portscan/ftpbounce) > show options 2

3 Module options (auxiliary/scanner/portscan/ftpbounce): 4

5 Name Current Setting Required Description

6 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

7 BOUNCEHOST 192.168.1.119 yes FTP relay host

8 BOUNCEPORT 21 yes FTP relay port

9 DELAY 0 yes The delay between connections, per thread, in millisecond s

10 FTPPASS mozilla@example.com no The password for the specified usernam e

11 FTPUSER anonymous no The username to authenticate as

12 JITTER 0 yes The delay jitter factor (maximum value by which to +/‐ D ELAY) in milliseconds.

13 PORTS 22‐25 yes Ports to scan (e.g. 22‐25,80,110‐900)

14 RHOSTS 192.168.1.119 yes The target address range or CIDR identifier

15 THREADS 50 yes The number of concurrent threads 16

17 msf auxiliary(scanner/portscan/ftpbounce) > exploit 18

19 [+] 192.168.1.119:21 ‐ TCP OPEN 192.168.1.119:22

20 [+] 192.168.1.119:21 ‐ TCP OPEN 192.168.1.119:23

21 [+] 192.168.1.119:21 ‐ TCP OPEN 192.168.1.119:24

22 [+] 192.168.1.119:21 ‐ TCP OPEN 192.168.1.119:25

23 [\*] 192.168.1.119:21 ‐ Scanned 1 of 1 hosts (100% complete)

24 [\*] Auxiliary module execution completed

十八：基于auxiliary/scanner/portscan/xmas发现内网存活主机

1 msf auxiliary(scanner/portscan/xmas) > show options 2

3 Module options (auxiliary/scanner/portscan/xmas): 4

5 Name Current Setting Required Description

6 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

7 BATCHSIZE 256 yes The number of hosts to scan per set

8 DELAY 0 yes The delay between connections, per thread, in millisecond s

9 INTERFACE no The name of the interface

10 JITTER 0 yes The delay jitter factor (maximum value by which to +/‐ D ELAY) in milliseconds.

11 PORTS 80 yes Ports to scan (e.g. 22‐25,80,110‐900)

12 RHOSTS 192.168.1.119 yes The target address range or CIDR identifier

13 SNAPLEN 65535 yes The number of bytes to capture

14 THREADS 50 yes The number of concurrent threads

15 TIMEOUT 500 yes The reply read timeout in milliseconds 16

17 msf auxiliary(scanner/portscan/xmas) > exploit

十九：基于auxiliary/scanner/rdp/rdp\_scanner发现内网存活主机

1 msf auxiliary(scanner/rdp/rdp\_scanner) > show options 2

3 Module options (auxiliary/scanner/rdp/rdp\_scanner): 4

5 Name Current Setting Required Description

6 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

7 CredSSP true yes Whether or not to request CredSSP

8 EarlyUser false yes Whether to support Earlier User Authorization Res ult PDU

9 RHOSTS 192.168.1.2,115,119 yes The target address range or CIDR ident ifier

10 RPORT 3389 yes The target port (TCP)

11 THREADS 50 yes The number of concurrent threads

12 TLS true yes Wheter or not request TLS security 13

14 msf auxiliary(scanner/rdp/rdp\_scanner) > exploit 15

16 [\*] Scanned 1 of 3 hosts (33% complete)

17 [+] 192.168.1.115:3389 ‐ Identified RDP

18 [\*] Scanned 2 of 3 hosts (66% complete)

19 [+] 192.168.1.119:3389 ‐ Identified RDP

20 [\*] Scanned 3 of 3 hosts (100% complete)

21 [\*] Auxiliary module execution completed

二十：基于auxiliary/scanner/smtp/smtp\_version发现内网存活主机

1 msf auxiliary(scanner/smtp/smtp\_version) > show options 2

3 Module options (auxiliary/scanner/smtp/smtp\_version): 4

5 Name Current Setting Required Description

6 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

7 RHOSTS 192.168.1.5 yes The target address range or CIDR identifier

8 RPORT 25 yes The target port (TCP)

9 THREADS 50 yes The number of concurrent threads 10

11 msf auxiliary(scanner/smtp/smtp\_version) > exploit

Micropoor