

目录

前言	1.1
安全分析概览	1.2
why为何要分析	1.2.1
安全分析流程	1.3
数据采集	1.3.1
日志	1.3.1.1
数据包	1.3.1.2
数据处理	1.3.2
大数据	1.3.2.1
人工智能	1.3.2.2
数据应用	1.3.3
过去	1.3.3.1
追踪溯源	1.3.3.1.1
现在	1.3.3.2
态势感知	1.3.3.2.1
将来	1.3.3.3
威胁预警	1.3.3.3.1
安全日志分析	1.4
常见系统日志	1.4.1
日志分析方法	1.4.2
日志分析难点	1.4.2.1
日志分析工具	1.4.3
ELK	1.4.3.1
Splunk	1.4.3.2
领域应用	1.5
物联网	1.5.1
工业信息	1.5.2
云安全	1.5.3
安全分析工具	1.6
网络分析工具	1.6.1
Wireshark	1.6.1.1
Capsa Free	1.6.1.2
Zenoss Core	1.6.1.3
NetworkMiner	1.6.1.4
The Dude	1.6.1.5

日志

Angry IP Scanner	1.6.1.6
Nimbus Threat Monitor	1.6.1.7
附录	1.7
参考资料	1.7.1

掌握黑客的行踪：安全分析

- 最新版本: v1.0
- 更新时间: 20210601

简介

通过安全分析，掌握黑客的行踪轨迹。先对安全分析进行概述，再介绍为何需要安全分析；详细介绍安全分析的整套流程，包括数据采集、数据处理、数据应用。其中数据采集有日志和数据包等；数据处理有大数据技术和人工智能技术；数据应用有过去时的追踪溯源、现在时的态势感知、将来时的威胁预警等；以及详细介绍安全日志分析的相关系统的日志，以及日志分析的具体方法，包括其中有哪些难点；以及主流的日志分析工具ELK和Splunk；接着介绍如何把日志分析应用到各个领域，比如物联网、工业信息、云安全等；整理常用的安全分析相关的工具，比如网络分析工具，包括Wireshark、Capsa Free、Zenoss Core、NetworkMiner、The Dude、Angry IP Scanner、Nimbus Threat Monitor等；最后附上参考资料。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

Gitbook源码

- [crifan/grasp_hacker_track_security_analysis: 掌握黑客的行踪：安全分析](#)

如何使用此Gitbook源码去生成发布为电子书

详见：[crifan/gitbook_template: demo how to use crifan gitbook template and demo](#)

在线浏览

- [掌握黑客的行踪：安全分析 book.crifan.com](#)
- [掌握黑客的行踪：安全分析 crifan.github.io](#)

离线下载阅读

- [掌握黑客的行踪：安全分析 PDF](#)
- [掌握黑客的行踪：安全分析 ePUB](#)
- [掌握黑客的行踪：安全分析 Mobi](#)

版权说明

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 admin 艾特 crifan.com，我会尽快删除。谢谢合作。

鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 crifan 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

更多其他电子书

本人 crifan 还写了其他 100+ 本电子书教程，感兴趣可移步至：

[crifan/crifan_ebook_readme: Crifan的电子书的使用说明](#)

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2021-06-01 20:59:29

安全分析概览

TODO:

Web日志安全分析浅谈 - 先知社区

<https://xz.aliyun.com/t/1121>

-
- 安全日志分析
 - 分析来源
 - 日志
 - 各种系统的
 - nginx
 - web服务器
 - 具体某应用
 - (原始) 数据 (包)
 - 防火墙
 - WAF = 网络应用防火墙
 - 路由器
 - 最终实现=目的
 - 态势感知
 - 攻击溯源
 - 黑客轨迹的溯源与识别
 - 谁去做 (分析)
 - 安全分析人员
 - 有时候是: 网站管理运维人员
 - 对应工作
 - 安全分析师
 - 安全日志分析师
 - 工作所需技能 = 核心流程
 - **40%的渗透测试**: 了解渗透攻击相关逻辑和相关日志规则
 - **40%大数据技术**: 处理数据, 包括先提取日志中有用数据
 - **20%的人工智能技术**: 用机器学习和AI, 根据数据建模和分析、聚类, 找出逻辑关联

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:06:12

why为何要分析

- 为什么要安全分析?
 - 背景
 - 网站被恶意黑客攻击的频率和网站的价值一般成正比
 - 即使网站价值低，也可能遇到低水平攻击
 - "脚本小子"的恶意测试攻击
 - 各种大范围漏洞扫描器
 - 安全行业有一句话
 - 世界上只有两种人，一种是知道自己被黑了的，另外一种是被黑了还不知道的
 - -> 公司或个人希望知道
 - 自己是否被攻击了？
 - 实时监控正在发生的安全事件、安全趋势
 - 发现风险
 - 谁攻击的?
 - 还原攻击者行为
 - 从何时开始攻击
 - 攻击所利用的工具、手法、漏洞
 - 攻击是否成功，是否已经造成损失和危害
 - 恶意行为取证
 - 如何防护?
 - 捕获漏洞、修复漏洞
 - 避免后续再被攻击
 - -> 如何实现?
 - 安全（日志）分析
 - -> 安全（日志）分析 目的
 - 网站安全自检查
 - 了解服务器上正在发生的安全事件
 - 为应急事件的分析取证

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-06-01 20:58:46

安全分析流程

- 安全分析的核心要点=总体流程

- 总体流程图



- 核心要点

- 数据采集
 - 数据源
 - 日志类
 - 流量类（原始数据包）
 - 数据处理
 - 大数据技术
 - 数据处理：去重合并、日志泛化、结构化处理
 - 数据存储：保存到相关数据库
 - 人工智能技术
 - 数据挖掘：机器学习、统计、关联、建模、统计
 - 数据应用
 - 最终用户看到的、听到的：产品 = 功能 = 名词
 - 过去 = 事后回溯 = 静态的、历史的：追踪溯源
 - 现在 = 事中发现 = 实时的：实时监测、威胁感知
 - 将来 = 事前预警：威胁预警

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新：2021-06-01 20:50:45

数据采集

安全分析的前提，是需要采集到对应的数据。

- 数据采集
 - (全方位全要素的)全量数据

- 概述



- 包含

- 实时安全数据
 - 多种采集方式
 - 隐患主动探测
 - 日志采集
 - 流量分析
 - 蜜罐诱捕
 - 历史和相关数据
 - 日常运维管理的数据
 - 举例
 - 等保数据
 - 威胁情报数据
 - 安全事件
 - 资产测绘数据
 - 黑客组织信息
 - IP信誉
 - 域名测绘数据
 - 第三方标准接口获取的数据
 - (海量)指纹库

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:51:08

日志

在安全日志分析之前，需要采集对应的日志。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-06-01 20:54:53

数据包

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:11:12

数据处理

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:01:34

大数据

- 大数据
 - 大数据基础架构
 - 数据源
 - 多源异构数据
 - 操作
 - 处理
 - 存储
 - 查询
 - 涉及
 - 质量评定
 - 标签化
 - 数据补全
 - 相关
 - 机器学习
 - 关联分析
 - 场景建模
 - 场景
 - 举例
 - 入侵识别
 - 发现各类潜在威胁攻击

数据可视化

- 数据可视化
 - 工具
 - ELK
 - 应用
 - 网络空间监管可视
 - 态势感知可视化



- 实现
 - 监管
 - 可见
 - 可管
 - 可控

关联分析

- 安全分析类产品
 - 涉及到关联分析
 - 相关概念
 - 日志分析
 - SOC
 - 态势感知
 - 风控
 - 关联分析模型
 - 大概种类
 - 基于 规则 的关联分析
 - 基于 统计 的关联分析
 - 基于 威胁情报 的关联分析
 - 基于 情境 的关联分析
 - 基于 大数据 的关联分析

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:49:34

人工智能

- 人工智能 & 机器学习
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:58:02

数据应用

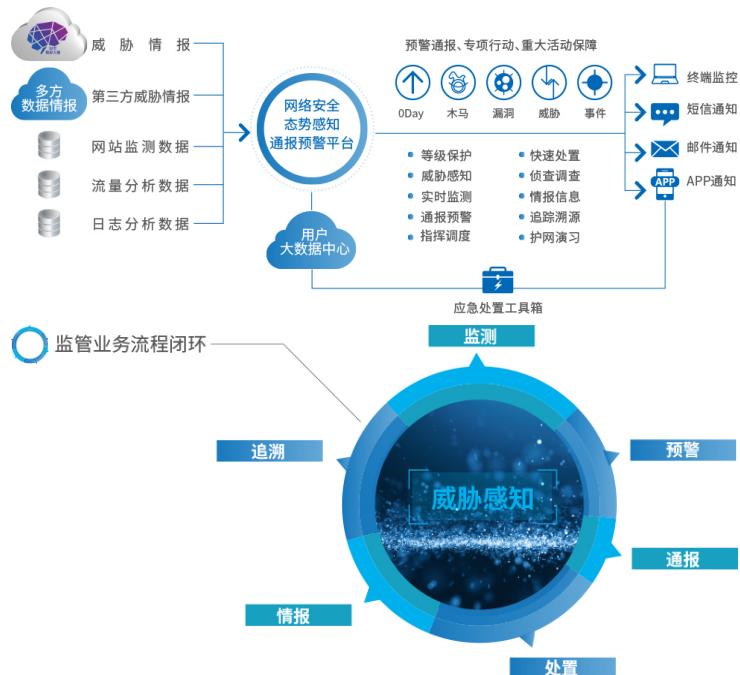
安全分析出相关数据，最后是用于实现不同的应用。

- 安全分析应用

- 概述



- 形成业务闭环



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook 最后更新: 2021-06-01 20:57:52

