

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
安全分析工具	1.4
网络分析工具	1.4.1
Wireshark	1.4.1.1
Capsa Free	1.4.1.2
Zenoss Core	1.4.1.3
NetworkMiner	1.4.1.4
The Dude	1.4.1.5
Angry IP Scanner	1.4.1.6
Nimbus Threat Monitor	1.4.1.7
附录	1.5
参考资料	1.5.1

掌握黑客的行踪：安全分析

- 最新版本: v0.4
- 更新时间: 20210528

简介

通过安全分析，掌握黑客的行踪轨迹。

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](mailto:admin@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： 2021-05-30 11:11:57

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

- 为何要安全分析?
 - 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?
 - 谁攻击的?
 - 搞清楚攻击的具体情况
 - 如何防护?
 - 如果正在被攻击: 如何反查, 反追踪
 - 后续如何避免再被攻击

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 11:10:14

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 = 静态的、历史的: 追踪溯源
 - 现在 = 实时的: 实时监测、威胁感知
 - 将来 : 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: 2021-05-30 11:04:49

数据采集

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 11:07:42

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: 2021-05-30 11:08:46

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

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 11:05:32

人工智能

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 11:09:58

数据应用

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: 2021-05-30 11:10:13

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

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 11:09:10

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

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 11:04:39

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
 - 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: 2021-05-30 11:06:13

Wireshark

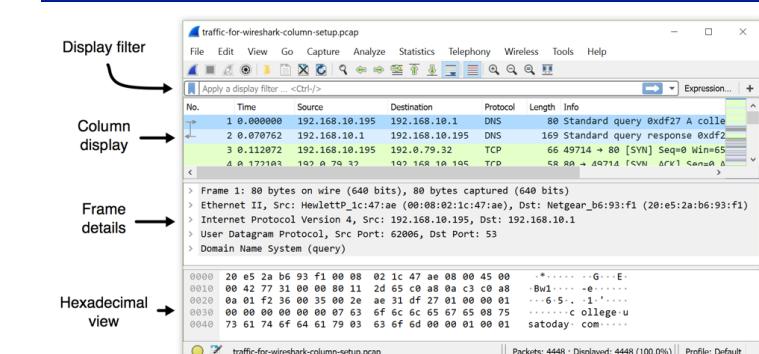
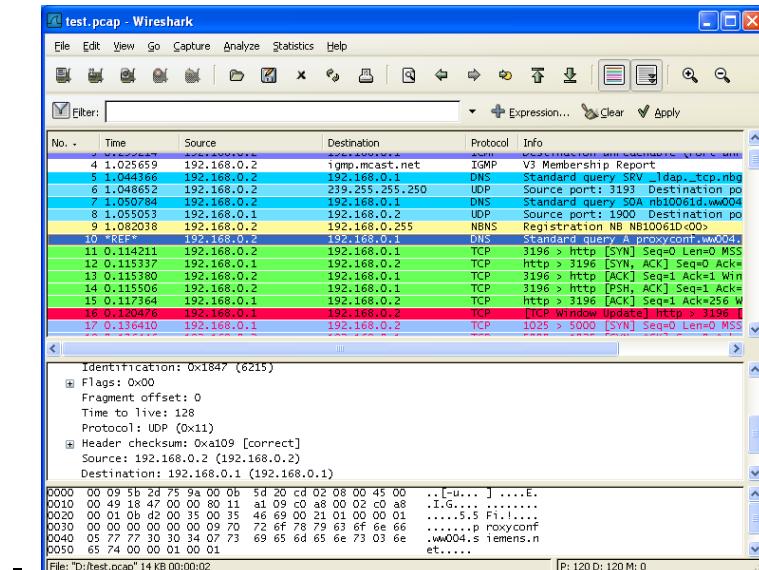
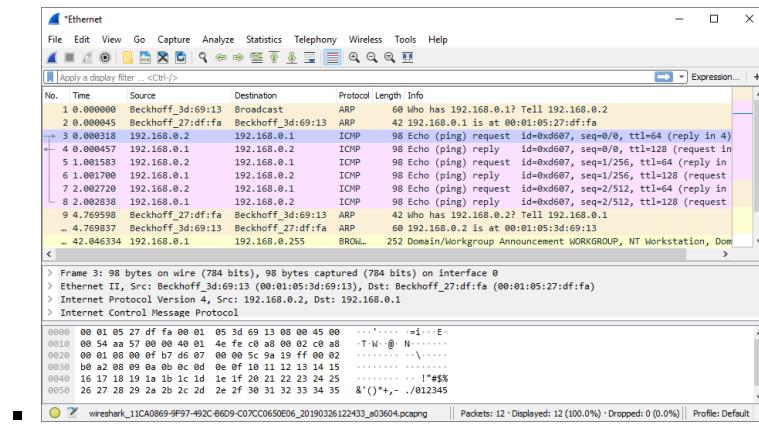
- Wireshark

