

# 入侵事件的高效发现、分析与取证

--基于SOAPA架构的智能安全平台

周宏斌 | 兰云科技联合创始人、高级副总裁

# 目录

## CONTENTS

安全之困

脱困之道

智能安全平台

01

# 安全之困



告警泛滥，有价值信息淹没在海洋中

基于特征检测，未知威胁发现能力弱

安全产品各自为战，无法形成防御体系

入侵事件发生后，分析，取证，还原难

02

# 脱困之道



提高未知威胁检测能力



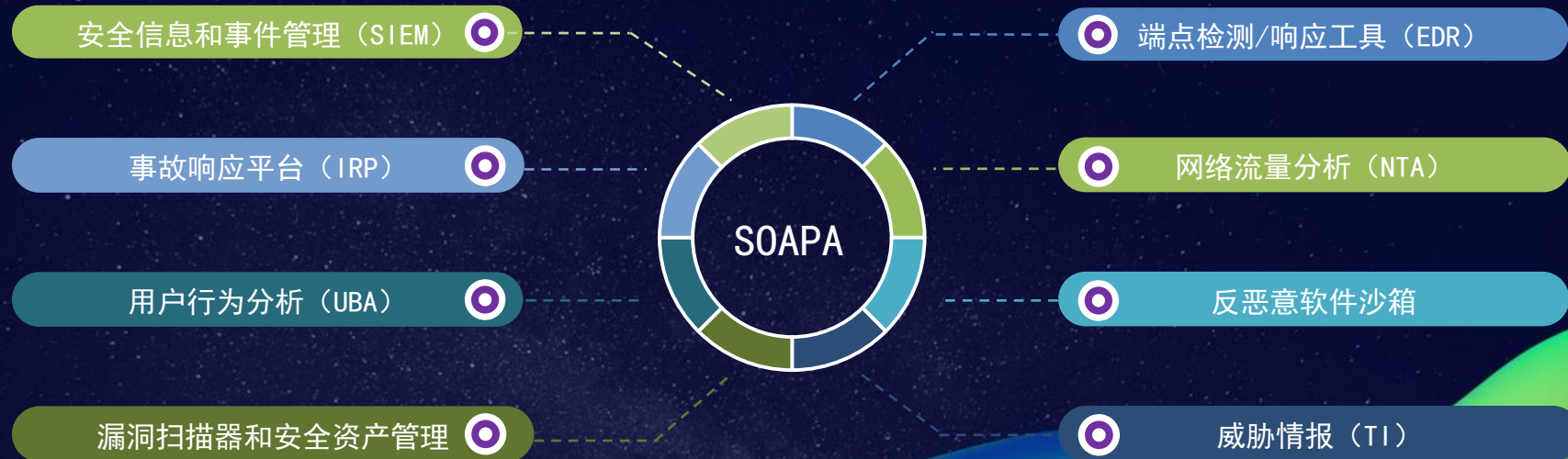
脱困之道

提高入侵事件分析能力



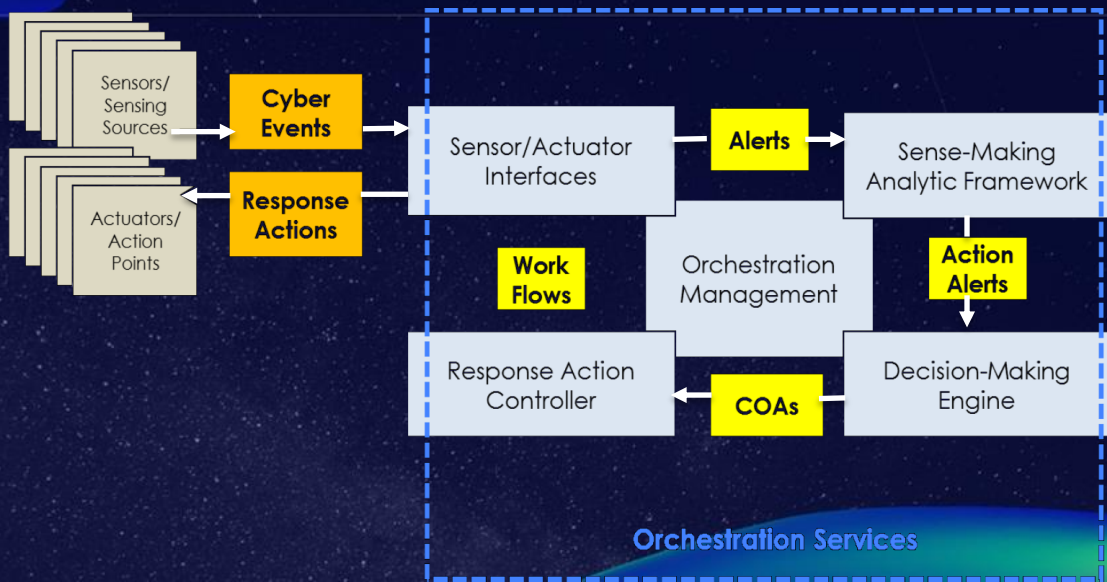


# 安全运作与分析平台架构 (SOAPA)





# 业务流程







# 反恶意软件沙箱

FTT

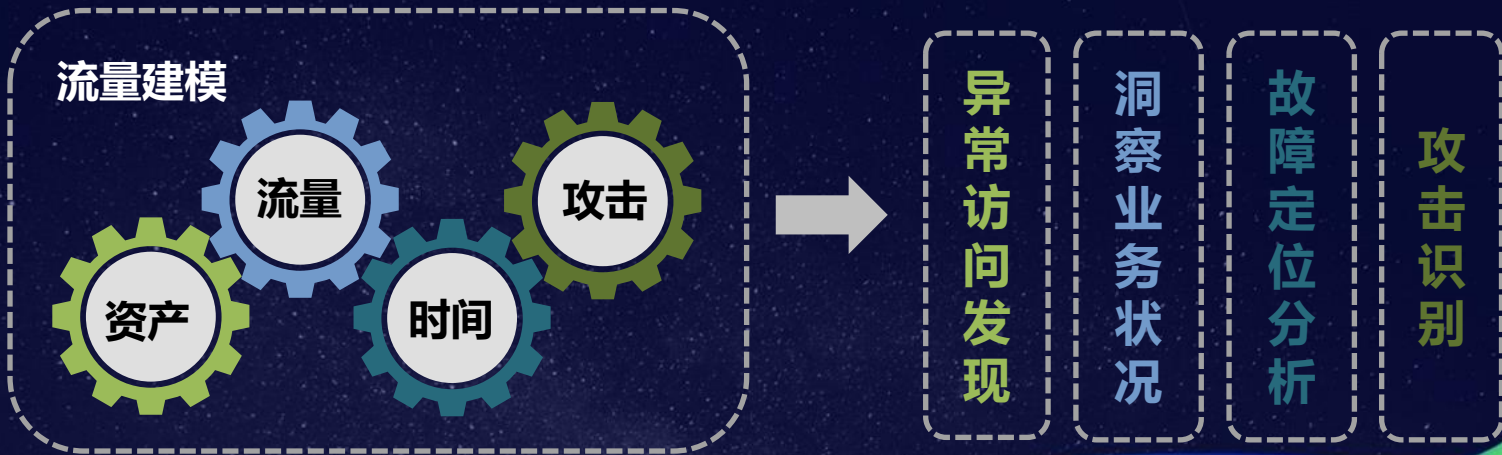
REEBUF

威胁情报中心





# 网络流量分析 (NTA)





# 用户行为分析 (UBA)



用户行为画像

统计方法

特征分析

机器学习建模



01

实时监测终端可疑进程和可疑行为

02

及时阻断恶意进程或隔离被控终端



# 原始报文存储及索引

## 原始报文存储及索引

分布式数据及状态同步管理

集群计算资源管理

Hadoop分布式文件系统

分布式缓存

数据采集器

分布式索引



关联分析

调查取证





**准确**：从内部检测到的攻击行为中提取信息，形成准确的内部威胁情报

准确

**及时**：内外部威胁情报通过信息同步升级机制，实现分钟级同步

**全面**：开放的外部威胁情报接口，及时获取外部威胁情报

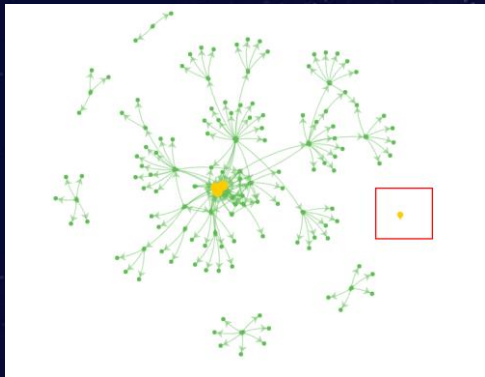
全面

及时





# 用户行为分析示例--WebShell检测



- 首先进行**访问数量统计**，被访问的URL地址的访问次数超过了一定数量，则认为这些URL正常
- 对剩余的URL地址进行**访问者IP分析**，如果URL对应的访问者IP来自大量不同IP，则该URL正常
- 再进行**文件类型分析**，webshell的文件类型一般为php、jsp、asp等，可将可疑URL数量降到几个到几十个的量级
- 最后利用平台的**交互式分析功能**，可快速确定被植入的WebShell

03

# 智能安全平台



# 兰天智能安全平台

FTT · REEBUF





