



Login

📅 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 | Login

[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

黑客渗透进入某工业企业内网，发现了登录界面，截获了登录时的流量包，根据社会工程学知识，密码是一串有意义的字符串flag。

题目考点

- 流量分析
- S7Comm协议

解题思路

找到HTTP 协议中登陆相关的数据包，密码即为flag

login.pcapng

http

No.	Time	Source	Destination	Protocol	Length	Info
15	5.432092993	192.168.0.192	150.158.198.76	HTTP	575	GET / HTTP/1.1
17	5.440491533	150.158.198.76	192.168.0.192	HTTP	239	HTTP/1.1 304 Not Modified
97	23.347342209	192.168.0.192	150.158.198.76	HTTP	692	POST / HTTP/1.1 (application/x-www-form
102	23.354881414	150.158.198.76	192.168.0.192	HTTP	768	HTTP/1.1 405 Not Allowed (text/html)
224	32.512595899	192.168.0.192	210.35.90.23	HTTP	606	GET / HTTP/1.1
228	32.521619640	210.35.90.23	192.168.0.192	HTTP	380	HTTP/1.1 301 Moved Permanently (text/ht
613	40.214562975	192.168.0.192	210.35.90.23	HTTP	608	GET / HTTP/1.1
616	40.222103447	210.35.90.23	192.168.0.192	HTTP	382	HTTP/1.1 301 Moved Permanently (text/ht

> Frame 97: 692 bytes on wire (5536 bits), 692 bytes captured (5536 bits) on
> Ethernet II, Src: VMware_3c:c5:13 (00:0c:29:3c:c5:13), Dst: TendaTec_11:b1
> Internet Protocol Version 4, Src: 192.168.0.192, Dst: 150.158.198.76
> Transmission Control Protocol, Src Port: 49112, Dst Port: 80, Seq: 510, A
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "key" = "heihei"
 Key: key
 Value: heihei
 Form item: "value" = "ssoprhwadszkjthk"
 Key: value
 Value: ssoprhwadszkjthk

01a0 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://login.lieying.fun/.../ccept-Encoding: gzip, deflate, ccept-Language: zh-CN,zh;q=0.9...key=heihei&value=ssoprhwadszkjthk

Value (urlencoded-form.value),17 bytes Packets: 1244 - Displayed: 8 (0.6%) Profile: Default

Flag

1 flag{ssoprhwadszkjthk}

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/aCaon2kd75MXsrAJ7D5EjN.html>

版权声明： 本博客所有文章除特别声明外，均采用 [CC 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

< Reverse analysis

Malware >