

目录

前言	1.1
Web安全概览	1.2
常见问题	1.2.1
网络攻击	1.3
攻击方式	1.3.1
DoS	1.3.1.1
DDoS	1.3.1.1.1
DDoS防护	1.3.1.1.1.1
工具和系统	1.4
WAF	1.4.1
安全操作系统	1.4.2
Kali Linux	1.4.2.1
网络分析工具	1.4.3
Wireshark	1.4.3.1
Capsa Free	1.4.3.2
Zenoss Core	1.4.3.3
NetworkMiner	1.4.3.4
The Dude	1.4.3.5
Angry IP Scanner	1.4.3.6
Nimbus Threat Monitor	1.4.3.7
代码审计工具	1.4.4
Checkmarx CxEnterprise	1.4.4.1
Armorize CodeSecure	1.4.4.2
Fortify	1.4.4.3
RIPS	1.4.4.4
证书	1.5
安全证书	1.5.1
网络证书	1.5.2
其他证书	1.5.3
安全标准	1.6
等保	1.6.1
ISO27001	1.6.2
安全组织	1.7
OWASP	1.7.1
附录	1.8

参考资料

1.8.1

防止被黑客攻击：Web安全

- 最新版本: v0.8
- 更新时间: 20210603

简介

学习Web安全，以防止被黑客攻击。先对Web安全进行概述，且给出常见问题和解释，包括Web安全对比网络安全、Web安全对比渗透测试；再解释网络攻击，包括常见的DoS和DDoS，以及DDoS的防护方法；整理相关工具和系统，包括WAF、安全操作系统Kali、网络分析工具包括Wireshark、Capsa Free、Zenoss Core、NetworkMiner、The Dude、Angry IP Scanner、Nimbus Threat Monitor等；以及代码审计工具CxEnterprise、Armorize CodeSecure、Fortify、RIPS等；再整理证书相关内容，包括安全证书，如CISP、CISM、CISAW、CCSRP、CISSP等，以及网络证书，如CCIE、CCNA、CCNP等，以及其他证书，如CISA、CDP、CompTIA A+、MCSA、MTA、Oracle、PMP等；总结了安全相关标准，比如信息系统安全等级保护、ISO27001等；以及安全组织，比如OWASP等；最后给出参考资料。

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/avoid_hacker_attack_web_security: 防止被黑客攻击：Web安全](#)

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

- [防止被黑客攻击：Web安全 book.crifan.com](#)
- [防止被黑客攻击：Web安全 crifan.github.io](#)

离线下载阅读

- [防止被黑客攻击：Web安全 PDF](#)
- [防止被黑客攻击：Web安全 ePub](#)
- [防止被黑客攻击：Web安全 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：2021-06-03 20:33:00

Web安全概览

搞懂Web安全，可以更好的防范被黑客攻击，从而保护你的数据和资产的安全。

此处介绍和Web网络相关的安全相关知识。

- Web安全
 - = 网络安全 = cybersecurity
 - 根据攻防角度分
 - 进攻
 - 名字和概念
 - 漏洞扫描
 - 端口扫描
 - Web攻击 = Web漏洞攻击
 - Web挖掘 = Web漏洞挖掘
 - Web渗透
 - 攻击方式
 - SQL注入
 - XSS
 - CSRF
 - 越权
 - 文件包含
 - 文件上传
 - 命令执行
 - WAF绕过
 - URL跳转
 - 钓鱼
 - 社工 = 社会工程学
 - 防守
 - 代码审计 = 安全代码审计 = 安全审计
 - 目的：写出高质量的漏洞少的代码
 - 日志分析 = 安全日志分析 = 日志关联分析
 - 深度包检测
 - 程序行为监视
 - 防护设备
 - 防火墙
 - WAF = Web应用程序防火墙
 - IDS = Intrusion Detection Systems = 入侵检测系统
 - IPS = Intrusion Prevention Systems = 入侵防御系统
 - 相关组织和标准
 - 组织：OWASP
 - 标准：OWASP10
 - 主要工作方向和内容
 - 渗透测试
 - 漏洞挖掘
 - 安全开发
 - 代码审计

- 代码审计 = 代码安全审计 = 安全编码审计 = 源代码审计 = 源代码安全分析
- 网络安保

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: 2021-06-03 20:28:37

常见问题

Web安全 vs 网络安全

- Web安全 vs 网络安全?
 - 狹义上: Web安全 == 网络安全
 - 英文Web = 中文: 网络
 - 广义上: 网络安全 > Web安全
 - 网络 = (基于浏览器的) Web + 其他能访问网络的领域 (比如 移动端的手机, 比如Android、iOS等) -> 网络安全 = Web安全 + 移动 (端) 安全
 - 甚至是: -> 网络安全 = Web安全 + 移动 (端) 安全 + 物联网安全 (~= 工控安全) 等

Web安全 vs 渗透测试

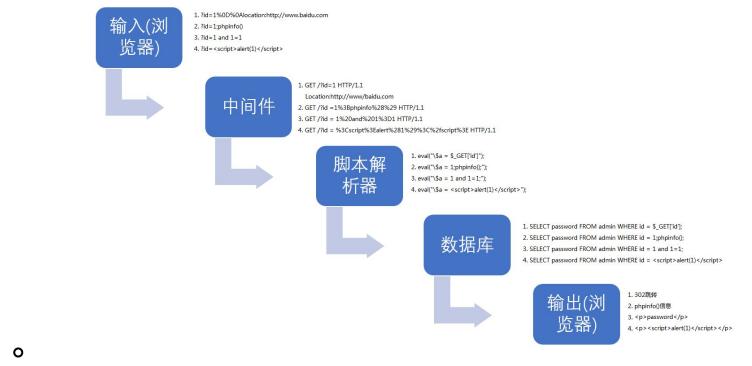
- Web安全 vs 渗透测试?
 - Web安全 = 80%的 渗透测试 + 20% 的 其他
 - 渗透测试
 - 攻: 黑客用渗透测试工具去攻击你的网站, 找到漏洞, 利用漏洞, 干坏事 (让你网站崩溃、偷走你的数据库等)
 - 防: 在合法授权前提下, 自己人去模拟黑客攻击, 自己 (或客户) 的网站 (或系统), 找出漏洞
 - 再及时修复漏洞, 防止被黑客攻击
 - 其他 = 模糊测试 + Web相关: 工具 (网络分析工具等) + 标准和组织 (ISO27001、等级保护、OSWAP等)

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: 2021-06-03 20:28:44

网络攻击

Web攻击 $\sim\!=$ 网络攻击

- web漏洞攻击内部过程



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: 2021-06-03 20:23:58

攻击方式

网络攻击有多种方式。

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: 2021-06-03 20:24:04

DoS

最常见的一种网络攻击方式就是：DoS

- Dos = Denial Of Service = 拒绝服务攻击
 - 别称
 - 洪水攻击
 - 目的：使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问

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：2021-06-03 20:32:11

DDoS

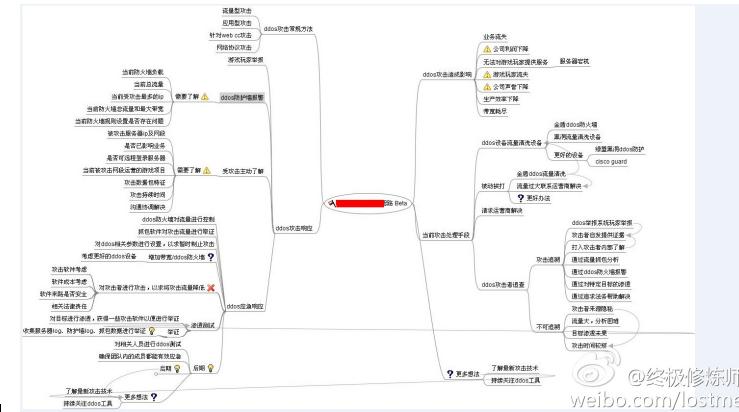
- DDos = Distributed DoS = Distributed Denial Of Service = 分布式拒绝服务攻击
 - 是什么：当黑客使用网络上两个或以上(被攻陷的)电脑(作为 僵尸)向特定的目标发动 拒绝服务 式攻击
 - 重点：DoS攻击不是来自一个地方，而是来自四面八方
 - 相关名词
 - 攻
 - DDoS攻击
 - 防
 - DDoS防护 = 防DDoS (攻击) = DDoS治理
 - 特点
 - 很难防得住
 - 一般被DDoS攻击的都是重要服务、知名网站
 - 比如银行、信用卡支付网关、甚至根域名服务器等
 - (被攻击的)结果=现象
 - 网络异常缓慢 (打开文件或访问网站)
 - 特定网站无法访问
 - 无法访问任何网站
 - 垃圾邮件的数量急剧增加
 - 无线或有线网络连接异常断开
 - 长时间尝试访问网站或任何互联网服务时被拒绝
 - 服务器容易断线、卡顿、lag
 - DDoS攻击形式
 - 攻击形式
 - 带宽消耗型
 - UDP洪水攻击 = User Datagram Protocol Floods
 - ICMP洪水攻击 = ICMP Floods
 - 死亡之Ping = Ping of death
 - 泪滴攻击
 - 资源消耗型
 - 协议分析攻击 = SYN flood = SYN洪水
 - LAND攻击
 - CC攻击 = Distributed HTTP flood = 分布式HTTP洪水攻击
 - 僵尸网络攻击
 - 应用程序级洪水攻击 = Application level floods
 - 防御=对策
 - 防御方式
 - 入侵检测
 - 流量过滤
 - 多重验证
 - 防御工具
 - 防火墙
 - 交换机
 - 路由器