过去

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:04:20

追踪溯源

通过分析得到多维度的威胁情报相关数据后，可以分析出相关信息：

- 报警研判
 - 黑客画像
 - 访问来源是否可疑
 - 举例
 - IDC服务器作为终端来访问Web应用
 - 通过Tor、VPN、代理的访问
 - 攻击定性
 - 攻击的目的
 - 攻击的危害
 - 攻击的技战术
- 威胁情报数据
 - IP资产画像
 - IP地址
 - 域名反查
 - 归属运营商
 - 关联威胁情报
 - 攻击行为
 - 资产类型
 - 域名画像
 - 域名信息
 - 关联IP
 - 关联子域名
 - Whois信息
 - ICP备案信息
 - 关联威胁情报
 - 失陷主机数据
 - 区域安全报告
 - 黑客组织及活动威胁情报
- 关联分析
 - 背景：黑客进行攻击的时候，难以做到任何一个网络资源仅在一次攻击中使用
 - 分析：黑客手中的其它IT资源，进而知道黑客进行的其它攻击事件
 - 相关相关域名、IP历史上是否被发现恶意攻击行为
 - 域名和IP相关的已知的恶意软件
 - 输出
 - 五大要素
 - 攻击
 - 人
 - 物
 - 地
 - 事
 - 关联关系

日志

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:54:16

现在

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:08:22

态势感知

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:07:48

将来

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:07:45

威胁预警

- 威胁预警
 - 威胁预警通知
 - 多种通知方式
 - app
 - 钉钉
 - 微信小程序
 - 短信
 - 通知内容
 - 0day检测预警
 - 在线检测重大典型漏洞
 - 比如
 - struts2远程代码执行漏洞
 - Petya勒索病毒
 - 高危远程溢出漏洞
 - 实现
 - POC定向精确验证

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:50:57

安全日志分析

安全分析，尤其是安全日志分析，就是去分析各种系统产生的日志，从而找出背后可能涉及的安全问题，比如被黑客攻击了。

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-06-01 20:55:50

常见系统日志

- 日志

 - 多种系统

 - Nginx

 - 日志举例

```
[root@localhost jerry]# tail -f access.log
[29/May/2017:21:57:38 +0800] "GET / HTTP/1.1" 200 2300 "-" "Mozilla/5.0 (Windows NT 6.1; rv:40.0) Gecko/20100101 Firefox/40.1"
[29/May/2017:21:57:38 +0800] "GET /index.html HTTP/1.1" 200 1942 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:32 +0800] "GET /page/1 HTTP/1.1" 200 6463 "http://www.baidu.com" "Scrapy-1.1.2 (http://scrapy.org)"
[29/May/2017:22:01:39 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "POST /36.html HTTP/1.1" 200 1499 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"
[29/May/2017:22:01:45 +0800] "GET /index.php HTTP/1.1" 200 4867 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36 OPR/46.0.2640.80"]

```

先知安全技术社区

 - 其中一条

61.144.119.65 -- [29/May/2017:22:01:32 +0800] "GET

 - 对应nginx配置

```
user www;
worker_processes 1;
error_log /var/log/nginx/error.log;
warn_log /var/log/nginx/warn.log;
notice_log /var/log/nginx/notice.log;
info_log /var/log/nginx/info.log;
pid /var/run/nginx.pid;

events {
    worker_connections 1024;
}

http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
                    '$status $body_bytes_sent "$http_referer"'
                    '"$http_user_agent"';
    $http_x_forwarded_for';
}

access_log /var/log/nginx/access.log main;
sendfile on;
tcp_nopush on;
tcp_nodelay on;
keepalive_timeout 65;
upstream on;

include /etc/nginx/conf.d/*.conf;
include /etc/nginx/conf.d/default.conf;
include /etc/nginx/conf.d/*.conf;
}

[创世黑客网 qianzhe11]
```

先知安全技术社区

 - 日志格式

 - \$remote_addr - \$remote_user [\$time_local]
"\$request" \$status \$body_bytes_sent
"\$http_referer" "\$http_user_agent"
"\$http_x_forwarded_for";

 - 翻译成中文

 - 远程IP - 远程用户 服务器时间 请求主体 响应状态 响应体大小 请求来源 客户端信息 客户端代理IP

黑客攻击相关日志

- 背景

 - 站在攻击者的角度，攻击者对网站进行渗透时，其中包含大量的扫描请求和执行恶意操作的请求

 - 这两者在日志中都有各自的特征

 - 扫描请求会访问大量不存在的地址

- 日志中的体现：大量的响应状态码为404
 - 不同的恶意请求都有各自相应的特征

• 举例

◦ 恶意请求

- 当有人对服务器进行SQL注入漏洞探测时
 - 以 `select` 为关键字进行过滤

■ 对策

- 加上时间条件，状态码等条件，能查询到最近可能成功的SQL注入攻击

注

- 实际情况中，会有很多噪声数据
 - 仅仅只依靠状态码来判断攻击是否成功是不可行的
 - 因为很多时候请求的确成功了，但并不能代表攻击也成功了

卷五

- 请求一个静态页面或者图片，会产生这样一个请求

- /logo.png?
attack=test';select/**/1/**/
/from/**/1
- 请求状态码为200，但是此注入攻击并没有得到执行

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:58:19

日志分析方法

分析日志的常规办法

- 分析日志的常规办法
 - 常规应急响应情况 = 常见的几种被黑情况
 - 带宽被占满，导致网站响应速度变慢，用户无法正常访问
 - 造成已知经济损失，客户被恶意转账、对账发现金额无端流失
 - 网站被篡改或者添加暗链，常见为黑客黑页、博彩链接等
 - 建议动作
 - 1. 先断网
 2. 对已知被黑的服务器进行断网
 - 1. 再分析日志
 2. 开始进行日志分析操作
 - 分析思路和对策
 - 对于相对初级的黑客：会上传webshell（后门文件）
 - 对策：检查是否存有明显的webshell
 - 检查方式
 - 搜索最近一周被创建、更新的脚本文件
 - 根据网站所用语言，搜索对应webshell文件常见的关键字
 - 后续操作
 - 找到webshell后门文件后
 - 通过查看日志中谁访问了webshell
 - 然后得出攻击者IP
 - 再通过IP提取出攻击者所有请求进行分析
 - 举例说明
 - 可能我们得到类似这样一个日志结果

```

00:01 GET http://localhost/index.php 9.9.9.9 200 [I]
00:02 GET http://localhost/index.php?id=1' 9.9.9.9 50
00:05 GET http://localhost/index.php?id=1' and 1=user
00:07 GET http://localhost/index.php?id=1' and 1=(sele
00:09 GET http://localhost/index.php?id=1' and 1=(sele
00:10 GET http://localhost/admin/ 9.9.9.9 404 [疑似攻击]
00:12 GET http://localhost/login.php 9.9.9.9 404 [疑似攻击]
00:13 GET http://localhost/admin.php 9.9.9.9 404 [疑似攻击]
00:14 GET http://localhost/manager/ 9.9.9.9 404 [疑似攻击]
00:15 GET http://localhost/admin_login.php 9.9.9.9 40
00:15 GET http://localhost/guanli/ 9.9.9.9 200 [疑似攻击]
00:18 POST http://localhost/guanli/ 9.9.9.9 200 [疑似攻击]
00:20 GET http://localhost/main.php 9.9.9.9 200 [疑似攻击]
00:20 POST http://localhost/upload.php 9.9.9.9 200 [疑似攻击]
00:23 POST http://localhost/webshell.php 9.9.9.9 200
00:25 POST http://localhost/webshell.php 9.9.9.9 200
00:26 POST http://localhost/webshell.php 9.9.9.9 200

```

- 注：为清晰呈现攻击路径，此日志为人工撰造
 - 通过找到后门文件 webshell.php，得知攻击者IP为 9.9.9.9

- 提取了此IP所有请求
- 从这些请求可以清楚看出攻击者从 00:01 访问网站首页
- 然后使用了单引号对网站进行SQL注入探测
- 然后利用报错注入的方式得到了用户名和密码
- 随后扫描到了管理后台进入了登录进了网站后台
- 上传了webshell文件
- 进行了一些恶意操作
- 结论
 - 从以上分析我们可以得出， /index.php 这个页面存在 SQL注入漏洞
 - 后台地址为 /guanli.php , /upload.php 可直接上传 webshell
- 补救方法
 - 修复注入漏洞
 - 更改管理员密码
 - 对文件上传进行限制
 - 限制上传目录的执行权限
 - 删除webshell

攻击溯源

- 攻击溯源
 - 背景：由于各种原因，实现攻击溯源难度较大
 - 已知=现状
 - 某些甲方内部安全团队有尝试实现过，但至今未要到产品实现的效果图
 - 某人找到某安全公司有一个类似的产品，以硬件方式实现的流量监控，从而获取到日志进行分析
 - 可以记录并分析整个请求包和响应包
 - 这可比从日志文件中拿到的信息全面多了
 - 从而将日志溯源分析降低了一个难度
 - 信息
 - 请求和响应数据完整，能进行更大维度的日志分析
 - 安全关联库较多，能关联出更为丰富的信息
 - 推测
 - 他们内部有一个IP库，每个IP是否为代理IP，所处什么机房都有相应的记录
 - 或者调用了IP位置查询接口，从而判断IP是否为代理IP、机房IP、个人上网出口IP，继而判定未使用跳板主机
 - 效果图