产品部署后发现通过邮件传播的**新型恶意软件**，成功运行后会窃取用户研发相关工具的用户名/密码等信息；通过深入分析，确定为定向攻击，攻击组织试图获取研发团队主管电脑的控制权限，进而获取**业务系统的源码**，为后续入侵做准备。

# 应用案例—未知威胁发现

威胁事件 / 恶意代码事件

|   | 文件名                       | 类型  | 源IP           | 源端口   | 目的IP        | 目的端口 | 协议   | 来源 | 时间                  | 已知威胁 | 未知威胁 |
|---|---------------------------|-----|---------------|-------|-------------|------|------|----|---------------------|------|------|
| 1 | 0ce36679dd3c24d737eed...  | doc | 192.168.7.199 | 54050 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:39:38 | 正常   | 高危   |
| 2 | 3b08bd6c73153e0e009134... | doc | 192.168.7.199 | 53898 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:39:05 | 正常   | 高危   |
| 3 | 4e99420899bd8359091929... | doc | 192.168.7.199 | 53814 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:38:53 | 正常   | 高危   |
| 4 | 4cc3228a79a437ba26f58d... | doc | 192.168.7.199 | 53811 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:38:53 | 正常   | 高危   |
| 5 | 3ab953ac4ce535f560b1b9... | doc | 192.168.7.199 | 53793 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:38:52 | 正常   | 高危   |
