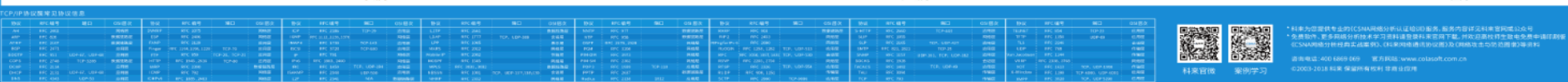




# 解构协议解码

李飞 成都科来软件有限公司 产品运营总监

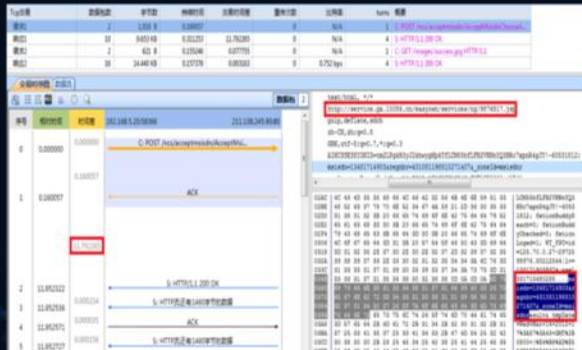
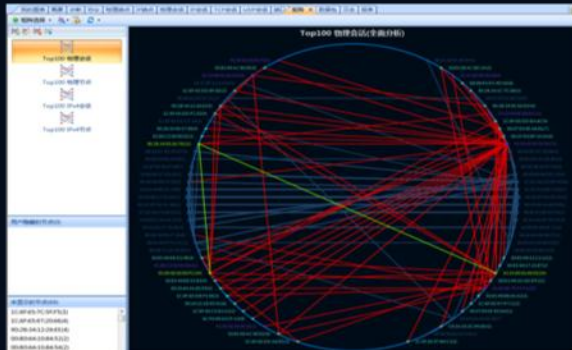
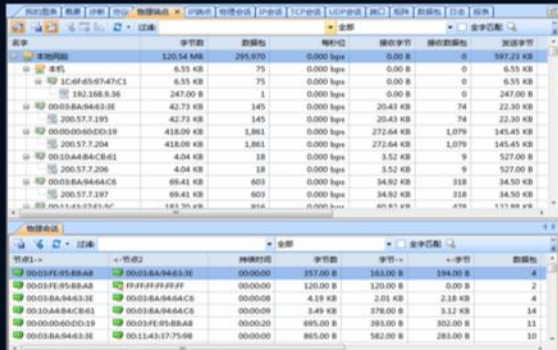
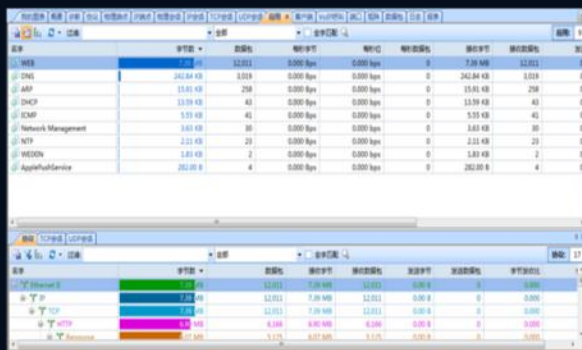






