目录

防止被黑客攻击：Web安全

- 最新版本：`v1.0`
- 更新时间：`20210608`

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 CodeSecue、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，比如网络安全法和等级保护、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

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

常见问题

Web安全 vs 网络安全

- Web安全 vs 网络安全?
  - 狭义上：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

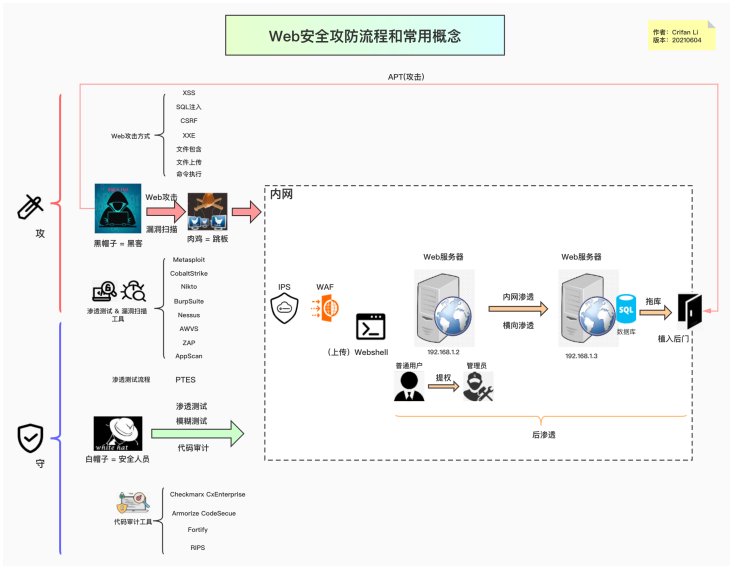
Web安全 vs 渗透测试

- 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）

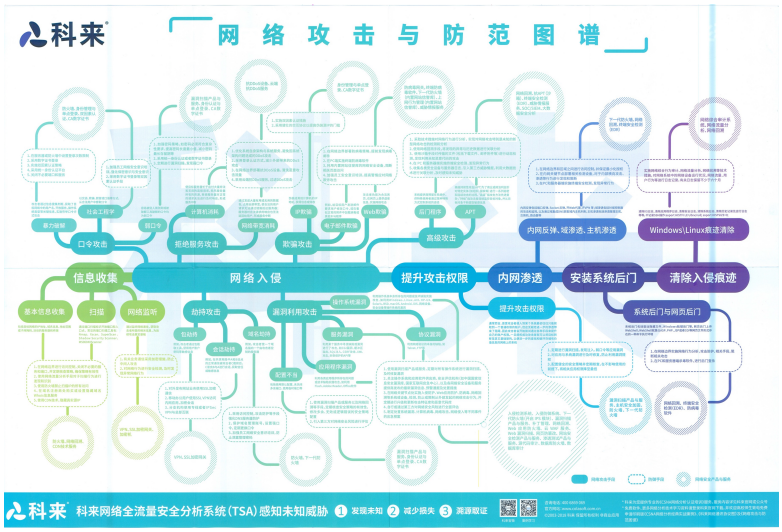
Web攻防和常见术语

搞Web安全，会遇到很多名词、术语和概念。

现已总结成一张图概览：

- Web安全攻防流程和常用概念
  - 在线浏览
    - Web安全攻防流程和常用概念 | ProcessOn免费在线作图
  - 图
    - 

以及别人整理的：

- 网络攻击与防御图谱
  - 

    - 有助于从大体上了解网络攻击的宏观流程和具体涉及内容

Web安全常见术语和概念

细节详见下面的解释：

肉鸡

被黑客入侵并被长期驻扎的计算机或服务器。可以随意控制，可以是任意系统的设备，对象可以是企业，个人，政府等等所有单位

抓鸡

利用使用量大的程序的漏洞，使用自动化方式获取肉鸡的行为

Webshell

通过Web入侵的一种脚本工具，可以据此对网站服务进行一定程度的控制

漏洞

硬件、软件、协议等等的可利用安全缺陷，可能被攻击者利用，对数据进行篡改，控制等

如何发现漏洞?

典型找到漏洞的方式有：

- 通过 `渗透测试` ，测出漏洞
- 用 `漏洞扫描器` 去扫描，找出漏洞

木马

通过向服务端提交一句简短的代码，配合本地客户端实现webshell功能的木马

提权 = 提升权限

操作系统低权限的账户将自己提升为管理员权限使用的方法

后门

黑客为了对主机进行长期的控制，在机器上种植的一段程序或留下的一个 `入口`

跳板

使用肉鸡IP来实施攻击其他目标，以便更好的隐藏自己的身份信息

旁站入侵 ~= 内网渗透

即同服务器下的网站入侵，入侵之后可以通过提权跨目录等手段拿到目标网站的权限。

常见的旁站查询工具有：`WebRobot` 、 `御剑` 、 `明小子` 和 `web在线查询` 等

C段入侵

即同C段下服务器入侵。

比如，目标ip为 `192.168.180.253` 入侵 `192.168.180.*` 的任意一台机器，然后利用一些黑客工具嗅探获取在网络上传输的各种信息。

常用的工具有：

- Windows
  - `Cain`
- Linux
  - `Sniffit`
  - `Snoop`
  - `Tcpdump`
  - `Dsniff`

测试

（安全领域中的）黑盒测试 = 不知道源码的攻击 ~= 渗透测试

在未授权的情况下，模拟黑客的攻击方法和思维方式，来评估计算机网络系统可能存在的安全风险。

黑盒测试不同于黑客入侵，并不等于黑站。黑盒测试考验的是综合的能力（ `OS` 、 `Database` 、 `Script` 、 `code` 、 `思路` 、 `社工` ）

思路与经验积累往往决定成败

（安全领域中的）白盒测试 = 知道源码的测试 ~= 代码审计

相对黑盒测试，白盒测试基本是从内部发起。白盒测试与黑盒测试恰恰相反，测试者可以通过正常渠道向被测单位取得各种资料，包括网络拓扑、员工资料甚至网站或其它程序的代码片断，也能够与单位的其它员工（销售、程序员、管理者……）进行面对面的沟通

APT攻击

`APT = Advanced Persistent Threat = 高级可持续性攻击` ，是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式

