CTF工业信息安全大赛实践与分析

原创

CanMeng'Blog 于 2020-03-17 13:41:02 发布 3050 收藏 28
文章标签： web 安全 安全漏洞 信息安全 数据安全

本篇文章主要结合作者工控信息安全及工控网络攻防平台CTF赛题编制等工作经验，首先对上周团队参与的2019工业信息安全大赛CTF线上比赛部分题目进行解析与总结，接着对CTF相关知识及平台进行介绍，最后对CTF收集的相关资源进行分享。我也是从今年开始接触CTF,所以写这篇文章的目的是希望能跟大家一起学习探讨工控安全CTF比赛相关知识。

一、概述

近年来，伴随着中国制造2025、两化融合及工业互联网等一系列国家战略逐步推进，工控网络安全作为一门新兴热门行业引起了不少人的关注，为了培养更多的工控安全人才，各种CTF安全比赛也是层出不穷，就连最近热播的“亲爱的亲爱的”电视剧里面K&K和SP战队也将CTF安全巡回大赛演绎的淋淋尽致，所以撰写一篇CTF相关的文章刻不容缓。

二、CTF 工业信息安全大赛线上题目回顾

2019 工业信息安全大赛第二场题目主要包括，破解加密数据、工控安全取证、恶意软件后门分析、隐藏的黑客、简单的工控固件逆向、奇怪的文件、简单的流量分析、另一个隐藏的黑客、特殊的工控流量10到题目，以及工业网络渗透测试和scada系统渗透测试2道场景题。

1.破解加解密数据题目分析

题目描述：

提供的加密算法文件如下：

```
m = "unknown"
e = 2
n = 0x6FBD096744B2B34B423D70C8FB19B541

assert(int(m.encode('hex'), 16) < n)
c = pow(int(m.encode('hex'), 16),e,n)
print c
#109930883401687215730636522935643539707
#330539799685O1614
```


1）解密方法，获取flag方式如下，flag为flag_EnCryp1

```python
# -*- coding: utf-8 -*-
import gmpy2
def main():
    n = 0x6FBD096744B2B34B423D70C8FB19B541
    e = 2
    # facordb
    p = 10848126018911527523
    q = 13691382465774455051
    cipher = 109930883401687215730636522935643539707
    N = n

    # rabin加密
    # rp + sq = 1 mod n
    inv_p = gmpy2.invert(p, q)
    inv_q = gmpy2.invert(q, p)
    mp = pow(cipher, (p + 1) / 4, p)
    mq = pow(cipher, (q + 1) / 4, q)
```



```python
    # 4个解
    a = (inv_p * p * mq + inv_q * q * mp) % N
    b = N - int(a)
    c = (inv_p * p * mq - inv_q * q * mp) % N
    d = N - int(c)
    # 找有效的解
    for i in (a, b, c, d):
        s = '%x' % i
        if len(s) % 2 != 0:
            s = '0' + s
    print(s.decode('hex'))
    pass

if __name__ == '__main__':
    main()
```

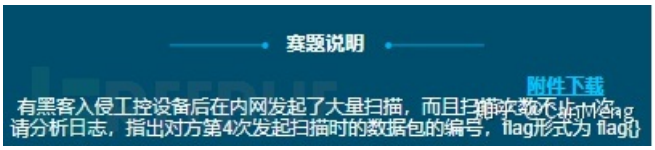
```
2.1答案
C:\Python27\python.exe E:/工作相关/项目开发/开展项目/网络攻防平台实训场景/比赛共题/工控安全取证题库
flag_EnCrypt
Process finished with exit code 0
```