○ 其他更好的思路

- 正常总是基本相似，异常却各有各的异常
- -> 用大数据（统计、建模）实现

- 搜集大量正常请求，为每个请求的所有参数的值定义正常模型
- 通过Waf或者攻击规则来剔除所有发起过攻击请求的IP
 - 从而得到所有来自用户的正常请求，将每个正常请求构造出对应的正常模型
 - 比如
 - <http://test.com/index.php?id=123>
 - <http://test.com/index.php?id=124>
 - <http://test.com/index.php?id=125>
 - 那么关于此请求的正常模型则为 [N,N,N] ,不匹配此模型的请求则为异常请求
 - 效果
 - 当对日志中的请求建立完正常的模型，通过正常模型来匹配找出所有不符合模型的请求时，发现效果的确不错

安全关联库

- 安全关联库
 - 举例
 - 全球IPV4信息知识库
 - 包括该IP对应的国家地区、对应的操作系统详情、浏览器信息、电话、域名等等。并对全球IP地址实时监控，通过开放的端口、协议以及其历史记录，作为数据模型进行预处理
 - 全球虚拟空间商的IP地址库
 - 如果访问者属于该范围内，则初步可以判定为跳板IP
 - 全球域名库
 - 包括两亿多个域名的详细信息，并且实时监控域名动向，包括域名对应的IP地址和端口变化情况，打造即时的基于域名与IP的新型判断技术，通过该方式可以初步判断是否为C&C服务器、黑客跳板服务器
 - 黑客互联网信息库
 - 全球部署了几千台蜜罐系统，实时收集互联网上全球黑客动向
 - 独有的黑客IP库
 - 对黑客经常登录的网站进行监控、对全球的恶意IP实时获取
 - 黑客工具指纹库
 - 收集了所有公开的（部分私有的）黑客工具指纹，当攻击者对网站进行攻击时，可以根据使用的黑客工具对黑客的地区、组织做初步判断
 - 黑客攻击手法库
 - 收集了大量黑客攻击手法，以此来定位对应的黑客或组织
 - 其他互联网安全厂商资源
 - 该系统会充分利用互联网各种资源，比如联动50余款杀毒软件，共同检测服务器木马程序

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2021-06-01 20:53:18

日志分析难点

- 日志分析难点
 - POST数据不记录导致分析结果不准确
 - 思考
 - 从不完整的信息中，分析得到一个肯定的答案，从逻辑上就不可行
 - 但是我们可以折中实现，尽量向肯定的答案靠近，即使得到一个90%肯定的答案，那也合乎我们想要的结果
 - 虽然POST数据不被记录，但是这些“不完整信息”依然能给我们提供线索
 - 如通过响应大小、响应时间、前后请求关联、POST地址词义分析、状态码等等依然能为我们的分析提供依据
 - 如某个请求在日志中的出现次数占访问总数30%以上，且响应大小平均值为2kb，突然某一天这个请求的响应值为10kb，且发起请求的IP曾被攻击特征匹配出过，那么可以80%的怀疑此请求可能存在异常
 - 如攻击者使用了联合注入查询了大量数据到页面
 - 当然这里只是举例，实际情况可能存在误报
 - 状态码很多时候不可信
 - 状态码虽然表示了响应状态，但是存在多种不可信情况，如服务器配置自定义状态码
 - 举例
 - 对于那些自行设置响应状态的，明明404却302的，明明500却要200的
 - 客户服务器配置网站应用所有页面状态码皆为200，用页面内容来决定响应
 - 服务器配置了302跳转，用302到一个内容为“不存在页面”
 - 举例
 - <http://www.baidu.com/test.php>
 - 思路
 - 对于不同的攻击行为，我们应该定义不同的响应规则
 - 如果攻击规则命中的为网站备份文件，那么应该判断请求大小必须超过1k-5k
 - 如攻击者发起/wwwroot.rar这种攻击请求，按照常理如果状态码为200，那么本来应该被定性为成功的攻击行为
 - 但是因为状态码不可信，我们可以转而通过响应大小来判断
 - 因为按照常规逻辑，备份文件一般都不止只有几kb大小
 - 如攻击者发起Bool注入请求则应该通过判断多个注入攻击请求的规律
 - Bool注入通常页面是一大一小一大一小这种规律
 - 如攻击者发起联合注入攻击，则页面响应大小会异常于多部分正常页面响应大小

- 如果攻击者发起延时注入请求，则页面响应时间则会和延时注入payload中的响应相近
 - 但是这需要分析攻击payload并提取其中的延时秒数来和日志中的响应时间进行比较误差值
- 攻击者使用多个代理IP导致无法构成整个攻击路径
 - 攻击者可能使用多个代理IP，用代理隐藏了真实IP
 - 淘宝上，一万代理IP才不到10块钱
 - 更不用说代理IP还可以采集免费的
 - 假设同一攻击者发起的每个请求都来自不同的IP，此时即使攻击规则命中了攻击者所有请求，也无法还原攻击者的攻击路径
 - 如果一个攻击者使用了大量的不同IP进行攻击，那么使用上面的方法可能就无法进行攻击行为溯源了
 - 思路
 - 虽然攻击者使用了多个IP，但是假设攻击者不足够心细，此时你可以通过攻击时间段、请求频率、客户端信息(Ua)、攻击手法、攻击工具(请求主体和请求来源和客户端信息中可能暴露工具特征)
 - 如sqlmap注入时留下的referer
- 无恶意webshell访问记录
 - 常规分析中，我们通过找到后门文件，从而利用这一线索得知攻击者IP继而得知攻击者所有请求，但是如果我们并没有找到webshell，又该用什么作为分析的入口线索呢？
 - 思路
 - 利用尽可能全面的攻击规则对日志进行匹配，通过IP分组聚合，提取发起过攻击请求的所有IP，再通过得到的IP反查所有请求，再配合其他方法检测提取出的所有请求中的可疑请求
- 编码避开关键字匹配
 - 攻击者使用了各种编码，16进制、Base64等等编码，使得日志中找不到恶意行为关键字
 - 再加上攻击者使用了代理IP使我们漏掉了分析中攻击者发起的比较重要的攻击请求
 - 关于编码、加密问题，某人也曾尝试过
 - 但是实际最后发现除了URL编码以外，其他的编码是无法随意使用的
 - 因为一个被加密或编码后的请求，服务器是无法正确接收和处理的
 - 除非应用本身请求就是加密或编码的
 - 且一般加密或编码出现在日志里通常都是配合其他函数实现的
 - 如 Char()、toHexString()、Ascii()
- APT分时段攻击
 - 攻击者分不同时间段进行攻击，导致时间上无法对应出整个攻击行为
 - 举例
 - 如果同一攻击者的攻击行为分别来源于不同的时间，比如攻击者花一周时间进行“踩点”，然后他就停止了行为
 - 过了一周后再继续利用所得信息进行攻击行为，此时因为行为链被断开了一周，我们可能无法很明显的通过时间维度来定位攻击者的攻击路径

- 思路

- 给攻击力路径定义模型，就拿在前面讲到的常规日志分析举例，那么攻击路径模型可定义为：访问主页>探测注入>利用注入>扫描后台>进入后台>上传webshell>通过webshell执行恶意操作
- 其中每一个都可以理解一种行为，而每种行为都有相应的特征或者规则
- 比如主页链接一般在日志中占比较大，且通常路径为 index.html、index.php、index.aspx,那么符合这两个规则则视为访问主页
- 而在探测注入行为中，一般会出现探测的payload
 - 如时间注入会匹配以下规则

```
.*(BENCHMARK\\(.*)\\).*  
.*(WAITFOR.*DELAY).*  
.*(SLEEP\\(.*)\\).*  
.*(THENDBMS_PIPE.RECEIVE_MESSAGE).*
```

- Bool注入

```
.*and.*(>|=|<).*  
.*/or.*(>|=|<).*  
.*/xor.*(>|=|<).*
```

- 联合注入

```
.*(order.*by).*  
.*/union.*select).*  
.*/union.*all.*select).*  
.*/union.*select.*from).*
```

- 显错注入

```
.*('|\"|\\\').*  
.*/extractvalue\\(.*)\\).*  
.*/floor\\(.*)\\).*  
.*/updatexml\\(.*)\\).*
```

- 利用注入则会体现出更完整，带有目的性的攻击请求，我们以同理制定规则即可，如查询当前数据库名、查询版本信息、查询数据库表名、列名则会发现 database、version、table_name、column_name（不同数据库存在不同差异，这里仅举例）
- 扫描后台则会产生大量的404请求，且请求较为频繁，请求特征通常为 /admin、/guanli、/login.php、/administrator

- 日志数据噪声

- 攻击者可能会使用扫描器进行大量的扫描
 - 此时日志中存在大量扫描行为
 - 此类行为同样会被恶意行为关键字匹配出
 - 但是此类请求我们无法得知是否成功扫描到漏洞
 - 可能也无法得知这些请求是扫描器发出的
- 扫描器可使用代理IP、可进行分时策略、可伪造客户端特征、可伪造请求来源或伪造成爬虫
- 海量恶意请求中很难得出哪些请求攻击成功了
- 思路

- 一种是给每种攻击方法定义成功的特征
 - 如延时注入可通过判断日志中的响应时间
 - 联合注入可通过与正常请求比较响应大小
 - Bool注入可通过页面响应大小的规律
 - 当然实际情况中，这种做法得到的结果可能是存在误报的
- 第二种办法就是通过二次请求，通过重放攻击者的请求，定义攻击payload可能会返回的结果，通过重放攻击请求获取响应之后进行判断
 - 注意：其实这里已经类似扫描器，只是攻击请求来自于日志，这种方法可能对服务器造成二次伤害，一般情况下不可取，且已经脱离日志分析的范畴

