目录

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

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

安全分析概览

TODO：

Web日志安全分析浅谈 - 先知社区

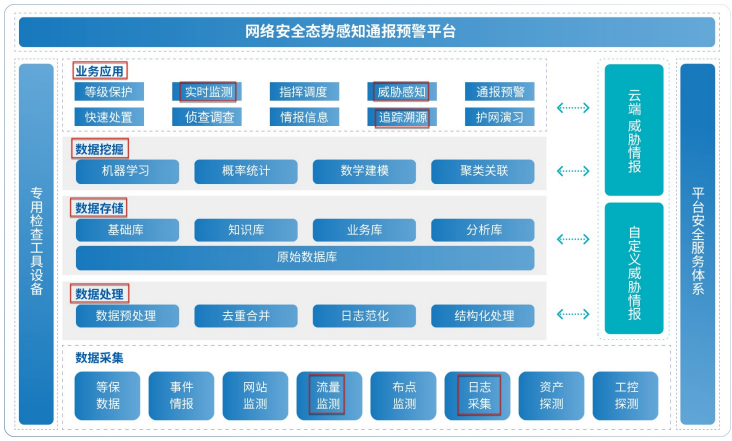
https://xz.aliyun.com/t/1121

- 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

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

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`

数据采集

日志

数据包

数据处理

大数据

人工智能

数据应用

过去

追踪溯源

现在

态势感知

将来

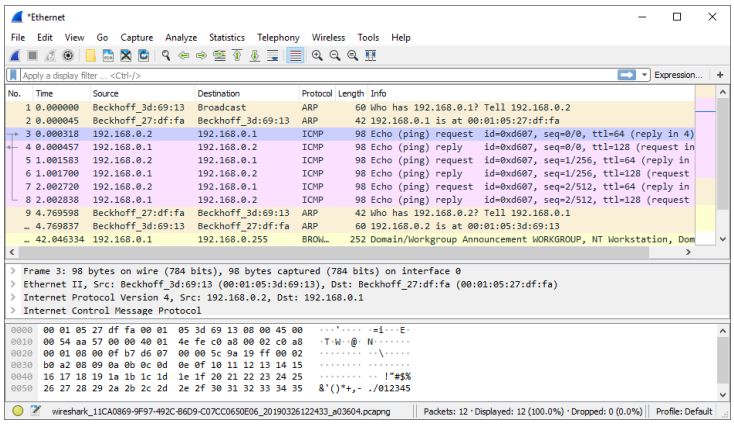
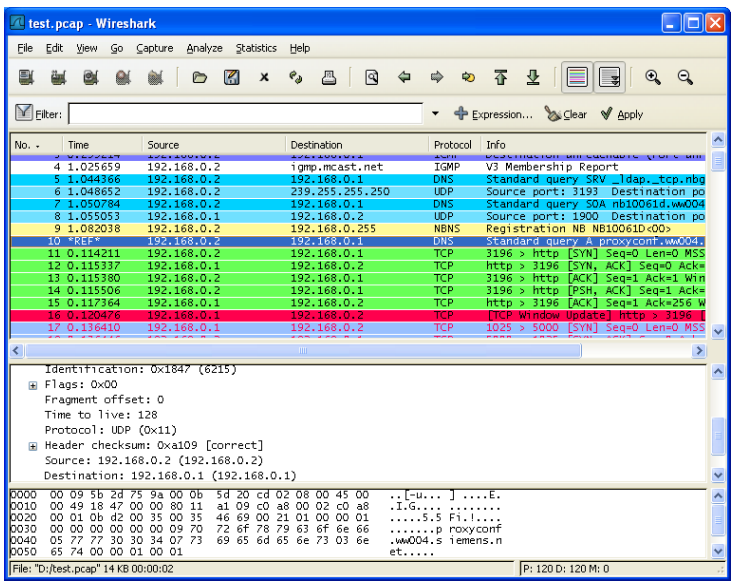
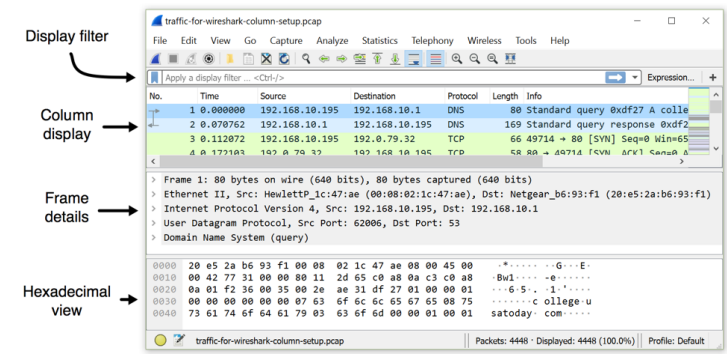
威胁预警