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: 2021-06-03 20:26:45

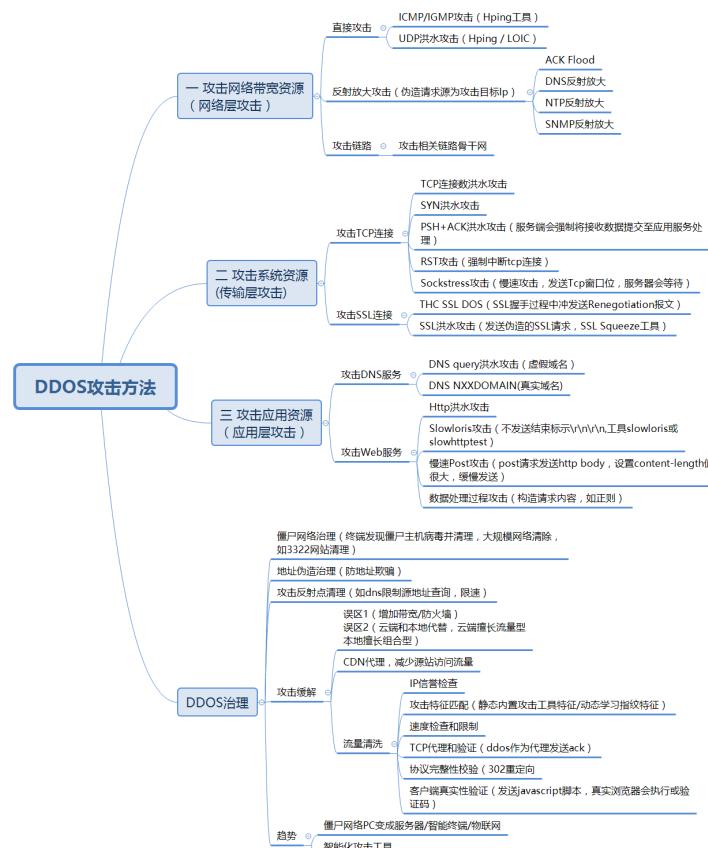
DDoS防护

DDoS攻击与防护总结

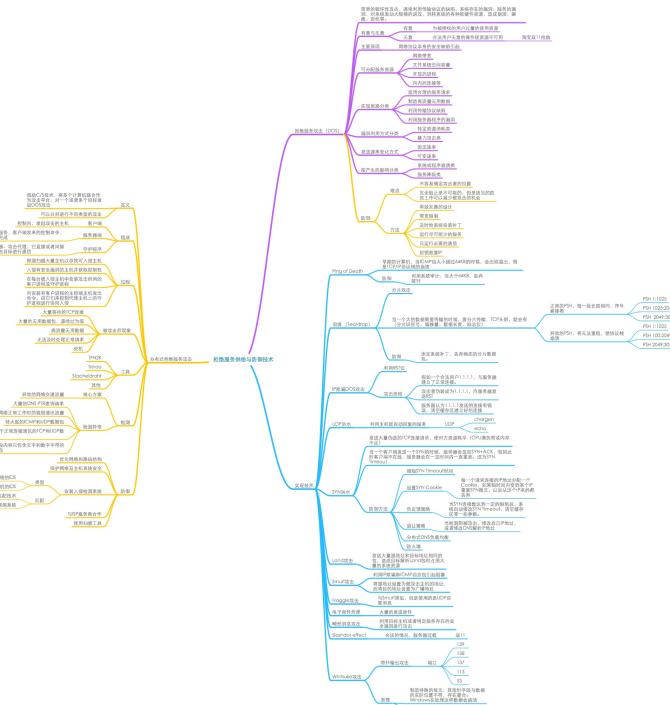
- DDoS攻击与防护总结
 - DDoS攻击及对策



- DDoS攻击方法和治理



- DDoS攻击与防御技术



DDoS防护产品

阿里云 游戏盾

- 阿里云 游戏盾
 - 一句话描述：阿里云针对游戏行业面对的DDoS、CC攻击推出的针对性的网络安全解决方案
 - 谁开发的：阿里云
 - 针对什么：DDoS、CC攻击
 - 适用行业：游戏行业
 - 什么东西：网络安全解决方案
 - 目的：
 - 帮助游戏行业用户用更低的成本缓解超大流量攻击和CC攻击
 - 解决以往的攻防框架中资源不对等的问题
 - 对比
 - 高防IP
 - 防护成本更低，效果更好
 - 除了能针对大型DDoS攻击（T级别）进行有效防御外
 - 还具备彻底解决游戏行业特有的TCP协议的CC攻击问题能力
 - 与传统单点防御DDoS防御方案相比
 - 游戏盾用数据和算法来实现智能调度，将“正常玩家”流量和“黑客攻击”流量快速分流至不同的节点，最大限度缓解大流量攻击；
 - 通过端到端加密，让模拟用户行为的小流量攻击也无法到达客户端
 - 同时

- 在传统防御中，黑客很容易锁定攻击目标IP，在攻击过程中受损非常小。

- 而游戏盾的智能调度和识别

- 可让用户“隐形”，让黑客“显形”