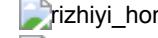
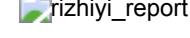
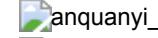
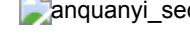
crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-06-01 20:54:27

日志分析工具

- 分析日志具体如何操作?
 - 最基本的: 用命令
 - 缺点: 效率低
 - 引申=高级的: 自动化 (的日志分析) 工具

日志分析工具

- 名称
 - 日志分析工具
 - ~ = 日志管理方案 = Log Management Solution
 - ~ = 日志管理和分析方案 = Log Management and Analysis Solutions
 - ~ = SIEM = Security Information and Event Management = 安全信息和事件管理
- 概述
 - 主流日志分析工具
 - ELK
 - ELK = ElasticSearch 、 Logstash 、 Kiabana
 - Splunk
- 详解
 - 日志分析工具
 - Win
 - Log Parser
 - 微软强大的日志分析工具
 - Event Viewer = 事件查看器
 - Weblog expert
 - windows日志分析工具
 - 其他
 - MSSQL_logview
 - Splunk
 - SysTools NTFS Log Analyzer
 - ELK
 - Linux
 - Webtrends
 - AWStats
 - Webalizer
 - Analog
 - Summary
 - Urchin
 - Nginx
 - 模块
 - nginx_upstream_check_module
 - 检查后端服务器的健康情况
 - Nginx日志分析工具
 - Goaccess

- 日志分析系统或服务
 - 日志易
 - <https://www.rizhiyi.com/>
 -  rizhiyi_homepage
 -  rizhiyi_report
 - 安全易
 - <https://www.anquanyi.com/>
 -  anquanyi_homepage
 -  anquanyi_security_report

相关

日志分析工具中和安全相关的功能

- 日志分析工具中和安全相关的功能
 - 普通功能
 - 威胁时序图
 - 疑似威胁分析
 - 疑似威胁漏报分析
 - 威胁访问流量
 - 威胁流量占比
 - 境外威胁来源国家(地区)统计
 - 境内威胁来源城市统计
 - 威胁严重度
 - 威胁响应分析
 - 恶意IP
 - 恶意URL分析
 - 威胁类型分析
 - 威胁类型分布
 - 威胁分类计数
 - 威胁来源热力图
 - 威胁总数
 - 威胁日志占比
 - 攻击溯源
 - 相关统计
 - 网站受攻击次数排名
 - 网站高危请求排名
 - 网站攻击者数量排名
 - 网站受攻击页面排名
 - 可疑文件排行
 - 被攻击时间统计
 - 攻击来源分布
 - 高危攻击者排行
 - 攻击者攻击次数排行
 - 网站危险系数排行
 - 攻击者数量统计
 - 各站点攻击者数量统计
 - 各扫描器占比

- 使用扫描器攻击者统计

常见日志系统

- 常见日志系统
 - Scribe : Facebook
 - Chukwa : Apache
 - Kafka : Linkedin
 - Flume : Cloudera

日志管理服务

- 日志管理服务
 - Linux系
 - rsyslogd : 普通日志管理服务
 - klogd : 内核信息日志文件服务
 - logrotate : 日志文件轮替服务

ELK vs Splunk

Scoreboard and Summary

	Splunk	ELK/Elastic Stack
Capability set	5/5	5/5
Ease of use	4/5	4/5
Community support	4/5	5/5
Release rate	5/5	5/5
Pricing and support	4/5	4/5
API and extensibility	5/5	5/5
3rd party integrations	5/5	4/5
Companies that use it	5/5	5/5
Learning curve	3/5	4/5
Security rating	836	779
Total	4.5/5	4.5/5

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:52:43

ELK

- ELK
 - 名称
 - ELK = ElasticSearch + Logstash + Kibana
 - 别称
 - Elastic Stack
 - ~= BELK
 - = Beats + ELK = Beats + ElasticSearch + Logstash + Kibana
 - 组成详解
 - ElasticSearch : 基于RESTful的、开源的、分布式的、搜索(查询和分析)引擎
 - 基于: Apache Lucene
 - 谁开发的: Elastic 公司
 - Logstash : 数据处理管道
 - 对日志进行收集、过滤并存储到Elasticsearch或其他数据库
 - Kibana : 数据可视化
 - 对日志分析友好的Web界面,可对Elasticsearch中的数据进行汇总、分析、查询
 - 截图



- 是什么： 数据分析平台 = Data Analytics Platform
 - 可用作： 开源日志分析平台
 - 特点： 开源、免费、高可配
 - -> 很多初创企业，作为日志分析平台，使用率最高

ELK日志分析基本流程

- ELK日志分析基本流程
 - 编写Logstash配置文件

```
agent.conf
input {
    file{
        path => "/var/log/*"      #日志所在文件夹 *表示文件夹下所有日志文件
        start_position => "beginning"
    }
}
filter {
    grok {
        match => { "message" => "%{IIS6}" }      #日志格式解析规则
    }
    geoip{
        source => "clientip"          #IP分析插件
    }
    attackfilter {
        source => "%{message}"       #攻击分析插件
    }
}
output {
    stdout { codec => rubydebug }
    elasticsearch {
        hosts => [ "localhost:9200" ]   #存储到Es
    }
}

日志解析规则

IIS6 %{TIMESTAMP_ISO8601:req_time} %{IP:server_ip} %{WORD:req_method} %{URI PATH:req_url} %{NOTSPACE:req_params}
%{NUMBER:server_port} %{NOTSPACE:username} %{IP:remote_ip} %{NOTSPACE:browser_info} %{Referer:req_Referrer}
%{NUMBER:res_code} %{NUMBER:windwos1} %{NUMBER:win32status} %{NUMBER:size}
```

- 将攻击规则应用于logstash的filter插件

```
... ...
33 regex: '*.*sql[()]*'
34 place: 'message'
35 regexid: 2
36 typeid: 2
37 typename: 'SQL注入攻击'
38 level: 3
39 leveldesc: '高危级别威胁'
40 actionid: 11
41 actiondesc: '正在进行延时sql注入'
42 actionlevel: 3
43 subtype: 'sub_type'
44
- id: 12
45 regex: '.*order.*by.*'
46 place: 'message'
47 regexid: 2
48 typeid: 2
49 typename: 'SQL注入攻击'
50 level: 3
51 leveldesc: '高危级别威胁'
52 actionid: 12
53 actiondesc: '正在查字段数目的sql注入'
54 actionlevel: 3
55 subtype: 'sub_type'
56
- id: 13
57 regex: '.*[\%20|\\\\]+union.*'
58 place: 'message'
59 regexid: 2
60 typeid: 2
61 typename: 'SQL注入攻击'
62 level: 3
63 leveldesc: '高危级别威胁'
64 actionid: 13
65 actiondesc: '正在进行会连接的sql注入'
```

- 利用载入了安全分析插件后的logstash进行日志导入

- 查询分析结果

```

18     "dept": "安全组",
19     "req_url": "/Themes/jd/n.html55.png",
20     "attack_info": {
21       "risk_desc": "",
22       "attack_detail": "",
23       "attack_rule": [
24       ],
25       "attack_status": 0,
26       "other": "",
27       "action_desc": [
28       ],
29       "attack_rule_id": [
30       ],
31       "attack_type_name": "",
32       "attack_source_place": [
33       ],
34       "attack_status_name": "正常请求",
35       "attack_type_id": 0,
36       "action_risk_level": 0,
37       "attack_detail_id": 0,
38       "risklevel": 0,
39       "sconer_rule": 0,
40       "action_id": [
41       ],
42       "attack_place": "",
43       "sconer_name": ""
44     },
45     "message": "2016-07-01 00:35:53 172.16.203.20 GET /Themes/jd/n.html55.png - 80 - 172.16.1.9 Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+"
46     "XHTML": "!!<!DOCTYPE html><html><head></head><body><img alt='JD logo' src='http://172.16.203.20/Themes/jd/n.html55.png' style='display: block; margin: auto;'></body></html>",
47     "req_method": "GET",
48     "uid": "2454",
49     "pctch": "2454",
50     "os": "Windows",
51     "ip": "172.16.203.20",
52     "device": "0",
53     "name": "Chrome",
54     "os_name": "Windows",
55     "device": "Other"
56   },
57   "res_code": "404",
58 }