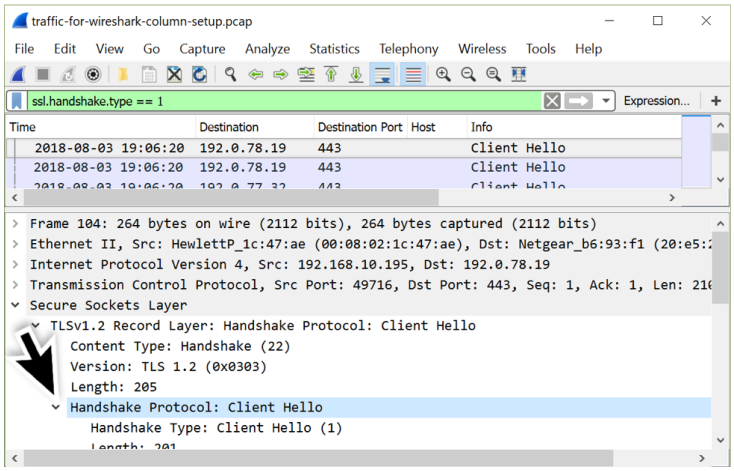
安全分析工具

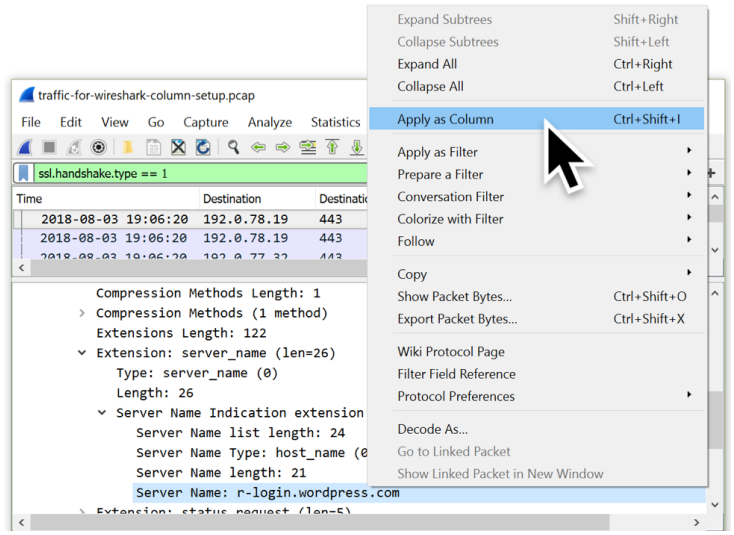
网络分析工具

- 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

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
    - 
    - 
    - 

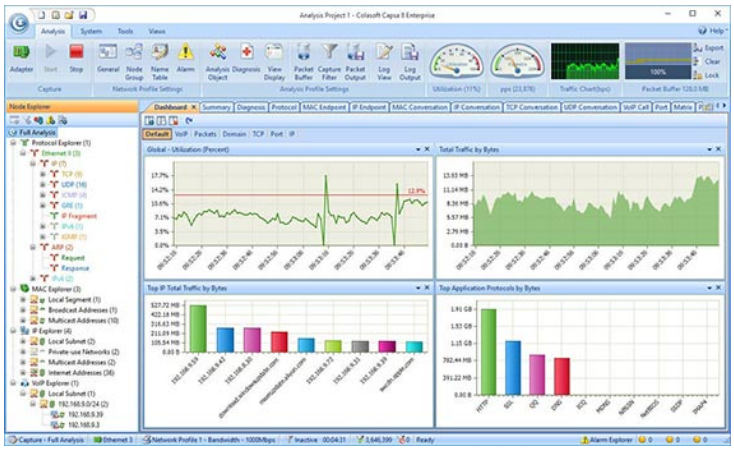
- 

- 

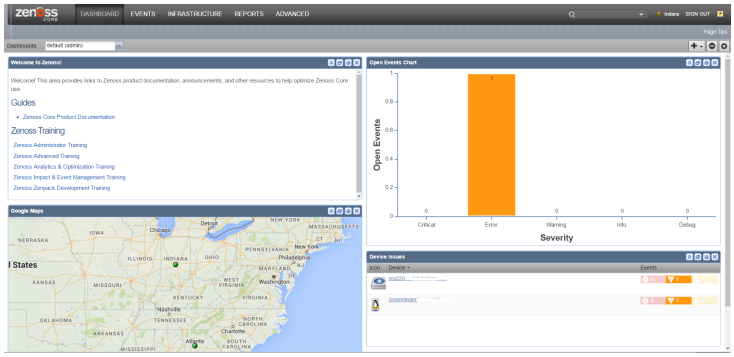
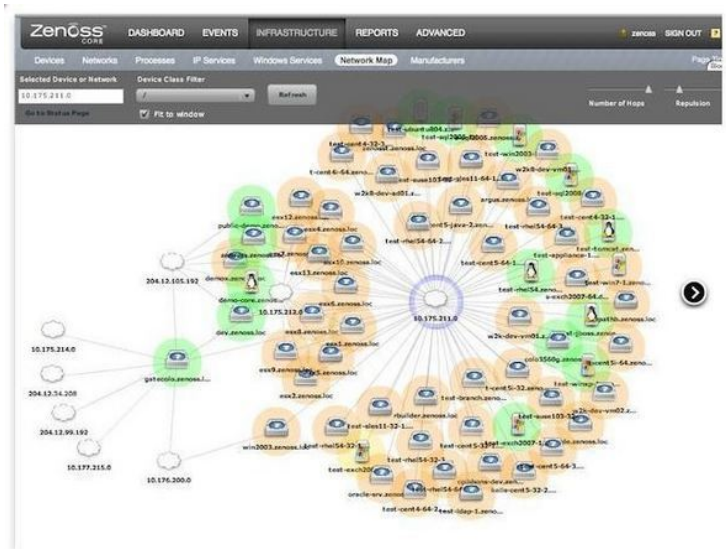
  - 功能特点
    - Deep inspection of hundreds of protocols, with more being added all the time
