

# 2021CTF工业信息安全技能大赛-异常的s7comm

原创 夜白君 于 2021-07-05 09:05:43 发布 2588 收藏 4 版权

分类专栏: 2021工业信息安全技能大赛-CTF 文章标签: 信息安全 unctf 渗透测试

 2021工业信息安全... 专栏收录该内容

36 订阅 24 篇文章 订阅专栏

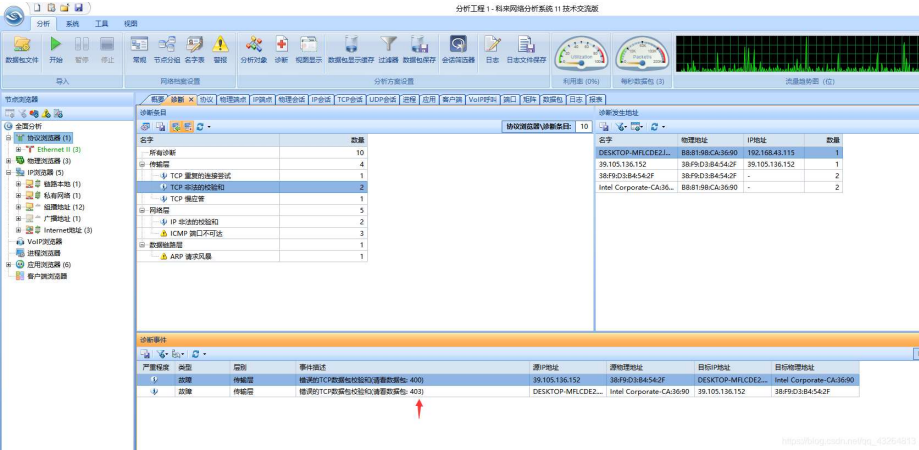
## 2021CTF工业信息安全技能大赛-异常的s7comm

工程师小夏在针对西门子300PLC设备不定期的停止运行，发现设备存在异常外联控制，再对审计设备进行分析中发现数据包中存在异常的eth.trailer、eth.fcs,请您帮助小夏找到外联地址并发送异常的HEX，对服务器返回的HEX进行解密。flag格式为:flag{}

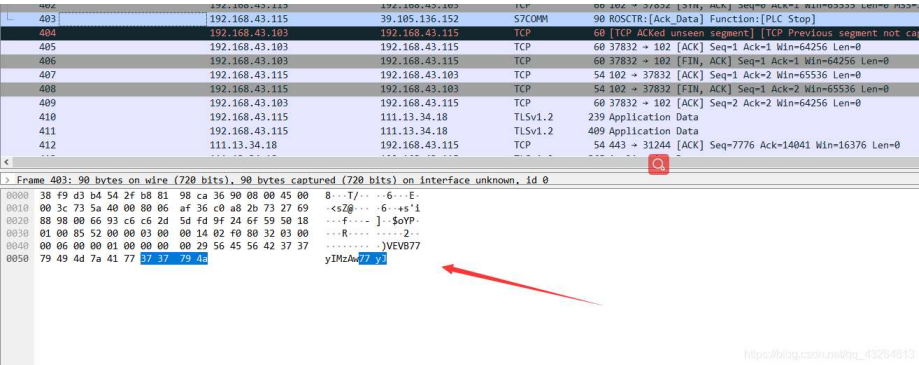
使用工具: Wireshark、NetCat、TEA加密/解密、CaptfEncoder、科来网络分析系统 11 技术交流版、NMAP

### 解题步骤:

#### 1.1、对数据包进行重放发现400、403存在问题



#### 2.查看数据包内容发现一串疑似base64加密



3.对其进行解码得到一个字符串为TEA (300)，根据提示知道要对一个开放37830端口的服务器进行提交可疑HEX值来获取一个加密字符串，使用NMAP 对科来导出的ip进行端口探测。

```
Nmap scan report for 39.105.136.152
Host is up (0.015s latency).

PORT      STATE SERVICE
37830/tcp  open  unknown
```

 夜白君 关注

2 4

The image shows a Wireshark packet capture analysis of a STCOM communication. The packet list on the left shows a packet of length 28 bytes. The packet details pane on the right shows the structure of the STCOM message, including fields like Protocol Id, Message Id, Redundancy Identification, Protocol Data Unit Reference, Parameter Length, Data Length, and Parameters. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. A red arrow points to the 'Data Length' field (0x00000000) in the details pane, which corresponds to the 'Data Length' field (0x00000000) in the packet bytes pane. Another red arrow points to the 'Data Length' field (0x00000000) in the packet bytes pane, which corresponds to the 'Data Length' field (0x00000000) in the details pane.