```

先知安全技术社区

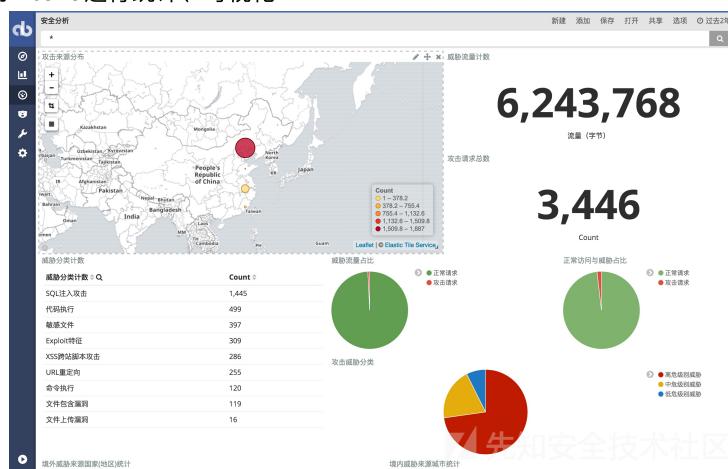
```

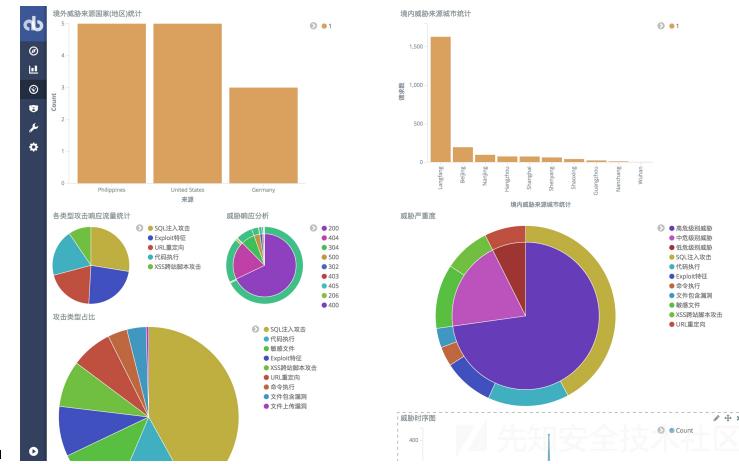
"source": {
  "inserttime": "2017-05-29T21:40:21.481Z",
  "geolip": {
    "ip": "172.16.203.20",
    "req_url": "/Themes/jd/n.html55.png",
    "attack_info": {
      "risk_desc": "中危级别威胁",
      "attack_detail": "攻击行为普通发出",
      "attack_rule": [
        "wwwroot"
      ],
      "attack_status": 1,
      "other": "",
      "action_desc": [
        "正常访问探测服务器各相目录是否存在网站备份"
      ],
      "attack_rule_id": [
        42
      ],
      "attack_type_name": "敏感文件",
      "attack_source_place": [
        "2016-07-01 02:23:28 172.16.203.20 HEAD /wwwroot.zip - 80 - 172.16.1.9 Mozilla/4.0+(compatible;MSIE+8.0;+Windows+NT+6.1;+Trident/4.0) 404 0 2 15\n"
      ],
      "attack_status_name": "攻击请求",
      "attack_type_id": 5,
      "action_risk_level": 2,
      "sconer_status": 0,
      "risklevel": 2,
      "sconer_rule": 0,
      "action_id": [
        42
      ],
      "attack_place": "message",
      "sconer_name": ""
    },
    "message": "2016-07-01 02:23:28 172.16.203.20 HEAD /wwwroot.zip - 80 - 172.16.1.9 Mozilla/4.0+(compatible;MSIE+8.0;+Windows+NT+6.1;+Trident/4.0) 404 0 2 15\n",
    "req_method": "HEAD",
    "uid": "2454",
    "os": "Windows",
    "name": "Other",
    "os_name": "Windows",
    "device": "Other"
  },
  "res_code": "404",
}

```

先知安全技术社区

○ 利用Kibana进行统计、可视化

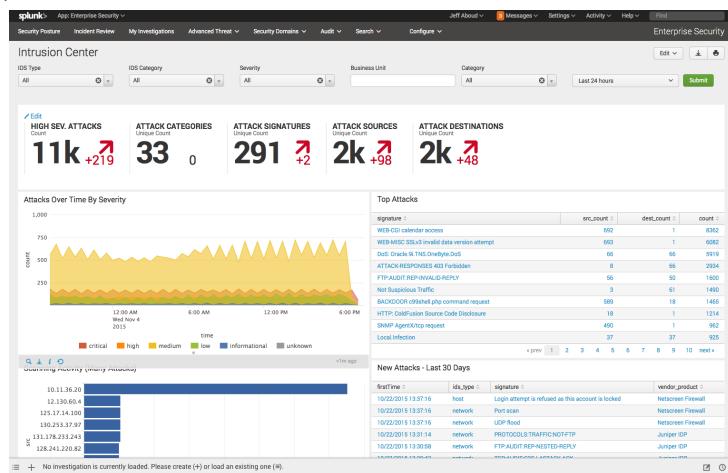




crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:54:38

Splunk

- Splunk
 - 是什么：一个 SIEM 方案，即日志管理和分析平台
 - 截图



- 特点
 - 私有查询语言： SPL = Search Processing Language

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2021-06-01 20:54:51

领域应用

此处介绍，安全分析，在不同领域内的应用。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-06-01 20:53:17

物联网

此处介绍，安全分析，在物联网中的应用。

物联网 安全分析 应用

- 物联网 安全分析
 - 核心流程



- 主要应用
 - 安全监测 + 安全防御 + 态势感知



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:55:24

工业信息

- 工业信息 安全分析



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2021-06-01 20:54:11

云安全

- 云安全 安全分析



crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:57:31

安全分析工具

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:07:01

网络分析工具

- 网络分析 = Network Analysis = NA
 - 关系密切的说法
 - NTA = Network Traffic Analysis = 网络流量分析
 - NTAS = Network Traffic Analysis System = 网络流量分析系统
 - 别称：威胁检测系统
 - 因为：可以从网络流量中分析出攻击，从而检测出威胁
 - Network Scan = 网络扫描
 - 工具
 - 网络扫描工具
 - 网络分析工具
 - 网络流量分析工具
 - 网络扫描器
 - 不同侧重点
 - 网络取证
 - 网络取证工具 = 网络取证分析工具 = NFAT = Network Forensic Analysis Tool
 - 举例
 - NetworkMiner
 - 抓包 ~= 网络流量分析 = 网络报文监听 = 网络协议分析
 - 抓包工具
 - 举例
 - Wireshark

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-06-01 20:56:45

Wireshark

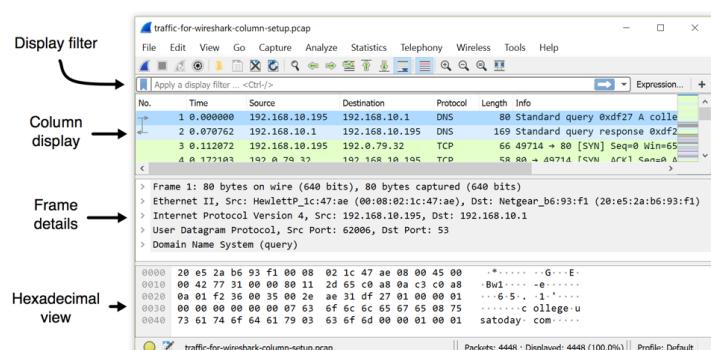
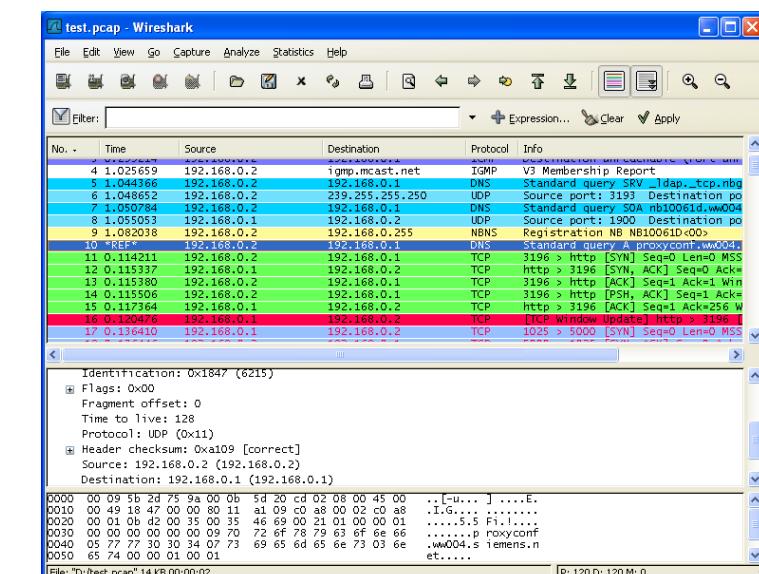
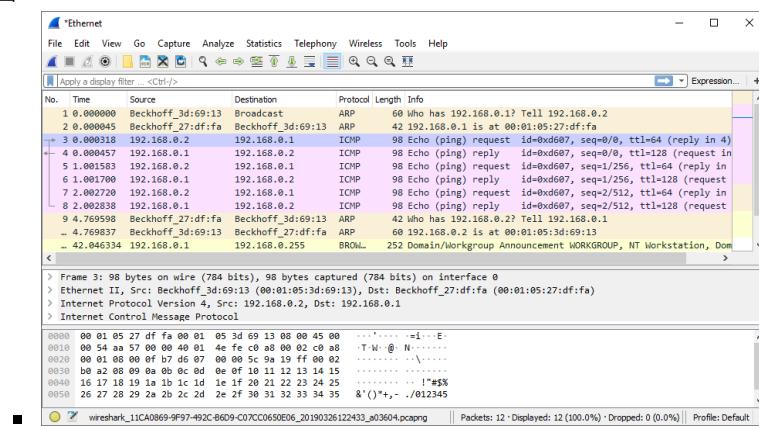
- Wireshark

