CrackMapExec

Information Security Inc.

iSEC
information security inc.

Contents

- About CrackMapExec
- Testing Environment
- Installing CrackMapExec
- Using CrackMapExec
- References

About CrackMapExec

- CrackMapExec (a.k.a CME) is a post-exploitation tool that helps automate assessing the security of *large* Active Directory networks

Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing CrackMapExec

- Installing dependencies

```
root@kali2017:~# apt-get install -y libssl-dev libffi-dev python-dev build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version (12.4).
libffi-dev is already the newest version (3.2.1-6).
libssl-dev is already the newest version (1.1.0f-5).
python-dev is already the newest version (2.7.13-2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Installing CrackMapExec

- Installing pipenv

```
root@kali2017:~# pip install pipenv
Collecting pipenv
Requirement already satisfied: flake8>=3.0.0 in ./.local/lib/python2.7/site-packages (from pipenv)
Requirement already satisfied: virtualenv in /usr/lib/python2.7/dist-packages (from pipenv)
Requirement already satisfied: pew>=0.1.26 in ./.local/lib/python2.7/site-packages (from pipenv)
Requirement already satisfied: pip>=9.0.1 in /usr/lib/python2.7/dist-packages (from pipenv)
Requirement already satisfied: requests>2.18.0 in ./.local/lib/python2.7/site-packages (from pipenv)
Requirement already satisfied: urllib3>=1.21.1 in /usr/lib/python2.7/dist-packages (from pipenv)
Requirement already satisfied: pyflakes<1.7.0,>=1.5.0 in ./.local/lib/python2.7/site-packages (from flake8>=3.0.0->pipenv)
Requirement already satisfied: enum34; python_version < "3.4" in /usr/lib/python2.7/dist-packages (from flake8>=3.0.0->pipenv)
Requirement already satisfied: configparser; python_version < "3.2" in /usr/lib/python2.7/dist-packages (from flake8>=3.0.0->pipenv)
Requirement already satisfied: pycodestyle<2.4.0,>=2.0.0 in ./.local/lib/python2.7/site-packages (from flake8>=3.0.0->pipenv)
Requirement already satisfied: mccabe<0.7.0,>=0.6.0 in ./.local/lib/python2.7/site-packages (from flake8>=3.0.0->pipenv)
Requirement already satisfied: virtualenv-clone>=0.2.5 in /usr/lib/python2.7/dist-packages (from pew>=0.1.26->pipenv)
Requirement already satisfied: shutilwhich; python_version == "2.7" in ./.local/lib/python2.7/site-packages (from pew>=0.1.26->pipenv)
Requirement already satisfied: backports.shutil-get-terminal-size; python_version == "2.7" in /usr/lib/python2.7/dist-packages (from pew>
=0.1.26->pipenv)
Requirement already satisfied: pathlib; python_version == "2.7" in ./.local/lib/python2.7/site-packages (from pew>=0.1.26->pipenv)
Requirement already satisfied: setuptools>=17.1 in /usr/lib/python2.7/dist-packages (from pew>=0.1.26->pipenv)
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python2.7/dist-packages (from requests>2.18.0->pipenv)
Requirement already satisfied: chardet<3.1.0,>=3.0.2 in /usr/lib/python2.7/dist-packages (from requests>2.18.0->pipenv)
Requirement already satisfied: idna<2.7,>=2.5 in ./.local/lib/python2.7/site-packages (from requests>2.18.0->pipenv)
Installing collected packages: pipenv
Successfully installed pipenv-8.3.2
```

Installing CrackMapExec

- Installing python3-pip

```
root@kali2017:~# apt-get install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-crypto python3-dev python3-keyring python3-keyrings.alt python3-secretstorage python3-setuptools python3-wheel python3.5-dev
Suggested packages:
  python3-crypto-dbg python-crypto-doc libkf5wallet-bin python-secretstorage-doc python-setuptools-doc
The following NEW packages will be installed:
  python3-crypto python3-dev python3-keyring python3-keyrings.alt python3-pip python3-secretstorage python3-setuptools python3-wheel
  python3.5-dev
```

Installing CrackMapExec

- Installing pew package

