

Startup_THM

Enumeration

```
# Ftp anonymous session allowed

# we see that a dir on webserver as /files which is basically the ftp server

# so we put a web shell on it and get a reverse shell
```

Nmap

```
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 10.4.30.255
|   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 5
|   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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1
(93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 -
6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

FTP:21

```
# Anonymous session allowed

# Got a few files in ftp
```

```
root@kali: ~ 121x27
Data connections will be plain text
At session startup, client count was 5
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:a0:0b:84:1d:22:01:a4:01:30:48:43:01:2b: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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Li
nux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%)
, Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACERoute (using port 21/tcp)
HOP RTT ADDRESS
1 207.84 ms 10.4.0.1
2 ... 3
4 463.52 ms 10.10.209.89

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
root@kali: ~ 121x27
(root@kali)-[~]
# nikto -h $ip
-----
+ Target IP:      10.10.209.89
+ Target Hostname: 10.10.209.89
+ Target Port:    80
+ Start Time:     2021-05-01 16:46:20 (GMT-4)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a di
fferent fashion to the MIME type
+ No CGI Directories found (use '-c all' to force check all possible dirs)
]

root@kali: ~ 114x27
(root@kali)-[~]
# gobuster dir -u "http://$ip/" -w Wordlists/dirb/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[*] Url:          http://10.10.209.89/
[*] Method:       GET
[*] Threads:      10
[*] Wordlist:      Wordlists/dirb/common.txt
[*] Negative Status codes: 404
[*] User Agent:    gobuster/3.1.0
[*] Timeout:      10s
=====
2021/05/01 16:46:13 Starting gobuster in directory enumeration mode
=====
./hta (Status: 403) [Size: 277]
./htpasswd (Status: 403) [Size: 277]
./htaccess (Status: 403) [Size: 277]
./files (Status: 301) [Size: 312] [--> http://10.10.209.89/files/]
./index.html (Status: 200) [Size: 808]
./server-status (Status: 403) [Size: 277]
Progress: 4118 / 4615 (89.23%)

root@kali: ~ 114x27
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> cd ftp
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx 2 65534 65534 4096 Nov 12 04:53 .
drwxr-xr-x 3 65534 65534 4096 Nov 12 04:53 ..
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> get .test.log
local: .test.log remote: .test.log
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .test.log (5 bytes).
226 Transfer complete.
```

#

SSH:22

HTTP:80

Gobuster