特点：

- 极强的隐蔽性

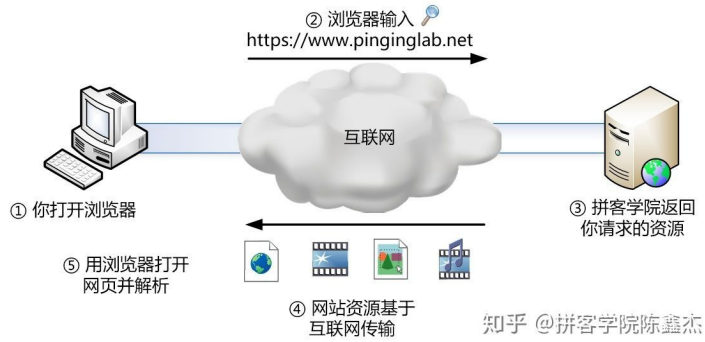
- 潜伏期长，持续性强
- 目标性强

Web攻击

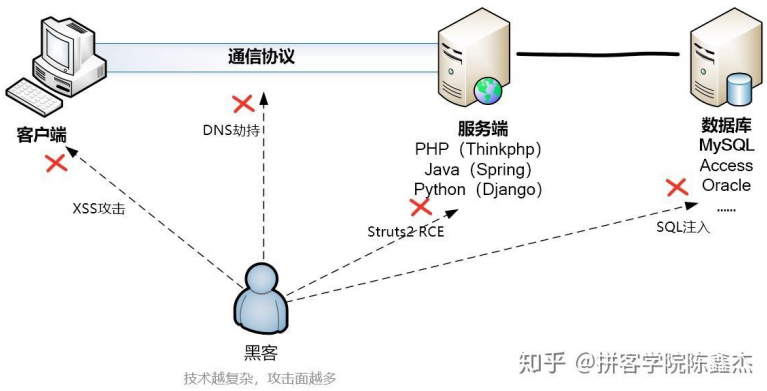
`Web攻击 ~= 网络攻击`

- 普通用户：上网 = 访问网络
  - 基本流程

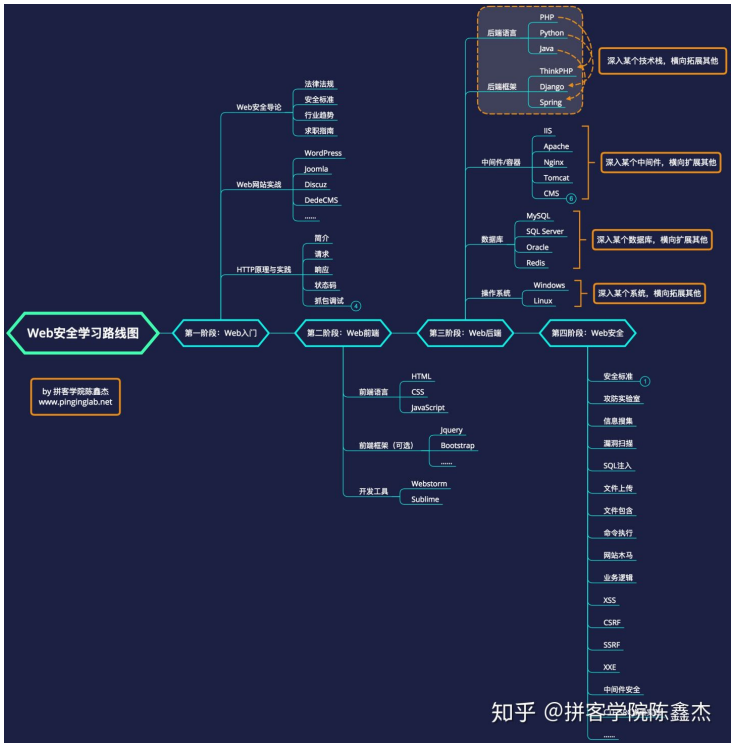
  - 详细过程



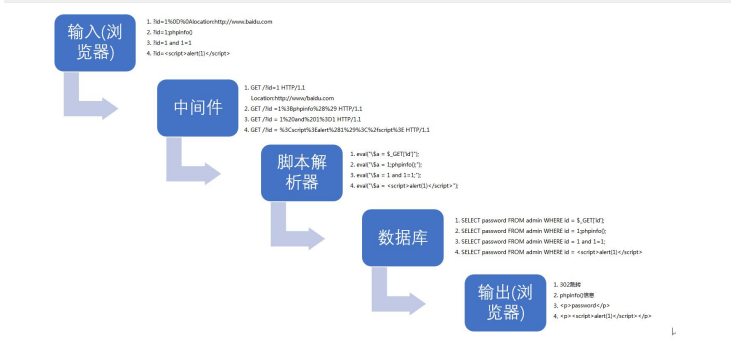
- Web攻击



  - 相关
- Web安全学习路线



- web漏洞攻击内部过程



攻击方式

网络攻击有多种方式。

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

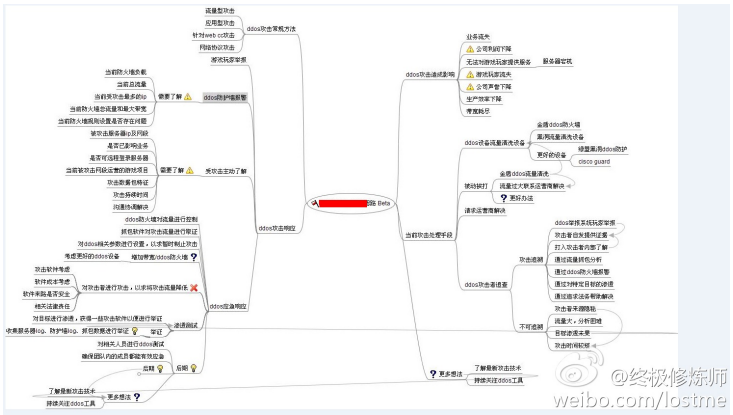
DDoS

- `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

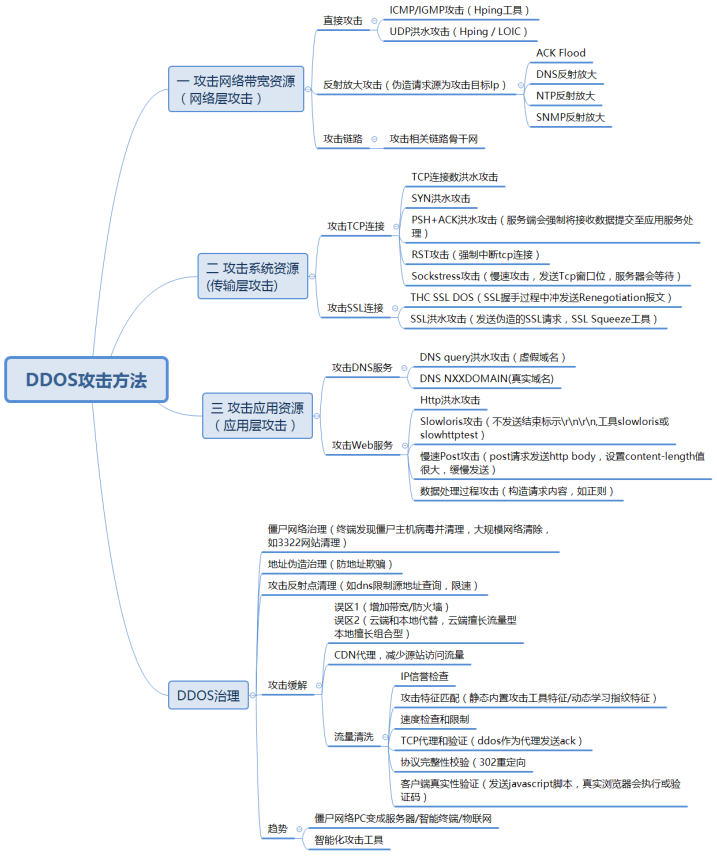
DDoS防护

DDoS攻击与防护总结

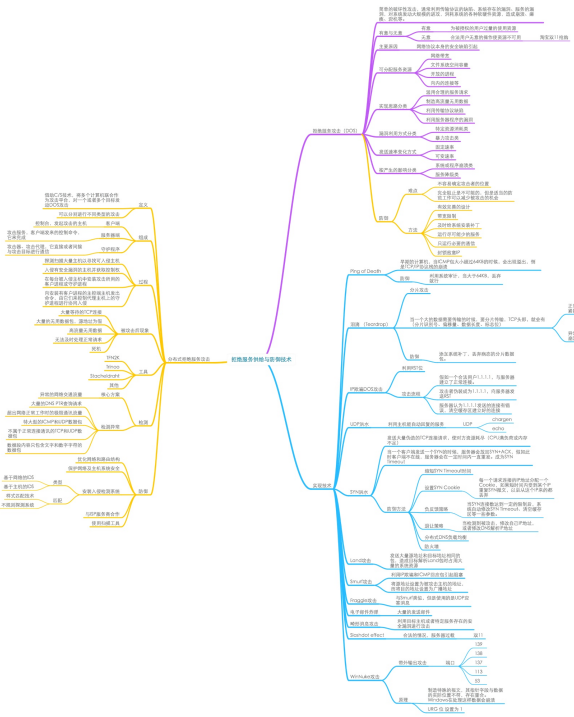
- DDoS攻击与防护总结
  - DDoS攻击及对策



  - DDoS攻击方法和治理



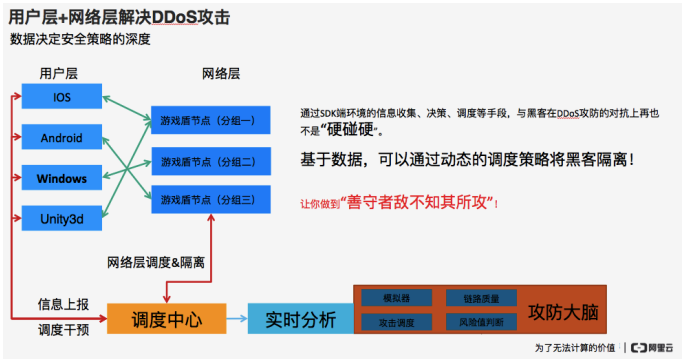
  - DDoS攻击与防御技术

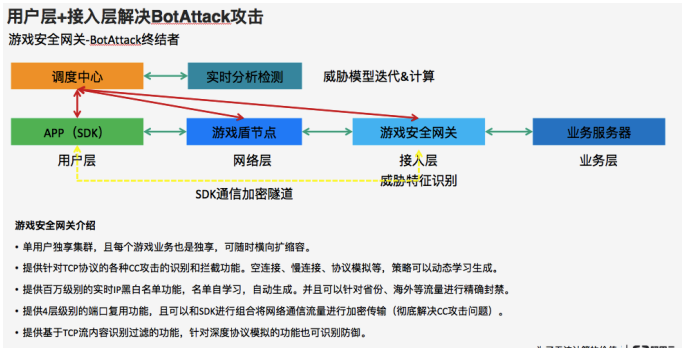


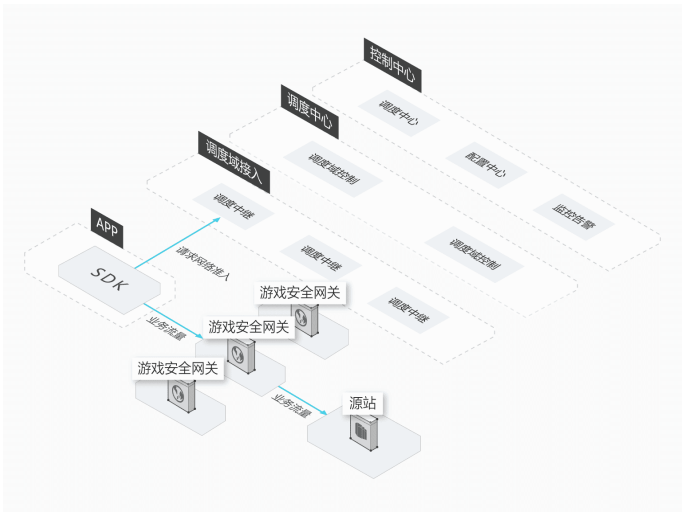
DDoS防护产品

阿里云 游戏盾

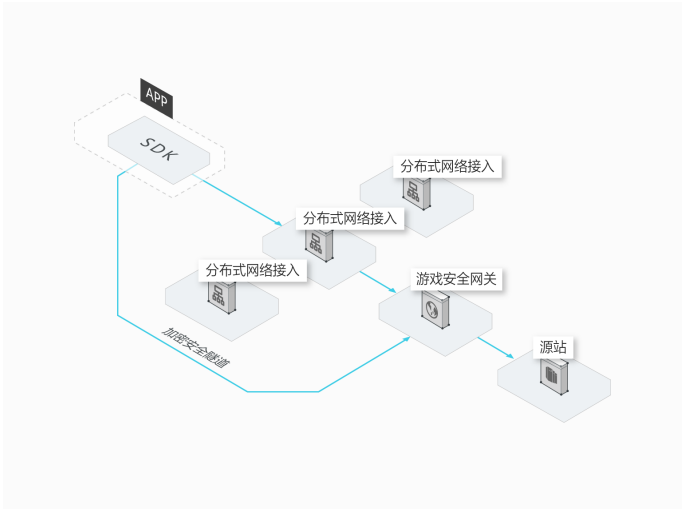
- 阿里云 游戏盾
  - 一句话描述：阿里云针对游戏行业面对的DDoS、CC攻击推出的针对性的网络安全解决方案
    - 谁开发的：阿里云
    - 针对什么：DDoS、CC攻击
    - 适用行业：游戏行业
    - 什么东西：网络安全解决方案
  - 目的：
    - 帮助游戏行业用户用更低的成本缓解超大流量攻击和CC攻击
      - 解决以往的攻防框架中资源不对等的问题
  - 对比
    - 高防IP
      - 防护成本更低，效果更好
        - 除了能针对大型DDoS攻击（T级别）进行有效防御外
        - 还具备彻底解决游戏行业特有的TCP协议的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
        - 

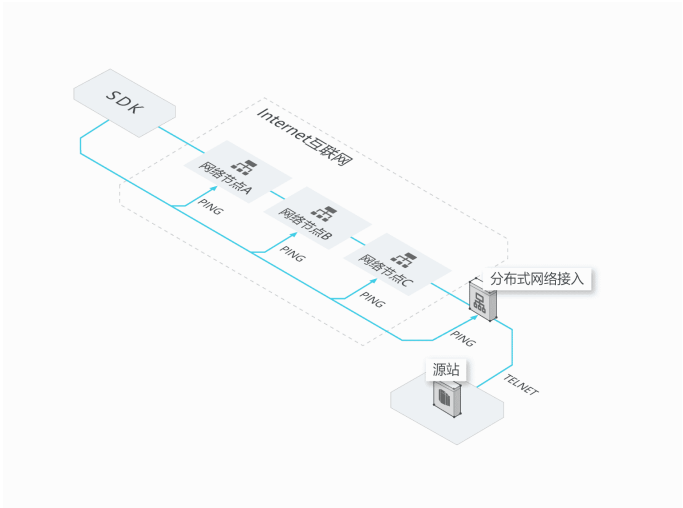
    - 游戏盾防御CC攻击的原理
        - 

- 客户应用举例
    - DDoS攻击防护
        - 

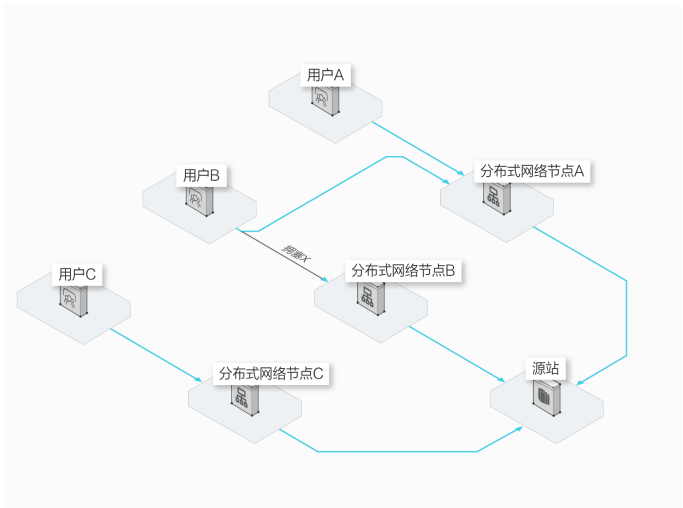
    - CC攻击防护



- 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

Web防护

渗透测试

详见独立教程：

潜入你的网络：渗透测试

模糊测试

TODO：

未知的未知：九大模糊测试工具 - 安全牛 https://www.aqniu.com/tools-tech/65203.html

谷歌开源模糊测试工具 ClusterFuzz 尝鲜记录 (进行中) · TesterHome https://testerhome.com/topics/18171

- `模糊测试`
  - 名词：`模糊测试` = `fuzz` = `fuzz testing` = `fuzzing`
  - 模糊测试工具
    - 效率之王：`AFL`
    - 慢工出细活：`Radamsa`
    - 战果累累：`Honggfuzz`
    - 精益求精：`Libfuzzer`
    - 开源医生：`OSS-Fuzz`
    - 瘦死的骆驼：`Sulley`
      - 模糊测试框架
    - 青出于蓝胜于蓝：`boofuzz`
    - 希望之星：`BFuzz`
    - 智能化之选：`Peach`
      - `PEACH` = `Peach` = `Peach Fuzzer` = `PeachTech`
    - 其他
      - `AutoDafe`
      - AI模糊测试工具
        - 微软：`Security Risk Detection`
        - 谷歌：`ClusterFuzz`
        - Synopsys：`Defensics Fuzz Testing`
        - `Fuzzbuzz`

模糊测试工具

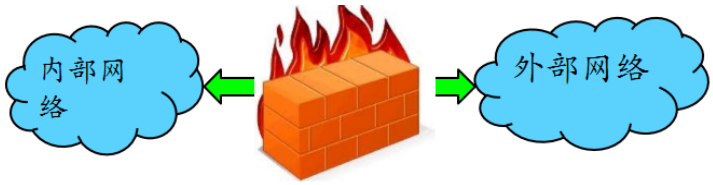
AFL

- `AFL` = `American Fuzzy LOP`
  -

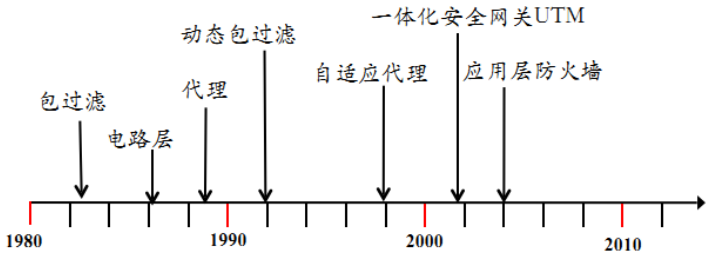
其他防护技术

防火墙

- `防火墙` = `Firewall`
  - 定义：在两个信任程度不同的网络之间设置的、用于加强访问控制的软硬件保护措施
  - 基本逻辑：隔绝内外网

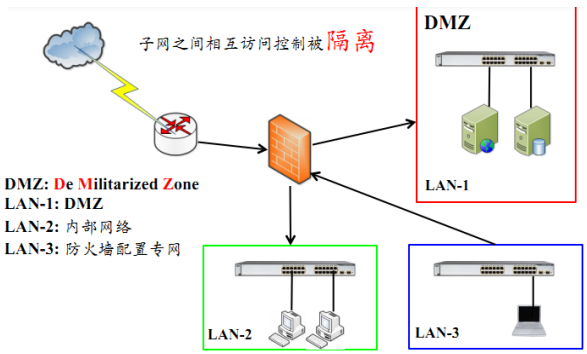


  - 作用
    - 防火墙能够强化安全策略，能够有效记录因特网上的活动，限制暴露用户点，是一个安全策略检查站
  - 缺点
    - 防外而不防内
    - 管理和配置复杂度较高
      - 如果配置不当容易导致安全漏洞
    - 很难为用户在防火墙内外提供一致的安全策略
    - 是一种粗粒度的访问控制
  - 历史

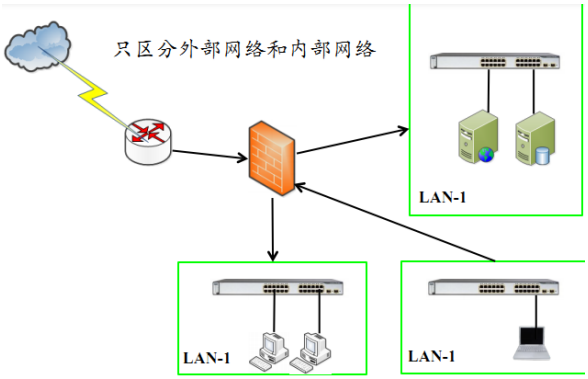


    - `UTM` = `Universal Threat Management` = `统一威胁管理`
      - 整合了防火墙、入侵检测、入侵保护、防病毒、防垃圾邮件等综合功能
    - 新一代的应用层防火墙 = `IPS`
  - 种类
    - 按防护类型分
      - 传统防火墙
      - 应用层防火墙
      - 防DDoS攻击防火墙
      - 垃圾信息过滤防火墙
  - 发展动态和趋势
    - 更强的性能
    - 可扩展的结构和功能
      - 缓存加速
      - 统一认证接口
      - 防 `DDoS`
      - 路由器