- 每一次攻击都会让黑客受损一次，攻击设备和肉鸡不再重复可用。

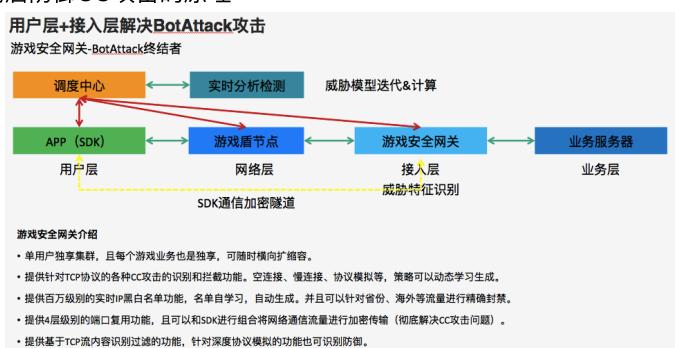
- 颠覆以往DDoS攻防资源不对等的状况

- 架构和原理

- 游戏盾防御DDoS攻击的原理

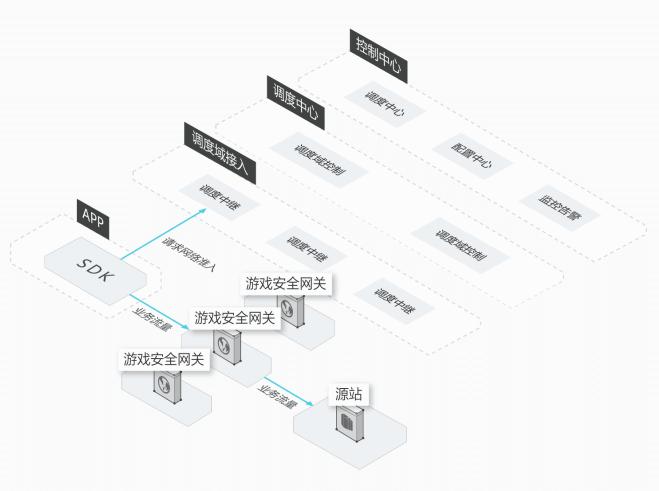


- 游戏盾防御CC攻击的原理

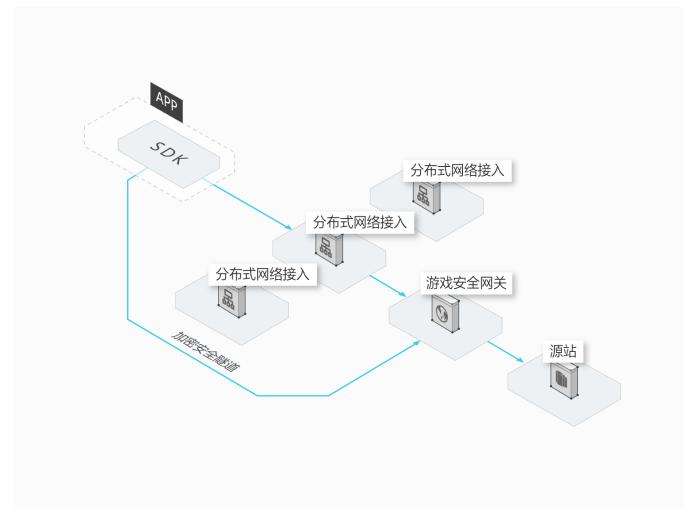


- 客户应用举例

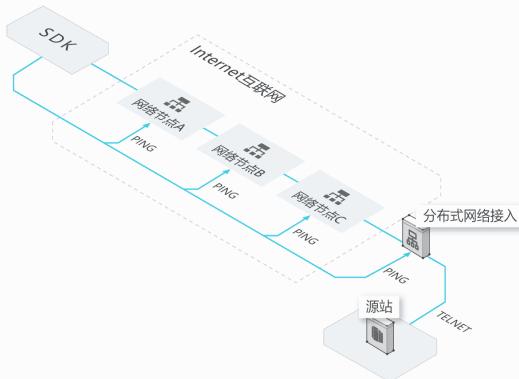
- DDoS攻击防护



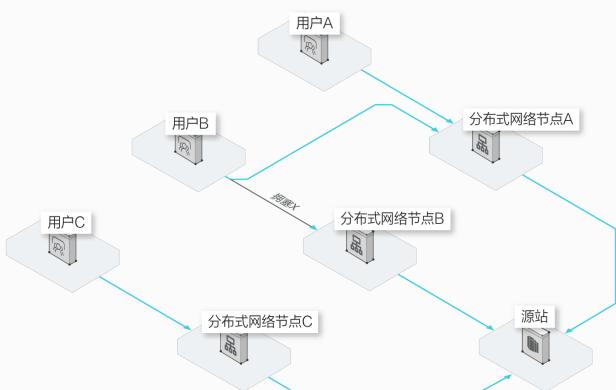
- CC攻击防护



■ 链路监测



■ 拥塞调度



■ 全网加速



极御

极御云安全(StopDDoS)是一家专业的 云安全服务商 。其也有一些抗DDoS的产品：

- 攻击防护产品
 - 抗D云WAF
 - 下一代Web类业务DDoS防御服务，自研云甲DDoS清洗系统，DDoS清洗中心覆盖全球主要国家，千万级CC攻击防御能力，让您的业务固若金汤
 - 云御游戏盾
 - 专为在线游戏打造的终极DDoS防御服务，多种DDoS清洗算法和规则，端云联动，无损清洗DDoS攻击，Anycast近源清洗和加速网络保障游戏丝滑流畅
 - 抗D高防IP
 - 专为 TCP 业务优化的 DDoS 防御服务，可防御游戏CC攻击，全网 10Tb防御能力，随时应对大型DDoS攻击
 - 高防服务器
 - 极具性价比的DDoS防御解决方案，集群化的DDoS防御能力，为个人和小型游戏提供DDoS安全防御服务

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：2021-06-03 20:24:30

工具和系统

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: 2021-06-03 20:31:33

WAF

TODO:

【整理】 WAF 安全

- WAF
 - 历史
 - Perfecto 的 AppShield : 主要用于电商
 - ModSecurity : 开源项目
 - 先: 基于 WAS TC 去制定保护规则
 - WAS TC =OASIS Web Application Security Technical Committee
 - 后: 基于 OWASP 的Top10去制定规则
 - OWASP = Open Web Application Security Project
 - 侧重防信用卡诈骗
 - 相关标准
 - PCI DSS = Payment Card Industry Data Security Standard
 - 现状
 - Web应用已成攻击者首要目标
 - 以硬件设备形式实现的传统WAF不足以提供全面的应用控制和可见性
 - 基于云的新时代WAF可以提供足够的Web防护
 - 交付安全投资的真正价值

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: 2021-06-03 20:31:07

安全操作系统

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: 2021-06-03 20:26:37

Kali Linux

- = Kali Linux
- 是什么：一个Linux操作系统，专门用于渗透测试，
 - Kali
 - = Kali Linux
 - 旧称： BackTrack Linux
 - 是什么：一个操作系统
 - 用途：专门用于安全、逆向、破解、渗透
 - 特点：自带大量相关工具
 - 被称为
 - 网络安全人员的专用系统
 - 资料
 - 主页
 - Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution
 - <https://www.kali.org>
 - 包含工具
 - 首页
 - Penetration Testing Tools - Kali Linux
 - <https://tools.kali.org>
 - Kali Linux Tools Listing | Penetration Testing Tools
 - <https://tools.kali.org/tools-listing>
 - 根据分类
 - Information Gathering
 - ace-voip
 - Amap
 - APT2
 - arp-scan
 - Automater
 - bing-ip2hosts
 - braa
 - CaseFile
 - CDPSnarf
 - cisco-torch
 - copy-router-config
 - DMitry
 - dnmap
 - dnsenum
 - dnsmap
 - DNSRecon
 - dnstracer
 - dnswalk
 - DotDotPwn
 - enum4linux
 - enumIAX

- EyeWitness
- Faraday
- Fierce
- Firewalk
- fragroute
- fragrouter
- Ghost Phisher
- GoLismero
- goofile
- hping3
- ident-user-enum
- InSpy
- InTrace
- iSMTP
- lbd
- Maltego Teeth
- masscan
- Metagoofil
- Miranda
- nbtscan-unixwiz
- Nikto
- Nmap
- ntop
- OSRFramework
- p0f
- Parsec
- Recon-ng
- SET
- SMBMap
- smtp-user-enum
- snmp-check
- SPARTA
- sslaudit
- SSLsplit
- sslstrip
- SSLyze
- Sublist3r
- THC-IPV6
- theHarvester
- TLSSled
- twofi
- Unicornscan
- URLCrazy
- Wireshark
- WOL-E
- Xplico
- Vulnerability Analysis
- BBQSQL

- BED
- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- copy-router-config
- Doona
- DotDotPwn
- HexorBase
- jSQL Injection
- Lynis
- Nmap
- ohrwurm
- openvas
- Oscanner
- Powerfuzzer
- sfuzz
- SidGuesser
- SIPArmyKnife
- sqlmap
- Sqlninja
- sqsus
- THC-IPV6
- tnscmd10g
- unix-privesc-check
- Yersinia
- Exploitation Tools
 - Armitage
 - Backdoor Factory
 - BeEF
 - cisco-auditing-tool
 - cisco-global-exploiter
 - cisco-ocs
 - cisco-torch
 - Commix
 - crackle
 - exploitdb
 - jboss-autopwn
 - Linux Exploit Suggester
 - Maltego Teeth
 - Metasploit Framework
 - MSFPC
 - RouterSploit
 - SET
 - ShellNoob
 - sqlmap
 - THC-IPV6
 - Yersinia

- Wireless Attacks
 - Airbase-ng
 - Aircrack-ng
 - Airdecap-ng and Airdecloak-ng
 - Aireplay-ng
 - airgraph-ng
 - Airmon-ng
 - Airodump-ng
 - airodump-ng-oui-update
 - Airolin-ng
 - Airserv-ng
 - Airtun-ng
 - Asleap
 - Besside-ng
 - Bluelog
 - BlueMaho
 - Bluepot
 - BlueRanger
 - Bluesnarfer
 - Bully
 - coWPAtty
 - crackle
 - eapmd5pass
 - Easside-ng
 - Fern Wifi Cracker
 - FreeRADIUS-WPE
 - Ghost Phisher
 - GISKismet
 - GqrX
 - gr-scan
 - hostapd-wpe
 - ivstools
 - kalibrate-rtl
 - KillerBee
 - Kismet
 - makeivs-ng
 - mdk3
 - mfcuk
 - mfoc
 - mfterm
 - Multimon-NG
 - Packetforge-ng
 - PixieWPS
 - Pyrit
 - Reaver
 - redfang
 - RTLSDR Scanner
 - Spooftooth

- Tkiptun-ng
- Wesside-ng
- Wifi Honey
- wifiphisher
- Wifitap
- Wifite
- wpaclean
- Forensics Tools=取证工具
 - Binwalk
 - bulk-extractor
 - Capstone
 - chntpw
 - Cuckoo
 - dc3dd
 - ddrescue
 - DFF
 - diStorm3
 - Dumpzilla
 - extundelete
 - Foremost
 - Galleta
 - Guymager
 - iPhone Backup Analyzer
 - p0f
 - pdf-parser
 - pdfid
 - pdgmail
 - peepdf
 - RegRipper
 - Volatility
 - Xplico
- Web Applications
 - apache-users
 - Arachni
 - BBQSQL
 - BlindElephant
 - Burp Suite
 - CutyCapt
 - DAVTest
 - deblaze
 - DIRB
 - DirBuster
 - fimap
 - FunkLoad
 - Gobuster
 - Grabber
 - hURL
 - jboss-autopwn

- joomscan
- jSQL Injection
- Maltego Teeth
- Nikto
- PadBuster
- Paros
- Parsero
- plecost
- Powerfuzzer
- ProxyStrike
- Recon-ng
- Skipfish
- sqlmap
- Sqlninja
- sqlsus
- ua-tester
- Uniscan
- w3af
- WebScarab
- Webshag
- WebSlayer
- WebSploit
- Wfuzz
- WhatWeb
- WPScan
- XSSer
- zaproxy
- Stress Testing
 - DHCPig
 - FunkLoad
 - iaxflood
 - Inundator
 - inviteflood
 - ipv6-toolkit
 - mdk3
 - Reaver
 - rtpflood
 - SlowHTTPTest
 - t50
 - Termineter
 - THC-IPV6
 - THC-SSL-DOS
- 其他方面对Kali的支持
 - Hopper Disassembler
 - Hopper - Download
 - <https://www.hopperapp.com/download.html?>
 - 专门提供Kali Linux的zip压缩包