| 6 | 32d6a78d7452d308636ccd... | doc | 192.168.7.199 | 53781 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:38:52 | 正常   | 高危   |
| 7 | 297ff1942ba0f4ecee854e... | doc | 192.168.7.199 | 53763 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:38:51 | 正常   | 高危   |
| 8 | 1228da7ae20959c5155455... | doc | 192.168.7.199 | 53737 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:38:50 | 正常   | 高危   |
| 9 | 0f8ef2eaa4cc905792b372... | doc | 192.168.7.199 | 53735 | 192.168.3.7 | 80   | HTTP | 网络 | 2017-12-05 11:38:50 | 正常   | 高危   |

## 威胁详情

| 序号 | 引擎ID   | 检测结果ID | 检测结果 | 风险级别 | 威胁类型 | 名称                              | 威胁描述      | 匹配规则ID       |
|----|--------|--------|------|------|------|---------------------------------|-----------|--------------|
| 1  | Office | 0      | 恶意   | 高    | 15   | <a href="#">DropExe.Heu</a>     | 释放PE文件    | 610000:53    |
| 2  | Office | 1      | 恶意   | 高    | 16   | <a href="#">HidePEFile.Heu</a>  | 隐藏PE文件    | 610005:62,68 |
| 3  | Office | 2      | 恶意   | 低    | 22   | <a href="#">SuspHttpReq.Heu</a> | 可疑的http请求 | 610025:476   |
| 4  | Office | 3      | 恶意   | 高    | 23   | <a href="#">RunSuspexe.Heu</a>  |           | 610031:58    |