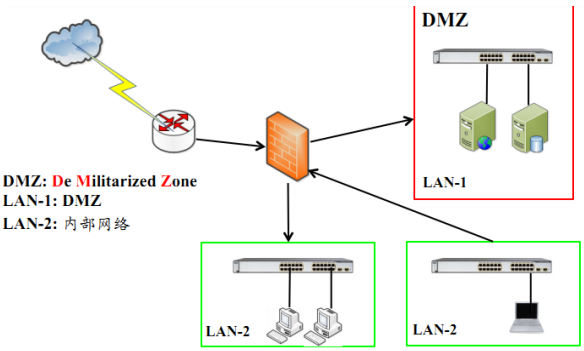
        - 尽可能的简化安装和管理
        - 积极适应持续变化的网络安全环境
            - 防病毒和黑客
            - 反垃圾信息
                - 垃圾邮件
                - 垃圾短信
                - 垃圾电话
    - 产品
        - 开源
            - Endian
            - ModSecurity
            - SmoothWall
            - pfSense
            - iptables
            - m0n0wall
        - 商业
            - Juniper
            - 华为
            - 思科
            - 联想网御神州
            - 绿盟
            - Safe3
    - 配置和应用
        - 模式
            - `路由模式`
                - 概述
                    - 防火墙的各个安全区域位于不同的网段且防火墙自身有 IP 地址。子网之间的相互访问控制被隔离
                - 架构



            - `透明模式`
                - 别称：`网桥模式`
                - 概述
                    - 只区分内部网络和外部网络。不需要对防火墙进行 IP 设置。内网用户意识不到防火墙的存在，隐蔽性较好。降低了用户管理的复杂性
                - 架构



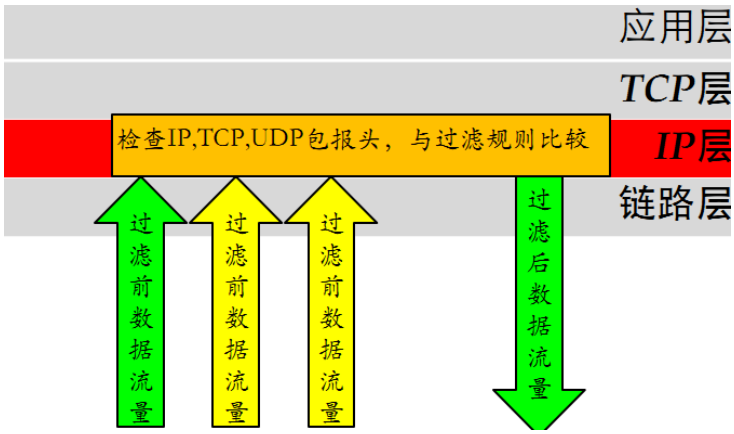
- 混合模式
  - 概述
    - 混合了路由模式和透明模式
    - 在实际生活中应用比较广泛
    - 在混合模式中，内网和服务器区域是透明模式，与外网间则是路由模式
  - 架构



防火墙关键技术

包过滤技术

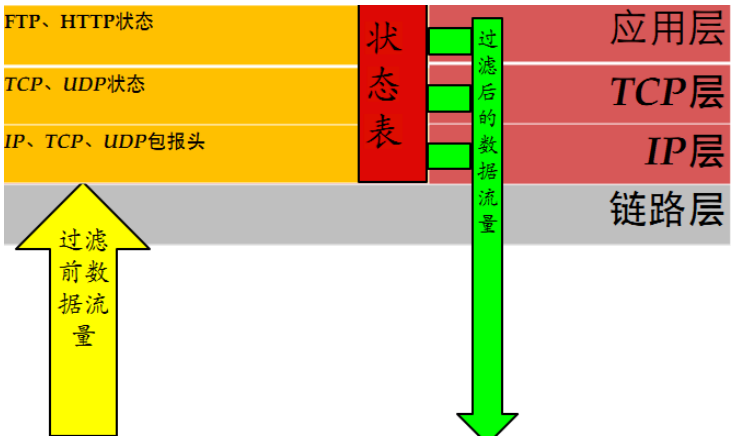
- 包过滤技术
  - 逻辑架构



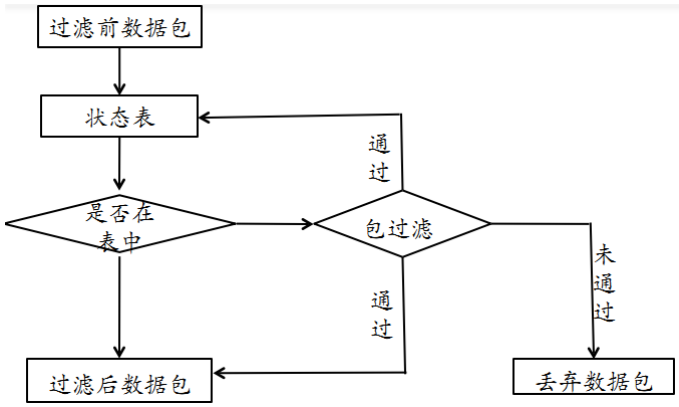
  - 检查数据包的报头信息，依照过滤规则进行过滤
    - 检查数据包内容
      - `IP`：源 IP 地址、目的 IP 地址、协议类型，选项字段等

        - `TCP`：源端口、目标端口、标志段等
        - `UDP`：源端口、目标端口
        - `ICMP`：类型
    - 优点
        - 不需要内部网络用户做任何配置
            - 对用户来说是完全透明的
        - 过滤速度快，效率高
    - 缺点
        - 不能进行数据内容级别的访问控制
        - 一些应用协议也并不适合用数据报过滤
            - 并且过滤规则的配置比较复杂，容易产生冲突和漏洞

状态检测技术

- 状态检测技术
    - 逻辑架构
        - 

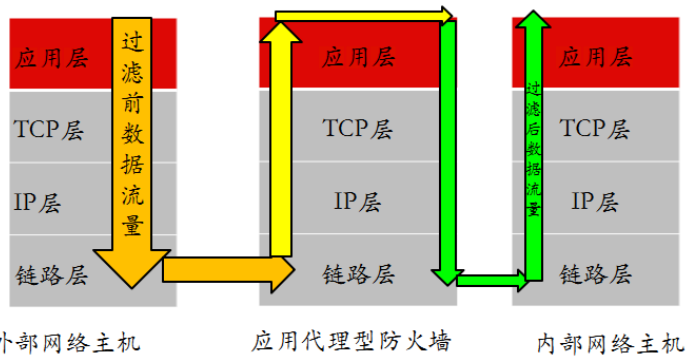
    - 检测逻辑
        - 从收到的数据包中提取状态信息，并根据状态表进行判断
            - 规则
                - 如果该包属于已建立的连接状态，则跳过包过滤的规则检测直接交由内网主机
                - 如果不是已建立的连接状态，则对其进行包过滤，依照规则进行操作
            - 状态表
                - 状态检测技术为每一个会话连接建立状态信息，并对其维护，利用这些状态信息对数据包进行过滤
                - 状态表是动态建立的，可以实现对一些复杂协议建立的临时端口进行有效的管理
                    - `动态状态表`是状态检测防火墙的核心，利用其可以实现比包过滤防火墙更强的控制访问能力
        - 状态检测技术基本流程图



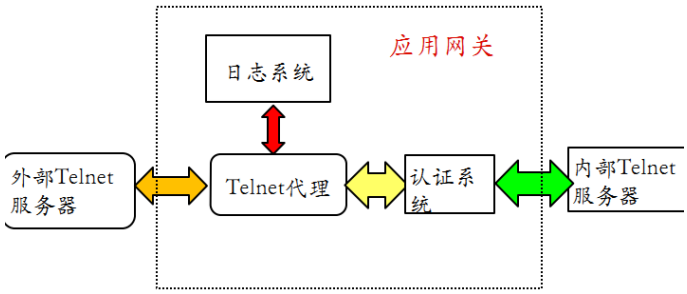
- 缺点
  - 没有对数据包内容进行检测
    - 不能进行数据内容级别的控制
  - 由于允许外网主机与内网主机直接连接，增加了内网主机被外部攻击者直接攻击的风险

代理服务技术

- 代理服务技术
  - 应用级代理 逻辑



  - 检测逻辑
    - 当接收到客户端发出的连接请求后，应用代理检查客户的源和目的 IP 地址，并依据事先设定的过滤规则决定是否允许该连接请求
      - 如果允许该连接请求，进行客户身份识别
      - 否则，则阻断该连接请求
    - 通过身份识别后，应用代理建立该连接请求的连接，并根据过滤规则传递和过滤该连接之间的通信数据
    - 当关闭连接后，应用代理关闭对应的另一方连接，并将这次的连接记录在日志内
  - 举例
    - Telnet



- 优点
  - 内部网络的拓扑、IP 地址等被代理防火墙屏蔽，能有效实现内外网络的隔离
  - 具有强鉴别和细粒度日志能力
    - 支持用户身份识别，实现用户级的安全
  - 能进行数据内容的检查
    - 实现基于内容的过滤，对通信进行严密的监控
- 缺点
  - 性能低，速度慢
    - 代理服务的额外处理请求降低了过滤性能，导致其过滤速度比包过滤器处理速度慢
  - 需要为每一种应用服务编写代理软件模块，提供的服务数目有限
  - 对操作系统的依赖程度高，容易因操作系统和应用软件的缺陷而受到攻击

WAF

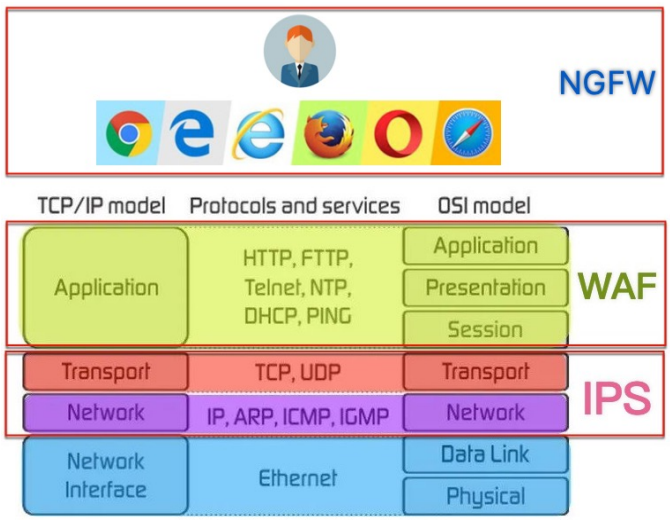
- `WAF` = `Web Application Firewall` = `网络应用防火墙`
  - 是什么：`AF` = `应用防火墙` 的一种，用于过滤、监控、阻止来自和去向Web服务的（有害的）HTTP流量
  - 具体形式：WAF不拘泥于形式，可以是
    - `软件`
    - `硬件`（设备）
    - （云端的）`服务` = SaaS
  - 背景：针对应用发起的攻击成为造成网络漏洞的主要原因
  - 作用：WAF帮你拦截一系列企图通过入侵系统来泄漏数据的攻击
  - 目的：保护Web应用免受各类应用层攻击
    - 比如SQL注入、XSS、文件包含、cookie中毒、不当的系统配置等
  - 历史
    - WAF产品
      - `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 `Top 10` 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
  - 工作原理
    - WAF通过过滤、监控和拦截恶意 `HTTP` 或 `HTTPS` 流量对Web应用的访问来保护您的Web应用，并能够阻止未经授权的数据离开应用
    - 为此，WAF需要遵守一套 `策略` = `policy`，帮助其确定哪些流量是恶意的，哪些流量是安全的
    - WAF的操作方式与代理服务器类似，虽然同为“中介”，但后者旨在保护客户端身份，前者却被称为反向代理，因为其使命在于保护 Web 应用服务器免受潜在恶意客户端的影响
    - 策略可定制，以满足您对Web应用或Web应用组合的独特需求。虽然许多WAF要求您定期更新策略以解决新的漏洞，但机器学习的进步使一些WAF能够自动更新。随着威胁环境愈发复杂和不确定，这种自动化变得越来越重要
  - 注意
    - WAF并不是最终的完整的安全方案，一般搭配其他安全相关系统一起使用，比如 `网络防火墙` = `Network Firewall` 、 `IPS` = `Intrusion`

`Prevention System` = `入侵防护系统`，以打造一套完整的安全防护体系

- 部署方式
  - 基于云 + 完全托管即服务
    - 如果您需要以最快、最便捷的方式将WAF引入您的应用（特别是在您的内部安全或IT资源有限的情况下），这是一个很好的选择。
  - 基于云 + 自我管理
    - 获享基于云的完整灵活性和安全策略的可移植性，同时仍然保留对流量管理和安全策略设置的可控性。
  - 基于云 + 自动配置
    - 开启最简单的云端WAF使用方式，并能够以一种轻松、经济的方式部署安全策略。
  - 内部 Advanced WAF（虚拟或硬件设备）
    - 满足最苛刻的部署要求，一次解决灵活性、性能和更高级的安全问题等多项核心任务

对比

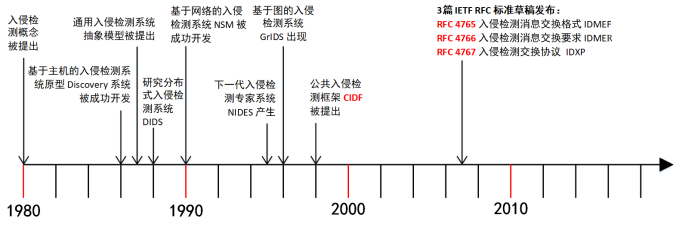
`WAF` vs `IPS` vs `NGFW`

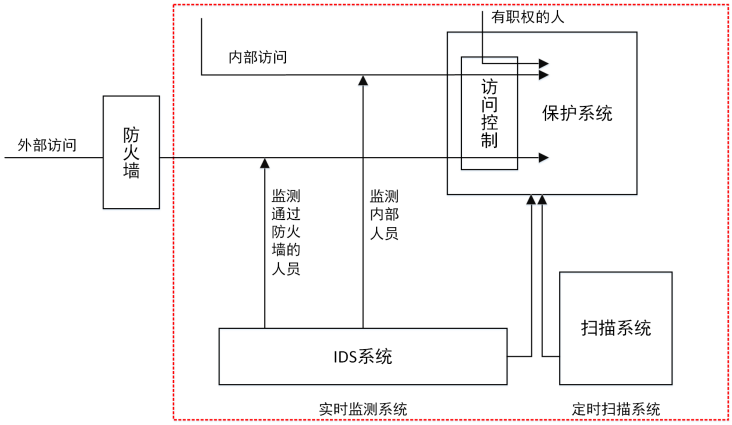
- `WAF` VS `IPS` VS `NGFW`
  - 名词
    - `WAF` = `Web应用防火墙`
    - `IPS` = `入侵防御系统`
    - `NGFW` = `下一代防火墙`
  - 区别
    - 概述
      - 