```
root@kali2017:~# pip3 install pew
Collecting pew
  Using cached pew-1.1.0-py2.py3-none-any.whl
Requirement already satisfied: setuptools>=17.1 in /usr/lib/python3/dist-packages (from pew)
Collecting virtualenv-clone>=0.2.5 (from pew)
  Downloading virtualenv-clone-0.2.6.tar.gz
Requirement already satisfied: virtualenv>=1.11 in /usr/lib/python3/dist-packages (from pew)
Building wheels for collected packages: virtualenv-clone
  Running setup.py bdist_wheel for virtualenv-clone ... done
  Stored in directory: /root/.cache/pip/wheels/24/51/ef/93120d304d240b4b6c2066454250a1626e04f73d34417b956d
Successfully built virtualenv-clone
Installing collected packages: virtualenv-clone, pew
Successfully installed pew-1.1.0 virtualenv-clone-0.2.6
```

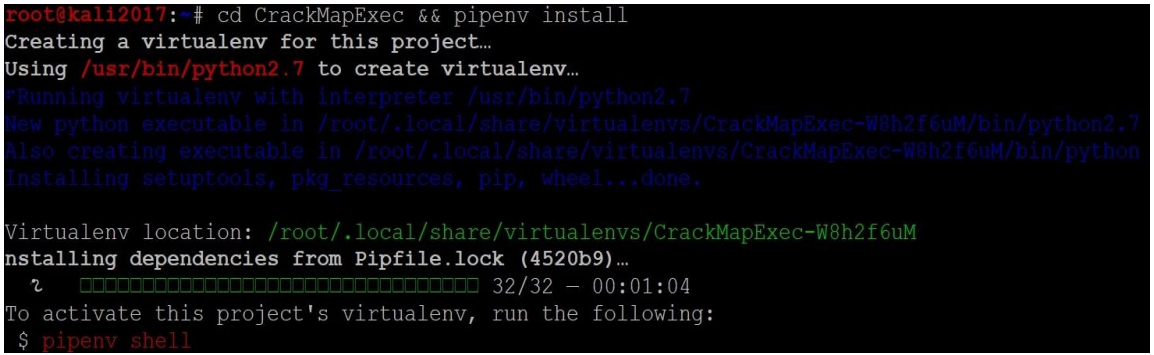
Installing CrackMapExec

- Clone the GitHub repository

```
root@kali2017:~# git clone --recursive https://github.com/byt3bl33d3r/CrackMapExec
Cloning into 'CrackMapExec'...
remote: Counting objects: 2394, done.
remote: Total 2394 (delta 0), reused 0 (delta 0), pack-reused 2394
Receiving objects: 100% (2394/2394), 5.52 MiB | 3.24 MiB/s, done.
Resolving deltas: 100% (1604/1604), done.
Submodule 'cme/data/cme_powershell_scripts' (https://github.com/byt3bl33d3r/CME-PowerShell-Scripts) registered for path 'cme/data/cme_pow
ershell_scripts'
Submodule 'cme/data/invoke-obfuscation' (https://github.com/danielbohannon/Invoke-Obfuscation) registered for path 'cme/data/invoke-obfus
cation'
Submodule 'cme/data/invoke-vnc' (https://github.com/artkond/Invoke-Vnc) registered for path 'cme/data/invoke-vnc'
Submodule 'cme/data/mimikittenz' (https://github.com/putterpanda/mimikittenz) registered for path 'cme/data/mimikittenz'
Submodule 'cme/data/mimipenguin' (https://github.com/huntergregal/mimipenguin) registered for path 'cme/data/mimipenguin'
Submodule 'cme/data/netripper' (https://github.com/NytroRST/NetRipper) registered for path 'cme/data/netripper'
Submodule 'cme/data/powersploit' (https://github.com/PowerShellMafia/PowerSploit) registered for path 'cme/data/powersploit'
Submodule 'cme/data/randomps-scripts' (https://github.com/xorrior/RandomPS-Scripts) registered for path 'cme/data/randomps-scripts'
```

Installing CrackMapExec

- Installing CrackMapExec



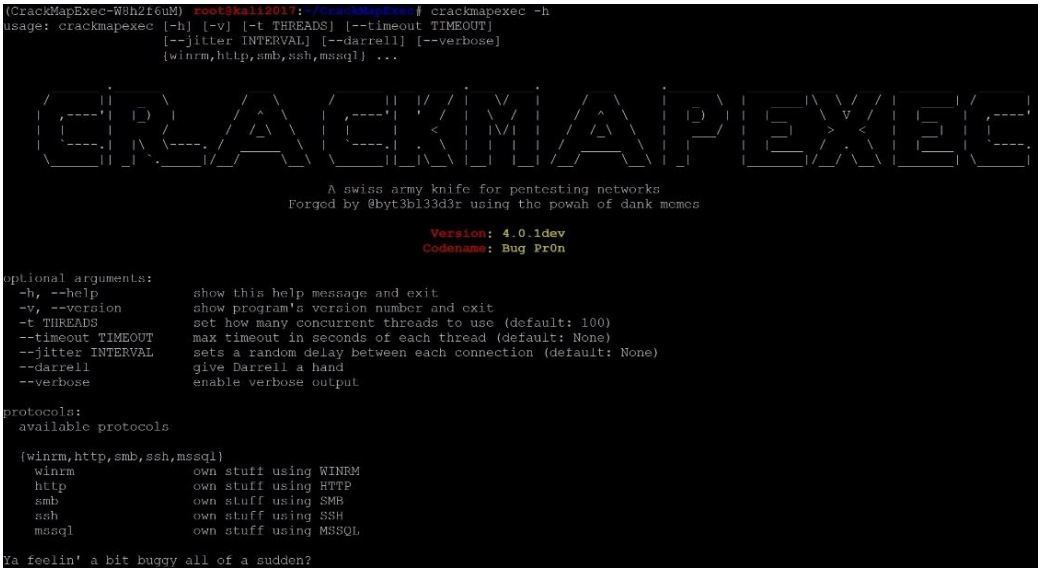
Installing CrackMapExec

- Installing CrackMapExec