题目总结与思考：

出题者刚开始只给了加密字符串，未提供加密算法，由于算法是自己写的，导致很多选手不能解出来，过了几个小时，出题方才提供了加密算法。

2.工控安全取证题目分析

题目描述：

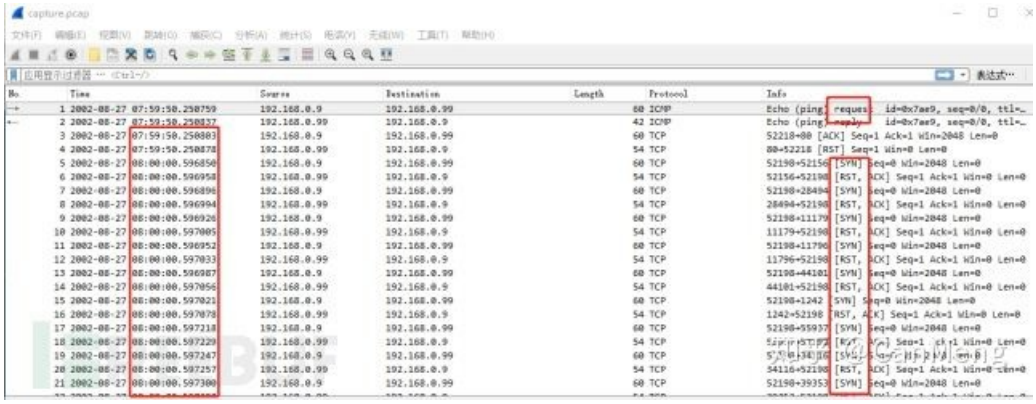


提供文件：capture.log

1）首先利用linux file命令查看日志文件属性，发现capture.log被出题者故意篡改过，对解题人进行迷惑。从下图中可以看出该文件为tcpdump 抓包后的文件

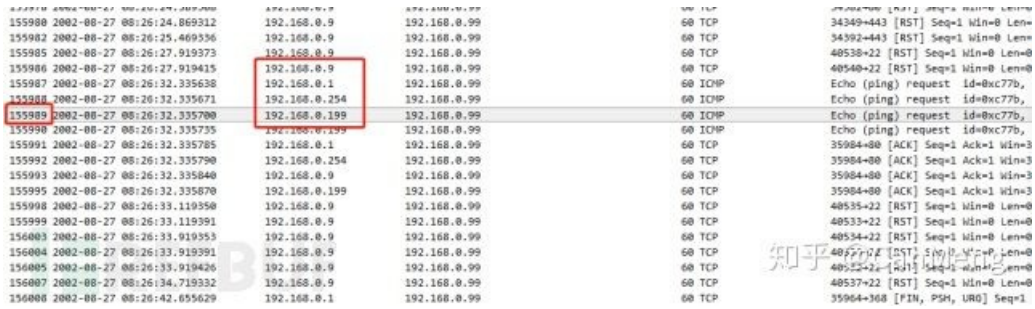
```
[root@localhost 工控安全取证]# file capture.log
capture.log: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 1514)
```

2）将文件名修改为capture.pcap 利用wireshark工具查看内容，如下



短时间内发送了大量syn端口扫描包，初步怀疑192.168.0.9主机发起syn端口扫描，找到第四次扫描包编号11，提交flag，平台提示答案不正确。

3)再次阅读题目理解出题人的意思，第四次发起扫描数据包编号，继续分析题目，发现数据报文有多个ip都对192.168.0.99目标机器进行扫描，分别为192.168.0.9、192.168.0.1、192.168.0.254、192.168.0.199，它们共同特点是每次发起端口扫描时候，先进行ping操作，尝试提交第四次发起扫描第一个报文编号155989，提交flag，显示成功。



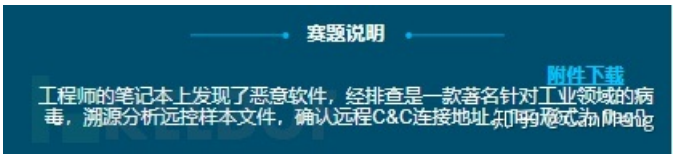
题目总结与思考：

1）一个黑客电脑为什么拥有多个源ip对目标机器进行端口扫描，第一种猜测可能是利用masscan等端口扫描工具时候，对源ip进行了隐藏与欺骗，防止触发IDS等系统告警。第二种可能是利用多个虚拟机分别进行扫描。可以利用masscan 192.168.0.99 -p–65535 –source-ip 192.168.0.199 –rate 2000进行自行验证。