    - Live capture and offline analysis
    - Standard three-pane packet browser
    - Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
    - Captured network data can be 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

Capsa Free

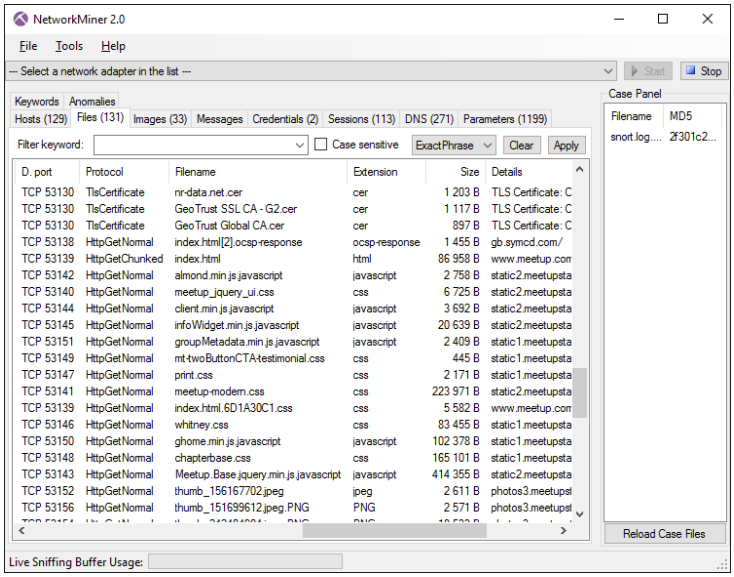
- `Capsa Free = Capsa Free Network Analyzer`
  - 概述
    - 网络分析工具，用于监控、故障排除和分析。来自Colasoft的Capsa Free提供了识别和监控超过300种不同协议的能力。用户可以记录网络配置文件，创建定制报告和设置自定义报警触发条件。此外，Capsa提供邮件监控，自动保存邮件内容以及易于使用的TCP时序图
  - 图
    - 
    - 