      - `IPS`：侧重**协议传输层**（`OSI` 的 `3`、`4` 层）
      - `WAF`：侧重**应用层**（`OSI` 的 `5`、`6`、`7` 层）
      - `NGFW`：侧重**Web应用**（`浏览器`、`邮件`、`SaaS` 等）
    - 详解
      - IPS 是一款目标范围更加广泛的安全产品
        - IPS 通常以签名和策略为基础

        - 换言之，它可以根据签名数据库和既定策略，检查众所周知的漏洞和攻击载体
        - IPS 根据数据库和策略建立一个标准，然后会在流量偏离标准时发出警报
        - 随着时间的推移，新漏洞层出不穷，签名和策略也会积少成多
        - 一般来说，IPS 保护对象是一系列协议类型的流量，例如 DNS、SMTP、TELNET、RDP、SSH 和 FTP
        - 通常情况下，IPS 会运行于第 3 层和第 4 层并对其提供保护，相较于网络层和会话层，对应用层（第 7 层）提供的保护力度着实有限
    - WAF的设计则专为保护应用层而生
        - 旨在分析应用层上各 HTTP 或 HTTPS 请求
        - 它通常会感知用户、会话和应用，了解其背后的 Web 应用及其提供的服务
        - 正因如此，WAF 可以看作是用户和应用之间的中介，并会提前对往来于两者之前的通信进行分析
        - 传统的 WAF 确保仅执行允许的操作（基于安全策略）
        - 对于许多组织来说，WAF 是应用值得信赖的第一道防线，尤其是在抵御 OWASP 十大漏洞方面
    - NGFW可以监控进入互联网的流量，覆盖网站、电子邮件账户和 SaaS
        - 简单地说，它是在保护用户（相对于 Web 应用）
        - NGFW 将强制执行基于用户的策略，并为安全策略添加上下文，此外还添加了 URL 过滤、防病毒或防恶意软件等功能，并有可能添加自己的IPS。WAF 是典型的反向代理（供服务器使用），而 NGFW 通常是正向代理（供浏览器等客户端使用）

IDS

- `IDS = Intrusion Detection System = 入侵检测系统`
  - 入侵检测
    - 发展简史
      - 

  - 入侵检测系统的作用
    - 

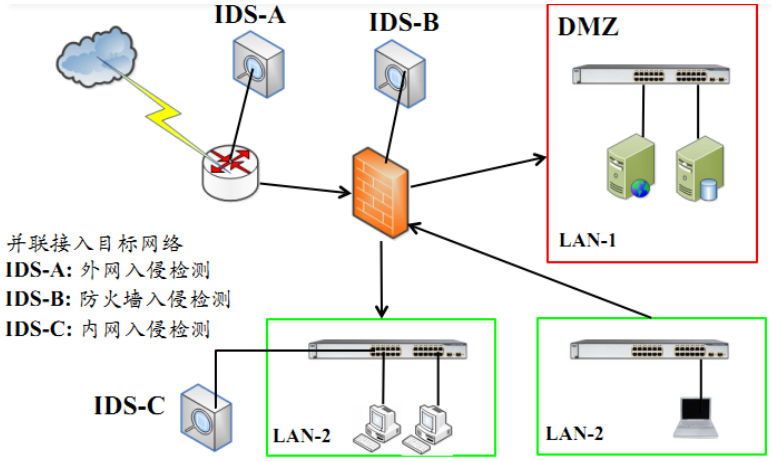
入侵检测标准化

- 入侵检测标准化
  - `HIDS = Host-based Intrusion Detection System = 基于主机的入侵检测系统`
  - `DIDS = Distributed Intrusion Detection System = 分布式入侵检测系统`
  - `IDES = Intrusion Detection Expert System = 入侵检测专家系统`
    - `NG-IDES = Next Generation IDES = 下一代入侵检测专家系统`
  - `NIDS = Network Intrusion Detection System = 基于网络的入侵检测系统`
  - `NSM = Network Security Monitor = 网络安全监测`
  - `GrIDS = Graph-based Intrusion Detection System = 基于图的入侵检测系统`
  - `CIDF = Common Intrusion Detection Framework = 通用入侵检测框架`
    - 是什么：`DARPA 为 IDS 数据交据交换而作出的一个尝试`
      - `DARPA = 美国国防高级研究项目局`
    - 作用和目的
      - 定义了IDS表达检测信息的标准语言以及IDS组件之间的通信协议
        - `IDMEF = Intrusion Detection Message Exchange Format = 入侵检测消息交换格式 = RFC 4765`
        - `IDMER = Intrusion Detection Message Exchange Requirements = 入侵检测消息交换要求 = RFC 4766`

        - `IDXP` = `Intrusion Detection Exchange Protocol` = `入侵检测交换协议` = `RFC 4767`
      - 符合CIDF规范的IDS和安全设备可以共享检测信息，协同工作
      - 集成各种安全设备使之协同工作
        - 分布式入侵检测的基础
  - 体系结构
    - 提出了一个标准的IDS的通用模型
  - 规范语言
    - `CISL` = `Common Intrusion Specification Language`
      - 诞生于 1999 年，定义了一个用来描述各种检测信息的标准语言
      - CISL 和它的“继承者”们
        - MISP
          - 之前： `MISP` = `Malware Information Sharing Platform` = `恶意软件信息共享平台`
          - 后来（重新定位）： `Open Source Threat Intelligence and Sharing Platform` = `开源威胁情报和共享平台`
        - `IODEF` = `Incident Object Description Exchange Format`
          - RFC 5070 IODEFv1
          - RFC 7970 - IODEFv2
        - RFC 4765= `IDMEF` = `入侵检测消息交换格式`
        - OpenTPX - Threat Partner eXchange
          - 开源的机读威胁情报和网络操作数据交换格式和工具
        - `STIX` = `Structured Threat Information eXpression`
          - OASIS Cyber Threat Intelligence (CTI) TC | OASIS
        - `Sigma`： Generic Signature Format for SIEM Systems
          - https://github.com/Neo23x0/sigma
        - `YARA`： 恶意软件特征匹配描述语言和工具
          - https://github.com/virustotal/yara
  - 内部通讯
    - 定义了IDS组件之间进行通信的标准协议
  - 程序接口
    - 提供了一整套标准的应用程序接口（API函数）

入侵检测系统的部署

- 入侵检测系统的部署



入侵检测 vs 威胁检测

- `入侵` = `intrusion`
  - 本意：an occasion when someone **goes into** a place or situation where they are not wanted or expected to be
- `威胁` = `threat`
  - 本意：a suggestion that something unpleasant or violent **will happen**, especially if a particular action or order is not followed
- 从「入侵」检测到「威胁」检测
  - 检测范围扩大
    - `入侵` 检测强调在能区分**内外网**的场景下，重点关注**从外到内**的攻击行为
    - `威胁` 检测不区分**内外网**
  - 检测时间提前
    - `入侵` 检测强调检测**已经发生**的攻击行为
    - `威胁` 检测强调预防**尚未发生**的攻击事件发生
  - 检测目标扩充
    - `入侵` 检测虽然在最早的术语定义中是包含**滥用**行为的，但在实际研究和产品落地实现时主流 IDS 依然以**狭义**的漏洞利用行为检测为主
    - `威胁` 检测的目标不再有遗漏：`攻击` 、`滥用` 、`恶意代码` 等等一网打尽
  - 自动化和协作共享防御目标没有变化

Sonrt

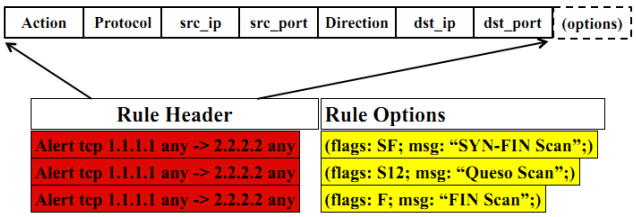
- `Sonrt`
    - 轻量级的网络入侵检测系统
    - 特点
        - 轻巧
            - 源代码不到1MB
        - 多平台=移植性高
            - 支持Linux, Windows, MacOS X, Solaris, BSD, IRIX, Tru64, HP-UX等平台
        - 高性能
            - 使用百兆网络线速处理
        - 可配置
            - 使用简单的规则语言，丰富的日志/配置分析工具
        - 免费
            - GPL 开源
    - 原理
        - 基于Libpcap 的报文嗅探接口
        - 基于规则的检测引擎和支持无限扩展的插件系统
        - 检测引擎
        - 基于指纹的规则
            - 采用模块化设计
            - 具有丰富的检测能力（内置规则）
                - 可进行隐蔽扫描，操作系统识别扫描,、缓冲区溢出攻击、后门和CGI漏洞利用等
    - 工作模式
        - 嗅探模式
        - 报文记录模式
        - `NIDS` 模式
    - 图
        - 捕获的数据报文

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/09-11:12:02.954779 10.1.1.6:1032 -> 10.1.1.8:23
TCP TTL:128 TOS:0x0 ID:31237 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x16B6DA  Ack: 0x1AF156C2  Win: 0x2217  TcpLen: 20
FF FC 23 FF FC 27 FF FC 24 FF FA 18 00 41 4E 53  ..#..'..$....ANS
49 FF F0                                         I..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/09-11:12:02.956582 10.1.1.8:23 -> 10.1.1.6:1032
TCP TTL:255 TOS:0x0 ID:49900 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1AF156C2  Ack: 0x16B6ED  Win: 0x2238  TcpLen: 20
0D 0A 0D 0A 53 75 6E 4F 53 20 35 2E 37 0D 0A 0D  ....SunOS 5.7...
00 0D 0A 0D 00                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

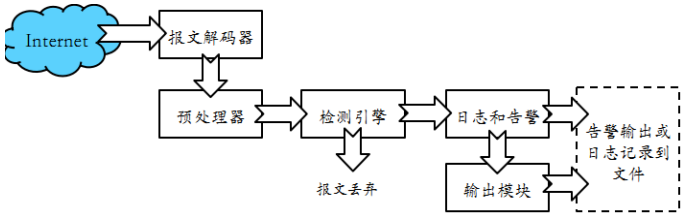
        - Sonrt规则
            - 支持多种规则

```
root@bt:/etc/snort/rules# grep "alert" -R *.rules | wc -l
4072
root@bt:/etc/snort/rules# ls
attack-responses.rules          community-web-dos.rules    policy.rules
backdoor.rules                  community-web-iis.rules    pop2.rules
bad-traffic.rules               community-web-misc.rules   pop3.rules
chat.rules                      community-web-php.rules    porn.rules
community-bot.rules             ddos.rules                 rpc.rules
community-deleted.rules         deleted.rules              rservices.rules
community-dos.rules             dns.rules                  scan.rules
community-exploit.rules         dos.rules                  shellcode.rules
community-ftp.rules             experimental.rules         smtp.rules
community-game.rules            exploit.rules              snmp.rules
community-icmp.rules            finger.rules               sql.rules
community-imap.rules            ftp.rules                  telnet.rules
community-inappropriate.rules   icmp-info.rules           tftp.rules
community-mail-client.rules     icmp.rules                 virus.rules
community-misc.rules            imap.rules                 web-attacks.rules
community-nntp.rules            info.rules                 web-cgi.rules
community-oracle.rules          local.rules                web-client.rules
community-policy.rules          misc.rules                 web-coldfusion.rules
community-sip.rules             multimedia.rules           web-frontpage.rules
community-smtp.rules            mysql.rules                web-iis.rules
community-sql-injection.rules   netbios.rules              web-misc.rules
community-virus.rules           nntp.rules                 web-php.rules
community-web-attacks.rules     oracle.rules               x11.rules
community-web-cgi.rules         other-ids.rules
community-web-client.rules      p2p.rules
```

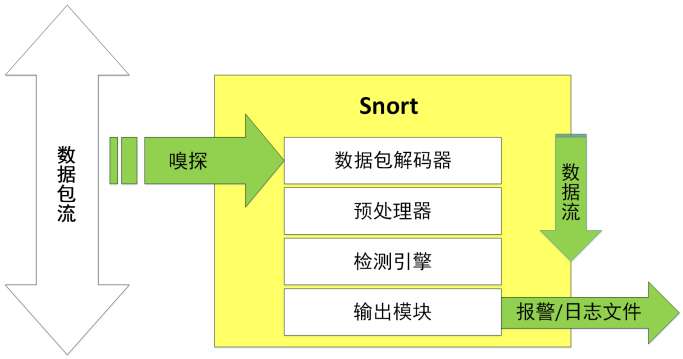
- Sonrt规则格式



- Sonrt流程



- Sonrt架构



Snort简史

- Snort简史
  - Snort 最早是由 Martin Roesch 在 1998 年用 C 语言开发
  - 2001 年应众多 Snort 商业化需求，Martin Roesch 创建了公司 Sourcefire
  - 2013 年 10 月，思科收购了 Sourcefire 并主导 Snort 的开源项目
    - 以 Snort 核心代码和订阅规则为基础，开发了商业版的防火墙、入侵检测等设备与服务并持续回馈到 Snort 开源项目