```
root@kali2017:~/CrackMapExec# pipenv shell
Spawning environment shell (/bin/bash). Use 'exit' to leave.
source /root/.local/share/virtualenvs/CrackMapExec-W8h2f6uM/bin/activate
root@kali2017:~/CrackMapExec# source /root/.local/share/virtualenvs/CrackMapExec-W8h2f6uM/bin/activate
(CrackMapExec-W8h2f6uM) root@kali2017:~/CrackMapExec# python setup.py install
/root/.local/share/virtualenvs/CrackMapExec-W8h2f6uM/local/lib/python2.7/site-packages/setuptools/dist.py:351: UserWarning: Normalizing '
4.0.1dev' to '4.0.1.dev0'
  normalized_version,
running install
running bdist_egg
running egg_info
creating crackmapexec.egg-info
writing requirements to crackmapexec.egg-info/requires.txt
writing crackmapexec.egg-info/PKG-INFO
writing top-level names to crackmapexec.egg-info/top_level.txt
```

Using CrackmapExec

- CrackMapExec help menu



Using CrackmapExec

- Find out what's on the network

```
(CrackMapExec-W8h2f6uM) root@kali2017:~/CrackMapExec# crackmapexec smb 192.168.86.0/24
SMB         192.168.86.16   445    MENDELPC         [*] Windows Server 2012 R2 Datacenter 9600 x64 (name:MENDELPC) (domain:MINI) (signing:True) (SMB
v1:True)
SMB         192.168.86.101  445    JOINEDDOMAIN     [*] Windows 10 Pro 15063 x64 (name:JOINEDDOMAIN) (domain:MINI) (signing:False) (SMBv1:True)
SMB         192.168.86.102  445    LABESXI          [*] Windows 10 Pro 15063 x64 (name:LABESXI) (domain:MINI) (signing:False) (SMBv1:True)
SMB         192.168.86.111  445    USERNBRTWO       [*] Windows 10 Pro 10240 x64 (name:USERNBRTWO) (domain:MINI) (signing:False) (SMBv1:True)
```

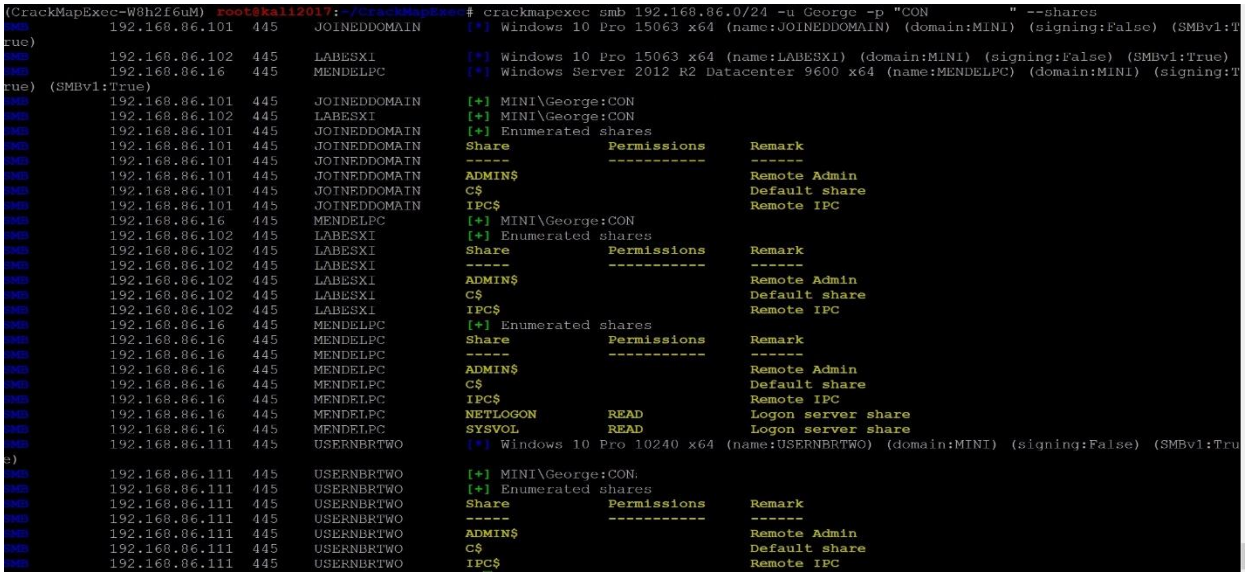
Using CrackmapExec

- Use a regular domain account to do some quick recon
- Using --pass-pol flag which dumps the domains password policy

```
(CrackMapExec-W8h2f6uM) root@kali2017:~/CrackMapExec# crackmapexec smb 192.168.86.0/24 -u George -p "CON:          " --pass-pol
SMB         192.168.86.16   445    MENDELPC         [*] Windows Server 2012 R2 Datacenter 9600 x64 (name:MENDELPC) (domain:MINI) (signing:T