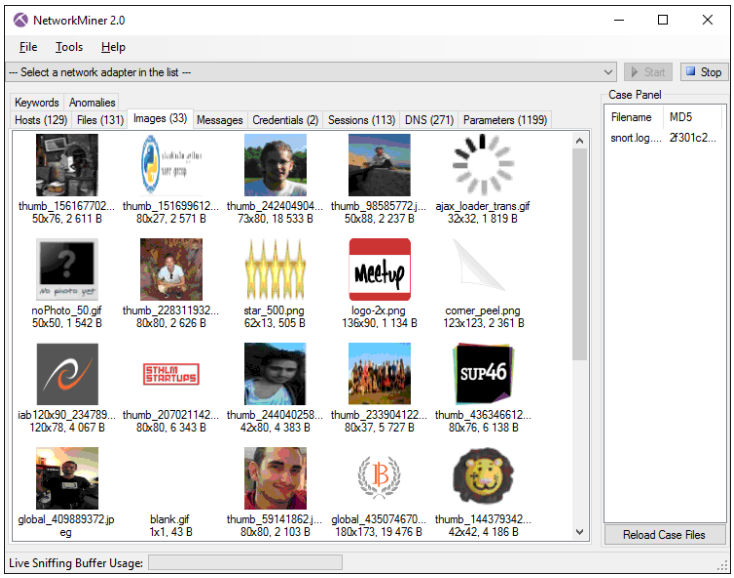
Zenoss Core

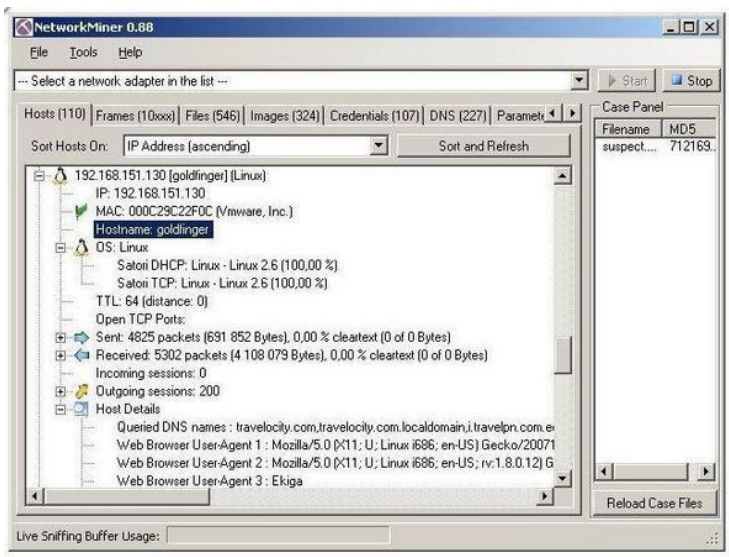
- `Zenoss Core` = `Zenoss Community Edition`
  - 是什么：一个网络管理平台
    - 基于 `Zope` 的应用服务器
    - 通过Web页面提供服务
  - 概述
    - 一个集成的网络和系统管理平台，Zenoss Core具备可用性，性能，事件，系统和网络设备配置的监控能力。随着数据流通过SNMP，SSH，WMI，JMX和Syslog，该平台提供了灵活的监控日志和事件管理。此外，该工具针对虚拟和云基础架构，包括VMware ESX，提供专门的监控功能
  - 图
    - 
    - 

