


工控CTF之协议分析8——特殊隧道

原创 Shadow、S 于 2022-12-20 21:15:50 发布 756 收藏 版权

分类专栏: CTF刷题 工控 文章标签: 安全 网络协议

CTF刷题 同时被 2 个专栏收录 8 订阅 27 篇文章 订阅专栏

协议分析

流量分析

主要以 **工控** 流量和恶意流量为主，难度较低的题目主要考察Wireshark使用和找规律，难度较高的题目主要考察协议定义和特征
简单只能简单得千篇一律，难可以难得五花八门

常见的工控协议有：Modbus、MMS、IEC60870、MQTT、CoAP、COTP、IEC104、IEC61850、S7comm、OMRON等

由于工控技术起步较早但是统一的协议规范制定较晚，所以许多工业设备都有自己的协议，网上资料数量视其设备普及程度而定，还有部分协议为国家制定，但仅在自己国内使用，网上资料数量视其影响力而定

CTF之协议分析文章合集

- 工控CTF之协议分析1——Modbus
- 工控CTF之协议分析2——MMS
- 工控CTF之协议分析3——IEC60870
- 工控CTF之协议分析4——MQTT
- 工控CTF之协议分析5——COTP
- 工控CTF之协议分析6——s7comm
- 工控CTF之协议分析7——OMRON
- 工控CTF之协议分析8——特殊隧道
- 工控CTF之协议分析9——其他协议