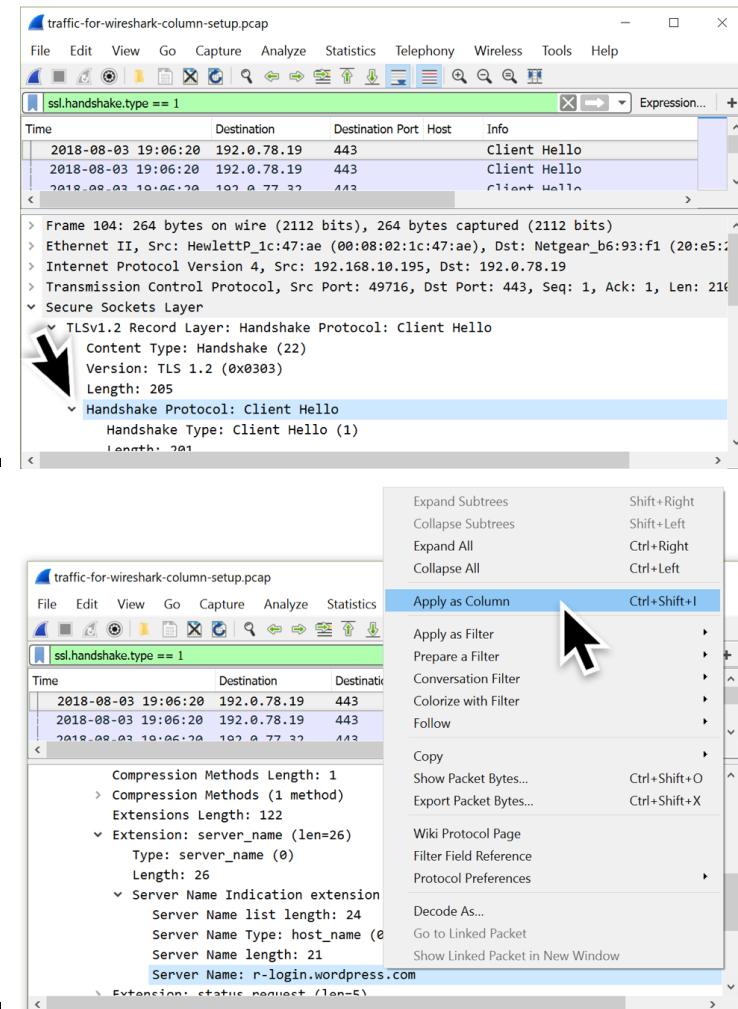
- 一句话描述：最流行的网络协议分析工具，主要用于网络数据包分析

- 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

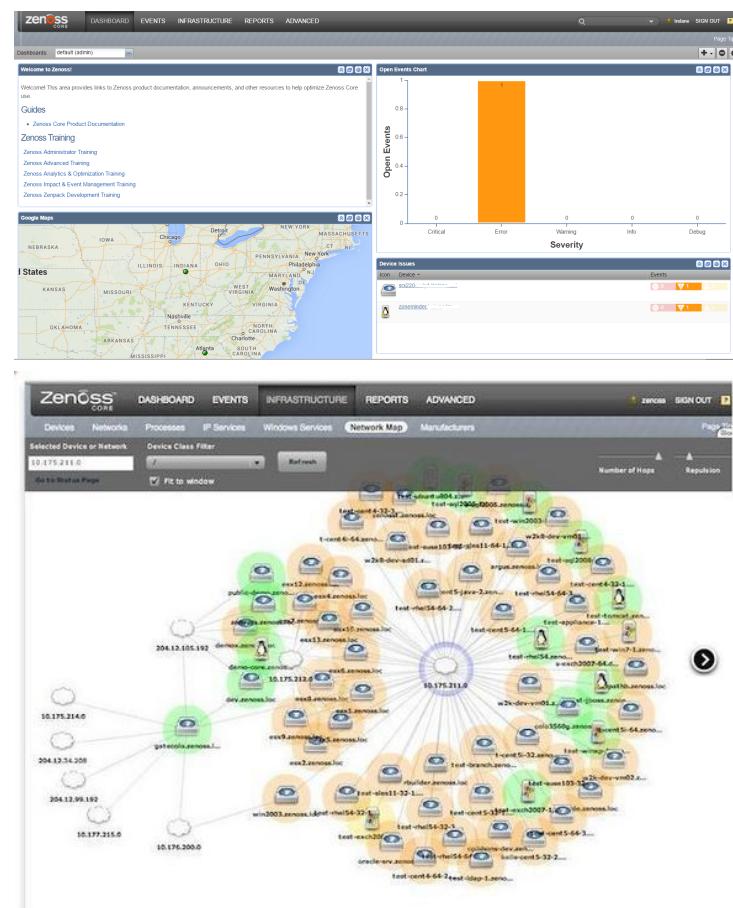


crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2021-05-30 11:03:00