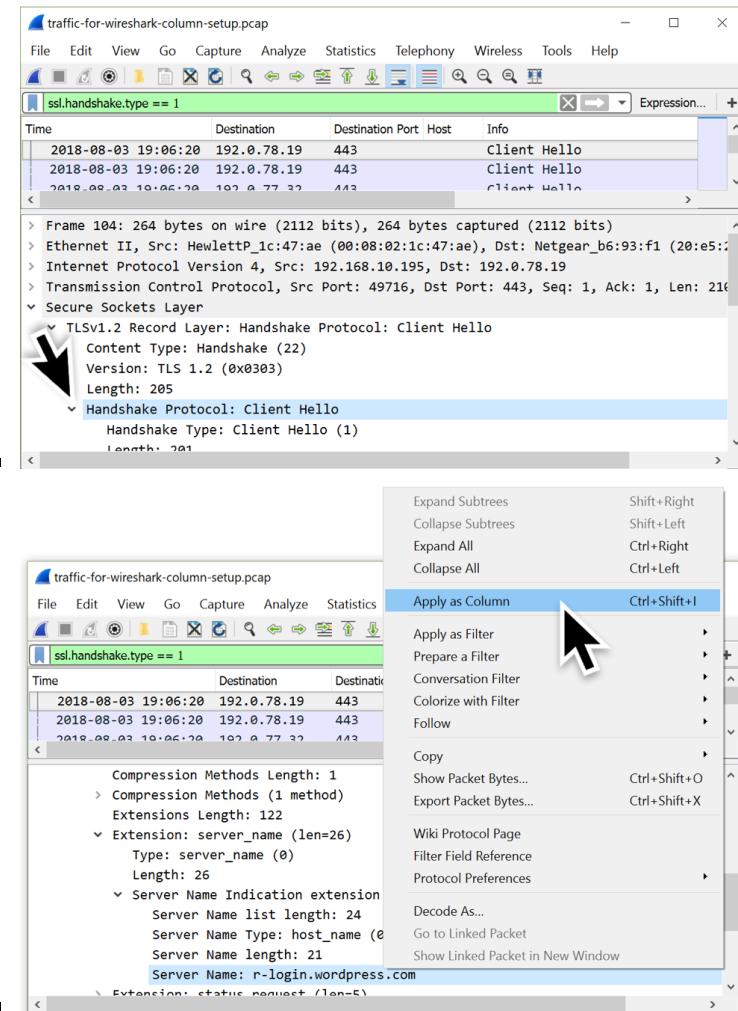
- 一句话描述：最流行的网络协议分析工具，主要用于网络数据包分析

- 概述

- Wireshark是一种网络协议分析工具，使用户能够深入分析网络活动，涵盖上百种协议以及各主要平台，包括Windows, Linux, OS X, Solaris, FreeBSD和NetBSD。数十种抓包文件格式的读写功能，通过GUI或TTY-mode浏览数据

- 图





○ 功能特点

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others

(depending on your platform)

- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:08:35

Capsa Free

- Capsa Free = Capsa Free Network Analyzer

- 概述

▪ 网络分析工具，用于监控、故障排除和分析。来自Colasoft的Capsa Free提供了识别和监控超过300种不同协议的能力。用户可以记录网络配置文件，创建定制报告和设置自定义报警触发条件。此外，Capsa提供邮件监控，自动保存邮件内容以及易于使用的TCP时序图

- 图

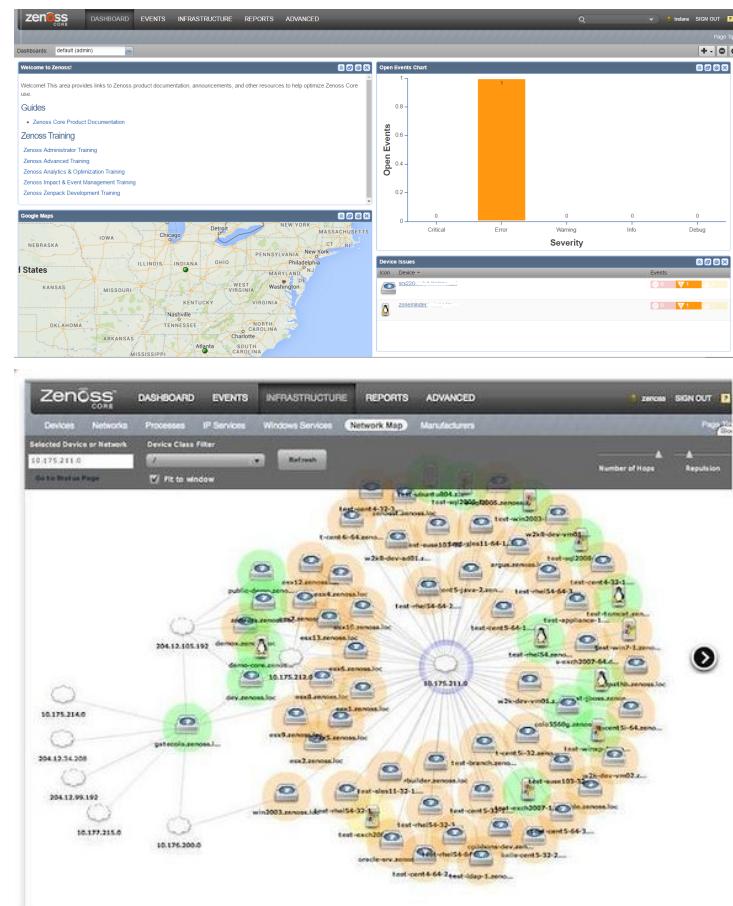


crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2021-05-30 11:03:00

Zenoss Core

- Zenoss Core = Zenoss Community Edition
 - 是什么：一个网络管理平台
 - 基于 Zope 的应用服务器
 - 通过Web页面提供服务
 - 概述
 - 一个集成的网络和系统管理平台，Zenoss Core具备可用性，性能，事件，系统和网络设备配置的监控能力。随着数据流通过SNMP，SSH，WMI，JMX和Syslog，该平台提供了灵活的监控日志和事件管理。此外，该工具针对虚拟和云基础架构，包括VMware ESX，提供专门的监控功能

- 图



crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2021-05-30 11:10:32

NetworkMiner

- NetworkMiner

- 一句话描述：一个开源的网络取证分析工具

- Logo



- 概述

- 有时，不仅需要分析网络流量。软件安全公司Netresec 的 NetworkMiner是一种基于Windows的网络取证分析工具，设计用来收集有关网络中的主机和数据，而非流量。它能够抓包甚至解析PCAP文件，以帮助用户监测网络中主机的OS,主机名，以及开放端口。此工具方便文件、证书的重组传输，而无需耗费额外的流量

- 功能

- 在线online

- 应用领域

- 网络取证分析= Network Forensic Analysis
 - 被动的网络嗅探= passive network sniff
 - 抓包= packet capturing

- 用于分析

- 操作系统operating systems
 - 会话sessions
 - 主机名hostnames
 - 开放端口open ports

- 离线offline

- 解析 PCAP 文件

- 用于重新生成/汇编成要发送的文件和证书

- 图

NetworkMiner 2.0

File Tools Help

Select a network adapter in the list ...

Keywords Anomalies Hosts (129) Files (131) Images (33) Messages Credentials (2) Sessions (113) DNS (271) Parameters (1199)

Filter keyword: Case sensitive ExactPhrase Clear Apply

D. port	Protocol	Filename	Extension	Size	Details
TCP 53130	TlsCertificate	nr-data.net.cer	cer	1 203 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust SSL CA - G2.cer	cer	1 117 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust Global CA.cer	cer	897 B	TLS Certificate: C
TCP 53138	HttpGetNormal	index.html[2].ocsp-response	ocsp-response	1 455 B	gb symcd.com/
TCP 53139	HttpGetChunked	index.html	html	86 958 B	www.meetup.com
TCP 53142	HttpGetNormal	almond.min.js javascript	javascript	2 758 B	static2.meetupsta
TCP 53140	HttpGetNormal	meetup_query_ui.css	css	6 725 B	static2.meetupsta
TCP 53144	HttpGetNormal	client_min.js javascript	javascript	3 692 B	static2.meetupsta
TCP 53145	HttpGetNormal	infoWidget.min.js javascript	javascript	20 639 B	static2.meetupsta
TCP 53151	HttpGetNormal	groupMetadata.min.js javascript	javascript	2 409 B	static1.meetupsta
TCP 53149	HttpGetNormal	mt-twoButtonCTA-testimonial.css	css	445 B	static1.meetupsta
TCP 53147	HttpGetNormal	print.css	css	2 171 B	static1.meetupsta
TCP 53141	HttpGetNormal	meetup-modern.css	css	223 971 B	static2.meetupsta
TCP 53139	HttpGetNormal	index.html.6D1A30C1.css	css	5 582 B	www.meetup.com
TCP 53146	HttpGetNormal	whitney.css	css	83 455 B	static1.meetupsta
TCP 53150	HttpGetNormal	ghome.min.js javascript	javascript	102 378 B	static1.meetupsta
TCP 53148	HttpGetNormal	chapterbase.css	css	165 101 B	static1.meetupsta
TCP 53143	HttpGetNormal	Meetup_Base_query.min.js javascript	javascript	414 355 B	static2.meetupsta
TCP 53152	HttpGetNormal	thumb_156167702.jpeg	jpeg	2 611 B	photos3.meetupst
TCP 53156	HttpGetNormal	thumb_151699612.jpeg	PNG	2 571 B	photos3.meetupst
TCP 53151	Http Get	thumb_151699612.PNG	PNG	10 523 B	photos3.meetupst

Case Panel

Filename MD5 snort.log... f3301c2...

Reload Case Files

Live Sniffing Buffer Usage:

NetworkMiner 2.0

File Tools Help

Select a network adapter in the list ...

Keywords Anomalies Hosts (129) Files (131) Images (33) Messages Credentials (2) Sessions (113) DNS (271) Parameters (1199)

Live Sniffing Buffer Usage:

NetworkMiner 0.88

File Tools Help

Select a network adapter in the list ...