Packet No.	Time	Source	Destination	Protocol	Length	Info
33	16.371454590000	39.105.136.152	202.96.154.100	STCOM	28	STCOM: 28 bytes [77/28]

Packet Details:

- STCOM [Stcom - ST Communication]
  - Header [Reader]
    - Protocol Id [61/1]
    - Message Id [62/1]
    - Redundancy Identification (Reserved) [63/2]
    - Protocol Data Unit Reference [64/2]
    - Parameter Length [65/2]
    - Data Length [66/2]
    - Parameters [71/14]
      - Function [72/9]
      - Unknown Bytes [73/9]
      - Length Part [77/1]
      - PI Service [78/9]
  - Extra Data:
    - 28 bytes [77/28]

Packet Bytes:

```

00000000  B8 81 98 CA 96 90 38 F9 D3 B4 54 2F 08 00 45 00 00 49 EC 89 40  ...6.8...T...E...J...8
00000010  8.9.v.1.....f.fo8
00000020  C6 2D 5D 9D 18 01 F6 89 18 00 03 00 00 21 32 19 85 32 01  --1f.....2.
00000030  00 00 06 00 00 10 00 29 10 00 00 00 00 09 50 53 4E 47  P.....P PROC
00000040  32 41 4D F1 31 32 31 7D FC 94 5A 21 00 00 00 49 31 58 78 4E  P.....P PROC
00000050  78 18 78 68 78 68 68 68 68 68 68 68 68 68 68 68 68 68  P.....P PROC

```

```
(root@kali)-[~/桌面]
# nc -nC 39.105.136.152 37830
29
29
00
00
0X32
0X32
```

 推荐热门

 工具榜单

 专享工具

 视频音频

 图形图像

 日期时间

 文字编辑

 加密解密

 编程开发

 计算换算

 金融理财

一个工具箱 - 好用的在线工具都在这里！

## TEA加密/解密

(a\_E^~O7o10!a=Yio嚮A0嚮!P6M|

密钥300

加密

解密

复制结果

flag3KJEWVJ3FoUIMn

[https://blog.csdn.net/qn\\_43264619](https://blog.csdn.net/qn_43264619)

## Flag{3KJJEwWJ3FoiJIMn}

2021CTF工业信息安全技能大赛第二场.rar 07-02  
2021CTF工业信息安全技能大赛第二场.rar

3 条评论 majorskywalker 热评 求附件 邮箱 sqx0817@gmail.com 谢谢! 写评论

...设备组态\_plc组态\_努力学习爱摸鱼的工程师的博客 7-19

【PLC学习一】设备组态 因为工作需要,开始学习工业控制必备的PLC编程,软件使用的是西门子博途V17. 设备...

2 4

- 2021CTF工业信息安全技能大赛-Fins协议通讯

qq\_43264813的博客 1001

2021CTF工业信息安全技能大赛-Fins协议通讯 工程师小夏在工控日志流量审计设备中发现某台PLC设备通讯...
- 台达plc与西门子v20变频器MODBUS-RTU通讯(设备上测试通过)\_台达plc与v...

7-14

西门子S7-200PLC与V20变频器MODBUS RTU通信教程 S7-200与V20的MODBUS RTU通讯 1、本教程的系...
- 如何远程读取西门子PLC数据并进行编程调试?\_西门子plc远程调试\_物通...

7-22

PLC设备本身不具备联网功能,采用网关来联网,可以定位设备的IP地址,建立一个远程调试操作的通道。2、以...
- 西门子HMI触摸屏设备“死机”或IO域出现“##”现象故障总结

Robot\_PLC\_自动化学院 5169

西门子HMI触摸屏设备“死机”或IO域出现“##”现象故障总结 当系统中有多台HMI设备连接同一个plc时, 如果IP...
- [纵横网络靶场社区]S7COMM协议分析

末初·mochu7 745

签到题, 过滤出s7comm协议, 降序排包的长度, 第一个包最后有一段hex 解码得到: is\_not\_real flag(is\_not\_...
- 如何快速实现西门子S7-200/300 PLC转Modbus-TCP协议与第三方数据对接...

7-21

因小季这边没有S7-300 PLC,拿西门子Smart 200 PLC 来举例:MW10地址的数据通过Modbus-TCP协议送到40...
- S7-1500与两台S7-1200 Profinet 通讯

ba\_wang\_mao的专栏 9039

警告: 本方案实现的是S7-1500和2台S7-1200都组态在同一个博图软件中, 然后实现S7-1500和2台S7-1200...
- 工控CTF之协议分析6——s7comm

song123sh的博客 1735

工控CTF之协议分析6——s7comm
- CTFHub S7协议恶意攻击分析 WP

qq\_61993117的博客 1473

S7协议恶意攻击分析 WP
- 西门子S7系列中间人攻击: 防御和流量异常检测 (三)