NetworkMiner

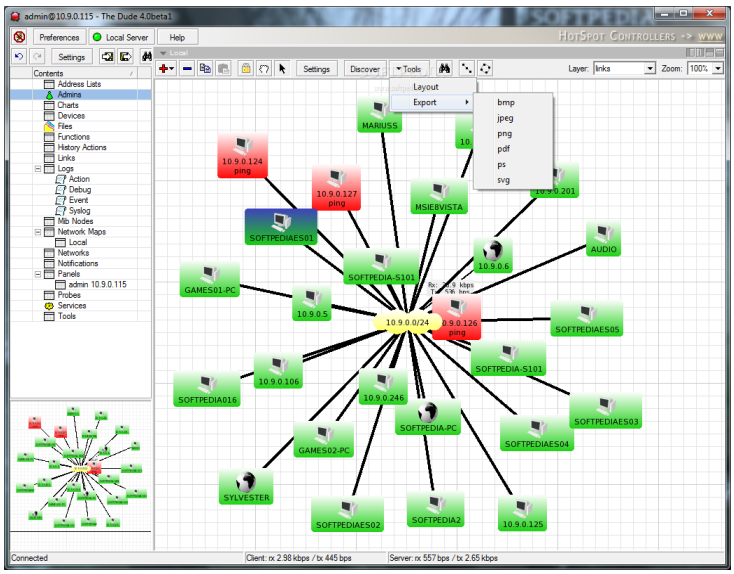
- `NetworkMiner`
  - 一句话描述：一个开源的网络取证分析工具
  - Logo
    - 
  - 概述
    - 有时，不仅需要分析网络流量。软件安全公司Netresec 的NetworkMiner是一种基于Windows的网络取证分析工具，设计用来收集有关网络中的主机和数据，而非流量。它能够抓包甚至解析PCAP文件，以帮助用户监测网络中主机的OS,主机名，以及开放端口。此工具方便文件、证书的重组传输，而无需耗费额外的流量
  - 功能
    - 在线online
      - 应用领域
        - 网络取证分析= `Network Forensic Analysis`
        - 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