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: 2021-06-03 20:26:38

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：2021-06-03 20:23:55

Wireshark

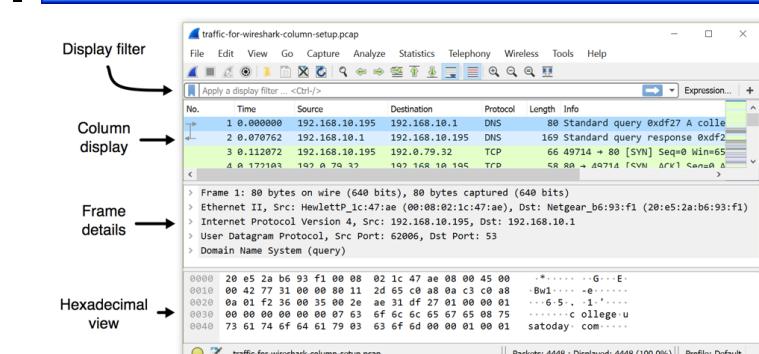
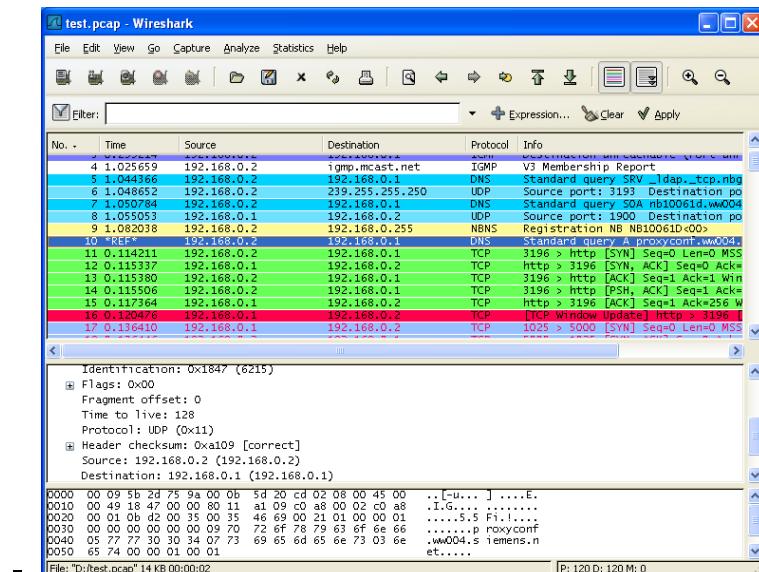
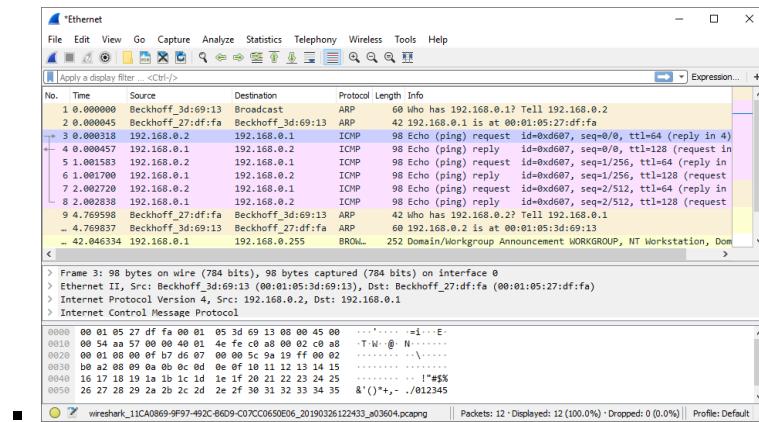
- Wireshark

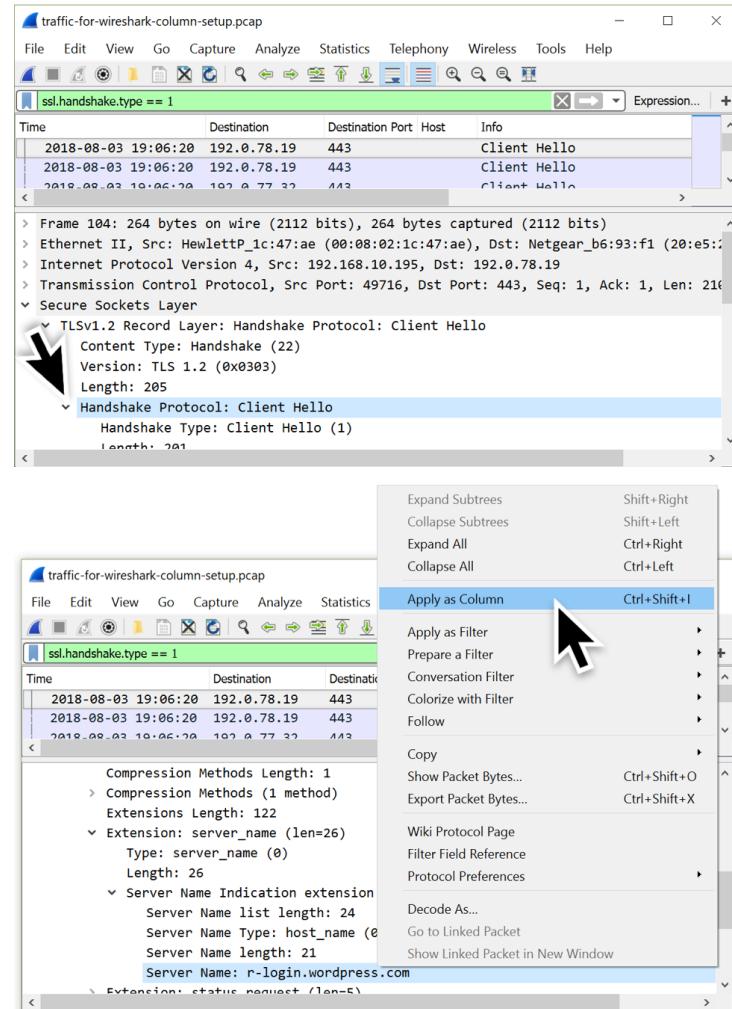
- 一句话描述：最流行的网络协议分析工具，主要用于网络数据包分析

- 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





- o 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: 2021-06-03 20:30:13

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

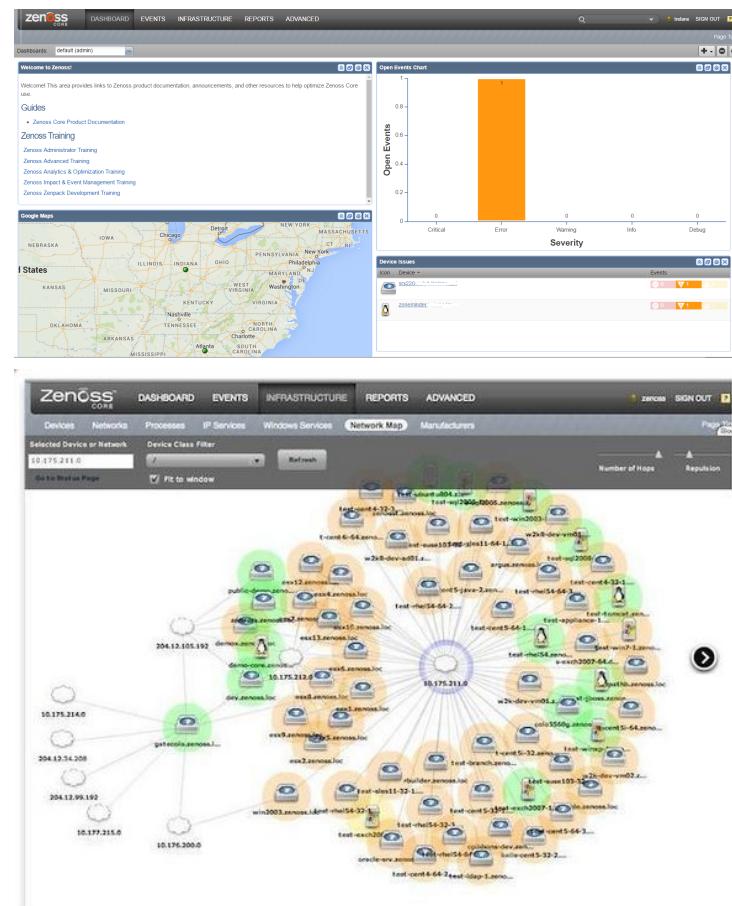


crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-06-03 20:29:20

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：2021-06-03 20:31:18

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

Three screenshots of NetworkMiner tools showing network analysis results:

- NetworkMiner 2.0**: Shows a list of captured files. The table includes columns for D. port, Protocol, Filename, Extension, Size, and Details. Examples include TCP 53130 TlsCertificate files (nr-data.net.cer, GeoTrust SSL CA - G2.cer, GeoTrust Global CA.cer) and various HTML and CSS files from www.meetup.com.
- NetworkMiner 2.0**: Shows a grid of file thumbnails. The thumbnails represent various images and files, such as profile pictures, logos (e.g., Meetup logo), and other small images.
- NetworkMiner 0.88**: Shows a hierarchical tree view of host details. The tree includes nodes for IP Address, MAC Address, Hostname, OS, and various network statistics like TTL, Open TCP Ports, and DNS queries. A specific host entry for 192.168.151.130 (goldfinger) is expanded, showing details like Satori DHCP, Linux 2.6 (100.00 %), and various DNS queries.