weixin\_43977912的博客 772

前言: 互联与共享成为工业控制系统新的发展方向, 工控系统与企业办公网和互联网逐渐相连, 工业控制网...
- CTF杂项总结 热门推荐

夏日のblog 1万+

目录 一、流量分析篇 二、文件头篇 三、压缩包篇 四、图片隐写篇 五、音频隐写篇 六、视频隐写 七、取证...
- CTF:S7comm协议受攻击报文分析

npu\_nazi的博客 204

某组织通过特殊手段获取到了城市供水企业的某些流量数据。作为安全研究人员需要分析出其中特殊流量数据...
- +

2021CTF工业信息安全技能大赛(济南站).zip

08-20

2021CTF工业信息安全技能大赛(济南站).zip
- +

2021CTF工业信息安全技能大赛(杭州站)

08-02

2021CTF工业信息安全技能大赛(杭州站)
- +

2021CTF工业信息安全技能大赛(常州站)

08-03

2021CTF工业信息安全技能大赛(常州站)
- +

2021CTF工业信息安全大赛第二场.rar

09-19

2021CTF工业信息安全大赛第二场题
- 西门子PLC S7-300出现通讯故障及远程维护办法

wtbl007的博客 1253

西门子S7-300是一款高性能、应用广泛的PLC设备, 模块化、分布式结构以及简单易学的操作, 使得西门子S...
- 西门子PLC S7-200cn和S7-200 smart 。 设备锁机程序

2301\_77710177的博客 206

有2个版本的西门子PLC 程序与对应昆仑通态触摸屏程序, 触摸屏程序包含两个版本一个是老版本MCGSSE软...
- TCP/IP协议专栏——以太网帧中的 Padding 和 Trailer 关系详解—...

weixin\_44081384的博客 2818

14 字节 ( Ethernet II 首部长度 ) + 28 字节 ( ARP 请求或应答 ) + 4 字节 ( 802.1Q ) + 14字节 (Padding 填充数...
- ctf安全竞赛入门 pdf 下载 最新发布

06-25

### 回答1: ctf安全竞赛是指网络安全领域的竞赛, 参加者需要展示其对于各种网络安全威胁的防范和攻击技...

“相关推荐”对你有帮助?

- 😞 非常没帮助

😐 没帮助

😐 一般

😊 有帮助

😄 非常有帮助

关于我们 招贤纳士 商务合作 寻求报道 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00

公安备案号11010502030143 京ICP备19004658号 京网文〔2020〕1039-165号 经营性网站备案信息  
北京互联网违法和不良信息举报中心 家长监护 网络110报警服务 中国互联网举报中心 Chrome商店下载 账号管理规范 版权与免责声明  
版权申诉 出版物许可证 营业执照 ©1999-2023北京创新乐知网络技术有限公司



夜白君

关注

2



4



6万+

2万+

11万+



原创

周排名

总排名

访问

等级

1290

351

60

108

152

积分

粉丝

获赞

评论

收藏























私信

关注

搜博主文章



热门文章

- 2021陇剑杯网络安全大赛-iOS  15348
- 2021年“绿城杯”网络安全大赛-Misc-流量分析  6296
- 2022第二届网刃杯网络安全大赛-ICS  5884
- 2022第二届网刃杯网络安全大赛-Re  4912
- 2021CTF工业信息安全技能大赛-PLC故障分析  3136

分类专栏

- 

漏洞复现

1篇
- 

HackTheBox

1篇
- 

2022第二届网刃杯网络安...

4篇
- 

2021年“莲城杯”网络安全...

13篇
- 

2021年“绿城杯”网络安全...

12篇
- 

2021陇剑杯网络安全大赛

8篇




最新评论

- 2021CTF工业信息安全技能大赛-异常的...  
iscaibird: 你好，可以问一下这个ciphey怎么安装吗
- 2021CTF工业信息安全技能大赛-损坏的...  
暮秋初九: 师傅你好好有原题吗
- 2021CTF工业信息安全技能大赛(常州站)...  
wgf42421: 用2022没显示这条有问题。。。同样从12303开始的。
- 夜刃CTF小组招募志同道合的CTFer  
\_小飒: 现在是web
- 夜刃CTF小组招募志同道合的CTFer  
夜白君: 什么方向

最新文章

- CVE-2013-7239 Memcached未授权访问漏洞复现
- HackTheBox系列-MonitorsTwo

 夜白君

关注

 2



 4

2023年 2篇      2022年 4篇  
2021年 77篇

目录

2021CTF工业信息安全技能大赛-异常的...

解题步骤:

- 1.1、对数据包进行重放发现400、40...
- 2.查看数据包内容发现一串疑似base...
- 3.对其进行解码得到一个字符串为TE...
- 4.使用nc连接目标端口，使用科来查...
- 5.将字符串进行16转ascii，再使用TE...
- 6.FLAG