文中题目链接如下

站内下载

网盘下载：<https://pan.baidu.com/s/1vWowLRkd0ldvL8GoMxG-tA?pwd=jkkkg>
提取码：jkkkg

特殊隧道

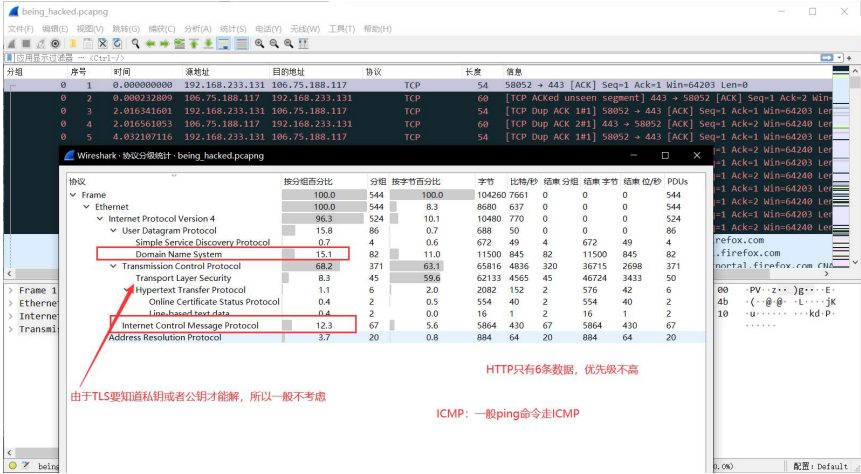
基于各类**数据传输协议的数据传输功能实现的数据传输**都可以称为隧道

实际上因为协议层层嵌套的关系，任何协议都可以算是基于其底层协议的隧道

如 基于TCP的隧道、基于UDP的隧道、基于ICMP的隧道
这种类型的题可能比较杂而且比较综合

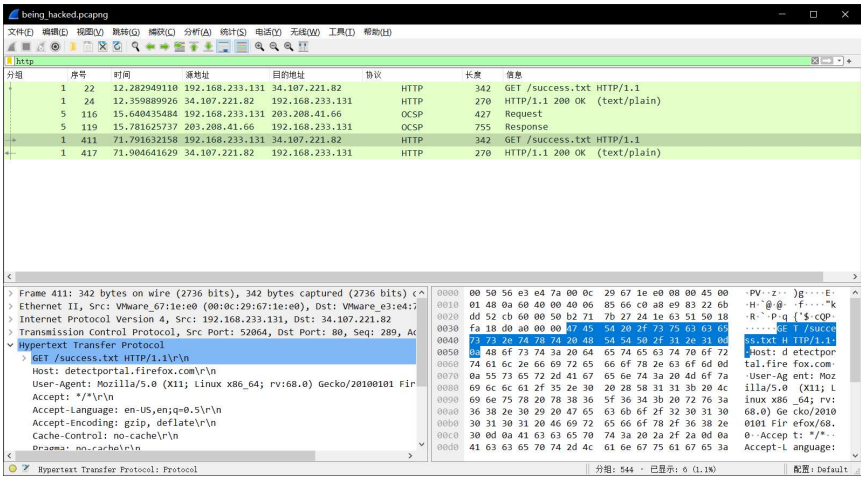
例题1 2022HMGK-being_hacked

先看协议分级，没有特殊的协议，那就逐步分析



先看dns, 发现都是一些很正常的域名请求, 最后有一个arp, 但是也没有异常点

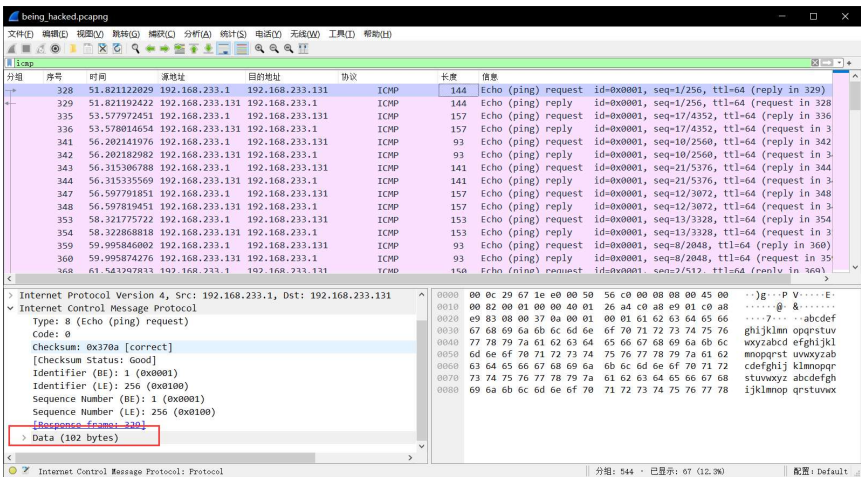
http请求也是一个很正常的



最后来看ICMP

发现都是ping请求, 传输的数据也都是字母表, 只不过长度不同, 这是不正常的, ping的时候发包长度默认32字节

发现数据长度都是100左右以及50左右的数字, 联想到ascii码表



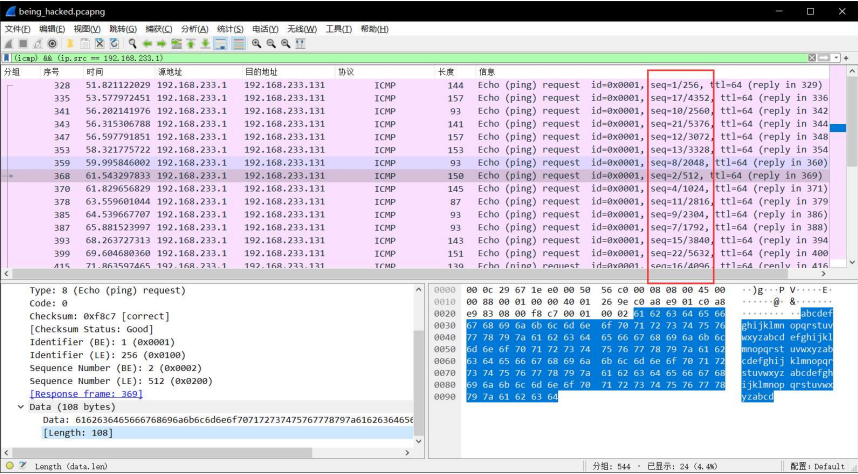
都是两条相同的数据, 请求和返回, 先筛选出一半来

(icmp) && (ip.src == 192.168.233.1)