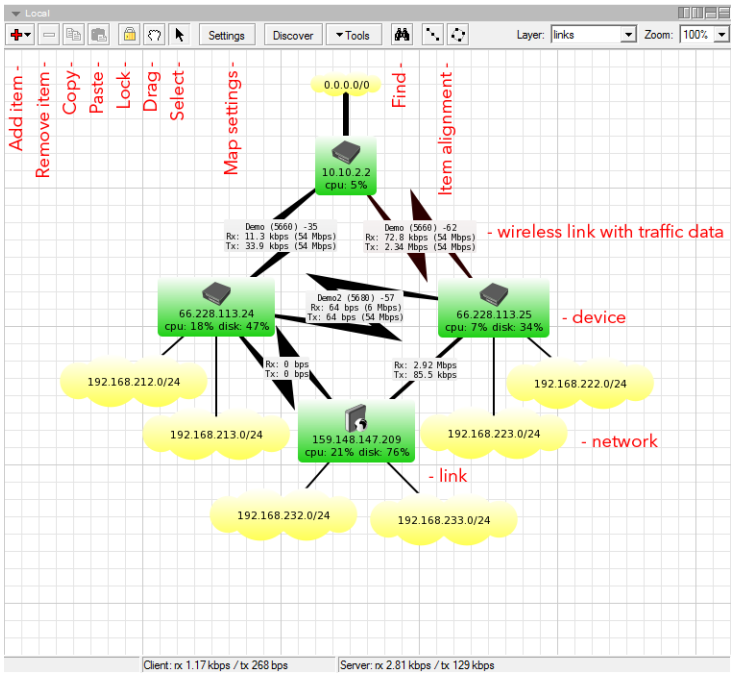


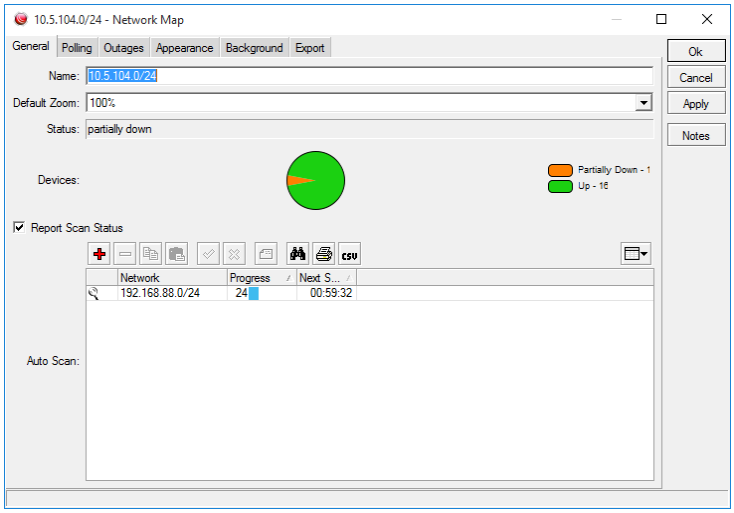


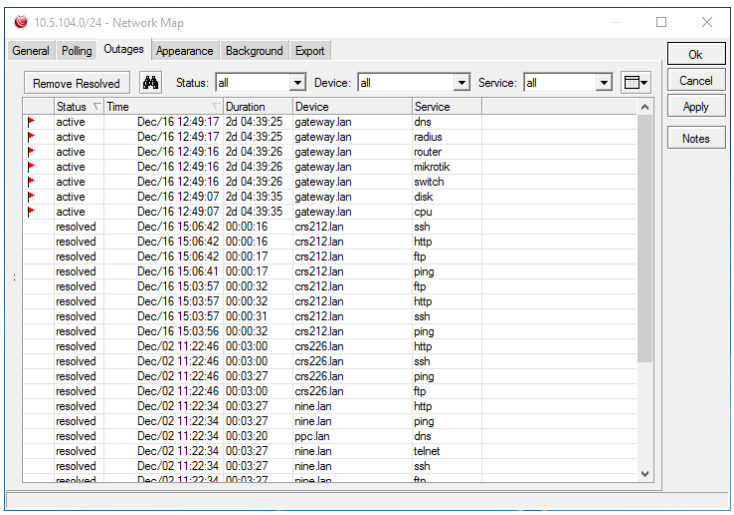


The Dude

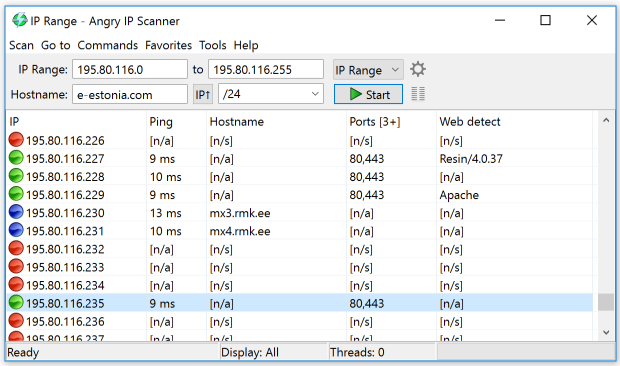
- `The Dude`
  - 是什么：网络监控器network monitor
  - 作用：极大地提高你管理网络的效率
    - 主要是可以画出内网的网络关系图，可视化后，方便理解和管理设备
  - 概述
    - 在指定子网内自动扫描设备。The Dude能够绘制网络地图，监控运行设备的服务器并在服务器有问题时自动告警。能够运行在Windows，Linux Wine, Darwine和MacOS，并支持设备的SNMP, ICMP, DNS 和 TCP 监控
  - 功能
    - 自动扫描内网所有设备
    - 画出网络结构布局图
    - 监控设备服务
    - 服务异常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