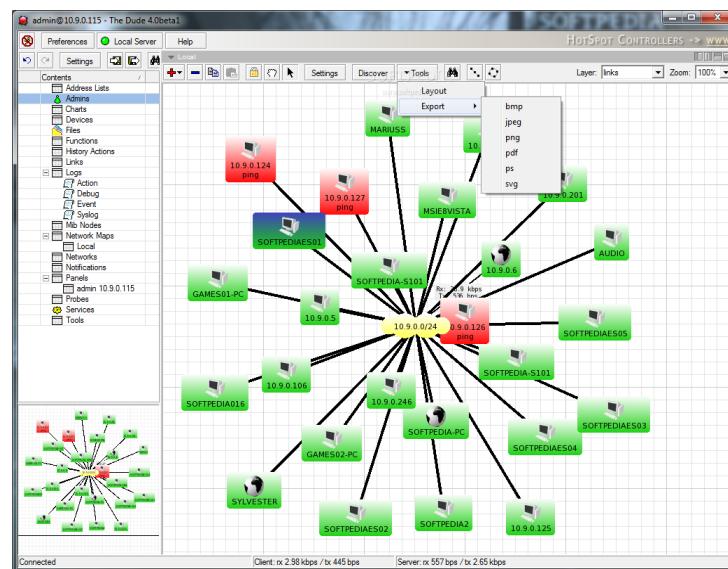
crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新：2021-06-03 20:23:04

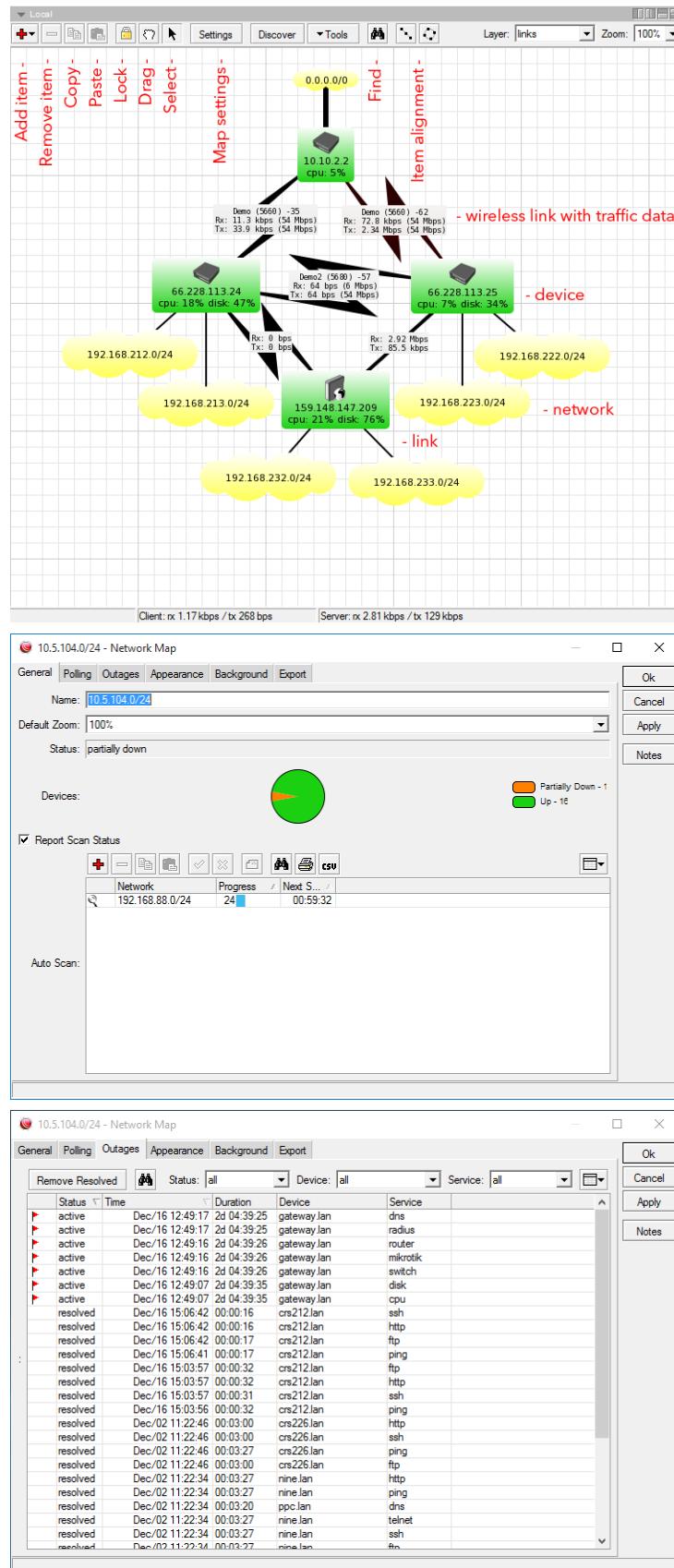
The Dude

- 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

Dos

IP Range - Angry IP Scanner					
IP Range: 66.249.93.32 to 66.249.93.200		IP Range		File Go to Commands Favorites Tools Help	
Hostname: ug-in-f99.google.com		IP	Netmask	Start	
IP	Ping	Hostname	Ports [2+]	Web detect	
66.249.93.82	123 ms	ug-in-f82.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		File Go to Commands Favorites Tools Help	
Hostname: e-estonia.com		IP	Netmask	Start	
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		File Go to Commands Favorites Tools Help	
Hostname: nbbee038141.local		IP	Netmask	Start	
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

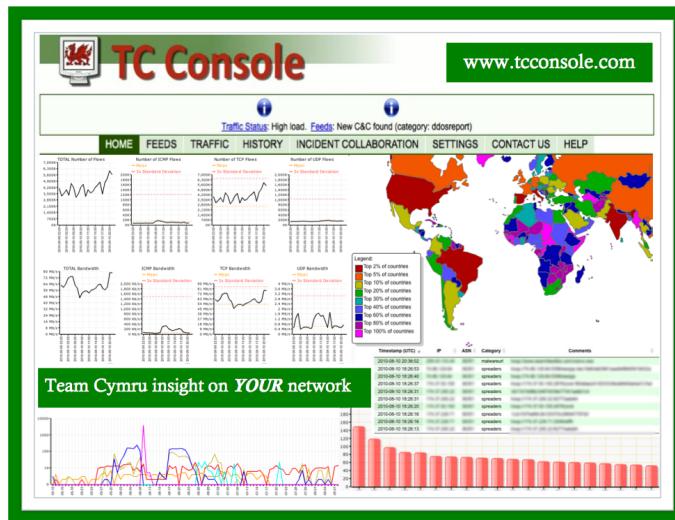
DoS

IP Range - Angry IP Scanner					
IP Range:		66.249.93.0	to	66.249.93.255	IP Range
Hostname:		g-in-f147.google.com		IP	Netmask
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	gsmtpt93-2.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]	

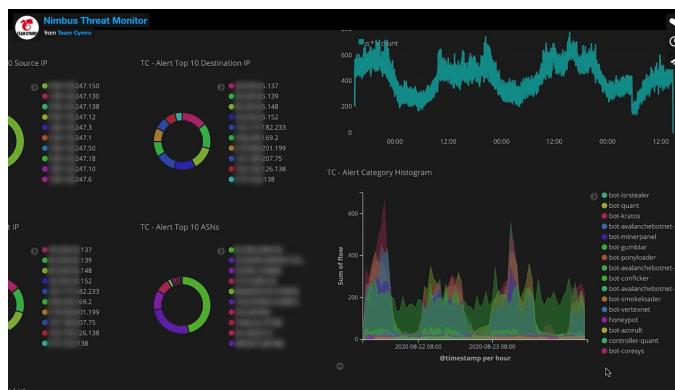
crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-06-03 20:26:53

Nimbus Threat Monitor

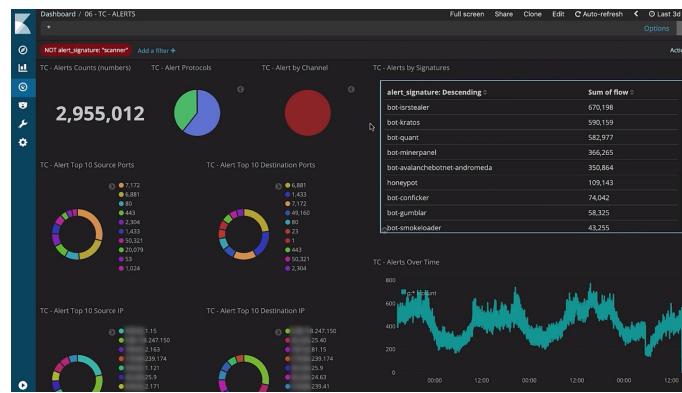
- Nimbus Threat Monitor
 - 旧称: TC Console
 - 主页
 - [Nimbus Threat Monitor - Team Cymru](#)
 - 概述
 - 此工具极大推进了网络可视化。由非盈利性安全研究公司 Team Cymru 提供，TC Concole 提供网络恶意行为的历史视图，以及网络通信数据，交叉比对该组织收集的全球关于恶意行为的统计数据。该工具免费，但只有愿意与 Team Cymru 数据库分享网络信息的组织才能获得
 - 图
 - 旧: TC Console