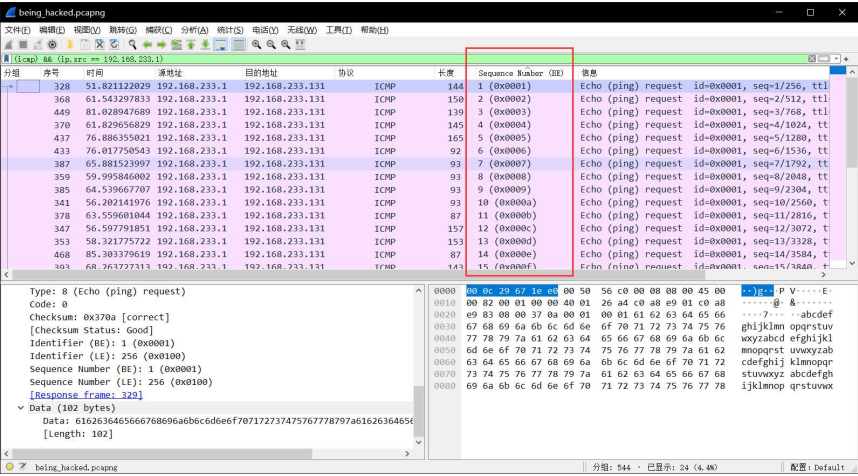
提取数据长度, 得到顺序错误的flag

E:\0\CTF\工控\工控CTF培训\fs3cso3lg-33emap2{y

重回流量包中，发现seq可能是排序



将seq作为一列，对数据排序



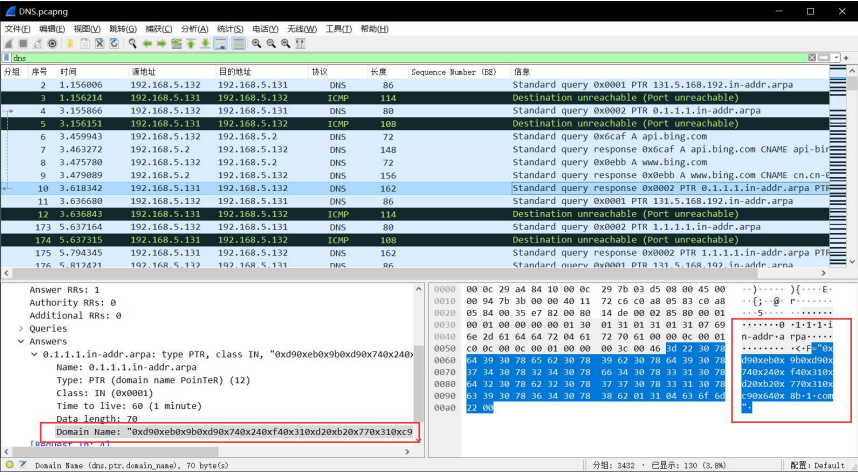
重新与脚本提取

```
(b'flag{23333-so-easy-icmp}')
```

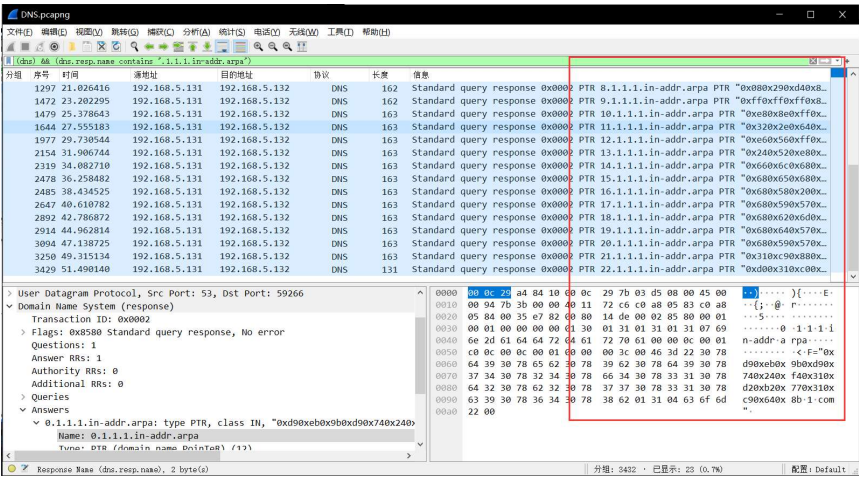
例题2 2021CISC兰州站—DNS

偏脑洞

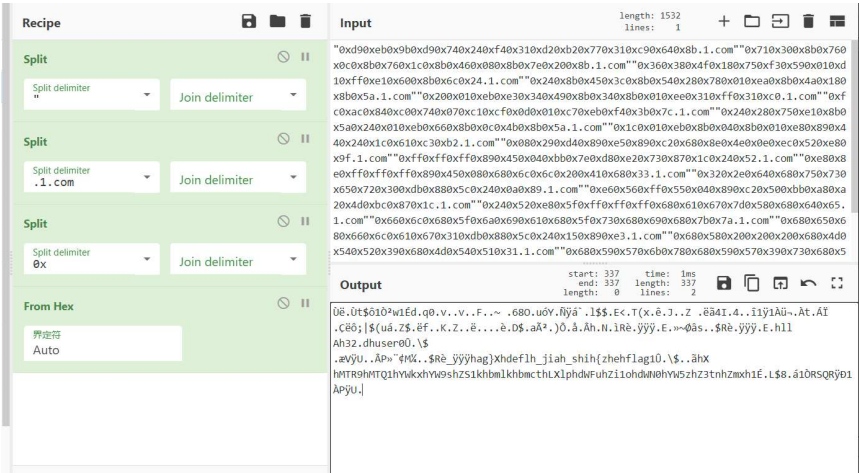
发现查询0.1.1.1返回的数据中有奇怪的域名，一串加密后的字符加上 .1.com，很明显这是不正常的