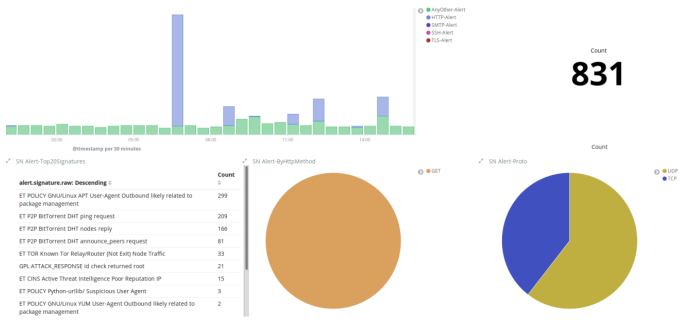
OpenAppID

- `OpenAppID`
  - 一句话描述
    - OpenAppId is an open, application-focused detection language and processing module for Snort that enables users to create, share, and implement application and service detection
      - 思科收购 Sourcefire 之后发布的 Snort 新衍生项目
        - 解决网络流量的「深度识别」需求之一：识别产生流量的具体关联应用
  - 兼容 Snort2 和 Snort3

Snort3 / Snort++

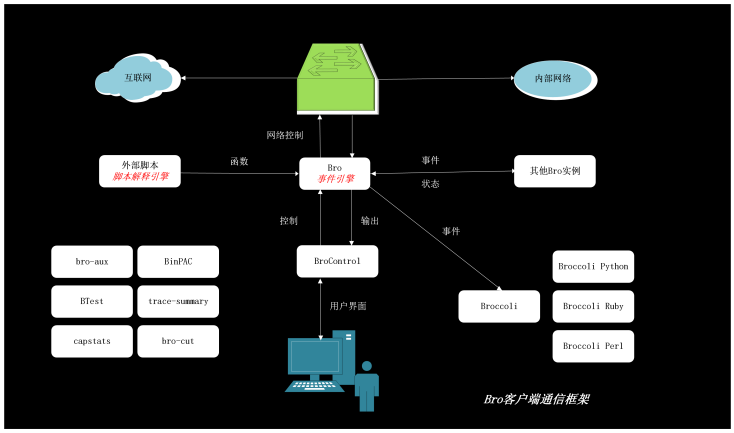
- 思科在 2013 年收购了 Snort 的母公司之后，于 2014 年发布了用 C++ 语言重写的 Snort3 Alpha ，又被称为 Snort++
- 相比于 Snort2 ， Snort3 的产品定位从 IDS 悄然变为 IPS(Intrusion Prevention System)
- 相比于 Snort2 的 主要变化 如下：
  - 支持多线程报文处理
  - 配置简化，支持脚本编程
  - 核心组件的插件化

Suricata

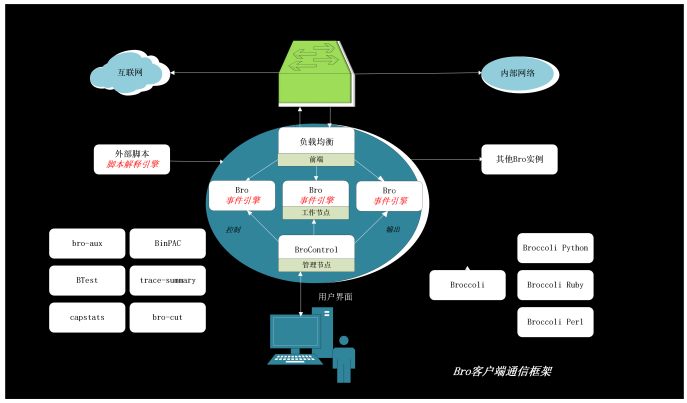
- `Suricata`
  - 是什么：Suricata 是 `OISF` 主导和支持的一个免费、开源、成熟、高性能和健壮的网络威胁检测引擎
    - `OISF` = `Open Information Security Foundation` = `非盈利性组织开放信息安全基金会`
  - 功能
    - 实时入侵检测
    - 内联
      - IPS
        - `IPS` = `Intrusion Prevention System` = `入侵保护`
      - NSM
        - `NSM` = `Network Security Monitoring` = `网络安全监控`
    - 离线pcap处理
  - 介绍
    - Suricata 使用可扩展的规则和签名语言来检查网络，流量，支持使用Lua脚本语言检测复杂威胁。
    - Suricata 使用标准 YAML 输入格式和 JSON 输出格式，使得和第三方 `SIEM` 工具（例如 `Splunk` 、 `ELK` 和其他数据库）集成十分容易
      - `SIEM` = `Security Information and Event Management` = `安全信息和事件管理`
  - 图
    - Suricata产生的报警日志可视化效果图
    - 

Zeek

- `Zeek`
  - 旧：`Bro`
  - 资料
    - 文档
      - Get Started — Book of Zeek (v4.0.1)
        - https://docs.zeek.org/en/lts/get-started.htmls
  - 主要特性
    - 部署
      - 运行在普通硬件和标准UNIX系统（包括 Linux, FreeBSD, MacOS）
      - 基于网络流量分流或镜像端口方式的完全被动流量分析
      - 基于标准 libpcap 接口捕获数据报文
      - 实时和离线分析
      - 支持大规模集群部署
      - 同时支持单机和集群配置的统一管理框架
      - 基于 BSD 协议开源
    - 分析
      - 全面行为日志记录用于离线分析和取证
      - 端口无关的应用层协议分析
      - 支持多种应用层协议（包括：DNS、FTP、HTTP、IRC、SMTP、SSH、SSL）
      - 应用层负载内容分析包括 MD5/SHA1 计算用于指纹
      - 完全 IPv6 支持
      - 隧道协议检测和分析（包括 Ayiya, Teredo, GTPv1）。Zeek 重组识别的隧道协议负载就像没有使用隧道协议一样去分析内层应用层协议数据。
      - 协议分析期间支持大量合法性检查方法
      - 支持 IDS 风格的模式匹配
    - 可编程性
      - 使用图灵完备语言来完成任意分析任务的表达刻画
      - 基于事件编程模型
      - 内置专业领域数据结构支持，例如 IP 地址（IPv4 和 IPv6 地址透明处理）、端口号和时钟
      - 广泛支持基于时间（窗口）的追踪和网络状态管理
    - 接口
      - 默认输出为格式化后的 ASCII 日志
      - 可选后端支持 ElasticSearch 和数据序列。更多数据库接口仍在开发中。
      - 支持外部数据实时导入集成分析。实时数据库仍在开发中。
      - 外部C语言编程库用于 Zeek 事件和外部程序交换。支持 Perl、Python 和 Ruby 语言混编。
      - 支持从脚本语言调用任何外部可执行程序。
  - 架构



- 主要组件
  - 事件引擎（核心）
  - 脚本解释引擎
- 集群架构拓扑图



- 对比
  - Zeek 相比较于 Snort 和 Suricata 具有以下独特特性
    - 可扩展性。同时支持单机和集群配置的统一管理框架，这使得我们所做的系统不会局限于原型演示系统，可以随时在流量采集这个需求上实现快速扩展；
    - 全面行为日志记录用于离线分析和取证，特别是这些日志还可以实时输出为 ASCII 格式文本文件，我们可以很方便的把这些日志实时导入到一个实时日志分析引擎进行二次分析。结合主机和设备日志、情景数据和威胁情报，为关联分析提供了必要的来源输入数据；
    - 可编程性，使得我们可以按需实时对网络流量进行就近在线分析和关键信息抽取，可以随时根据系统架构中不同组件的实现方案进行灵活适配，满足系统总体架构设计需求。

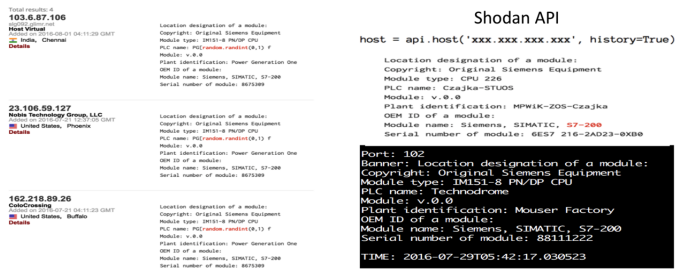
OPNsense

- `OPNsense`
  - 开源易用的基于安全加固 BSD 的防火墙和路由平台（入侵防护系统）
    - 基于 `pfSense` 和 `m0n0wall` 自2014年起独立分支开发

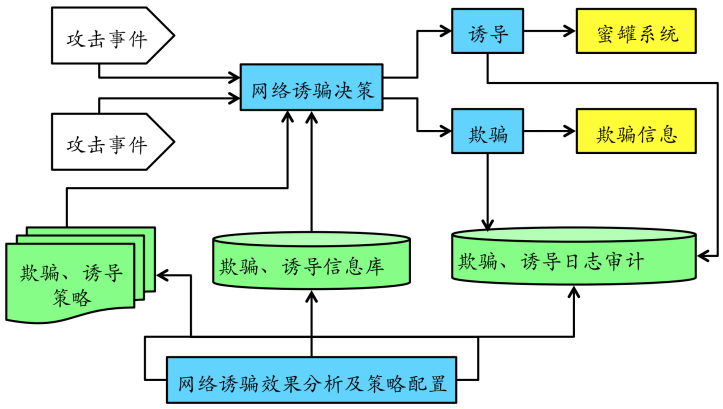
蜜罐HonyPot

- `蜜罐 = Honeypot`
  - 别称：蜜网
  - 含义：高仿真、高交互的专用工业入侵诱捕系统
    - 可以理解为：网络攻防领域的钓鱼执法
  - 作用：专指用来侦测或抵御未经授权操作或者是黑客攻击的陷阱，因原理类似诱捕昆虫的蜜罐因而得名
  - 特点：发现未知攻击的有效工具
  - 举例
    - 通过Shodan搜索国外蜜罐

通过Shodan搜索国外蜜罐案例

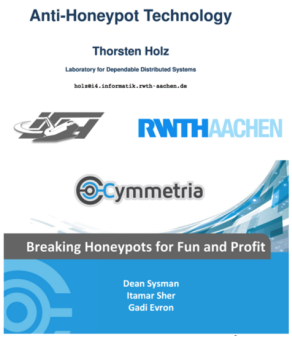


  - 基本架构



  - 发展历史
    - 蜜罐技术的发展里程碑
      - 1990年：小说《The Cuckoo's Egg》发表，蜜罐的概念第一次出现在公众视野
      - 1997年：Fred Cohen 发布 DTK 项目，一个用于模拟网络服务的虚拟系统，这是第一个公开的蜜罐系统
      - 2000年：蜜网项目组成立，同时发布了 Gen II 蜜网项目，在这个项目中，真实系统被用于蜜罐用途
  - 经典蜜罐项目
    - `DTK = Deception Toolkit`
      - Fred Cohen 等人于1997年首次对外公开发布，提供一些欺骗的手段（工具）来阻止攻击，是低交互蜜罐的雏形，支持简单的脚本编程自定义交互行为
    - `Honeyd`

        - 搭建虚拟蜜罐与蜜罐网络的轻量级守护进程，模拟几乎任何类型的应用层服务与任何发行版的操作系统，例如：IIS、FTP、telnet 等。属于低交互蜜罐，支持脚本定制和配置。建议运行在沙盒环境中，例如可以通过 systrace 来监控蜜罐中的 API 调用和文件 IO 等行为
    - `Nepenthes` = `猪笼草`
        - Georg Wicherski 独立开发 mwcollect，Paul Baecher 和 Markus Koetter 开发了 Nepenthes。2006 年 2 月 mwcollect 被整合进 Nepenthes，mwcollected v4 的开发得到了卡巴斯基实验室资助（2009.2-2010.1）。这同样是一个运行在 Linux 上的低交互虚拟蜜罐，可以模拟多种 Windows 服务，自动下载恶意代码并发送到预定义服务器进行集中检测和分析
    - `Dionaea`
        - 起始于 2009 年的 Nepenthes 后继项目，设计用于诱捕恶意攻击，得到恶意程序样本。属于低交互式蜜罐，支持分布式诱捕和与其他模块协同，如 p0f
- 存在问题
    - 

    - 

工具和系统

安全操作系统

Kali Linux

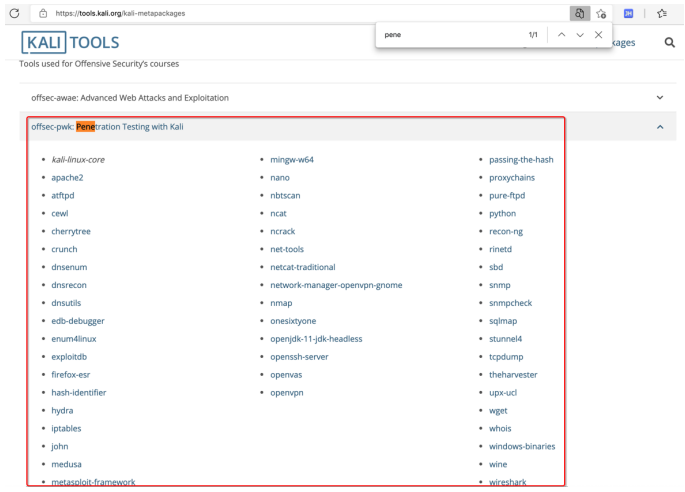
- = `Kali Linux`
- 是什么：一个Linux操作系统，专门用于渗透测试，
- `Kali`
  - = `Kali Linux`
    - 旧称：`BackTrack Linux`
  - 是什么：一个操作系统
    - 用途：专门用于安全、逆向、破解、渗透
    - 特点：自带大量相关工具
  - 被称为
    - 网络安全人员的专用系统
  - 资料
    - 主页
      - Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution
        - https://www.kali.org
  - 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