Hosts (110) | Frames (10xxx) | Files (546) | Images (324) | Credentials (107) | DNS (227) | Parameters (1199)

Sort Hosts On: IP Address (ascending) Sort and Refresh

- 192.168.151.130 [goldfinger] (Linux)
 - IP: 192.168.151.130
 - MAC: 000C29C2F0C (Vmware, Inc.)
 - Hostname: goldfinger
 - OS: Linux
 - Satori DHCP: Linux - Linux 2.6 (100.00 %)
 - Satori TCP: Linux - Linux 2.6 (100.00 %)
 - TTL: 64 (distance: 0)
 - Open TCP Ports:
 - Sent: 4825 packets (691 852 Bytes), 0.00 % cleartext (0 of 0 Bytes)
 - Received: 5302 packets (4 108 079 Bytes), 0.00 % cleartext (0 of 0 Bytes)
 - Incoming sessions: 0
 - Outgoing sessions: 200
 - Host Details:
 - Queried DNS names : travelocity.com,travelocity.com.localdomain,i.travelpn.com.e...
 - Web Browser User-Agent 1: Mozilla/5.0 (X11; U; Linux i686; en-US) Gecko/20071...
 - Web Browser User-Agent 2: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.12) G...
 - Web Browser User-Agent 3: Ekiqa

Case Panel

Filename MD5 suspect... 712169.

Reload Case Files

Live Sniffing Buffer Usage:

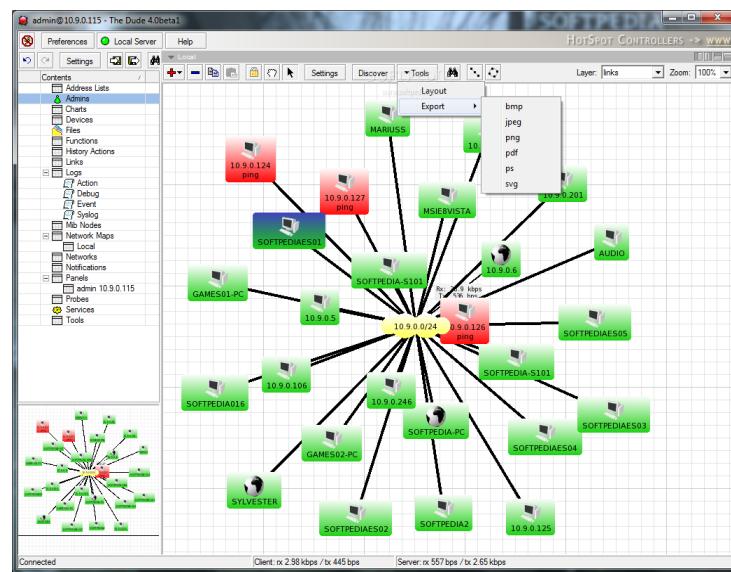
crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2021-05-30 11:09:40

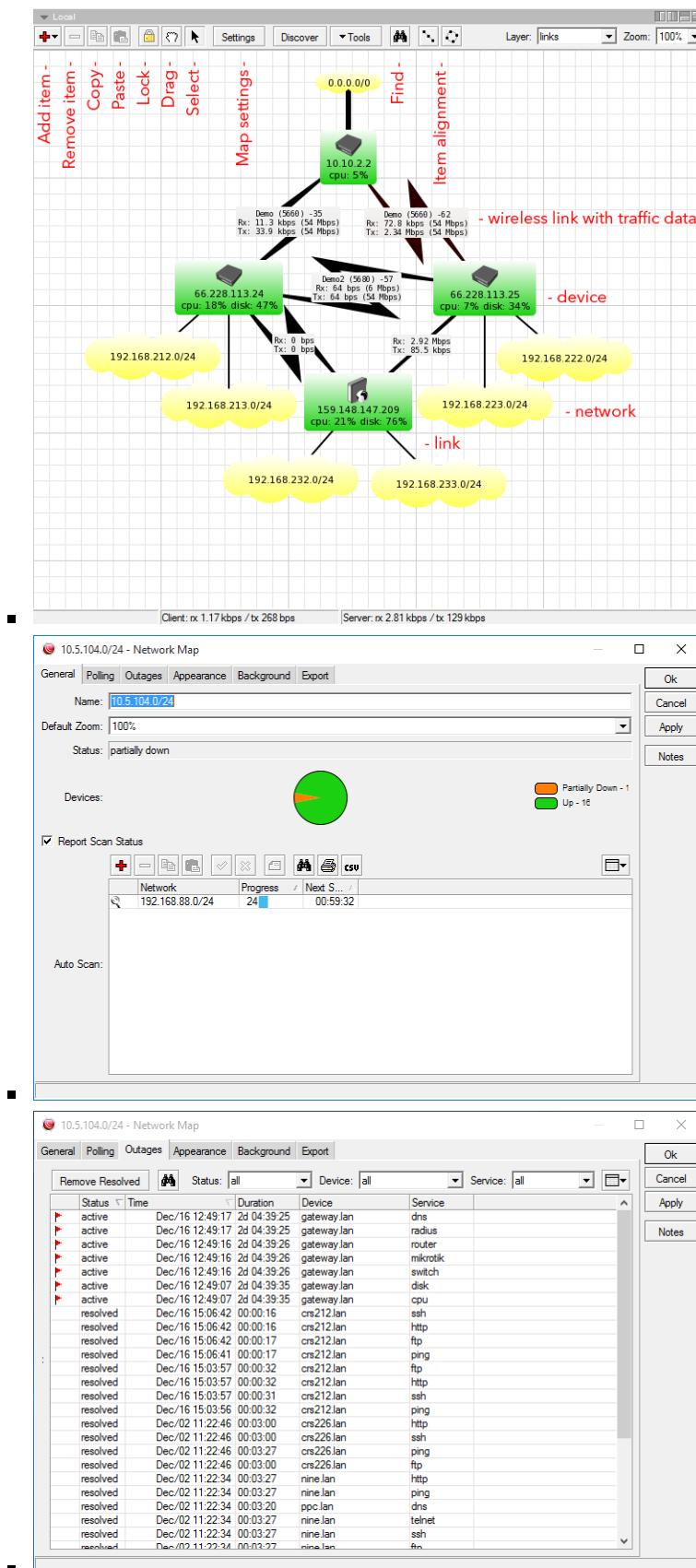
The Dude

- The Dude

- 是什么：网络监控器network monitor
- 作用：极大地提高你管理网络的效率
 - 主要是可以画出内网的网络关系图，可视化后，方便理解和管理设备
- 概述
 - 在指定子网内自动扫描设备。The Dude能够绘制网络地图，监控运行设备的服务器并在服务器有问题时自动告警。能够运行在Windows, Linux Wine, Darwin和MacOS，并支持设备的SNMP, ICMP, DNS 和 TCP 监控
- 功能
 - 自动扫描内网所有设备
 - 画出网络结构布局图
 - 监控设备服务
 - 服务异常报警
 - 不仅可以监控（设备），还可以管理（设备）

- 图





Angry IP Scanner

- Angry IP Scanner
 - 别称: ipscan
 - 是什么: 一个开源的跨平台的网络扫描工具
 - 设计宗旨: 速度快, 易用
 - 概述
 - 一种轻量级IP扫描工具, 使用多线程扫描技术快速扫描, 结果能够保存到CSV, TXT, XML 或 IP-Port 列表文件中。基于Java的灵活框架, 并且能够通过插件扩展额外信息收集功能
 - 图
 - Windows
 - Windows 10
 - Windows 7/Vista
 - Windows XP

IP	Ping	Hostname	Ports [3+]	Web detect
195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
195.80.116.228	10 ms	[n/a]	80,443	[n/a]
195.80.116.229	9 ms	[n/a]	80,443	Apache
195.80.116.230	13 ms	mx3.rmk.ee	[n/a]	[n/a]
195.80.116.231	10 ms	mx4.rmk.ee	[n/a]	[n/a]
195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.235	9 ms	[n/a]	80,443	[n/a]
195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

▪ Windows 7/Vista

IP	Ping	TTL	Hostname	Ports [4+]
66.249.93.73	38 ms	246	ug-in-f73.google.com	[n/a]
66.249.93.74	50 ms	246	ug-in-f74.google.com	[n/a]
66.249.93.75	43 ms	246	ug-in-f75.google.com	[n/a]
66.249.93.76	43 ms	245	ug-in-f76.google.com	[n/a]
66.249.93.77	36 ms	245	ug-in-f77.google.com	443
66.249.93.78	52 ms	246	ug-in-f78.google.com	80,443
66.249.93.79	41 ms	246	ug-in-f79.google.com	80,443
66.249.93.80	[n/a]	[n/s]	[n/s]	[n/s]
66.249.93.81	44 ms	245	ug-in-f81.google.com	80,443
66.249.93.82	46 ms	245	ug-in-f82.google.com	80,443
66.249.93.83	50 ms	246	ug-in-f83.google.com	80,443
66.249.93.84	41 ms	246	ug-in-f84.google.com	80,443
66.249.93.85	43 ms	245	ug-in-f85.google.com	80,443
66.249.93.86	[n/a]	[n/s]	[n/s]	[n/s]

▪ Windows XP

IP Range - Angry IP Scanner					
IP	Ping	Hostname	Ports [2+]	Web detect	
66.249.93.82	123 ms	ug-in-f92.google.com	80,443	gws	
66.249.93.83	133 ms	ug-in-f83.google.com	80,443	gws	
66.249.93.84	123 ms	ug-in-f84.google.com	80,443	gws	
66.249.93.85	117 ms	ug-in-f85.google.com	80,443	GFE/1.3	
66.249.93.86	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.87	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.88	76 ms	ug-in-f88.google.com	80,443	gws	
66.249.93.89	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.90	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.91	66 ms	ug-in-f91.google.com	80,443	gws	
66.249.93.92	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.93	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.94	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.95	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.96	2083 ms	ug-in-f96.google.com	[n/a]	[n/a]	
66.249.93.97	2053 ms	ug-in-f97.google.com	[n/a]	[n/a]	