再往后有看到，查询1.1.1.1, 2.1.1.1, 3.1.1.1等等，返回的结果也都是这种很奇怪的域名
先将其筛选出来

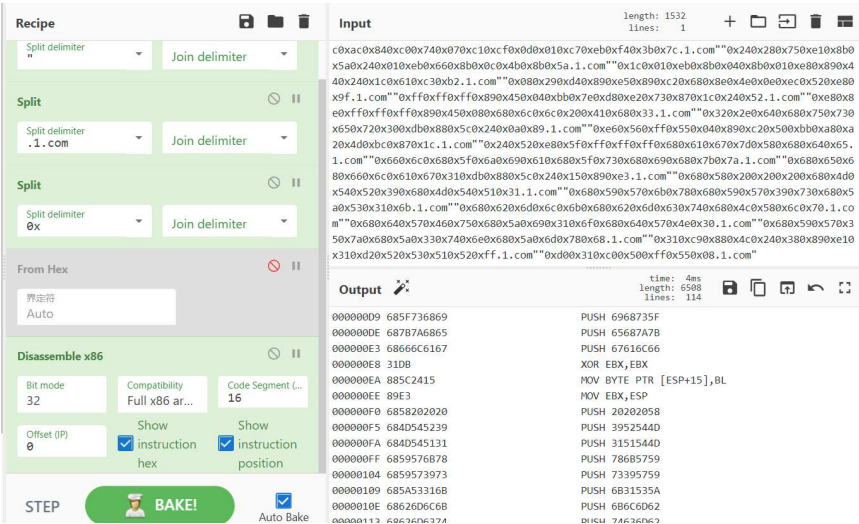


提取数据并尝试解码



得到一串看似规则的乱码

各种尝试之后，想到汇编，这个实际上是一个可执行的shellcode



忙活半天是一个假的flag

Recipe

Find / Replace

Find
PUSH
REGE X

Replace

☒ Global match

☐ Case insensitive

☒ Multiline matching

☐ Dot matches all

From Hex

Delimiter
Auto

Reverse

By
Character

From Base64

Input

PUSH 587D6761
PUSH 6C666564
PUSH 61696A5F
PUSH 6968735F
PUSH 65687A7B
PUSH 67616C66

Output

flag{zhe_shi_jiade flag}X

往后接着找，因为他其实有多个PUSH

Find / Replace

Find
PUSH
REGE X

Replace

☒ Global match

☐ Case insensitive

☒ Multiline matching

☐ Dot matches all

From Hex

Delimiter
Auto

Reverse

By
Character

From Base64

Input

PUSH 20202058
PUSH 3952544D
PUSH 3151544D
PUSH 786B5759
PUSH 73395759
PUSH 6B31535A
PUSH 6B6C6D62
PUSH 74636D62
PUSH 706C584C
PUSH 75465764
PUSH 6F31695A
PUSH 304E5764
PUSH 7A355759
PUSH 6E74335A

Output

flag{gansuctf-huan-ying-nide-daolai114514}

文章知识点与官方知识档案匹配，可进一步学习相关知识

网络技能树 支撑应用程序的协议 应用层的作用 35916 人正在系统学习中

2020全国工业互联网安全技术技能大赛题目
含有misc, re, crypto, pwn及题目说明

10-28

Hack The Boo 2022 CTF 题目writeups
HackTheBoo 2022 CTF WP

Ba1_Ma0的博客 642

CTF数据分析题:A记录_ctf dns流量 typea_怀揣梦想的大鸡腿的博客-CSDN...
分析:首先,看视频,那么是视频网站。 截取了数据包,那么格式给了,是cap,无线网络的数据包。 这次提...

7-23

CTFHUB- DNS重绑定 Bypass(小宇特详解)_小宇特详解的博客
tdsourcetag=s_pctim_aiomsg DNS重绑定

7-23

CTF杂项总结

Shadow、S

关注

1 0

https://blog.csdn.net/song123sh/article/details/128388457

5/8

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...

