WhoMovedMyFlag

发表于 2021-03-15 更新于 2021-05-21 分类于 Challenge， 2020， XCTF高校网络安全专题挑战赛， 华为云专题赛， Misc
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | 华为云专题赛 | Misc | WhoMovedMyFlag

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

解题思路

打开流量包，发现有两个流，第一个是HTTP的，通过wget访问了一个叫做tshd的文件。通过文件名猜测是tinyshell后门软件，提取出来以后拖到ida里看一下可以很明显的看到第二个流的对端C2地址，172.17.0.24，然后还有另外一个字符串，猜测是密钥：6.3.0-18+deb9u1

```
1 git clone https://github.com/orangetw/tsh
```

按照secret:6.3.0-18+deb9u1 端口8888 ,这里为了绕过tsh端的校验，需要手动在pel.c中patch sha1中的40个字节，patch成第一个数据包中的40个字节即可，然后编译tsh备用。

编写流量重放脚本

```
peer0_0= [
0x0a, 0xb3, 0x48, 0xad, 0x08, 0x26, 0xc6, 0x45,
0x18, 0x71, 0x2b, 0x9d, 0xf0, 0x8a, 0xf6, 0x3e,
0x3a, 0x5e, 0xfb, 0x96, 0x71, 0xf4, 0xc4, 0xe0,
0xcc, 0x37, 0x46, 0x94, 0xb3, 0x91, 0xb0, 0xbe,
0xe7, 0x6a, 0xf2, 0x09, 0x12, 0x9d, 0x69, 0x7f,
0x05, 0xfc, 0x2a, 0x24, 0xec, 0x76, 0x5e, 0xde,
0x53, 0x2b, 0x25, 0xb8]
peer0_1=[
0x97, 0xb5, 0xfe, 0xbf, 0xe4, 0x8f, 0x28, 0x9f,
0x8e, 0x6f, 0xac, 0xc2, 0xd5, 0xc4, 0xac, 0x01,
0xa8, 0xd8, 0x7a, 0xa4, 0x26, 0xad, 0xca, 0xea,
0xbc, 0x35, 0x75, 0x28, 0x7c, 0xa0, 0xed, 0xa5,
0xba, 0x02, 0xeb, 0x63, 0xa5, 0xb8, 0x56, 0x3c,
0x7a, 0xe5, 0x65, 0x9a, 0x83, 0xb1, 0x13, 0xdf,
0xf5, 0x49, 0x08, 0x17]
peer0_2=[
0x84, 0x58, 0x07, 0x3e, 0x49, 0x59, 0x5c, 0x9c,
0x05, 0xb1, 0x94, 0x24, 0x01, 0x13, 0x46, 0x7d,
0x6f, 0x3a, 0x86, 0xf5, 0xfe, 0x64, 0x19, 0xf1,
0x8e, 0xe6, 0x0e, 0xf1, 0x3a, 0xdd, 0x8b, 0x4f,
0xa9, 0xa6, 0xc5, 0x34, 0xbb, 0x69, 0x53, 0x61,
0xc6, 0x41, 0xeb, 0xb6, 0x8b, 0xd1, 0x59, 0x82,
0xe2, 0xfa, 0xbe, 0xf1, 0x3c, 0xd5, 0xc6, 0x75,
0x81, 0x83, 0x2b, 0x98, 0x64, 0xe3, 0xaa, 0xd9,
0x14, 0x5b, 0xc3, 0xa8, 0xaf, 0x74, 0xda, 0x49,
0x31, 0xab, 0xd1, 0xfe, 0x52, 0xcf, 0x80, 0x57,
0x43, 0x68, 0xaf, 0xa0, 0x20, 0x7c, 0xe8, 0x34,
0x36, 0x7c, 0x3d, 0x0b, 0xc3, 0xe3, 0xb0, 0x1b,
0x38, 0x12, 0x68, 0xb3, 0xad, 0x97, 0x6e, 0x7c,
0xb7, 0x78, 0x1f, 0xa4, 0x11, 0xf7, 0xd1, 0x62,