产品部署后发现多起办公网用户**违规访问财务数据库**的安全事件，财务数据属于核心机密信息，管理员基于事件源IP**定位到内部员工个人**，并对其违规行为**进行追责**，对内部潜在数据泄露者起到震慑作用，降低了内部数据泄露的风险。










# 应用案例—违规访问发现





# 应用案例—违规访问发现



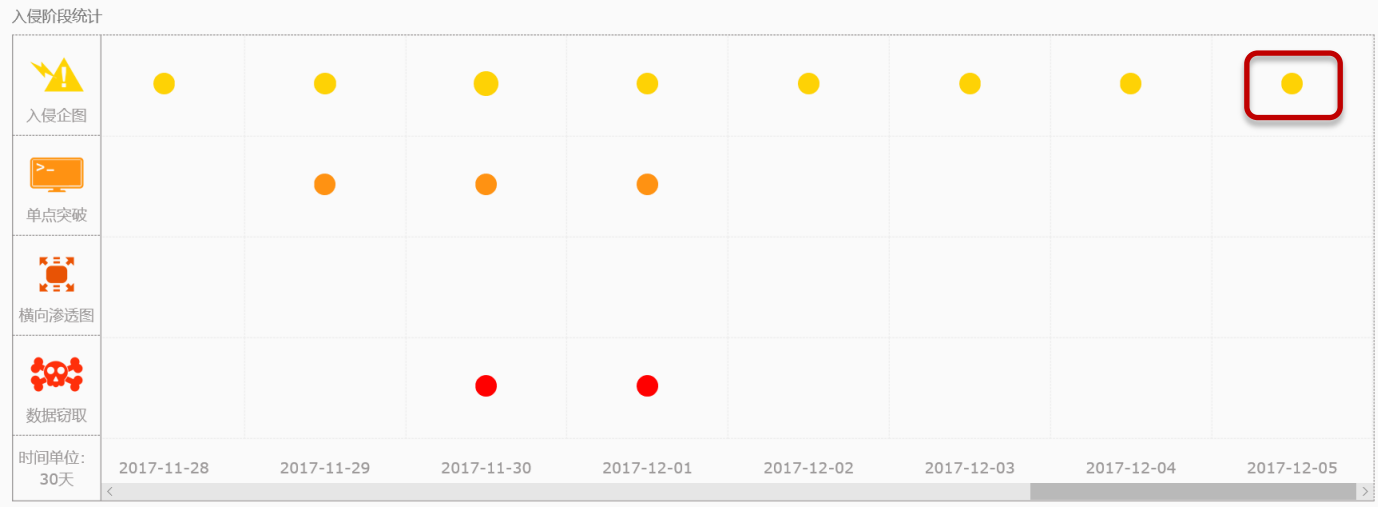
|                        |   |
|------------------------|---|
| ▼ 192.168.100.18(Xfer) | +   |
| 192.168.100.101        | -  |
| 192.168.100.104        | -  |
| 192.168.100.106        | -  |
| 192.168.100.100        | -  |
| 192.168.100.103        | -  |
| 192.168.100.105        | -  |
| 192.168.100.102        | -  |



某重要峰会期间，客户收到某监督部门通告，客户内部员工存在攻击金砖会议官网的行为，通过兰天平台**留存的原始报文及网络会话等信息**分析发现内部员工没有攻击行为，是正常访问，是该安全部门所用系统的**误报**，事件得以及时解决。