# 科来网络分析系统（技术交流免费版）

FIT 2019





# CSNA网络分析认证

FI 2019

CSNA-A 《网络分析服务认证》 各种实战方法训练

CSNA-E 《网络分析体系认证》 网络分析知识体系

CSNA-S 《高级安全实战认证》 高级攻击分析为主







## 相关学习资源

FIIT 2019

### 软件下载

科来网络分析系统11.1（技术交流免费版）

网络分析工具

科来MAC地址扫描器

科来Ping工具

科来数据包播放器

科来数据包生成器

### 学习资源

网络攻击与防范图谱

科来网络通讯协议图，TCP/IP网络协议图免费下载

科来网络故障诊断图

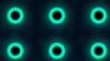
网络分析案例集

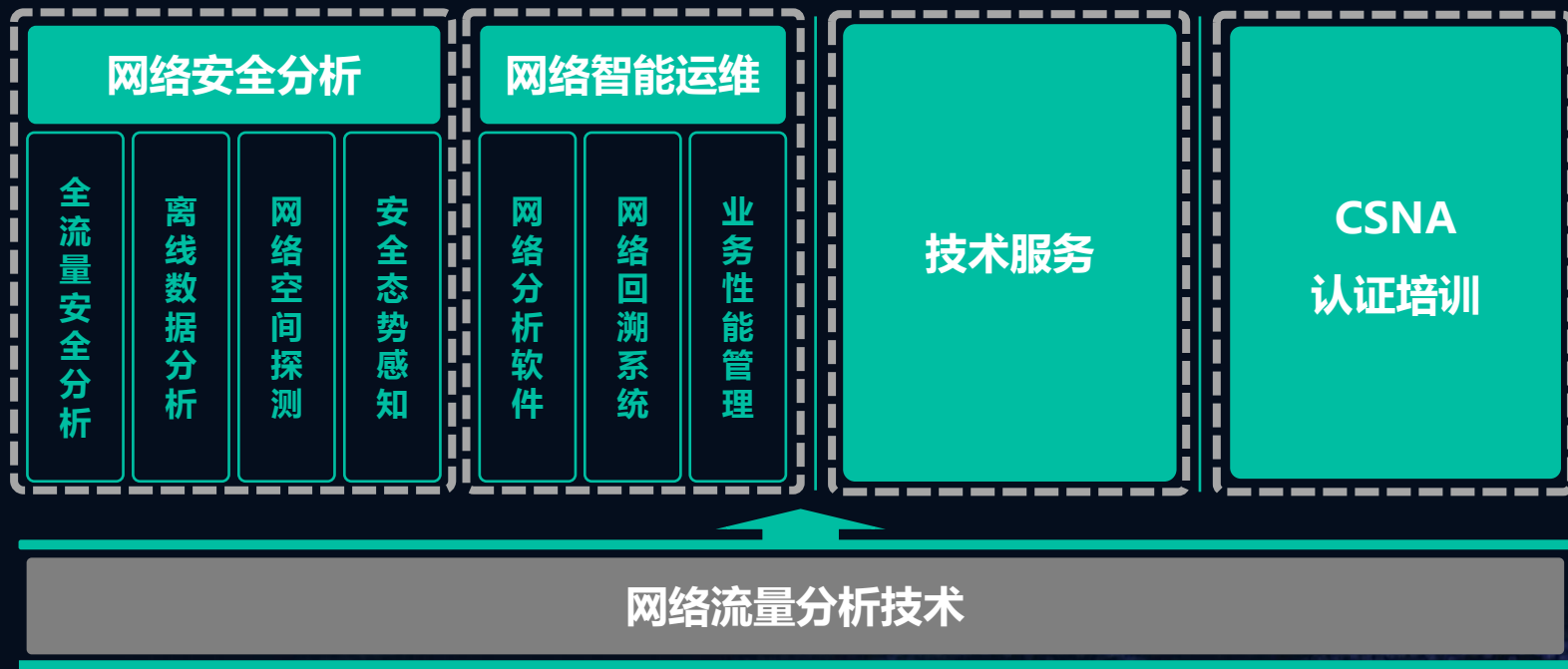
数据包样本

网络分析过滤器

网络分析技术学习资料

术语表



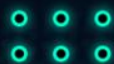




# 网络流量分析的一般过程

FIIT 2019

- ◆ 网络流量分析核心数据分析
- ◆ 基本的互联网通信协议都有在RFC文件内详细说明





# 协议解码举例

IT 2019

仪表盘 概要 诊断

仪表盘 概要 诊断

概要 诊断 协议 物理端点 IP端点 TCP会话 矩阵 数据包 日志 报表

0000 00 17 16 02  
001D 6E 73 7C 11  
003A 2F 63 72 6F  
0057 63 65 70 74  
0074 68 2D 43 4E  
0091 32 2C 33 34  
00AE 64 65 66 6C  
00CB 34 2E 30 20  
00E8 6E 64 6F 77  
0105 3B 2D 2E 4E  
0122 52 20 33 2E  
013F 2E 33 30 37  
015C 6F 2E 63 6F  
0179 0D 0A 43 6F  
0196 6C 64 48 76  
01B3 3D 33 26 73  
01D0 51 25 33 44  
01ED 62 39 35 32  
020A 63 68 6F 6E  
0227 39 66 36 63  
0244 34 65 5F 30  
0261 35 30 32 38  
027E 32 64 30 38  
029B 25 32 43 30  
02B8 61 39 65 64  
02D5 63 32 33 31  
02F2 35 32 63 33  
030F 30 64 62 32  
032C 49 74 65 6D  
0349 34 31 36 32  
0366 5F 64 65 66  
0383 32 63 30 30  
03A0 36 62 3B 20  
03BD 74 41 25 33  
03DA 31 35 34 39  
03F7 25 38 45 25  
0414 35 25 42 37  
0431 39 37 5F 5B  
044E 69 74 6F 72  
046B 65 73 73 69  
0488 65 2F 75 5F  
04A5 74 61 2E 74  
04C2 70 22 7D 5D

以太网 - II

目标地址: [S...]  
源地址: [S...]  
协议类型: [S...]  
版本: [Vers...]  
头部长度: [S...]  
区分服务字: [S...]  
不同的服...  
传输协议: [S...]  
拥塞: [C...]  
总长度: [To...]  
标识: [Iden...]  
分段标志: [S...]  
保留: [R...]  
分段: [F...]  
更多分段...  