- 新: Nimbus Threat Monitor



DoS



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: 2021-06-03 20:31:50

代码审计类

- 工具

- CxEnterprise
 - = Checkmarx CxEnterprise
- Armorize CodeSecure
- Fortify
 - = Fortify SCA
- RIPS

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: 2021-06-03 20:24:41

Checkmarx CxEnterprise

- Checkmarx CxEnterprise

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: 2021-06-03 20:31:02

Armorize CodeSecue

- Armorize CodeSecue

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: 2021-06-03 20:30:25

Fortify

- Fortify

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: 2021-06-03 20:32:30

RIPS

- RIPS

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: 2021-06-03 20:22:55

证书

搞安全，会涉及到一些证书，尤其是和安全、网络等相关的证书。

关于证书的基础知识：

- 证书类型
 - 三类
 - 厂商认证
 - 依托厂商在行业的影响力、产品垄断等优势而推出的认证，由厂商对认证进行背书
 - 举例
 - 厂商 惠科 的各种认证，比如 CCIE 、 CCNA 和 CCNP
 - 行业认证
 - 同样依托行业影响力或相关标准的制定等提供认证的背书
 - 举例
 - 行业协会 国际信息系统安全认证协会 = ISC 的认证 CISSP
 - 政府(机构)认证
 - 有政府背景的机构来提供认证
 - 举例
 - 中国政府（的机构 中国信息安全测评中心）的认证 CISP

此处主要涉及到的证书：

- 2大类
 - 网络证书 和 安全证书
 - 概述
 - 目前行业内受认可的信息安全认证主要有 CISP 和 CISSP
 - 国内外的网络安全人员认证
 - 比较综合性的国外认证品牌
 - 有： CISSP 、 GIAC 、 Security+ 、 CISA / CISM 等
 - 这些国外的认证品牌的专业水平很高，在全球都有很大的影响力，但因为各种原因（诸如费用较高、英文培训和考试、无国内培训班或考点等），在国内的发展有限
 - 国内比较主流的认证品牌有： CISP 、 CCSRP 、 CISAW 等
 - 随着我国国内网络安全从业人员社会化技能认证的日益推进，国内的认证品牌将会进一步发展壮大
 - 作用
 - 找（安全相关）工作 = 求职的敲门砖 = 招聘时标注有XX认证的优先考虑
 - 升职加薪 = 镀金以提高身价
 - 项目投标（时候报人员）
 - 其他相关
 - 其他相关领域的一些证书，比如数据管理等

安全证书

国内

CISP

- CISP = Certified Information Security Professional = 注册信息安全专业人员
- 一句话描述：CISP，经中国信息安全测评中心实施国家认证，是信息安全领域唯一采用国家注册制度的认证证书，是国家对信息安全人员资质的最高认可
- 始于：2004年
- 证书类型：政府(机构)认证
- 发证机构：中国信息安全测评中心
 - CISP 系经 中国信息安全测评中心 实施国家认证
- 证书长什么样



- 考证要求：需要工作经验
- 考取难度：★★★☆☆
- 适应类型：国有企业、政府、军工、8+2行业信息安全主管及为国内提供信息安全服务的安全公司从业人员
 - 面向对象：面向信息安全企业、信息安全咨询服务机构、信息安全测评机构、政府机构、社会各组织、团体、大专院校以及企事业单位中负责信息系统建设、运行维护和管理工作的信息安全专业人员所颁发的专业注册证书

◦ 费用：

- 总价：12800元/人
 - 培训费：8800元/人
 - 课程安排

CISP 课程安排	
第一天	信息安全保障
	网络安全监管
第二天	信息安全管理
	业务连续性
第三天	安全工程与运营
	信息安全评估
第四天	信息安全支撑技术
	物理与网络通信安全
第五天	计算环境安全
	软件安全开发

- 培训机构：指定授权人员注册维持机构
 - 根据中国信息安全测评中心《关于调整CISP人员注册维持费用的通知国信安[2017]26号》文件要求自2017年7月1号开始CISP/CISM持证人员将由指定授权人员注册维持机构对学员证书维持、年金收取、证书换证、证书续证、后续教育学分统一管理
- 考试费：4000元/人
 - 包括两次补考费用
 - 也就是说有三次考试机会，再考就每次500考试费
- 证书维持费用=证书年金=年金
 - 考试成功后第一个3年免年金，从第4年开始缴纳年金
 - CISP 证书有效期为3年，证书维持费用三年一缴
 - CISP 人员注册维持费用标准为500元/人/年
 - 另，证书维持手续费200元/次

◦ 认证要求

- 注册要求
 - 教育与工作经历
 - 硕士及以上：具有1年工作经历
 - 本科毕业：具有2年工作经历
 - 大专毕业：具有4年工作经历
 - 专业工作经历
 - 至少具备1年从事信息安全有关的工作经历
- 培训资格
 - 在申请注册前，成功地完成了CNITSEC或其授权培训机构组织的注册信息安全专业人员培训课程相应资质所需的分类课程，并

取得培训合格证书

- 通过由CNITSEC举行的注册信息安全专业人员考试
- 能力要求
 - 具备一定的信息安全基础知识，了解并掌握 GB/T 18336、ISO 15408、ISO 17799 等有关信息安全标准，具有进行信息安全服务的能力

○ 认证说明

- 概述

- CISP是认证类型总称



- 实际上分为四项认证证书

- CISE = Certified Information Security Engineer = 注册信息安全工程师
 - 工程师
- CISO = Certified Information Security Officer = 注册信息安全管理人員
 - 管理员
- CISPA = 注册信息安全审核员 = 注册信息安全审计师
 - 审计师
- CISD = CISDRP = 注册信息安全灾难恢复工程师
 - 开发人员

- 面向对象不同，适用面也不同

■ 详解

- CISE / CISO

- 概述：侧重安全技术和安全管理，教材一样，课程一样，同班上课，只是考卷不同而已
- 详解

- CISE

- 如果一直干技术工作的，建议选CISE
- 主要从事信息安全技术领域的工作，具有从事信息系统安全集成、安全技术测试、安全加固和安全运维的基本知识和能力

- CISO

- 一直干管理或咨询的，建议选CISO
- 主要从事信息安全管理领域的工作，具有组织信息安全风险评估、信息安全总体规划编制、信息安全策略制度制定和监督落实的基本知识和能力

- CISPA = CISPAudit

- 侧重安全审计方面的知识
- 主要从事信息安全审计工作，在全面掌握信息安全基本知识技能的基础上，具有较强的信息安全风险评估、安

全检查实践能力

- CISD
 - 面向软件开发人员，侧重软件安全开发
 - 申请中国信息安全测评中心软件安全开发企业认证绑定的是个证书，所以要申请开发类企业认证的，注意要考的是CISD
 - 主要从事信息系统灾难恢复工作，在全面掌握信息安全基本知识技能的基础上，具有较强的信息系统灾难恢复建设和管理的实践能力
- 最新情况
 - 近几年该认证体系不断丰富，引入了更多认证：
 - CISP-CSE：对应云安全
 - CISP-BDSA：大数据安全
 - CISP-ICSSE：工控安全
 - CISP-PTE/PTS：渗透测试
 - CISP-IRE：应急响应
 - CISP-DSG：数据治理
 - CISP-PIP：个人信息保护
 - CISP-F：调查取证
 - 在信息安全项目招投标、控标，和信息安全相关行业资质申请中均有明确的持证要求，要求必须达到一定数量持证人员及资质，方可竞标
 - 深受国家政府党政机关、金融、通信、电力、国防、军工、交通、烟草、税务、等行业的广泛认可
- 注意
 - CISP为强制培训，也就是说不能直接考试，必须报一个授权培训机构（培训也采取授权制，必须有授权才能培训和考试）接受8天的培训后才能参加考试（2018年起调整为五天）
 - 未来会逐步结合在线学习等，降低培训时间要求
 - 报考时要选择考试类型，根据自己能力和擅长方向选择。不要因为听谁说哪个好考就考哪个

CISM = 注册信息专员

- CISM = Certified Information Security Member = 注册信息专员
 - 概述
 - 中国信息安全测评中心开展的信息安全 基本技能 的认证培训
 - CISM 面向政府机构、社会团体、企事业单位中从事信息安全相关工作的人员
 - CISM 证书由中国信息安全测评中心颁发，持证人员掌握保障信息系统安全的基本知识和技能，具备从事信息安全相关工作的基本能力
 - 证书
 - CISM 证书有效期为3年，证书维持费用三年一缴
 - CISM 人员注册维持费用标准为200元/人/年