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

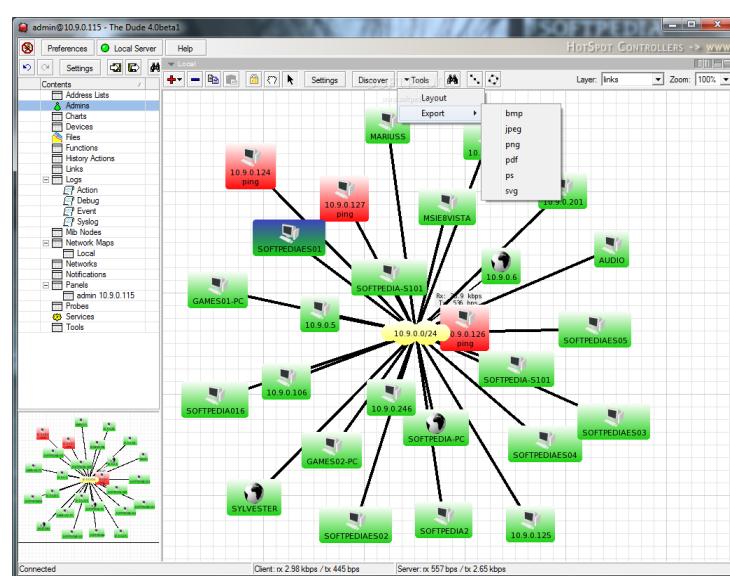
Live Sniffing Buffer Usage:

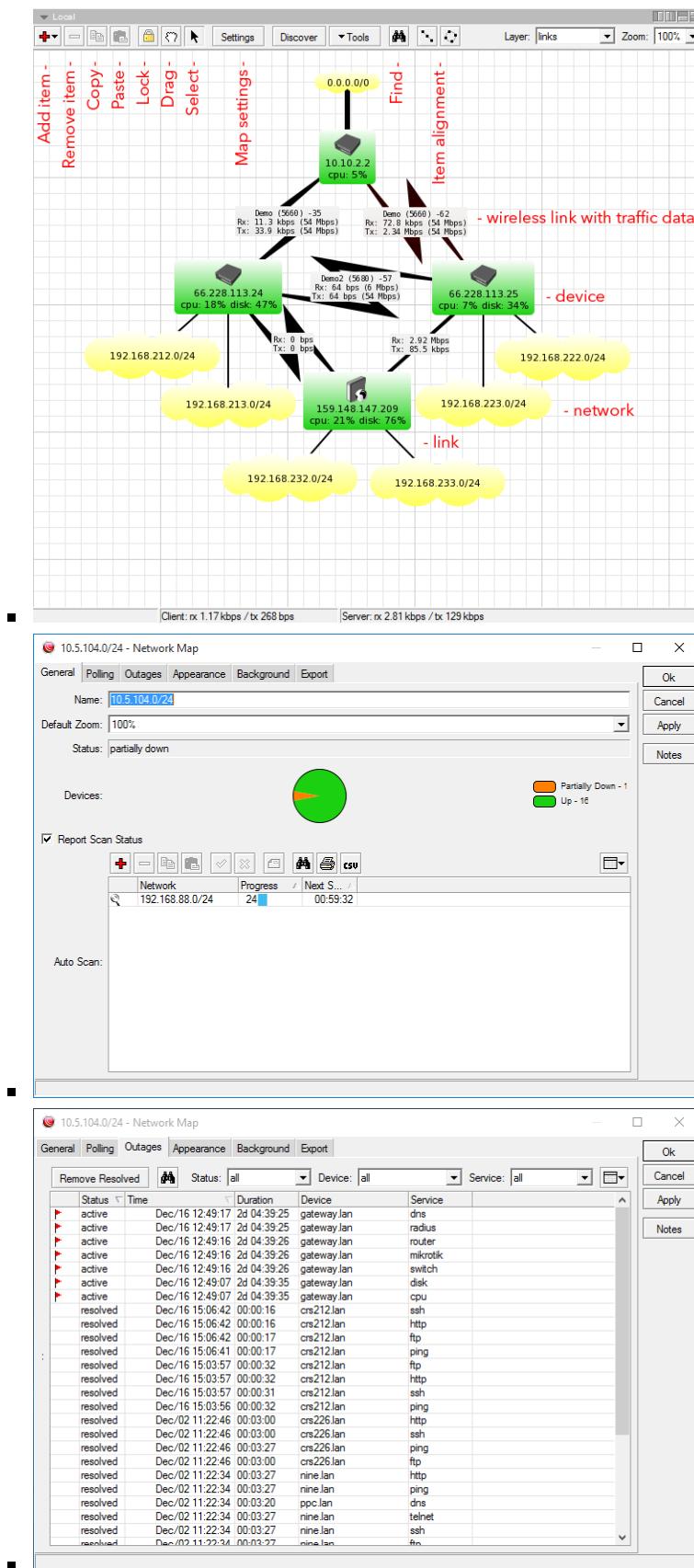
crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2021-05-30 11:09:40