分段偏移量: [S...]  
生存时间: [S...]  
上层协议: [S...]  
校验和: [Ch...]  
源IP地址: [S...]  
目标IP地址: [S...]

TCP - 传输控

源端口: [So...]  
目标端口: [S...]  
序列号: [Se...]  
下一个序...  
确认号: [Ac...]  
TCP偏移量: [S...]  
标志: [Flag...]  
紧急位: [S...]  
确认位: [S...]  
紧迫位: [S...]  
重置位: [S...]  
同步位: [S...]  
终止位: [S...]  
窗口: [Wind...]  
校验和: [Ch...]

节点1->

<-节点2

数据包

字节

协议

持续时间

字节->

192.168.10.138:3946	123.125.50.23:110	20	2.328 KB	POP3	0	647 B	1.6
192.168.10.138:3948	203.209.228.241:110	83	64.837 KB	POP3	1	1.827 KB	63.0
192.168.10.138:3951	203.209.228.241:110	82	64.774 KB	POP3	1	1.827 KB	62.9
192.168.10.138:3971	203.209.228.241:110	83	64.837 KB	POP3	0	1.827 KB	63.0
192.168.10.138:4013	203.209.228.241:110	82	64.774 KB	POP3	0	1.827 KB	62.9
192.168.10.138:4017	203.209.228.241:110	83	64.831 KB	POP3	0	1.884 KB	62.9
192.168.10.138:4145	203.209.228.241:110	84	64.894 KB	POP3	8	1.884 KB	63.0
192.168.10.138:4148	203.209.228.241:110	98	66.050 KB	POP3	22	2.351 KB	63.6

数据包 数据流 时序图

数据包 数据流 时序图

端点 1: IP 地址 = 192.168.10.138, TCP  
端点 2: IP 地址 = 123.125.50.23, TCP

相对时间	概要	192.168.10.138: ...
0.000000	Seq = 0, Next Seq = 1	Window = 8192
0.173119		SYN
0.173222	Seq = 1, Ack = 0, Next ...	Window = 68
0.271441		PSH, ACK, 载荷长度 = 87
0.277948	Seq = 1, Ack = 87, Nex...	Window = 67
0.323141		ACK
0.323317		PSH, ACK, 载荷长度 = 15
0.335482	Seq = 16, Ack = 102, N...	Window = 67
0.372609		PSH, ACK, 载荷长度 = 37
0.381130	Seq = 32, Ack = 139, N...	Window = 67

+OK Welcome to coremail Mail Pop3

USER long\_323

+OK core mail

PASS [REDACTED]

+OK 26 message(s) [1203339 byte(s)]

STAT





## 可以输出结构化的元数据

2019



### 网络会话层元数据

源IP、源端口、源IP国家、  
目的IP、目的端口、目的IP  
国家、协议、数据包个数、  
会话开始时间、会话结束  
时间、会话持续时间...