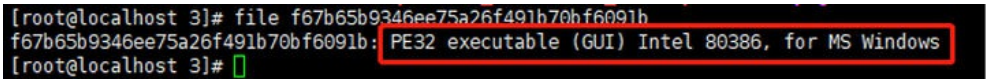
2）黑客对工控网络攻击，首先会利用诸如nmap、masscan等工具利用syn、fin或者ack等方式进行快速端口扫描，识别出重要工业控制资产类型，比如西门子plc(默认102端口)、施耐得plc(默认502端口)等控制设备，接着在进行工控资产识别，识别出plc具体厂商、型号、固件版本等信息。最后结合cnvd等漏洞库对plc发起攻击，比如利用如下漏洞进行plc 拒绝服务攻击。

3.恶意软件后门题目分析

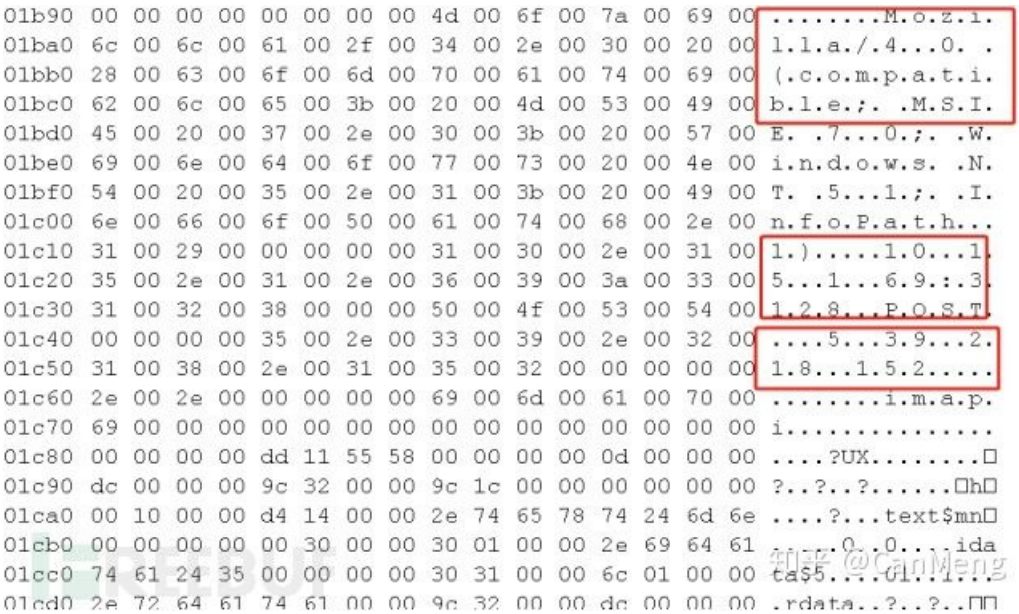
题目描述：



1)首先利用linux file命令查看文件类型，发现该恶意软件是windows平台下可执行文件，如下图所示



2)利用二进制查看工具对文件内容进行分析,关键内容如下所示



3）根据题目意思，寻找恶意样本发起远程连接的地址，可以推断，10.151.69.3.128主机通过http post方式往c&c远程地址5.39.218.152建立连接与通信，提交5.39.218.152 flag，提示成功。

题目总结与思考：

1）真实工业环境中，由于对工程师站、操作员站以及员工笔记本非法安装软件可能会引入捆绑的恶意软件，当工程师笔记本接入工业控制环境，工控网络、设备可能会被恶意软件发起信息收集、网络攻击等恶意行为，造成不可估量的后果。