rue) (SMBv1:True)
SMB         192.168.86.101  445    JOINEDDOMAIN     [*] Windows 10 Pro 15063 x64 (name:JOINEDDOMAIN) (domain:MINI) (signing:False) (SMBv1:T
rue)
SMB         192.168.86.102  445    LABESXI          [*] Windows 10 Pro 15063 x64 (name:LABESXI) (domain:MINI) (signing:False) (SMBv1:True)
SMB         192.168.86.16   445    MENDELPC         [+] MINI\George:CON
SMB         192.168.86.16   445    MENDELPC         [+] Dumping password info for domain: MINI
SMB         192.168.86.16   445    MENDELPC         Minimum password length: 7
SMB         192.168.86.16   445    MENDELPC         Password history length: 24
SMB         192.168.86.16   445    MENDELPC         Maximum password age:
SMB         192.168.86.16   445    MENDELPC
SMB         192.168.86.16   445    MENDELPC         Password Complexity Flags: 000001
SMB         192.168.86.16   445    MENDELPC             Domain Refuse Password Change: 0
SMB         192.168.86.16   445    MENDELPC             Domain Password Store Cleartext: 0
SMB         192.168.86.16   445    MENDELPC             Domain Password Lockout Admins: 0
SMB         192.168.86.16   445    MENDELPC             Domain Password No Clear Change: 0
SMB         192.168.86.16   445    MENDELPC             Domain Password No Anon Change: 0
SMB         192.168.86.16   445    MENDELPC             Domain Password Complex: 1
SMB         192.168.86.16   445    MENDELPC
SMB         192.168.86.16   445    MENDELPC         Minimum password age:
SMB         192.168.86.16   445    MENDELPC         Reset Account Lockout Counter: 30 minutes
SMB         192.168.86.16   445    MENDELPC         Locked Account Duration: 30 minutes
SMB         192.168.86.16   445    MENDELPC         Account Lockout Threshold: None
SMB         192.168.86.16   445    MENDELPC         Forced Log off Time: Not Set
```

Using CrackmapExec

- Enumerating all the shares



References

- Kitploit
http://www.kitploit.com/2015/09/crackmapexec-swiss-army-knife-for.html

- Kali Linux
https://www.kali.org/downloads/