Kali中的工具

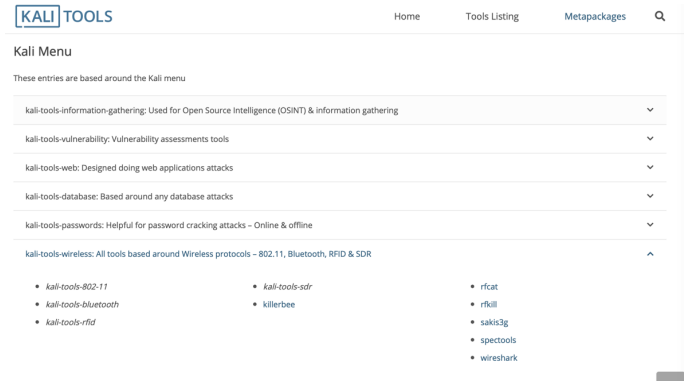
- Kali中的工具
  - 首页
    - Penetration Testing Tools - Kali Linux
      - https://tools.kali.org
    - Kali Linux Tools Listing | Penetration Testing Tools
      - https://tools.kali.org/tools-listing

根据用途分

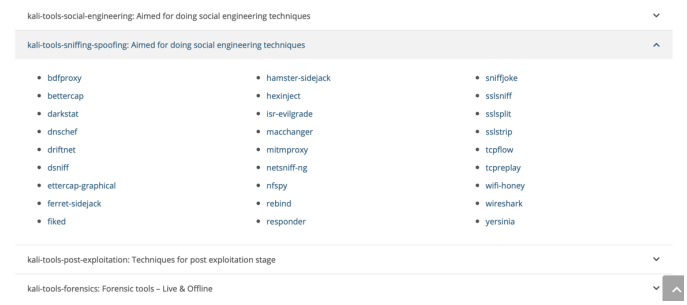
- Kali Metapackages
  - Kali Metapackages | Penetration Testing Tools
    - https://tools.kali.org/kali-metapackages
      - Metapackages 目的是方便你，根据自己的用途，安装特定领域的工具
        - 可以根据自己的需要，去找对应领域或用途的工具
  - 举例
    - 渗透测试 Penetration Test



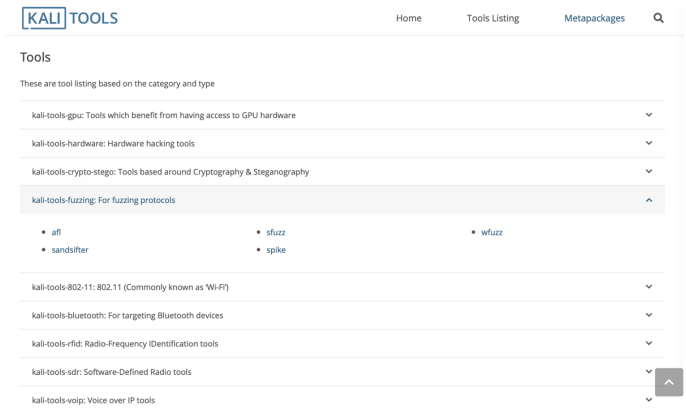
- 无线 Wireless



- 嗅探 Sniff



- 模糊测试 Fuzz



根据不同类型分

- 根据不同分类
  - 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

        - Parsero
        - Recon-ng
        - SET
        - SMBMap
        - smtp-user-enum
        - snmp-check
        - SPARTA
        - sslcaudit
        - 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
        - sqlsus
        - 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
        - Airolib-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
        - Spooftooph
        - 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
    - Sniffing & Spoofing
        - bettercap
        - Burp Suite
        - DNSChef
        - fiked
        - hamster-sidejack
        - HexInject
        - iaxflood
        - inviteflood
        - iSMTP
        - isr-evilgrade
        - mitmproxy
        - ohrwurm
        - protos-sip
        - rebind
        - responder
        - rtpbreak
        - rtpinsertsound
        - rtpmixsound
        - sctpscan
        - SIPArmyKnife
        - SIPp
        - SIPVicious
        - SniffJoke
        - SSLsplit
        - sslstrip
        - THC-IPV6
        - VoIPHopper
        - WebScarab
        - Wifi Honey
        - Wireshark

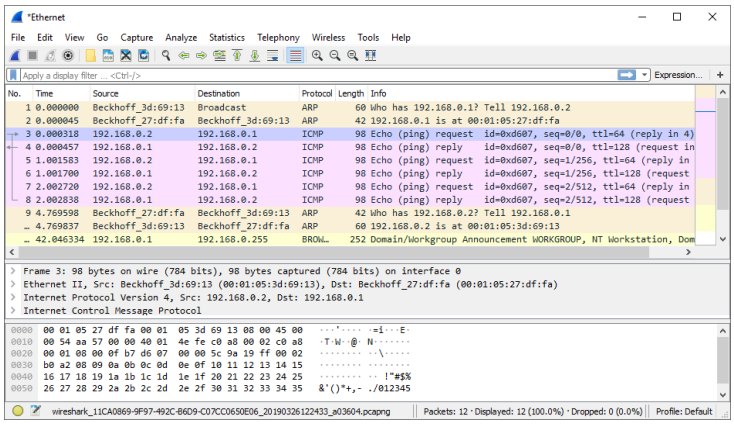
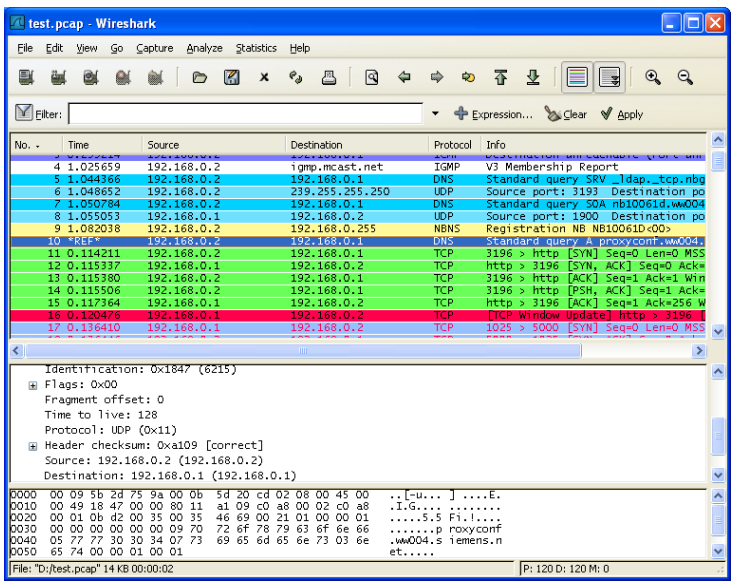
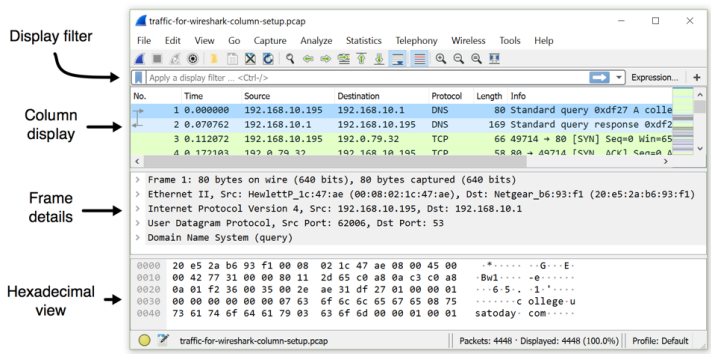
        - xspy
        - Yersinia
        - zaproxy
    - Password Attacks
        - BruteSpray
        - Burp Suite
        - CeWL
        - chntpw
        - cisco-auditing-tool
        - CmosPwd
        - creddump
        - crowbar
        - crunch
        - findmyhash
        - gpp-decrypt
        - hash-identifier
        - Hashcat
        - HexorBase
        - THC-Hydra
        - John the Ripper
        - Johnny
        - keimpx
        - Maltego Teeth
        - Maskprocessor
        - multiforcer
        - Ncrack
        - oclgausscrack
        - ophcrack
        - PACK
        - patator
        - phrasendrescher
        - polenum
        - RainbowCrack
        - rcracki-mt
        - RSMangler
        - SecLists
        - SQLdict
        - Statsprocessor
        - THC-pptp-bruter
        - TrueCrack
        - WebScarab
        - wordlists
        - zaproxy
    - Maintaining Access
        - CryptCat
        - Cymothoa
        - dbd
        - dns2tcp

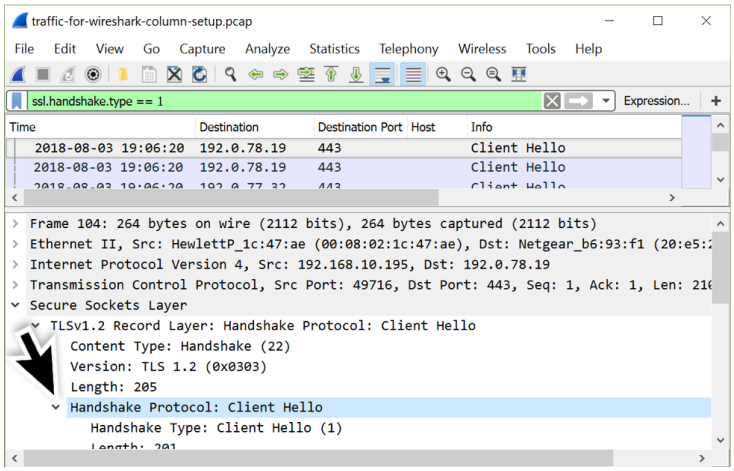
        - HTTPTunnel
        - Intersect
        - Nishang
        - polenum
        - PowerSploit
        - pwnat
        - RidEnum
        - sbd
        - shellter
        - U3-Pwn
        - Webshells
        - Weevely
        - Winexe
    - Hardware Hacking
        - android-sdk
        - apktool
        - Arduino
        - dex2jar
        - Sakis3G
        - smali
    - Reverse Engineering
        - apktool
        - dex2jar
        - diStorm3
        - edb-debugger
        - jad
        - javasnoop
        - JD-GUI
        - OllyDbg
        - smali
        - Valgrind
        - YARA
    - Reporting Tools
        - CaseFile
        - cherrytree
        - CutyCapt
        - dos2unix
        - Dradis
        - MagicTree
        - Metagoofil
        - Nipper-ng
        - pipal
        - RDPY

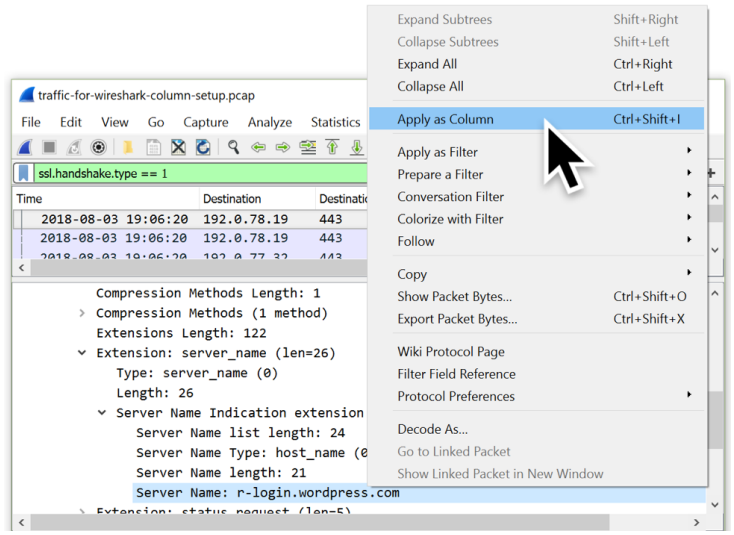
网络分析工具

- 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

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
    - 
    - 
    - 

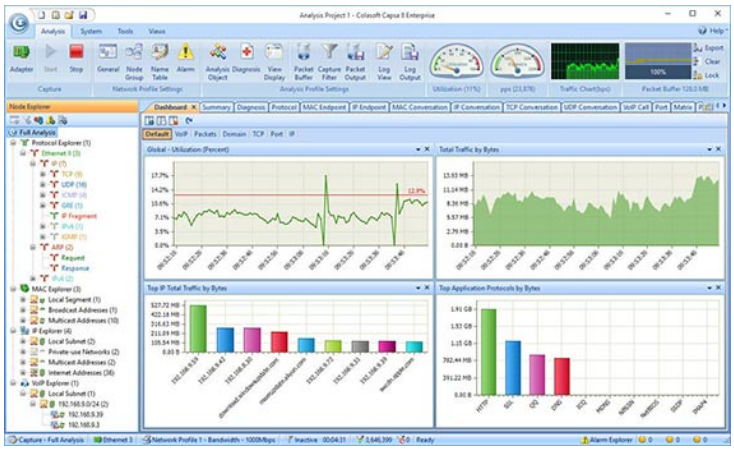




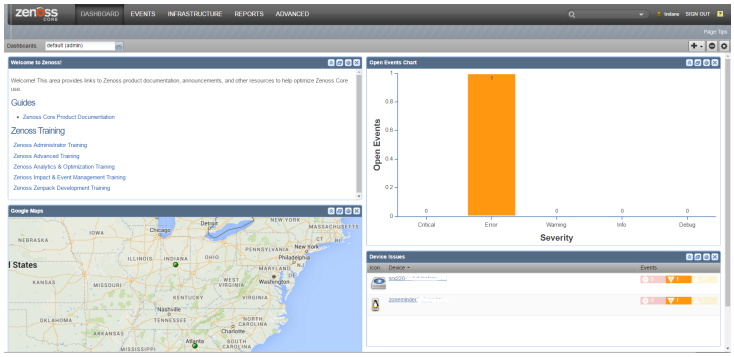
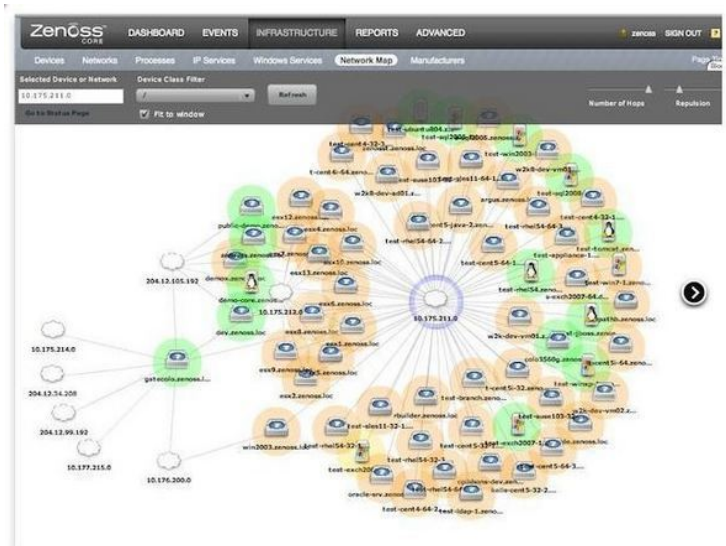
- 功能特点
  - Deep inspection of hundreds of protocols, with more being added all the time
  - Live capture and offline analysis
  - Standard three-pane packet browser
  - Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
  - Captured network data can be browsed via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