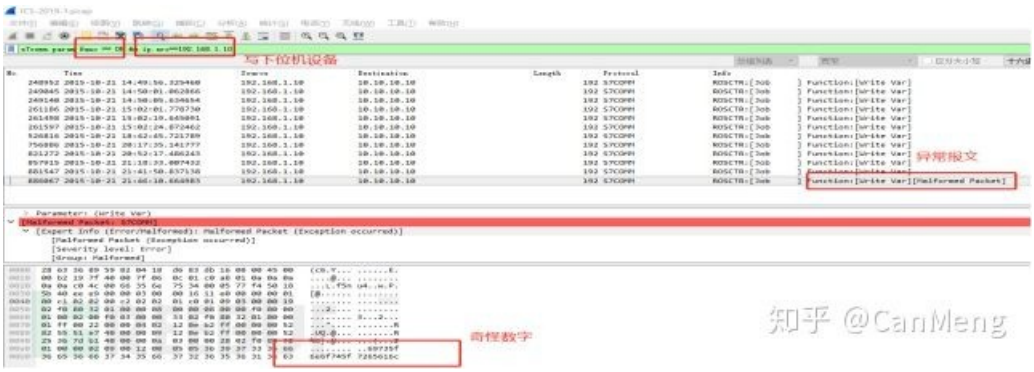
2）此题目描述和恶意样本内容与2018年工业信息安全大赛-西部赛区第4题为同一题，属于原题重现，所以平时多做多分析工控CTF历年大赛真题才是王道，题目资源可以从底部CTF相关赛题参考连接获得。

4.特殊的工控流量题目分析

题目描述：

1）首先利用wireshark打开数据包，初步流量数据报文，发现工控流量只有s7common，利用过滤条件过滤出工控流量如下图所示

2）根据以往编制工控协议CTF赛题相关经验，一般异常数据会出现在黑客篡改plc 寄存器的数据，引起plc非正常工作，所以首先想到对05写下位机设备功能码流量数据进行排查，如下图所示：



3）提取这串奇怪的数字发现为16进制，利用工具进行字符串转化，并提交is_not_real，平台显示成功，如下图所示：

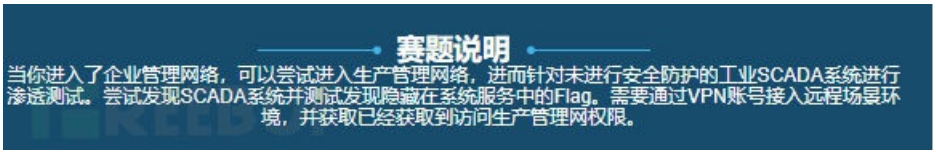
题目总结与思考：

1）工控协议异常流量，大多数早期工控协议如S7、modbus、ehternetip等均无授权、无认证保护，无防重放攻击等安全机制、任何攻击者都可以直接向使用这些工控协议的设备发起连接，进行寄存器值修改或者写入非协议规约的值，导致压力、流量等控制参数超出正常值，或plc设备异常，引起工控环境遭受破坏，造成不可估量的后果。

2）异常工控协议流量出题规律一般为往下位机设备写入一个不符合规约的值，或上载、下载一个带有flag.txt的文件，找出文件内容；也可能黑客对返回上位机开关量0xff 修改为0×00，欺骗上位机未对某设备进行关闭操作的知识点进行出题。

5、工业网络渗透测试及SCADA系统渗透测试场景题目分析

题目描述如下:



题目总结与思考：

由于需要答对前10道题目，场景题目才有机会进入，遗憾不能看到真实场景，所以根据自己以往出场景题经验，能对出题人的思路进行猜测。

1.举办方在远程服务器或自己公司搭建了一个webscada系统某工控行业工艺场景，并将webscada进行了发布。利用webscada存在的已知漏洞，比如目录遍历、弱密码算法之类的漏洞，进行服务器权限控制，进入服务器，寻找flag。