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, Darwine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）

冬





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 Range: 66.249.93.32 to 66.249.93.200		IP Range		Hostname	
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 Range: 195.80.116.186 to 195.80.116.186		IP Range		Hostname	
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 Range: 172.28.43.1 to 172.28.43.255		IP Range		Hostname	
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]	

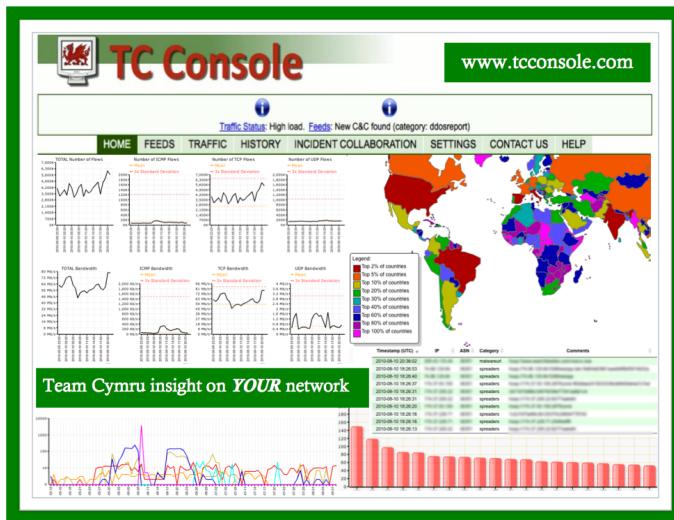
■ Older Linux

IP Range - Angry IP Scanner					
File		Go to	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]	

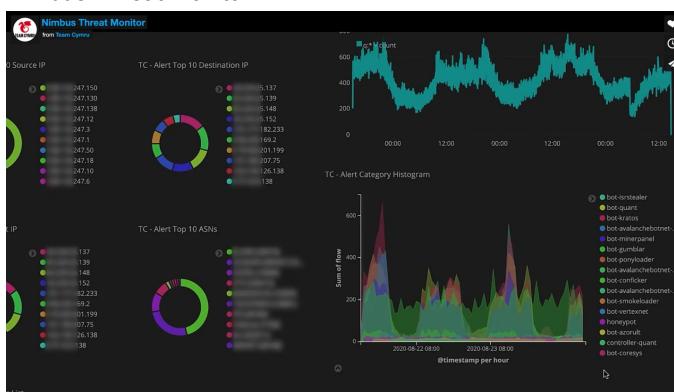
crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-30 11:03:59

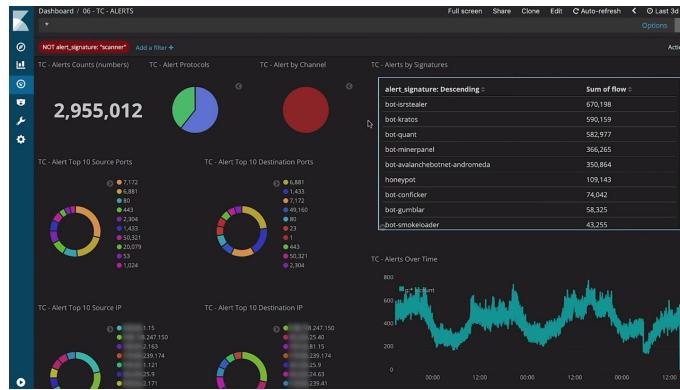
Nimbus Threat Monitor

- 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](#)
- [...](#)

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 11:09:22