利用DNS协议回显数据 hl1293348082的专栏 317
这个问题已经是去年提出的了，之前也看到过，在 CTF 题目环境中利用过却对原理不慎了解，在公司...

CTF-数据分析(三)_对所给的菜刀数据包分析,获得flag_红烧兔纸的博客-CS... 7-11
CTF-数据分析(三) 5.数据包分析- DNS (来源:网络) 1.关卡描述 2.解题步骤 2.1 点击题目查看描述并下...

工控CTF (wp) aarong的博客 7089
这里写自定义目录标题欢迎使用Markdown编辑器新的改变功能快捷键合理的创建标题，有助于目录的...

CTF——MISC——流量分析 热门推荐 小锤队长的博客 2万+
目录 一、流量包修复 二、协议分析 三、数据提取 例题： 1，题目：Cephalopod(图片提取) 2,题目： ...

工控CTF之协议分析2——MMS song123sh的博客 1035
工控CTF之协议分析2——MMS

工控CTF之协议分析7——OMRON song123sh的博客 864
工控CTF之协议分析7——OMRON

CTF-网络数据分析溯源(DNS服务器地址) asd158923328的博客 1991
根据题意 进入环境，下载文件，用wireshark加载 wireshark筛选udp.port==53或者DNS 使用率最高的...

DNS协议分析 u012425770的博客 3818
DNS (Domain Name System, 域名系统) 是因特网上作为域名和IP地址相互映射的一个分布式数据...

2021CTF工业信息安全大赛第一场题.rar 07-02
2021CTF工业信息安全大赛第一场题.rar

从CTF到工控安全.pdf 02-26
从CTF到工控安全.pdf

一道MMS工控协议CTF题的WriteUp-附件资源 03-05
一道MMS工控协议CTF题的WriteUp-附件资源

工控CTF协议分析学习题目合集 12-20
主页工控CTF学习配套题目，搭配学习

DNS攻击流量识别思考 makaisghr的专栏 1917
DNS攻击流量识别思考 分析思路 考察DNS安全问题，因此首先寻找都有哪些DNS安全问题。主要思...

DNS隧道特征 Ds的博客 488
传统基于UDP DNS Tunnel特征 1、DNS攻击建模 密集请求型：例如随机子域名DDoS、反射型DDoS...

MISC：流量包取证 (pcap文件修复、协议分析、数据提取) 小哈里的博客 2454
鼠标协议：每一个数据包的数据区有四个字节，第一个字节代表按键，当取 0x00 时，代表没有按键、...

DNS协议分析 第6关 指定服务器的DNS报文分析 qq_67667368的博客 231
指定服务器的DNS报文分析

ctf中常用的PHP伪协议 最新发布 02-15
在CTF比赛中，经常会使用PHP伪协议来绕过服务器的安全限制或者执行本不应该执行的操作。 PHP...

“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

 Shadow、S
码龄4年 高校学生

126 原创

4万+ 周排名

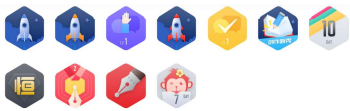
2万+ 总排名

25万+ 访问

 等级

 Shadow、S 关注

1 0



私信

关注

搜博文文章

Q

热门文章

- 【计算机网络】IP地址详解 27683
- DOS攻击 21648
- ACL原理及配置 14442
- eNSP下载安装超详细，华为模拟器下载安装 11328
- 域——windows服务器域详解 8888

分类专栏

	CTF刷题	27篇
	工控	9篇
	渗透测试	55篇
	逆向分析	1篇
	网络安全	46篇
	计算机网络	16篇

最新评论

- 【计算机网络】IP地址详解
大口喝咖啡: 应该是本地地址吧
- 华为模拟器eNSP免费下载
指尖上的围春: 链接挂了
- 域——windows服务器域详解
Shadow、S: 什么参数，具体点
- 域——windows服务器域详解
sweet-琉璃: 参数不正确怎么办呢？
- 华为模拟器eNSP免费下载
打码不打你: 文件没了

最新文章

- LitCTF2023 WP
- 工控CTF之协议分析7——OMRON
- 工控CTF之协议分析6——s7comm

2023年 1篇

2022年 91篇

2021年 34篇

目录

协议分析

CTF之协议分析文章合集

共151页 10860字

Shadow、S

关注

1

0

例题2 2021CISC兰州站—DNS



Shadow、S

关注



1



0