### 应用层元数据（量巨大）

如HTTP协议，主要25个关键字  
段，包括user-agent、cookie、  
host、refer等；  
如15种DNS协议字段、  
SMTP/POP3协议字段...





# 应用与业务场景

FIIT 2019





# 网络安全检测举例：网络窃密行为发现

2019

- ① **异常行为模型**：元数据模型：HTTP 1.1；Content-Type: image/png or jpg；Content-Length: >50MB；Or 数据交易次数>150
- ② **回溯分析**：发现HTTP头部标明传输为图片格式，但数据包头没有图片格式头部请求路径一致，每次“图片”大小不一样，每次传输超过100MB，传图片前2小时层解析过境外的服务器，并且有可疑通讯

```
GET /image/login_bt1.png HTTP/1.1
Referer: http://[redacted]com/image/
Accept: */*
Range: bytes=132645864-
User-Agent: Mozilla/4.0 (Windows 95;US) Opera 3.6
Host: [redacted].com
Connection: Keep-Alive
Cache-Control: no-cache
```

```
HTTP/1.1 206 Partial Content
Content-Type: image/png
Accept-Ranges: bytes
ETag: "270443163"
Last-Modified: Thu, 03 Nov 2016 14:28:33 GMT
Content-Range: bytes 132645864-265289727/265289728
Content-Length: 132643864
Date: Fri, 04 Nov 2016 02:04:12 GMT
Server: nginx
```

```
GET /image/login_bt1.png HTTP/1.1
Referer: http://[redacted]com/image/
Accept: */*
Range: bytes=132645864-
User-Agent: Mozilla/4.0 (Windows 95;US) Opera 3.60 [en]
Host: [redacted]com
Connection: Keep-Alive
Cache-Control: no-cache
```

```
HTTP/1.1 206 Partial Content
Content-Type: image/png
Accept-Ranges: bytes
ETag: "270443163"
Last-Modified: Thu, 03 Nov 2016 14:28:33 GMT
Content-Range: bytes 132645864-265289727/265289728
Content-Length: 132643864
Date: Fri, 04 Nov 2016 02:04:12 GMT
Server: nginx
```

新=柳).編溫??.問慘0?5b錫M?, 補I購?S?鸡富筵間磨?o鐘?韓.%;  
.豹#?錫椅賦?/?錫媽?Q(偏2穰e ...?烤.鈺y.部d1.8?7?鏗QL^4.  
az.{ } 落-9R備n?z1?未.漫.?趁撻媽'樓?蟻U簞7吟  
f棉L?.娛.祗蟻 1q蟻?.X?`关?消! y蟻3B鈔合p8Ep?星?鐵盤樣  
... ..

节点 1: IP 地址 = [redacted], TCP 端口 = 49667  
节点 2: IP 地址 = 10.200.1.54, TCP 端口 = 80

```
GET /image/login_bt1.png HTTP/1.1
Referer: http://[redacted]com/image/
Accept: */*
User-Agent: Mozilla/4.0 (Windows 95;US) Opera 3.60 [en]
Host: [redacted]com
Connection: Keep-Alive
Cache-Control: no-cache
```

```
HTTP/1.1 200 OK
Content-Type: image/png
Accept-Ranges: bytes
ETag: "270443163"
Last-Modified: Thu, 03 Nov 2016 14:28:33 GMT
Content-Length: 265289728
Date: Fri, 04 Nov 2016 02:04:06 GMT
Server: nginx
```

..? I.X. .漢推嗎?網環膠膠綫u?仿kmU摺\$<@參.??O?w?徑樣[輯P誌(M  
館曉\_闊.築規錫x^a給a^ 20 鶴.< 8半/ 嬰媽;P詢侯,濕魁.../道  
f包?e ?早冷?2o園蠅蚰鈔激?鈔卜傳1??还間[, ??伦.p色R莖莖?紅  
... ..