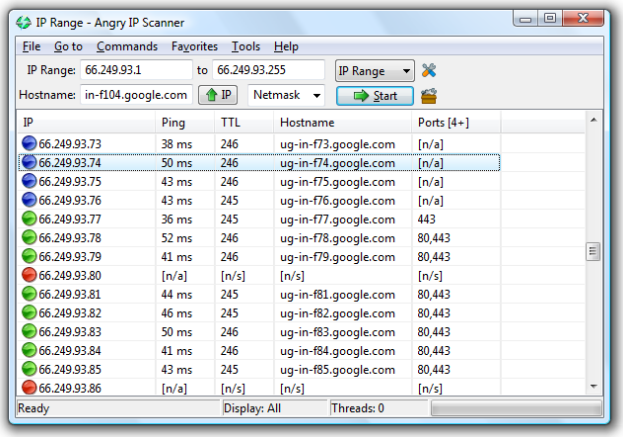




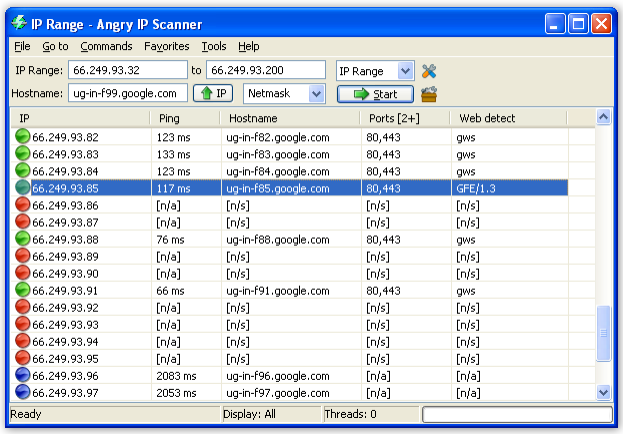


Angry IP Scanner

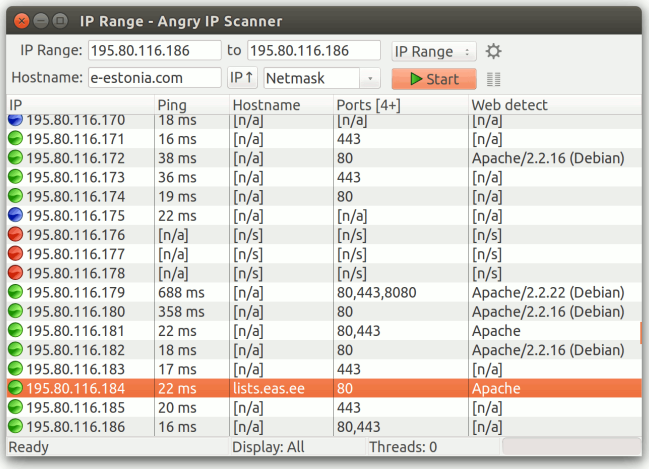
- `Angry IP Scanner`
  - 别称：`ipscan`
  - 是什么：一个开源的跨平台的网络扫描工具
  - 设计宗旨：速度快，易用
  - 概述
    - 一种轻量级IP扫描工具，使用多线程扫描技术快速扫描，结果能够保存到CSV, TXT, XML 或 IP-Port 列表文件中。基于Java的灵活框架，并且能够通过插件扩展额外信息收集功能
  - 图
    - Windows
      - Windows 10
        - 

