CTFHub

Writeup



Attachment

□ 2021-09-01 □ Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-上海站

Challenge □ 2021 □ 工业信息安全技能大赛 □ 巡回赛-上海站 □ Attachment

点击此处获得更好的阅读体验

WriteUp来源

来自 Venom 战队

题目描述

安全运维人员,发现员工发送一个带有附件,附件本身看不出问题,但是怀疑是通过数据隐藏方式传递信息,尝试分析该文件,找出文件中的flag。

题目考点

解题思路

在流量中发现一串b64加密 dEhJc21BWWJFckVMQXR1RHRPRkxhZw== , 解码后即为flag

```
49 41.062731667 192.168.0.196 192.168.0.196 192.168.0.255 UP 385 54915 - 54915 Lem263
59 42.066640159 192.168.0.196 192.168.0.255 UP 385 54915 - 54915 Lem263
59 42.74278291 Whare_41.49180 Whare_2275:94 APP 69 192.168.0.191 TCL 192.168.0.199 192.168.0.191 TCL 96 49922 - 8008 [SMN] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [SMN] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP 66 49922 - 8008 [ACK] Seeped Actic Winned2240 Leme MSS-1466 WS-1 SACK_PENH-1 TCP MSS-1466 WS-1 SACK_PENH-1 TCP WS-1466 WS-1 SAC
```

Flag

1 flag{tHIsmAYbErELAteDtOFLag}

本文作者: CTFHub

本文链接: https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回

赛-上海站/x17pvpU8rXc5q7CVvxfDqj.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 ♣ # 工业信息安全技能大赛 ♣ # 巡回赛-上海站

AnomalyAnalysis

Reverse analysis >

© 2019 – 2022 **CTFHub**

由 Hexo & NexT.Gemini 强力驱动