0x58, 0xa1, 0x89, 0xdf, 0x12, 0xa9, 0x62, 0x33,
0x86, 0xff, 0x59, 0x31, 0xfb, 0x5e, 0x72, 0xc0,
0xc4, 0xdc, 0x6d, 0x53, 0x1b, 0x63, 0x33, 0x48,
0x35, 0xda, 0x91, 0xda, 0xa5, 0xba, 0x73, 0xe8,
0x94, 0x5e, 0xe5, 0x68, 0x3f, 0x1a, 0x11, 0x02,
0xe0, 0x09, 0xc1, 0x35, 0x8d, 0xff, 0x01, 0x6e,
0xd4, 0xf1, 0xe2, 0x48, 0xe3, 0xc7, 0xb2, 0x4b,
0x4f, 0xa6, 0xa0, 0xc5, 0x6d, 0x0f, 0x4f, 0x45,
0x74, 0x8f, 0x33, 0xd9, 0xa6, 0xab, 0x28, 0xfc,
0xa2, 0x9a, 0x0c, 0x69, 0x21, 0x64, 0x89, 0x95,
0xb8, 0x5b, 0xbb, 0x32, 0x48, 0x4b, 0x6e, 0xe9,
0x52, 0x55, 0x3d, 0x78, 0xeb, 0x29, 0x19, 0x3e,
0xe7, 0xaf, 0xfd, 0x1f, 0x61, 0x10, 0x6d, 0x89,
0x8c, 0xe4, 0xb7, 0xb5, 0x08, 0x45, 0xb9, 0x73,
0x66, 0x6d, 0x73, 0x81, 0x43, 0x3e, 0x28, 0x0e,
0x15, 0x43, 0xbb, 0xca, 0x13, 0x3e, 0x7a, 0x24,
0x8b, 0x3a, 0x3a, 0x5c, 0xcf, 0x91, 0x61, 0x5a,
0x41, 0x44, 0xa0, 0x8a, 0xf3, 0x7e, 0x7c, 0x65,
0xe3, 0x23, 0x76, 0x26, 0x03, 0x32, 0x57, 0xc2,
0xc6, 0x48, 0xbc, 0xae, 0xf8, 0xd9, 0xc7, 0x42,
0xe9, 0x6f, 0x7f, 0xb4, 0xa6, 0x3b, 0x1d, 0x78,
0x0f, 0xfe, 0x1e, 0x00, 0xf2, 0xdb, 0x64, 0x53,
0x2c, 0xd9, 0x28, 0xbe, 0x9d, 0x35, 0xf4, 0x24,
0x78, 0x06, 0x2c, 0x18, 0x36, 0xc7, 0xd9, 0xc8,
0xd0, 0x40, 0xbd, 0xe0, 0x9b, 0x92, 0xa3, 0x9c,
0x36, 0x64, 0xcd, 0x83, 0xf6, 0x4f, 0xd7, 0xb1,
0x1f, 0x93, 0xaa, 0x7a]

peer0 = [peer0_0, peer0_1, peer0_2]

import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("127.0.0.1",8888))
for x in peer0:
    s.recv(1000)
    s.send("".join(map(chr,x)))
```

```
1
2
3 使用反向监听模式：`.\tsh cb` 重放流量可得flag
```

cat /etc/flag exit root@e3baa00f5c9a:/tmp# cat /etc/flag ctf{c67d123f74a091a8e4b12015} root@e3baa00f5c9a:/tmp# exit logout

```
1
2
3 ## Flag
4
5 ```纯文本
6 ctf{c67d123f74a091a8e4b12015}
```

- **本文作者：** CTFHub
- **本文链接：** https://writeup.ctfhub.com/Challenge/2020/XCTF高校网络安全专题挑战赛/华为云专题赛/Misc/rv6tv726JRFhzLsVP64gGo.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 # 2020 # Misc # XCTF高校网络安全专题挑战赛 # 华为云专题赛

EthEnc

divination