```
./hta (Status: 403) [Size: 277]
./htpasswd (Status: 403) [Size: 277]
./htaccess (Status: 403) [Size: 277]
./files (Status: 301) [Size: 312] [--> http://10.10.209.89/files/]
./index.html (Status: 200) [Size: 808]
./server-status (Status: 403) [Size: 277]
```

Exploitation

PostExploitation

After logging we tried manual emuration but its of no use

Then i found a incident directory which is owned by www-data

In it we get a packetdump file and after thouroughly reading it we get lennies password c4ntg3t3n0ughsp1c3

WE saw a print.sh script earlier in /etc/directory which was owned by lennie user

In lennie script directory we have a planner script run by root and we have only execute permission

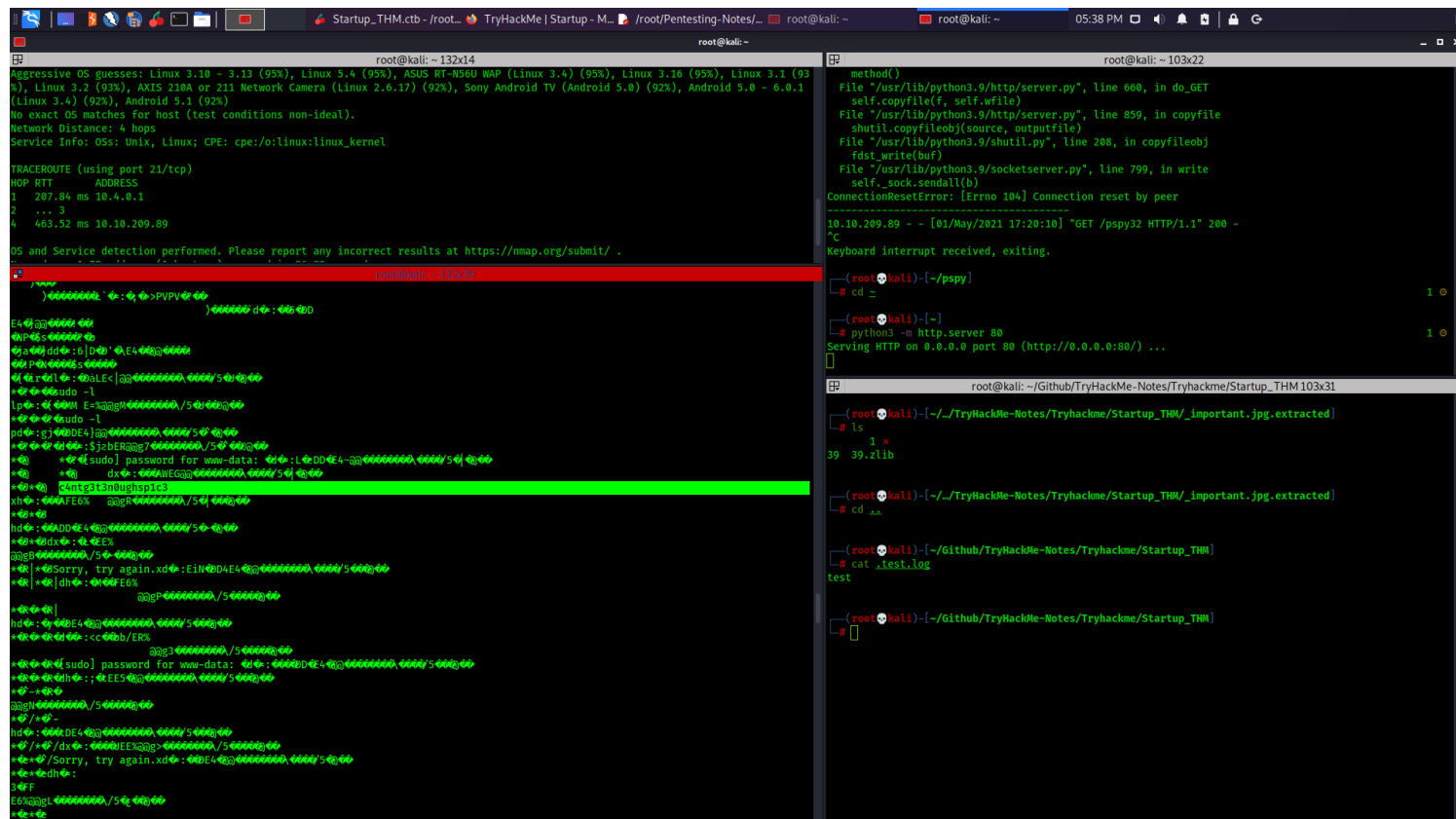
so we copied bash binary to a tmp binary and set suid to it and echoed it into print.sh script because its owned by us

we then wait for the secret cronjob to run and then we simply run our binary as priveleged mode (-p) and got root

www-data to lennie

after logging in we see a directory named incidents and it has a wiresharfk packetdump file

after thouroughly reading it we get password of lennie



```
root@kali: ~ 132x14
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT ADDRESS
1 207.84 ms 10.4.0.1
2 ... 3
4 463.52 ms 10.10.209.89

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

root@kali: ~ 103x22
method()
File "/usr/lib/python3.9/http/server.py", line 660, in do_GET
self.copyfile(r, self.wfile)
File "/usr/lib/python3.9/http/server.py", line 859, in copyfile
shutil.copyfileobj(source, outfile)
File "/usr/lib/python3.9/shutil.py", line 208, in copyfileobj
fdst.write(buf)
File "/usr/lib/python3.9/socketserver.py", line 799, in write
self._sock.sendall(b)
ConnectionResetError: [Errno 104] Connection reset by peer
10.10.209.89 - - [01/May/2021 17:20:10] "GET /pspy32 HTTP/1.1" 200 -
Keyboard interrupt received, exiting.