      - Windows 7/Vista
        - 

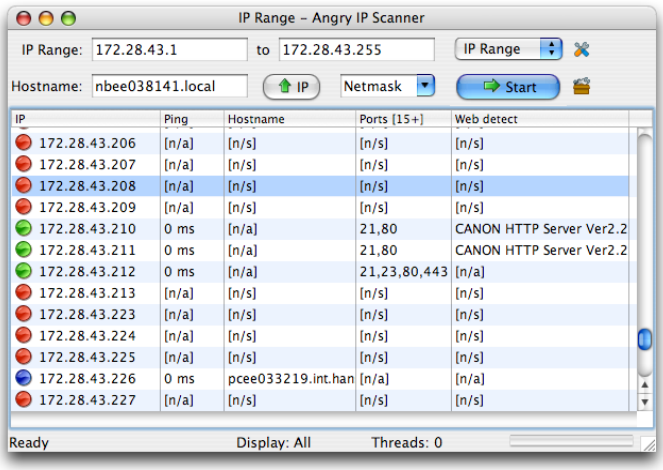
      - Windows XP



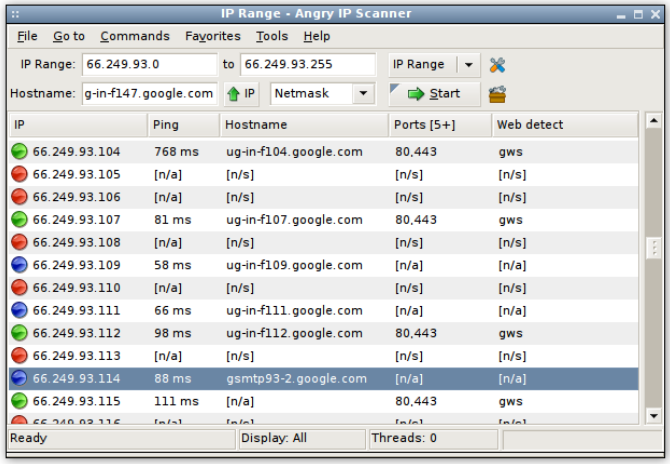
- Ubuntu



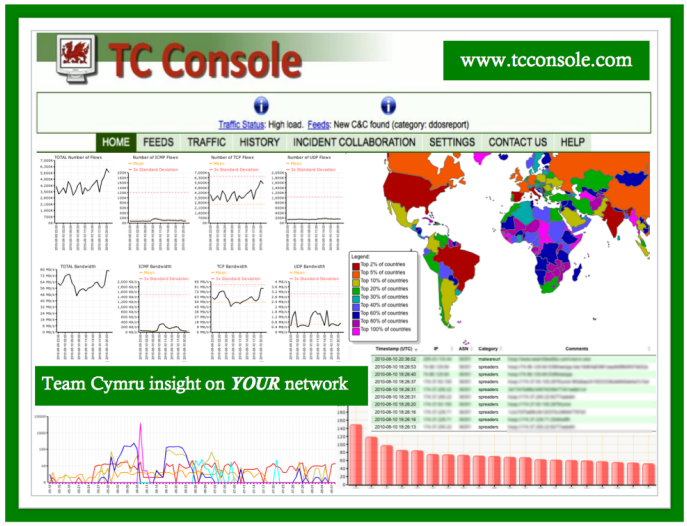
- Older Mac OS X



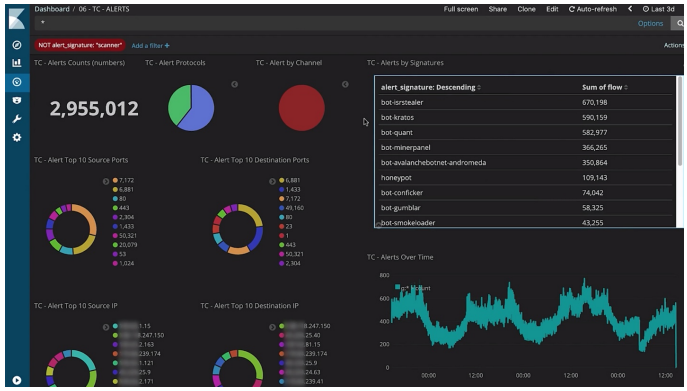
- Older Linux



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
      - 

- 

附录

下面列出相关参考资料。

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