■ Ubuntu

IP Range - Angry IP Scanner					
IP	Ping	Hostname	Ports [4+]	Web detect	
195.80.116.170	18 ms	[n/a]	[n/a]	[n/a]	
195.80.116.171	16 ms	[n/a]	443	[n/a]	
195.80.116.172	38 ms	[n/a]	80	Apache/2.2.16 (Debian)	
195.80.116.173	36 ms	[n/a]	443	[n/a]	
195.80.116.174	19 ms	[n/a]	80	[n/a]	
195.80.116.175	22 ms	[n/a]	[n/a]	[n/a]	
195.80.116.176	[n/a]	[n/s]	[n/s]	[n/s]	
195.80.116.177	[n/a]	[n/s]	[n/s]	[n/s]	
195.80.116.178	[n/a]	[n/s]	[n/s]	[n/s]	
195.80.116.179	688 ms	[n/a]	80,443,8080	Apache/2.2.22 (Debian)	
195.80.116.180	358 ms	[n/a]	80	Apache/2.2.16 (Debian)	
195.80.116.181	22 ms	[n/a]	80,443	Apache	
195.80.116.182	18 ms	[n/a]	80	Apache/2.2.16 (Debian)	
195.80.116.183	17 ms	[n/a]	443	[n/a]	
195.80.116.184	22 ms	lists.eas.ee	80	Apache	
195.80.116.185	20 ms	[n/a]	443	[n/a]	
195.80.116.186	16 ms	[n/a]	80,443	[n/a]	

■ Older Mac OS X

IP Range - Angry IP Scanner					
IP	Ping	Hostname	Ports [15+]	Web detect	
172.28.43.206	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.207	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.208	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.209	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.210	0 ms	[n/a]	21,80	CANON HTTP Server Ver2.2	
172.28.43.211	0 ms	[n/a]	21,80	CANON HTTP Server Ver2.2	
172.28.43.212	0 ms	[n/a]	21,23,80,443	[n/a]	
172.28.43.213	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.223	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.224	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.225	[n/a]	[n/s]	[n/s]	[n/s]	
172.28.43.226	0 ms	pcee033219.int.han	[n/a]	[n/a]	
172.28.43.227	[n/a]	[n/s]	[n/s]	[n/s]	

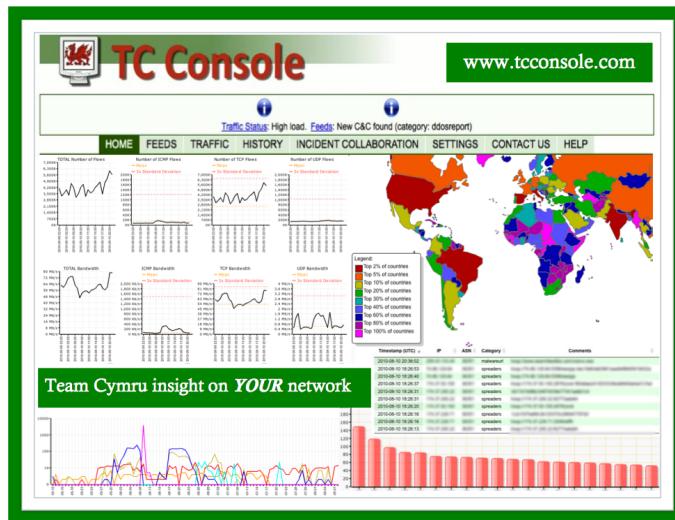
■ Older Linux

IP Range - Angry IP Scanner					
File		Commands		Favorites	Tools
IP Range:		66.249.93.0	to	66.249.93.255	IP Range
Hostname:		g-in-f147.google.com	IP	Netmask	Start
IP	Ping	Hostname	Ports [5+]	Web detect	
66.249.93.104	768 ms	ug-in-f104.google.com	80,443	gws	
66.249.93.105	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.106	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.107	81 ms	ug-in-f107.google.com	80,443	gws	
66.249.93.108	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.109	58 ms	ug-in-f109.google.com	[n/a]	[n/a]	
66.249.93.110	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.111	66 ms	ug-in-f111.google.com	[n/a]	[n/a]	
66.249.93.112	98 ms	ug-in-f112.google.com	80,443	gws	
66.249.93.113	[n/a]	[n/s]	[n/s]	[n/s]	
66.249.93.114	88 ms	gsmtcp93-2.google.com	[n/a]	[n/a]	
66.249.93.115	111 ms	[n/a]	80,443	gws	
66.249.93.116	[n/a]	[n/a]	[n/a]	[n/a]	

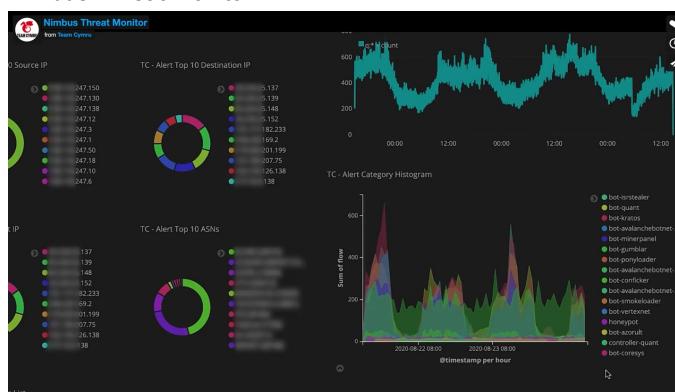
crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:03:59

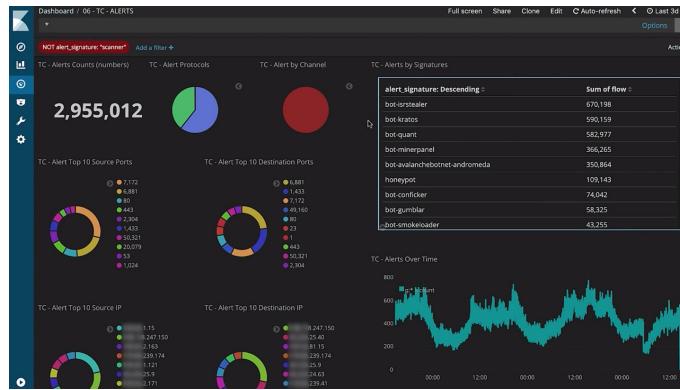
Nimbus Threat Monitor

- Nimbus Threat Monitor
 - 旧称: TC Console
 - 主页
 - [Nimbus Threat Monitor - Team Cymru](#)
 - 概述
 - 此工具极大推进了网络可视化。由非盈利性安全研究公司 Team Cymru 提供，TC Concole 提供网络恶意行为的历史视图，以及网络通信数据，交叉比对该组织收集的全球关于恶意行为的统计数据。该工具免费，但只有愿意与 Team Cymru 数据库分享网络信息的组织才能获得
 - 图
 - 旧: TC Console



- 新: Nimbus Threat Monitor





crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:03:35

附录

下面列出相关参考资料。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:07:37

参考资料

- [Web日志安全分析浅谈 - 先知社区 \(aliyun.com\)](#)
- [Free Network Analyzer, Free Packet Sniffer, Capsa Free - Colasoft](#)
- [Zenoss Core - Wikipedia](#)
- [NetworkMiner - The NSM and Network Forensics Analysis Tool ↗](#)
- [MikroTik Routers and Wireless - Software](#)
- [The Dude Network Software - Automatic Network Mapper - Darknet](#)
- [Angry IP Scanner - the original IP scanner for Windows, Mac and Linux](#)
- [Wireshark · Go Deep.](#)
- [Beckhoff Information System - English](#)
- [The Power of Wireshark](#)
- [Wireshark Tutorial: Changing Your Column Display](#)
- [Facebook Nimbus Threat Monitor replaces TC console](#)
- [TC Console - New Tool Highlights Malicious Activity on your Network | RIPE Labs](#)
- [Nimbus Threat Monitor - Team Cymru](#)
- [Web日志安全分析浅谈 - 先知社区 \(aliyun.com\)](#)
- [云安全解决方案_安恒信息 \(dbappsecurity.com.cn\)](#)
- [奇安信威胁情报中心 \(qianxin.com\)](#)
- [从政策演进轨迹分析拜登政府的“网络安全观-网络与信息中心 \(cug.edu.cn\)](#)
- [工业信息安全解决方案_安恒信息 \(dbappsecurity.com.cn\)](#)
- [网络安全态势感知通报预警平台_安恒信息 \(dbappsecurity.com.cn\)](#)
- [关于SOC、态势感知, 5种常见的关联分析模型 - 赛克蓝德的个人页面 - OSCHINA - 中文开源技术交流社区](#)
- [大数据日志分析：挖掘传统行业日志大数据的无限价值 - 知乎 \(zhihu.com\)](#)
- [常见日志、抓包和系统监控分析软件_Enweitech Software Works-CSDN博客](#)
- [工作机会 \(rizhiyi.com\)](#)
- [Splunk和ElasticSearch深度对比解析 \(github.com\)](#)
- [Splunk vs ELK: Which Works Best For You? | UpGuard](#)
- [高级威胁检测系统_威胁检测 - 腾讯云](#)
-

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-01 20:54:24