# 应用案例—安全取证







# 应用案例—安全取证

|    | 组      | 名称           | 源                                    | 目的                                    | 级别 | 攻击阶段 | 开始时间             | 结束时间             |
|----|--------|--------------|--------------------------------------|---------------------------------------|----|------|------------------|------------------|
| 1  | + 暴力破解 | 服务端频繁的向客户端返回 | 192.168.9.151:21                     | 192.168.11.202                        | 中危 | 入侵企图 | 2017-12-05 17:08 | 2017-12-05 17:08 |
| 2  | + 扫描攻击 | nmap工具扫描     | 192.168.9.151                        | 192.168.11.202:80                     | 低危 | 入侵企图 | 2017-12-05 17:08 | 2017-12-05 17:08 |
| 3  | + 网络威胁 | 恶意DNS        | 192.168.5.155:51589                  | 8.8.8.8:53                            | 低危 | 入侵企图 | 2017-11-29 15:38 | 2017-11-29 15:38 |
| 4  | + 流量检测 | ids低危告警事件    | 192.168.100.104,192.168.100.106,192. | 192.168.100.32,192.168.100.35,192.16  | 低危 | 入侵企图 | 2017-11-29 11:20 | 2017-11-29 11:40 |
| 5  | + 流量检测 | ids中危告警事件    | 192.168.100.100,192.168.100.108,192. | 159.253.153.210,201.167.56.118,192.1  | 中危 | 入侵企图 | 2017-11-29 11:02 | 2017-11-29 11:40 |
| 6  | + 流量检测 | ids低危告警事件    | 192.168.100.103,192.168.100.104      | 1.1.1.1,192.168.100.17                | 低危 | 入侵企图 | 2017-11-29 11:02 | 2017-11-29 11:04 |
| 7  | + 网络威胁 | webShell     | 192.168.3.125                        | 120.92.44.196,123.125.7.234,112.90.6  | 高危 | 单点突破 | 2017-11-29 02:01 | 2017-11-29 02:01 |
| 8  | + 网络威胁 | webShell     | 123.103.57.13,101.26.39.11:80        | 192.168.7.86                          | 高危 | 单点突破 | 2017-11-29 02:01 | 2017-11-29 02:01 |
| 9  | + 网络威胁 | webShell     | 192.168.5.20                         | 123.125.7.234,111.202.114.74,111.206  | 高危 | 单点突破 | 2017-11-29 02:01 | 2017-11-29 02:01 |
| 10 | + 网络威胁 | webShell     | 192.168.3.172                        | 192.168.9.2:80                        | 高危 | 单点突破 | 2017-11-29 02:01 | 2017-11-29 02:01 |
| 11 | + 网络威胁 | webShell     | 192.168.6.197                        | 112.90.61.242,111.206.76.48,114.112.0 | 高危 | 单点突破 | 2017-11-29 02:01 | 2017-11-29 02:01 |
| 12 | + 网络威胁 | webShell     | 192.168.5.228                        | 192.168.3.25:8080                     | 高危 | 单点突破 | 2017-11-29 02:01 | 2017-11-29 02:01 |



# 应用案例—安全取证

## ▼ 关联分析事件列表

|                        |                  |                      |    |                     |                              |    |
|------------------------|------------------|----------------------|----|---------------------|------------------------------|---|
| 名称                     | 源                | 目的                   | 级别 | 时间                  | 描述                           |    |
| 服务端频繁的向客户端返回FTP登录失败的信息 | 192.168.9.151:21 | 192.168.11.202:53947 | 中危 | 2017-12-05 17:08:54 | 192.168.9.151,192.168.11.202 | <a href="#">详情</a>  |
| 服务端频繁的向客户端返回FTP登录失败的信息 | 192.168.9.151:21 | 192.168.11.202:53992 | 中危 | 2017-12-05 17:08:54 | 192.168.9.151,192.168.11.202 | <a href="#">详情</a>  |
| 服务端频繁的向客户端返回FTP登录失败的信息 | 192.168.9.151:21 | 192.168.11.202:53992 | 中危 | 2017-12-05 17:08:52 | 192.168.9.151,192.168.11.202 | <a href="#">详情</a>  |
| 服务端频繁的向客户端返回FTP登录失败的信息 | 192.168.9.151:21 | 192.168.11.202:53992 | 中危 | 2017-12-05 17:08:48 | 192.168.9.151,192.168.11.202 | <a href="#">详情</a>  |

显示第 1 到第 4 条记录，总共 4 条记录



# 应用案例—安全取证

| 原始事件详情 |  |                                    |
|--------|--|------------------------------------|
| 网络攻击事件 |  | <a href="#">下载PCAP文件</a>           |
| 事件编号   |  | 2,61442513-6lsqckgswnhwj4gesmkwuv1 |
| 源IP    |  | 192.168.11.202:21                  |
| 目的IP   |  | 192.168.9.151:53947                |
| 协议类型   |  | TCP                                |



# 应用案例—安全取证

006b2d629a6715689e955b2d49e43cab.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