CISAW = 信息安全保障人员认证

- CISAW = 信息安全保障人员认证
 - 始于：2011年

- 发证机构：中国网络安全审查技术与认证中心
 - 原中国信息安全认证中心
 - 是国家市场监督管理总局直属事业单位，同时在业务上接受中央网信办的指导
- 三大等级
 - 预备认证
 - 资格认证
 - 基础级
 - 专业认证
 - 专业级
 - 专业高级
- 专业认证子类
 - 安全集成
 - 风险管理
 - 应急服务
 - 安全软件
 - 安全运维
 - 电子政务
 - 电子数据取证
 - 网络攻防
 - 网络情报分析
 - WEB安全
 - 工控网络安全
 - 网络舆情分析与处置

CCSRP = 网络与信息安全应急人员认证

- CCSR = 网络与信息安全应急人员认证
 - 始于：2017年
 - 发证机构：国家计算机网络应急技术处理协调中心
 - 简称：国家互联网应急中心
 - 是中共中央网络安全和信息化委员会办公室（以下简称中央网信办）的直属事业单位
 - 两大类认证
 - 通用信息人员认证
 - 方向
 - 管理
 - 技术
 - 每个方向设置不同的等级
 - 面向行业的人员认证
 - 不同行业
 - 通信
 - 电力
 - 石油炼化
 - 轨道交通
 - 能够兼顾不同行业的安全技能要求的差异性

国外

CISSP = 信息系统安全专业认证

- CISSP = 信息系统安全专业认证
 - 证书类型：行业认证
 - 发证机构：ISC
 - ISC = 国际信息系统安全认证协会 = International Information Systems Security Certification Consortium
 - 考证要求：需要工作经验
 - 考取难度：★★★★☆
 - 比CISP难度多一星
 - 因为英语和6小时的考试时间，比较摧残人
 - 适应类型：外企、涉外服务、大型企业（包括国有企业，有不少国企也比认CISSP）如银行等信息安全主管和信息安全从业者
 - 费用：
 - 培训：不强制 -> 无需培训也可直接考试
 - 国内很多培训公司都提供
 - 考试：考试费 599美元
 - 这是一次考试的费用，如果没通过，下次还要交考试费
 - 证书



- 作用：代表国际信息系统安全从业人员的权威认证
- 认证对象
 - 面向从事商业环境安全体系建构、设计、管理或控制的专业人员
 - 对从业人员的技术及知识积累进行测试
- ISC 共有9项认证
 - CISSP = 注册信息系统安全师
 - 8个延伸出来的系列认证
 - CSSLP = 注册软件生命周期安全师
 - CCFPSM = 注册网络取证师
 - CAP = 注册信息安全许可师
 - SSCP = 注册系统安全员
 - HCISPPSM = 医疗信息与隐私安全员
 - CISSP专项加强认证
 - CISSP-ISSAP = Information Systems Security Architecture Professional = 信息系统安全架构专家
 - CISSP-ISSEP = Information Systems Security Engineering Professional = 信息系统安全工程专家
 - CISSP-ISSMP = Information System Security Management Professional = 信息系统安全管理专家
- 考试内容=领域：8个
 - 安全和风险管理

- 资产安全
- 安全架构和安全模型
- 通信和网络安全
- 身份和访问管理
- 安全评估和测试
- 安全操作
- 软件开发安全
- 要求
 - 在两个或两个以上CISSP领域有五年相关工作经验
- 现状
 - 根据Global Knowledge的数据
 - 到2020年，持证人员的平均工资为141452美元
 - CISSP证书持有者
 - 平均年龄为48.1岁
 - 从事安全工程师或分析师工作
 - 普遍拥有6.1项证书
- 评价
 - CISSP因为推出比较早，所以相对比较知名
 - 目前认证中也就CISSP因为资格老，比较多人知道，所以考的较多，其他的嘛，屈指可数
 - CISSP考试相对难些
 - CISSP考试难点在于两个地方，一是英文考试，二是考试时间。
 - 考题
 - 考卷250道题，其中50道是不计分的（哪50道题都不知道）
 - 考试时间
 - 6小时，也就是360分钟
 - 平均不到一分半要答一道题
 - 中间还需要上厕所，吃东西，所以每道题时间就一分钟多
 - 英文
 - 对英语的要求不是一点点的高
 - 后来改成中英文都有
 - 愿意看中文的看中文，不愿意看中文的看英文
 - 不过根据之前参加考试的反馈，中文题翻译的质量实在不咋的，很多人题都读不懂，还不如用英文
 - 并且六个小时的考试，大脑高度紧张，压力是真不小的

安全证书对比

CISP vs CISM

- CISP VS CISM
 - 要点
 - CISP = Certified Information Security **Professional**
 - Professional =专业人员
 - CISM = Certified Information Security **Member**
 - Member =会员=普通人员

- 专业程度
 - CISP 培训面向信息安全专业人员，课程内容和深度均比 CISM 广而且深
- 历史
 - CISP 从2002年首次举办培训至今，已经有10年历史了
 - CISM 从2005年推出，至今也有7年历史。

CISP vs CISSP

- CISP vs CISSP
 - 相同点
 - CISP 和 CISSP：都是偏重信息安全管理的 = 信息安全类认证
 - 技术知识讲的宽泛且浅显，考试都是一带而过 = 特点：一英里宽一英寸深
 - 这两个认证证明持证人员对信息安全知识了解比较全面
 - 两者没本质区别
 - CISSP从2011年就开始谋求在中国与CISP互认，互认的备忘录都签了
 - 当时双方还做了知识体系的对比，知识体系没太多差别，基本都是一致的
 - 主要差别在法律法规上。所以双方没有本质区别
 - 不同点
 - CISSP
 - 要求持证人员的信息安全工作经验都要5年以上
 - 特点
 - 由于 CISSP 推出时间较早，目前已经国际化运作，因此被称为国际认证
 - CISP
 - 要求大专学历4年以上工作经验
 - 特点
 - CISP 是中国信息安全测评中心推出，有政府背景给认证做背书

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：2021-06-03 20:24:18

网络证书

CCIE = 思科认证互联网专家

- CCIE = 思科认证互联网专家
 - 概述：美国Cisco公司于1993年开始推出的专家级认证考试，被全球公认为IT业最权威的认证
 - 作用：证书持有者被认为是具有专业网络技术知识和丰富工作经验的最好证明
 - 证书



- 认证领域：6个
 - 路由和交换认证
 - 服务提供商认证
 - 安全认证
 - 协作认证
 - 数据中心认证
 - 无线认证

CCNA = 思科认证网络工程师

- CCNA = 思科认证网络工程师
 - 概述
 - 最初关注的是路由和交换，但近年来又围绕安全、云计算、协作、安全操作、设计、数据中心技术、工厂、服务提供商和无线等领域又增加了新的证书
 - 证书长什么样



- 有效期
 - CCNA证书的有效期为3年
 - 3年之后需要参加再认证（Recertification）的考试
 - 如果你在这3年时间内考取了更高级别的思科认证，则CCNA认证的有效期自动更新
- 现状
 - 根据Global Knowledge数据，2019年北美思科证书持有者的平均工资为101533美元
 - 数据显示，2019年16%的IT从业人员持有思科认证，其中CCNA路由和交换最为常见。
 - 在通过CCNA认证的员工中，71%持有CCNA路由和交换证书，18%的员工持有CCNA安全证书

CCNP = 思科认证网络专家

- CCNP = 思科认证网络专家
 - 概述
 - 获得CCNP认证的专业人员可以为具有100到500多个节点的大型企业网络安装、配置和运行LAN、WAN和拨号访问业务。从2015年1月29日起，CCNP考试科目启用新的CCNP考试政策
 - 证书长什么样



- 现状

- CCNP路由和交换是思科认证中第二大最常见的认证，通过认证的员工中有33%都持有该证书
- Global Knowledge发现，到2020年，CCNP路由和交换证书持有者的平均工资将达到119178美元，他们最有可能成为网络工程师或分析师
- 思科于2020年2月23日发布了新的认证框架，其中CCNP Enterprise取代了CCNP路由和交换。所有新的CCNP认证都要求考生通过两项考试：一项核心考试和一项技术领域的集中考试

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：2021-06-03 20:29:22

其他证书

CISA = 国际信息系统审计师

- CISA = Certified Information Systems Auditor = 注册信息系统审计师
 - 别称
 - 国际信息系统审计师
 - 原因：是国际的、全球的认证
 - 概述
 - 由 ISACA = Information Systems Audit and Control Association =(国际) 信息系统审计与控制协会 发起
 - 始于1978年
 - 已经成为涵盖信息系统审计、控制与安全等专业领域的全球公认的标准
 - 证书长什么样



-
- CISA考试领域
 - 信息系统的审计流程（占21%）
 - IT治理和管理（占17%）
 - 信息系统的购置、开发和实施（占12%）；
 - 信息系统的运营和业务恢复能力（占23%）
 - 信息资产的保护（占27%）
- CISA适合哪些人学习？
 - 信息系统审计的从业人员、IT审计师
 - 信息安全经理、IT风险管理、IT内控管理的从业者
 - CIO、IT经理、信息系统的管理人员
 - 财务、经营审计专业人员
 - 企业内部负责信息系统规划、项目管理、研发、运维等工作的从业人员
 - 信息安全咨询顾问、IT管控咨询顾问、IT专业服务提供从业人员
 - CISA应试者
- 现状
 - CISA名列薪资最高的证书之列。一直以来，CISA以其市场价值持续高居这个排行榜前列
 - CISA被全球范围的企业和专业人士视为IT/IS认证的“黄金标准”