# 网络安全检测举例：用户与实体行为分析（UEBA）

2019

哪些用户访问？活跃度？

和哪些主机通信？

安全事件类型和频度



流量区间如何？

系统外联分布和频度

实体

通信协议有哪些？

IP、账号、主机

时间点

应用程序偏好

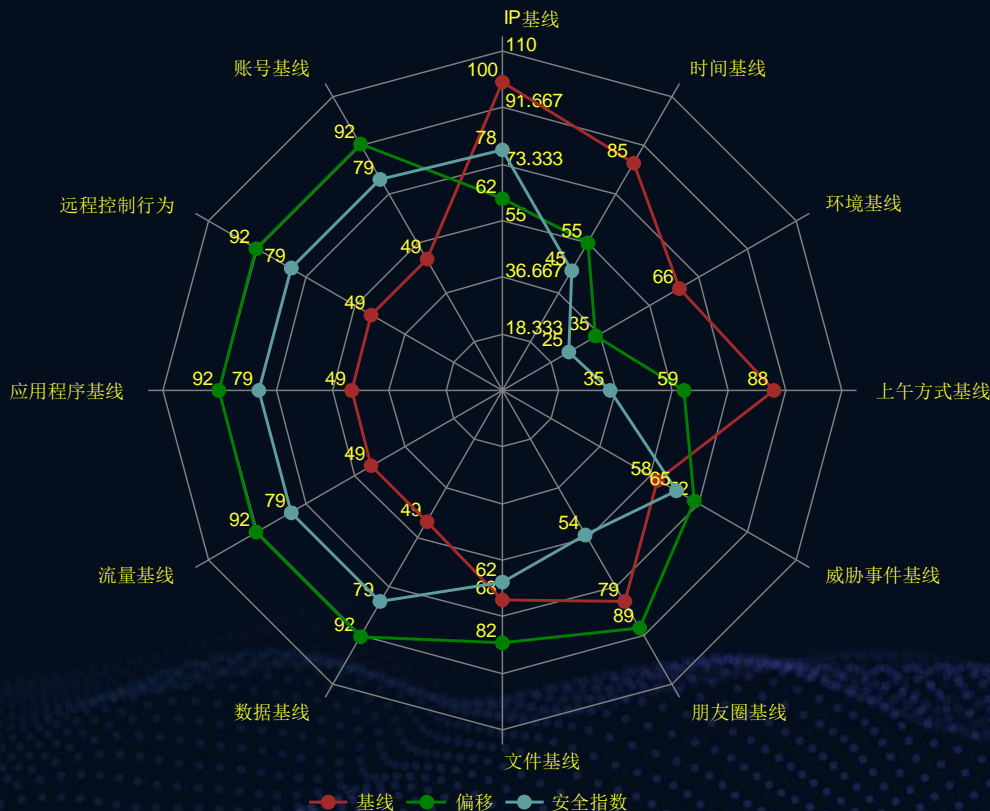


流量和频度

网络环境

人

设备环境





### 运行监控

网络运行 业务运行 交易行为

### 态势感知

网络攻击 资产态势 失陷主机

### 事件定位

全数据查询 多段对比 钻取式分析

### 驱动处置

处置建议 处置策略

### 数据分析

网络元数据建模

机器学习

告警归集

关联匹配

### 数据仓库

HDFS分布式文件系统

HBase分布式列存储数据库

### 流量数据

网络流量分析

### 终端数据

EDR, 杀毒

### 日志数据

防火墙、入侵防御  
防病毒、入侵检测

### 其他接口

威胁情报  
漏洞库, 事件通报





# 网络空间探测

2019

应用服务

设备信息

威胁情报

流量日志



详细信

位置

ASN

应用程

操作系

设备类

所属组

运营商

## • 端口 (选中查看服务信息, 最多同时选择3项)

81

83

443

80

21

22

1521

8080

## • 服务

81

tcp

xtremerat

HTTP/1.1 200 OK  
Server: nginx/1.12.2  
Date: Mon, 19 Nov 2018 07:20:38 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
Bdpagetype: 1  
Bdqid: 0x86179b22000137ca

83

tcp

http-simple-new

HTTP/1.1 200 OK  
Server: nginx/1.12.2  
Date: Mon, 19 Nov 2018 07:20:38 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
Bdpagetype: 1  
Bdqid: 0x86179b22000137ca

81

81

tcp

HTTP/1.1 200 OK  
Server: nginx/1.12.2  
Date: Mon, 19 Nov 2018 07:20:38 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive

## • 相关IP (10)

IP	标签	时间
1.2.4.3	低信誉IP	2018-10-18
2.4.3.5	恶意软件	2018-09-01
5.7.6.8	僵尸网络	2018-07-07

▼ 查看全部

## • 相关域名 (5)

域名	标签	时间
xxx.com	低信誉IP	2018-10-18
xx.cn	恶意软件	2018-09-01
xxxx.net	僵尸网络	2018-07-07

▼ 查看全部

## • 相关样本 (99)

样本	标签	时间
f43e45ff23ac52	信息窃取	2018-10-18



# 网络与交易性能分析

2019

业务性能分析

Internet Banking

生成SLA报告

业务设置

集中监控

业务指标分析

监控

分析

2017-03-09 08:28:00 - 2017-03-09 09:28:00

< 警报

警报 >

刻度: 分钟 小时 天

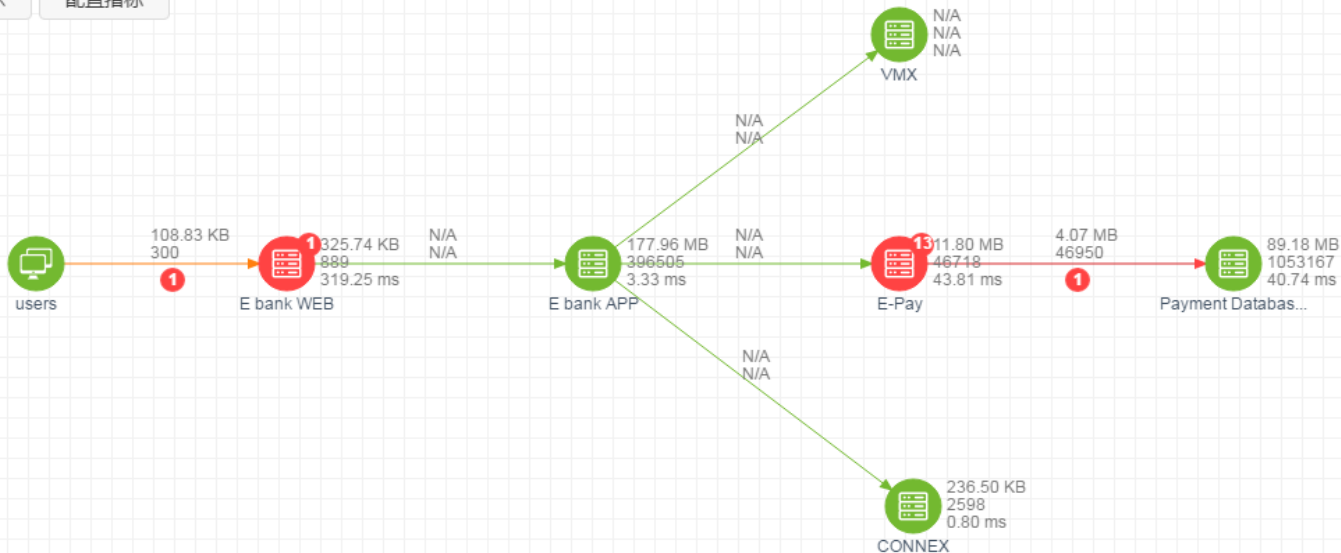
■ 正常 ■ 高 ■ 中 ■ 低



全景显示

居中显示

配置指标





# 协议解码

将非结构化数据转成结构化  
为大数据分析做好数据准备

新的  
协议

新协议、新协议版本  
解码需求变更

解码  
性能

流量快速增长  
更高的性能需求





# 科来快速解码引擎 ( FPDE )

## Fast Protocol Decode Engine

专为协议解码设计的一种解释语言技术



**灵活可扩展**

协议、字段自定义  
快速部署



**高性能**

万兆+全解码  
高稳定性





# 科来网路元数据分析探针 (MDA)

2019



- ◆ 单机1Gbps-40Gbps流量全解码
- ◆ 内置400+协议解码器
- ◆ 脚本化解码器开发语言，二次开发难度低
- ◆ 自定义解码数据封装
- ◆ 支持Kafka、Syslog、Flume等接口对外输出







REEBUF | TIT

THANKS