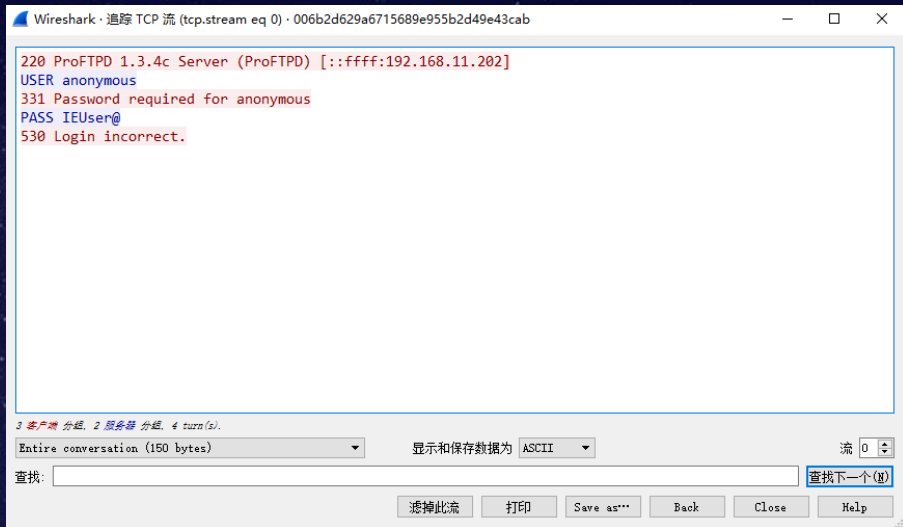
应用显示过滤器 ... <Ctrl+> 表达式...

| No. | Time     | Source         | Destination    | Protocol | Length | Info   |
|-----|----------|----------------|----------------|----------|--------|--|
| 1   | 0.000000 | 192.168.9.151  | 192.168.11.202 | TCP      | 66     | 53947→21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1            |
| 2   | 0.000007 | 192.168.11.202 | 192.168.9.151  | TCP      | 66     | 21→53947 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=64 |
| 3   | 0.000014 | 192.168.9.151  | 192.168.11.202 | TCP      | 60     | 53947→21 [ACK] Seq=1 Ack=1 Win=525568 Len=0                                |
| 4   | 0.000037 | 192.168.11.202 | 192.168.9.151  | FTP      | 115    | Response: 220 ProFTPD 1.3.4c Server (ProFTPD) [::ffff:192.168.11.202]      |
| 5   | 0.000160 | 192.168.9.151  | 192.168.11.202 | TCP      | 60     | 53947→21 [ACK] Seq=1 Ack=62 Win=525312 Len=0                               |
| 6   | 0.000631 | 192.168.9.151  | 192.168.11.202 | FTP      | 70     | Request: USER anonymous  |
| 7   | 0.000639 | 192.168.11.202 | 192.168.9.151  | TCP      | 60     | 21→53947 [ACK] Seq=62 Ack=17 Win=14656 Len=0                               |
| 8   | 0.000664 | 192.168.11.202 | 192.168.9.151  | FTP      | 91     | Response: 331 Password required for anonymous                              |
| 9   | 0.001154 | 192.168.9.151  | 192.168.11.202 | TCP      | 60     | 53947→21 [ACK] Seq=17 Ack=99 Win=525312 Len=0                              |
| 10  | 0.001258 | 192.168.9.151  | 192.168.11.202 | FTP      | 68     | Request: PASS IEUser@  |
| 11  | 0.001291 | 192.168.11.202 | 192.168.9.151  | FTP      | 76     | Response: 530 Login incorrect.   |

> Frame 4: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)  
> Ethernet II, Src: Vmware\_26:1e:00 (00:0c:29:26:1e:00), Dst: Micro-St\_9e:f1:c8 (4c:cc:6a:9e:f1:c8)  
> Internet Protocol Version 4, Src: 192.168.11.202, Dst: 192.168.9.151  
> Transmission Control Protocol, Src Port: 21, Dst Port: 53947, Seq: 1, Ack: 1, Len: 61  
> File Transfer Protocol (FTP)



# 应用案例—安全取证



谢谢