- 中国获得CISA认证的审计师分布在银行、证券、政府、高端制造业、信息服务业等高端行业内，越来越受到国内各大企事业单位认可
- 据Global Knowledge预计，到2020年，CISA证书持有者的平均收入将达到132278美元
- Global Knowledge发现，证书持有者的平均年龄为46.9岁，从事IT审计工作，通常持有3.3个证书

CDP = Certified Data Professional = 数据专业认证

- CDP = Certified Data Professional = 数据专业认证
 - 2015年诞生的一项认证
 - 取代了2004年至2015年由计算机专业技术认证机构（ICCP）提供的数据管理专业认证（CDMP）
 - 证书长什么样



- CDP的专业证书领域
 - 业务分析
 - 数据管理
 - 数据仓库
 - 信息系统管理
- 其他说明
 - 想要获得CDP证书需要参加为期四天的数据管理现场研讨会，并通过书面考试。证书持有者必须通过90分钟的IS（信息系统）核心考试、90分钟的业务核心和数据管理考试以及其他专业化考试
 - 超过一半的CDP证书持有者拥有至少10年的行业经验，四分之一的人有6至10年的行业经验，只有不到22%的人工作经验在6年以下

CompTIA A +

- CompTIA A +
 - 概述
 - CompTIA A +认证代表着计算机技术人员的入门级能力，是一个厂商中立的国际认证，涵盖各种技术和操作系统。美国计算机行业协会

(CompTIA- Computing Technology Industry Association)是在全球ICT领域最具影响力的、最大的、全球领先的行业协会，自1982年成立之日起，一直致力于通过各种标准、专业能力、教育和商业解决方案促进信息技术(ICT)产业及相关从业人员的发展

- 证书长什么样



-
- 考试
 - 持证人员必须通过两项90分钟的考试
 - 一项涵盖移动设备、网络技术、硬件、虚拟化和云计算和网络故障排除
 - 另一项涵盖安装和配置操作系统、安全、软件故障排除和操作步骤
- 现状
 - 数据显示，2019年北美CompTIA证书持有者的平均工资为93097美元，其中最受欢迎的CompTIA认证是Security +, A +和Network +

微软

MCSA = 微软认证解决方案专员

- MCSA = 微软认证解决方案专员
 - 概述
 - 为入门级工作者设计，证明他们对微软产品、角色和知识领域的熟练程度
 - MCSA认证是许多微软认证解决方案专家（MCSE）认证的基础，这些认证针对的是经验更丰富的IT工作者
 - 证书长什么样



- - 解释
 - 微软的认证侧重于用户设计和构建技术解决方案的能力。MCSA认证围绕特定角色和专有产品，例如Microsoft Azure、SQL Server、Office 365、SharePoint Server、Skype for Business、Microsoft Dynamics 365、Exchange Server和Windows Server
 - 现状
 - 2019年IT技能和薪酬调查显示，16%的人持有微软认证，其中19%的微软持证者持有MCSA：Windows Server 2008证书，17%持有MCSA：Windows Server 2012证书

MTA = 微软技术专员认证

- MTA = 微软技术专员认证
 - 概述
 - 一项入门级认证，可验证Microsoft SQL Server, Visual Studio, Windows和Windows Server 2016的基础技术知识
 - 考试
 - 考试的核心能力范围涵盖80%信息专业知识与20%的技能
 - 证书长什么样



- - 解释
 - MTA认证涉及很多基本技术概念、评估和验证核心技术知识。对于希望进入技术领域的人来说，这是一个很好的起点
 - 现状

- 调查显示，2019年北美微软证书持有者的平均工资为104127美元。
MTA考试不具备获得微软认证专家（MCP）的资格，也不是获得
MCSA或MCSD认证的先决条件

Oracle

Oracle数据库认证

- Oracle数据库认证
 - 概述
 - Oracle认证代表了你对数据库和Java知识和技能的掌握。Oracle数据库设计和SQL编程教授IT从业人员分析复杂的业务场景，设计和创建数据模型，以及使用SQL创建数据库
 - 证书长什么样



- 现状
 - Oracle在数据库设计以及SQL和PL/SQL编程方面侧重于数据的组织、管理和使用。数据显示，2019年北美Oracle数据库认证证书持有者的平均工资为116961美元

PMP = 项目管理专业人士资格认证

- PMP = 项目管理专业人士资格认证
 - 概述
 - 项目管理专业人士资格认证（PMP）是由美国项目管理协会（Project Management Institute(简称PMI)）发起的，严格评估项目管理人员知识技能是否具有高品质的资格认证考试。在决定谁委托重要的组织项目计划时，证书通常是关键的区分因素
 - 证书长什么样



- - 条件
 - 想要获得认证的个人必须接受35个小时的PMP相关培训。
 - 此外，没有学士学位的人必须具有7500个小时的项目管理经验，拥有学士学位或更高学位的人则需要4500个小时的项目管理经验
 - 现状
 - 数据显示，2020年PMP证书持有者的平均工资为143493美元
 - PMP认证持有者的平均年龄为48.7岁，通常是项目经理，总共持有4.5项证书

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：2021-06-03 20:27:16

安全标准

- 搞安全方面，要了解
 - 安全标准 ~= 信息安全管理体系 ~= 国内外相关安全标准和法律法规
- 目的
 - 熟悉相关的标准和条款
 - 制定合规基线，合规检查方案
 - 找出不合规的地方=问题
 - 提供修正建议=解决方案

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：2021-06-03 20:28:33

等保

- 等保 = 等级保护 = 信息系统安全等级保护

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: 2021-06-03 20:30:54

ISO27001

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: 2021-06-03 20:27:34

安全组织

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: 2021-06-03 20:27:04

OWASP

- 在Web安全领域，有个组织叫：
 - OWASP
 - = Open Web Application Security Project
 - = 开源Web应用安全项目
 - = 开源Web应用安全组织
- 中文主页
 - Welcome to OWASP CHINA — OWASP-CHINA
 - <http://www.owasp.org.cn>

OWASP 10

- OWASP 组织每年会推出一个 标准： OWASP 10
 - OWASP列出了最重要的10个方面的安全攻击
 - 说明
 - 列出排名前10的攻击类型
 - 每年都会出一个报告
 - 最早：2003年
 - 最新：2017年
 - 2017年的OWASP 10
 - Injection=注入攻击
 - 涉及方面
 - SQL
 - SQL Injection = SQL注入
 - NoSQL
 - OS
 - LDAP
 - LDAP Injection
 - 坏结果
 - 运行了不该运行的（恶意的）代码
 - Expression Language (EL) Injection
 - Command Injection
 - 获取了不该获取的数据=盗取数据
 - 心得
 - 编写接受数据的模块时要非常小心
 - 举例
 - `request.getParameter()`
 - `request.getCookie()`
 - `request.getHeader()`
 - Broken Authentication
 - =失效的身份
 - Sensitive Data Exposure
 - XXE
 - XML External Entities
 - Broken Access Control

- =访问控制缺失
- Security Misconfiguration
 - =安全配置错误
- XSS
 - =Cross-Site Scripting
- Insecure Deserialization
- Using Components with Known Vulnerabilities
 - =使用含有已知漏洞的组件
- Insufficient Logging & Monitoring

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: 2021-06-03 20:25:03

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: 2021-06-03 20:27:18

参考资料

- [CISA | 什么是CISA\(信息系统审计师认证\)? - 知乎](#)
- [History of ISACA | Global Business & Technology Community | ISACA](#)
- [一文读懂CISA认证 | 薪资最高证书之一 - 知乎](#)
- [CISA | 什么是CISA\(信息系统审计师认证\)? - 知乎](#)
- [CISP与CISM有什么区别, CISP和CISM证书权威性如何? - 知乎](#)
- [CISP/CISM证书维持办法 - 【官网】国家信息安全水平考试NISP——NISP全国运营中心](#)
- [DDOS 攻击的防范教程 - 阮一峰的网络日志](#)
- [Web application firewall - Wikipedia](#)
- [拒绝服务攻击 - 维基百科, 自由的百科全书](#)
- [Denial-of-service attack - Wikipedia](#)
- [Cyberattack - Wikipedia](#)
- [网络攻击 - 维基百科, 自由的百科全书](#)
- [cdn 真实ip_百度搜索](#)
- [游戏盾_分布式DDoS防护系统 - 阿里云](#)
- [什么是游戏盾 - 产品简介| 阿里云](#)
- [核心原理产品简介游戏盾-阿里云](#)
- [产品架构产品简介游戏盾-阿里云](#)
- [云防御高防CDN高防服务器游戏盾极御云安全](#)
- [零基础如何学习 Web 安全? - 知乎 \(zhihu.com\)](#)
- [什么是 Web 应用防火墙 \(WAF\)? | 术语 | F5](#)
-

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: 2021-06-03 20:24:10