三、CTF 相关知识介绍

1.CTF比赛模式

CTF主要比赛模式分为线上模式和线下模式，包括解题模式、攻防模式、混合模式。

解题模式：

大多数为线上比赛，选手自由组队，出题者把平时信息安全遇到的问题抽象成一道题目，比如一个带有攻击的流量数据包让选手分析 一段密文让选手解密，一个图片里面隐藏线索让选手找等等，或者搭建一个靶场，让选手利用靶场漏洞，进行关键信息寻找。通过寻找题目中一串奇怪的字符串，也就是所谓的flag，提交它，就能获得这道题目的分数。通常用于在线选拔赛，题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

攻防模式：

大多数为线下比赛，通常3-5人组建参赛队伍，参赛队伍对自己服务器进行保护，对别人的服务器进行攻击。每个队伍的服务器拥有相同的配置和缺陷，比如账户弱口令、关键应用配置错误、web目录遍历与提取等缺陷，然后队员需要找出这些漏洞并进行加固防止对方攻破自己服务器获取分数，同时利用这些漏洞来攻击别人的服务器，拿到其他队伍的权限后，获取到相应flag后并提交。

混合模式：

结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

2.CTF 内容

CTF知识体系：

主要包括，程序分析、操作系统、数据库、计算机网络、安全工具、网络嗅探与协议分析、网络信息收集、密码学、取证分析、安全检测与渗透、防火墙技术原理、逆向分析、漏洞挖掘与利用、恶意代码分析、wireshark流量分析等。

CTF题目类型：

主要包括，WEB、逆向、PWN、移动安全、密码学和杂项等分类

> Web主要包括，sql注入、xss、文件上传、包含漏洞、命令执行等
> Pwn 主要包括，堆栈溢出、绕过保护机制、攻击远程服务器等
> Reverse主要包括，逆向破解程序、代码混淆等
> Mobile主要包括对安卓、ios 等app应用理解
> 密码学主要包括，现代密码、古典密码、近代密码及自编写密码算法理解
> 杂项主要包括，隐写、取证、编解码、压缩包等

3.CTF比赛平台

利用CTF平台及相关靶场主要提供多种对抗实操模式，主要包括单兵演练、闯关演练、红蓝对抗、分组对抗、夺旗竞赛等功能，并可配置多种比赛场景。

利用CTF平台，提供网络安全、工业网络攻防、虚拟化场景、漏洞挖掘、逆向分析、考试练习等实操。

四、CTF 资源推荐

1.《CTF 工具集》包括web工具、渗透环境、隐形工具、逆向工具、漏洞扫描工具、sql注入工具、暴力破解工具、加解密工具等等。

> 参考地址： https://www.ctftools.com/down/

2.《CTF 竞赛入门指南》包括linux基础、web安全基础、逆向工程基础、密码学基础、安卓基础、漏洞分析、CTF主要工具使用、题解篇、实战篇等。

> 参考地址： https://firmianay.gitbooks.io/ctf-all-in-one/content/

3. 《工控CTF大赛相关赛题》包括2018工业信息安全大赛、2019工业信息安全大赛、2018护网杯等题目。

> 参考地址： https://github.com/ddyy0308/CTF

4.《awesome-ctf》

> 参考地址： https://github.com/apsdehal/awesome-ctf

五、总结

本次线上比赛第一二场题目未见有工控资产指纹识别、组态软件工业流程分析、plc梯形图运算等相关试题，也许是这些类型的题目对非工控人员难度太大的原因，可能线下赛会有此类型题目出现。

由于工控安全是一门多技术交叉学科，需要同时掌握好信息安全和工业控制自动化等相关技术，目前这方面的专业人才较为缺乏，所以希望通过工控CTF竞赛、工控网络攻防实训平台、工控安全行业靶场来促进工业互联网安全人才的技能提升。

***本文作者：yy0308，转载请注明来自http://FreeBuf.COM**