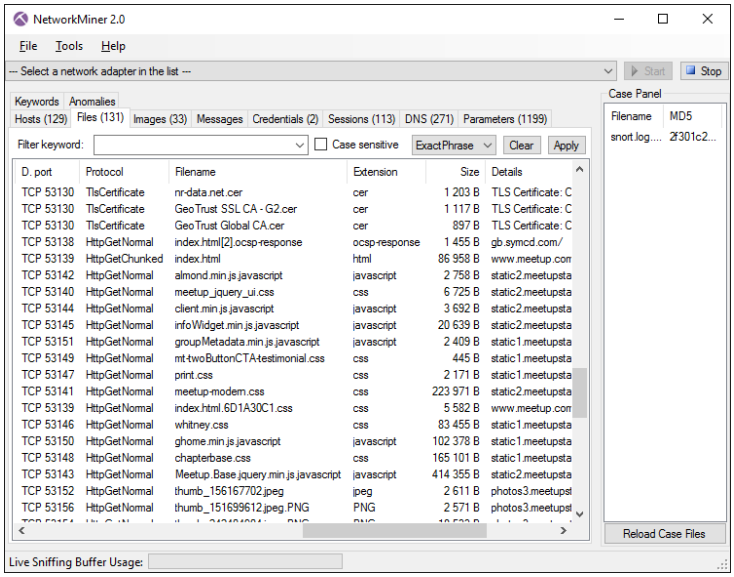
- `Capsa Free` = `Capsa Free Network Analyzer`
  - 概述
    - 网络分析工具，用于监控、故障排除和分析。来自Colasoft的Capsa Free提供了识别和监控超过300种不同协议的能力。用户可以记录网络配置文件，创建定制报告和设置自定义报警触发条件。此外，Capsa提供邮件监控，自动保存邮件内容以及易于使用的TCP时序图
  - 图
    - 
    - 

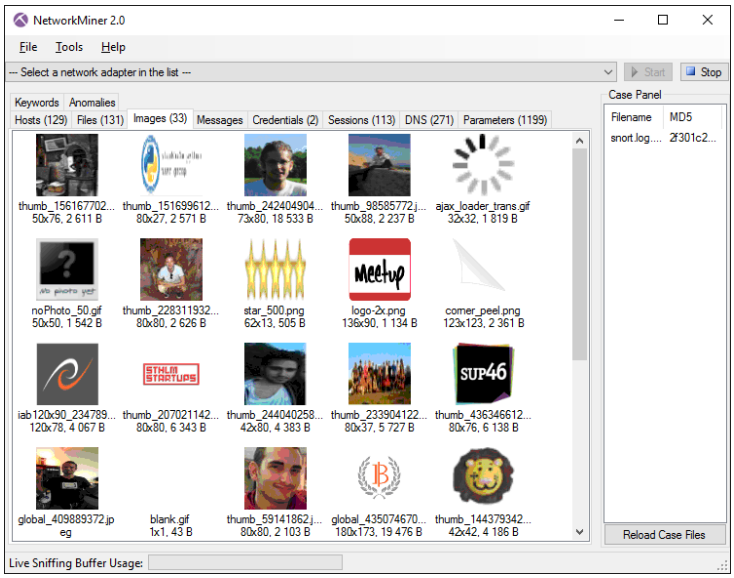
Zenoss Core

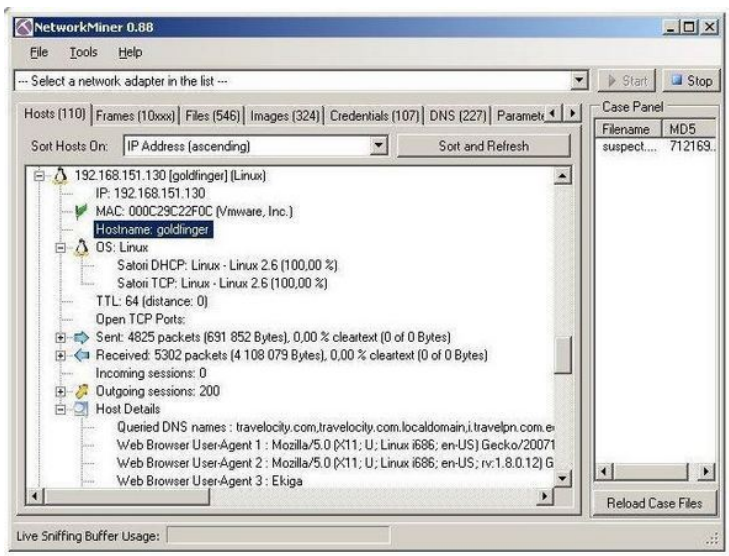
- `Zenoss Core` = `Zenoss Community Edition`
  - 是什么：一个网络管理平台
    - 基于 `Zope` 的应用服务器
    - 通过Web页面提供服务
  - 概述
    - 一个集成的网络和系统管理平台，Zenoss Core具备可用性，性能，事件，系统和网络设备配置的监控能力。随着数据流通过SNMP，SSH，WMI，JMX和Syslog，该平台提供了灵活的监控日志和事件管理。此外，该工具针对虚拟和云基础架构，包括VMware ESX，提供专门的监控功能
  - 图
    - 
    - 

NetworkMiner

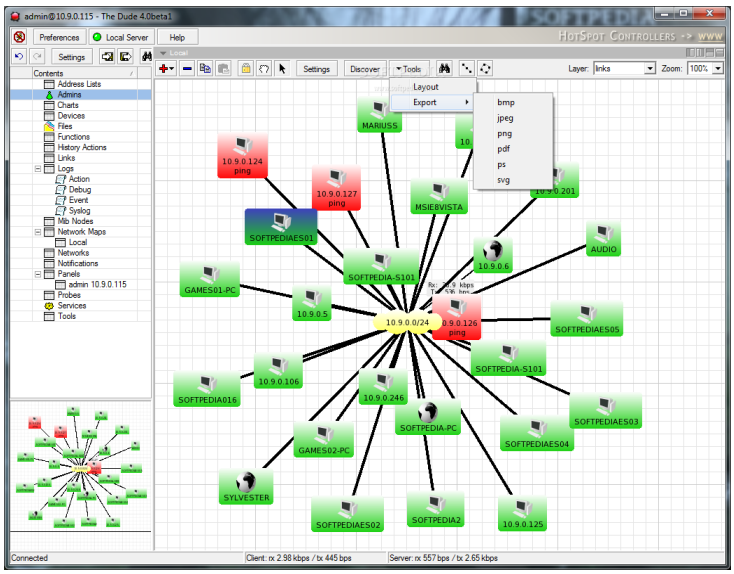
- `NetworkMiner`
  - 一句话描述：一个开源的网络取证分析工具
  - Logo
    - 
  - 概述
    - 有时，不仅需要分析网络流量。软件安全公司Netresec 的NetworkMiner是一种基于Windows的网络取证分析工具，设计用来收集有关网络中的主机和数据，而非流量。它能够抓包甚至解析PCAP文件，以帮助用户监测网络中主机的OS,主机名，以及开放端口。此工具方便文件、证书的重组传输，而无需耗费额外的流量
  - 功能
    - 在线online
      - 应用领域
        - 网络取证分析= `Network Forensic Analysis`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

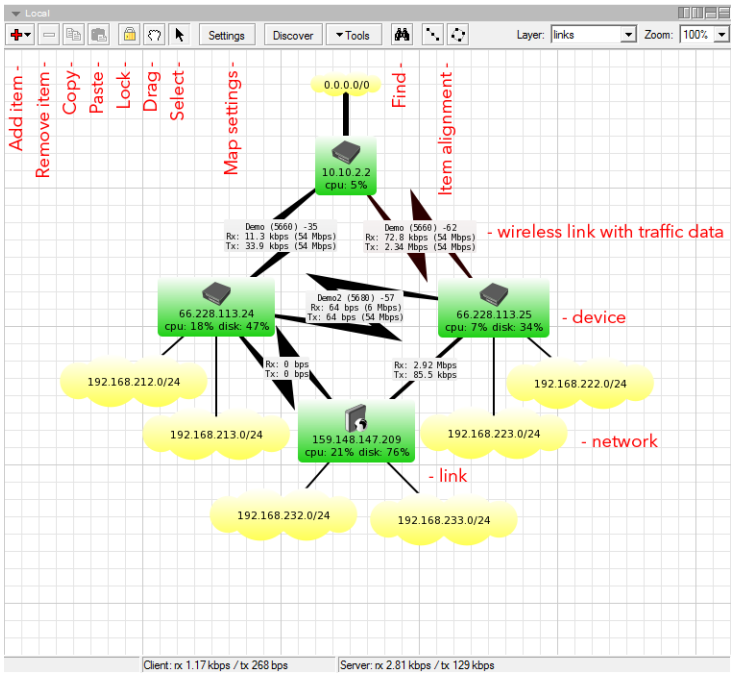


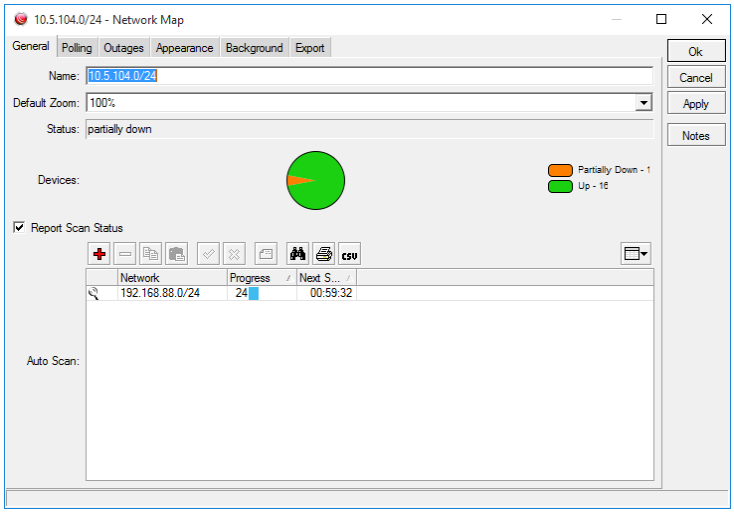


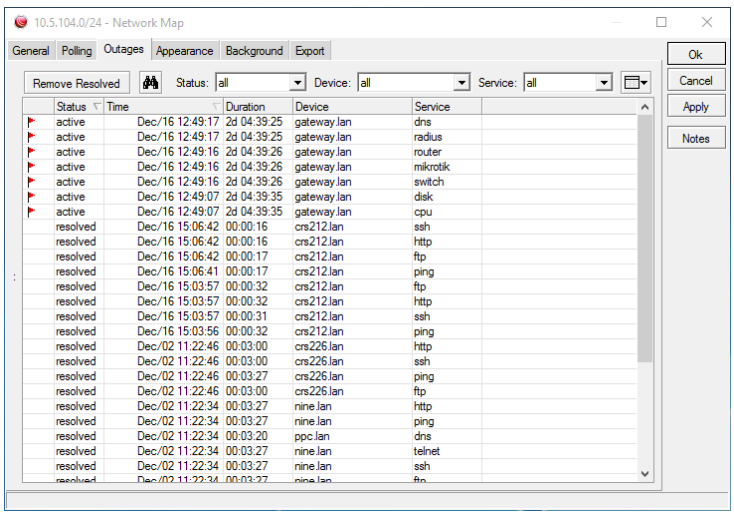


The Dude

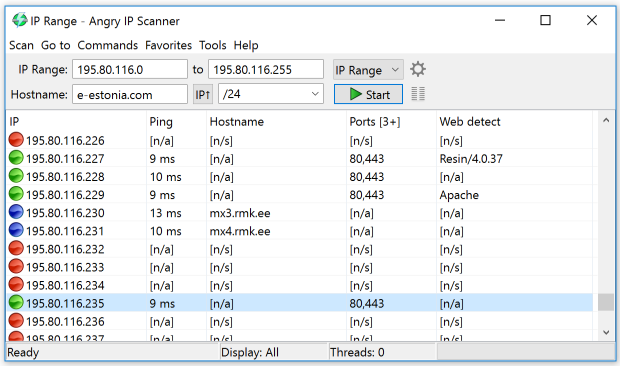
- `The Dude`
  - 是什么：网络监控器network monitor
  - 作用：极大地提高你管理网络的效率
    - 主要是可以画出内网的网络关系图，可视化后，方便理解和管理设备
  - 概述
    - 在指定子网内自动扫描设备。The Dude能够绘制网络地图，监控运行设备的服务器并在服务器有问题时自动告警。能够运行在Windows，Linux Wine, Darwine和MacOS，并支持设备的SNMP, ICMP, DNS 和 TCP 监控
  - 功能
    - 自动扫描内网所有设备
    - 画出网络结构布局图
    - 监控设备服务
    - 服务异常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