root@kali: ~ 103x31
ls
1 x
39 39.2lib

root@kali: ~ 103x31
cat _test1.log
test

root@kali: ~ 103x31
cat _test1.log
test
```

#

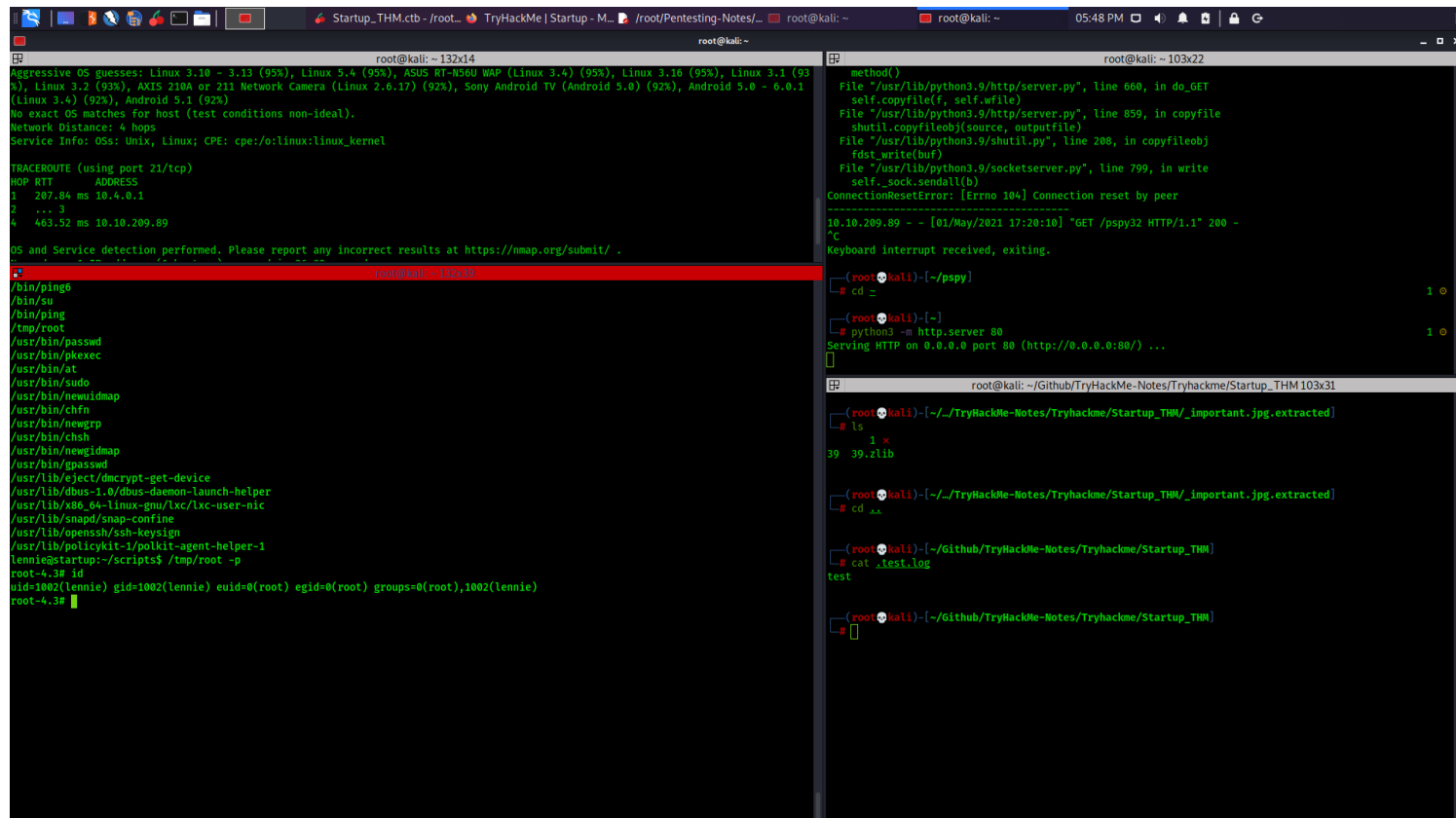
lennie to root

WE saw a print.sh script earlier in /etc/directory which was owned by lennie user

In lennie script directory we have a planner script run by root and we have only execute permission

so we copied bash binary to a tmp binary and set suid to it and echoed it into print.sh script because its owned by us

we then wait for the secret cronjob to run and then we simply run our binary as priveleged mode (-p) and got root



Loot

Credentials

lennie user password

c4ntg3t3n0ughsp1c3

#

Flags

USer flag

THM{03ce3d619b80ccbf3b7fc81e46c0e79}

Root FLag

THM{f963aaa6a430f210222158ae15c3d76d}