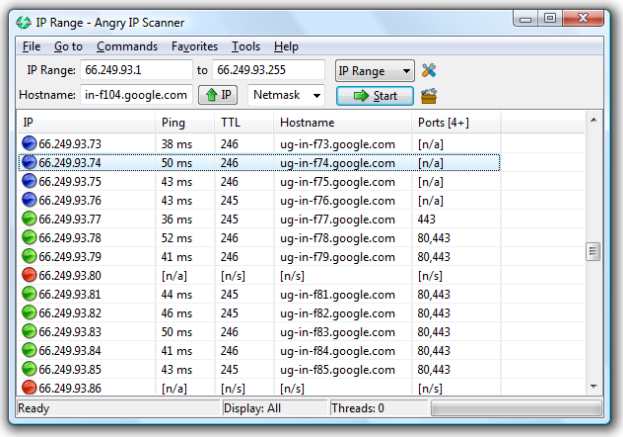




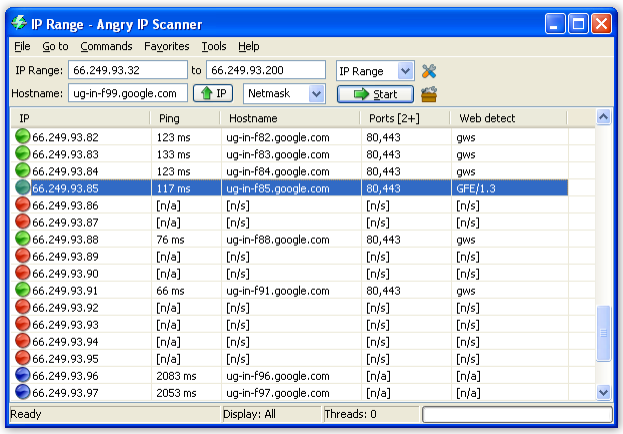


Angry IP Scanner

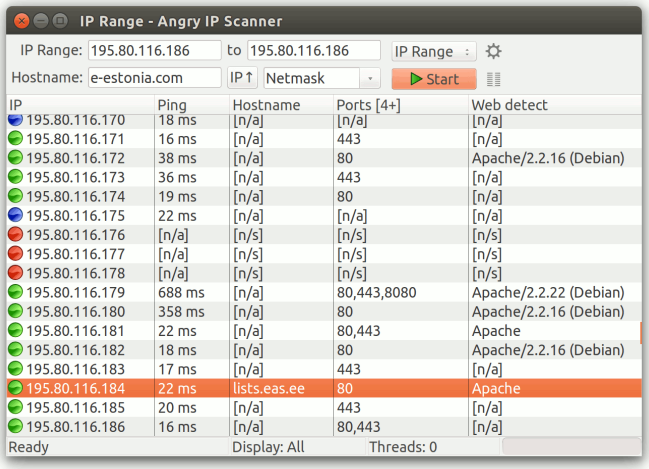
- `Angry IP Scanner`
  - 别称：`ipscan`
  - 是什么：一个开源的跨平台的网络扫描工具
  - 设计宗旨：速度快，易用
  - 概述
    - 一种轻量级IP扫描工具，使用多线程扫描技术快速扫描，结果能够保存到CSV, TXT, XML 或 IP-Port 列表文件中。基于Java的灵活框架，并且能够通过插件扩展额外信息收集功能
  - 图
    - Windows
      - Windows 10
        - 

      - Windows 7/Vista
        - 

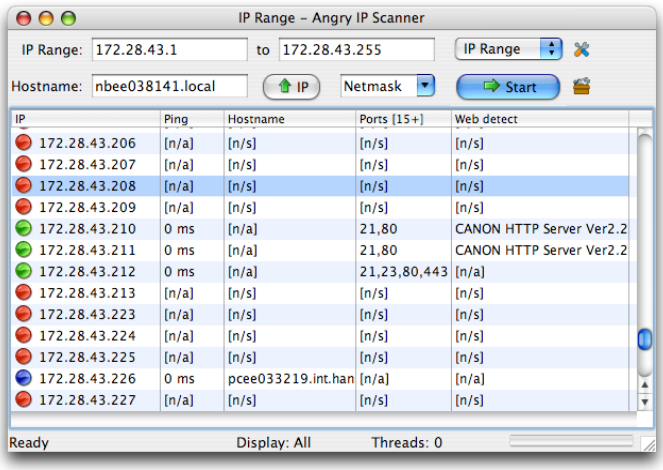
      - Windows XP



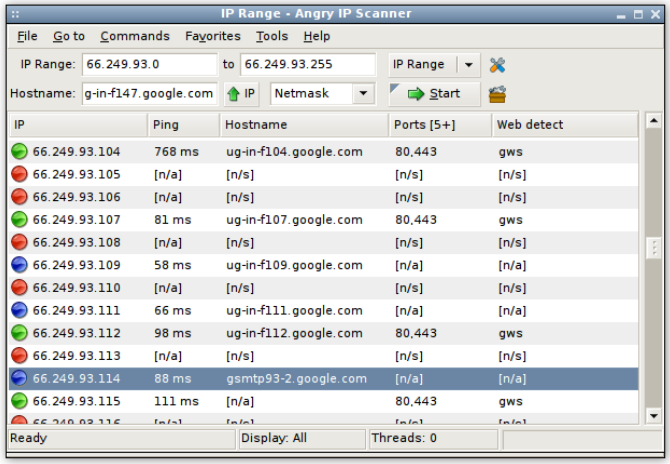
- Ubuntu



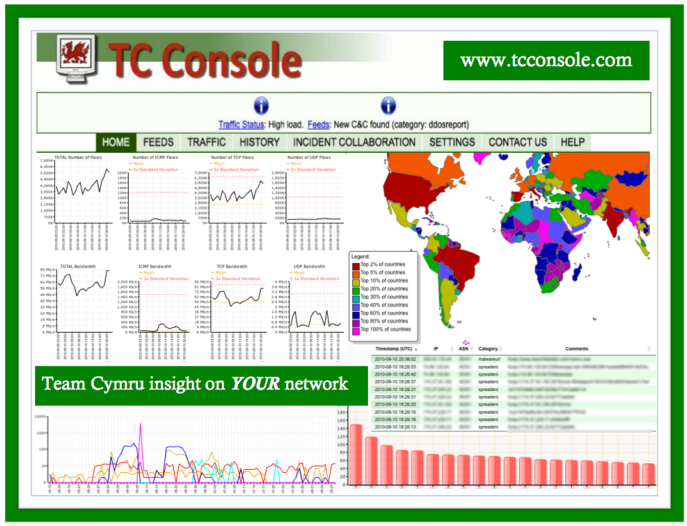
- Older Mac OS X



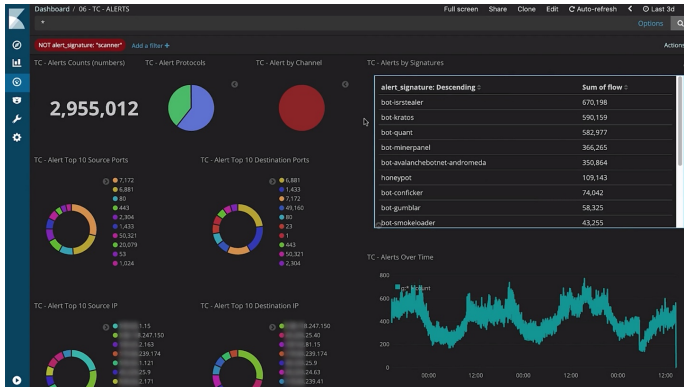
- Older Linux



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
      - 



代码审计类

- 工具
  - `CxEnterprise`
    - = `Checkmarx CxEnterprise`
  - `Armorize CodeSecue`
  - `Fortify`
    - = `Fortify SCA`
  - `RIPS`

Checkmarx CxEnterprise

- `Checkmarx CxEnterprise`

Armorize CodeSecue

- `Armorize CodeSecue`

Fortify

- `Fortify`

RIPS

- `RIPS`

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 `思科` 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
    - 
    - 

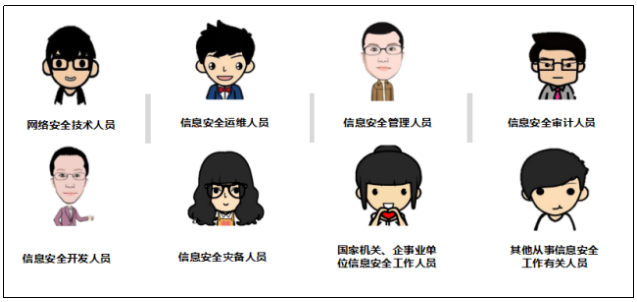
      

  - 考证要求：需要工作经验
  - 考取难度：★★★☆☆
  - 适应类型： 国有企业、政府、军工、8+2行业信息安全主管及为国内提供信息安全服务的安全公司从业人员
    - 面向对象：面向信息安全企业、信息安全咨询服务机构、信息安全测评机构、政府机构、社会各组织、团体、大专院校以及企事业单位中负责信息系统建设、运行维护和管理工作的信息安全专业人员所颁发的专业注册证书

- 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员`
                - 管理员
            - `CISP-A` = `注册信息安全审核员` = `注册信息安全审计师`
                - 审计师
            - `CISD` = `CISP-DRP` = `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
        - `CISP-A` = `CISP-Audit`
            - 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` = 注册信息安全员

- `CISM` = `Certified Information Security Member` = `注册信息安全员`
  - 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

- CCSRP = 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
        - 通用信息安全人员认证
            - 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 = Internationa Information Systems Security Cerification 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，有不少国企也比较认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半点的高
                    - 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**

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

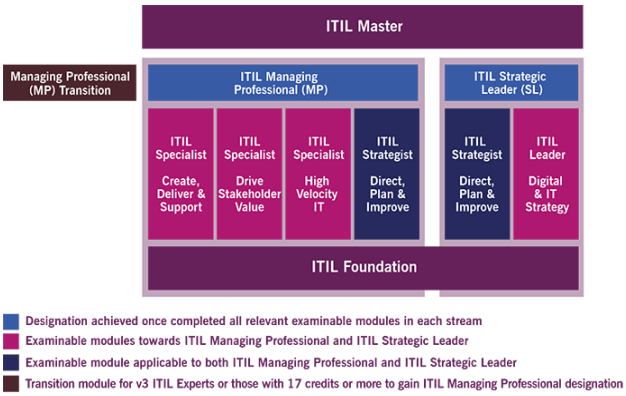
  - 现状

- 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

其他证书

ITIL = 信息技术基础设施库

- ITIL = Information Technology Infrastructure Library = 信息技术基础设施库
  - 是什么：一个国际通用的IT服务管理方面的认证
    - a IT management framework
  - 作用：帮助每个企业的IT部门完善流程，实现规范化、精细化运作
    - 提供了 ITSM
      - ITSM = IT Service Management = 信息技术服务管理
  - 概述
    - 由 英国商务部 于上个世纪80年代末发展的一套IT服务管理最佳实践指南，它由一系列出版物、各种资格认证及一个国际用户组织（ itSMF ）支持
      - OGC = Office of Government Commerce = 英国商务部
    - ITIL致力于协助组织机构建立IT服务管理架构，已经成为全球范围内用得最广泛的IT服务管理最佳实践
    - ITIL自上世纪八十年代开始发展，经过行业专家、顾问和实施者的共同努力，已经成为IT服务管理领域最佳实践事实上的国际标准
      - ITIL经过40年的发展，已经成为IT服务管理领域最好的国际标准
    - ITIL是一种全新的、基于流程的IT管理模式，可快速帮助企业IT部门从职能/后勤部门转型为服务部门，并实现规范、精细、可量化的IT管理，提供可保证的IT服务质量
  - 特点
    - 这个认证站的高度比较高，一般都是倾向管理者的，站在全局的角度考虑自己权限范围内的IT建设的
  - 现状
    - 这个证书目前在外企(欧美企业)中比较流行，特别是大型制造型企业
      - 如果你经常上51JOB之类的招聘网站的话，你会发现 ITIL 在欧美的外企中要求的特别多
    - 全球10,000 多家在各行业处于领先地位的组织都在使用ITIL流程改进IT服务的效率和沟通，大量的成功实践表明实施ITIL可以大幅度提高IT部门营运效率，提高IT组织服务质量
    - 在过去的15 年里，每一次ITIL 的更新对产品和服务支持的内容、质量、以及提供服务的供应商都产生了很大的影响
    - 有这个证书，对于想进外企的人来说，就是一个敲门砖
    - 即使你成为企业的管理者，或者IT部门负责人都是需要ITIL证书的
  - 历史 & 更新
    - 2000： ITIL 2 = ITIL v2
      - 更侧重过程process
    - 2007： ITIL 3 = ITIL v3
      - 2011：小更新
        - 又称： ITIL 2011 V3
    - 2019： ITIL 4 = ITIL v4
  - 级别
    - ITIL v3

        - 5个等级
            - `ITIL Foundation` = `ITIL基础认证`
                - 获取其他证书的基础，是对ITIL入门者的核心基础认证
                    - 只有考取了ITIL foundation证书才能考取更高等级的证
                - 适用于：从事IT服务管理的人员
                    - 要求他们了解IT服务管理的和IT基础设施的重要性，掌握服务管理的流程及相互间接口，ITIL的基本概念，ITIL中的十大流程以及各流程之间的关
            - `ITIL Practitioner` = `ITIL从业者认证`
                - 该证书主要是针对从事IT服务管理特定流程的人员，要求其具有一定实践经验
                    - 也就是说考取该证书，需要报考人员有IT方面的实践经验。
            - `ITIL Intermediate` = `ITIL中级认证`
            - `ITIL Expert` = `ITIL专家认证`
            - `ITIL Master` = `ITIL大师认证`
                - 最高级别
    - `ITIL v4`
        - 4个等级
            - `ITIL Foundation`
            - `ITIL Managing Professional` = `ITIL MP` = `ITIL职业经理人`
            - `ITIL Strategic Leader` = `ITIL SL` = `ITIL战略领导者`
            - `ITIL Master` = `ITIL大师认证`
        - 不同等级之间的关系
            - 

`CISA` = 注册信息系统审计师

- `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

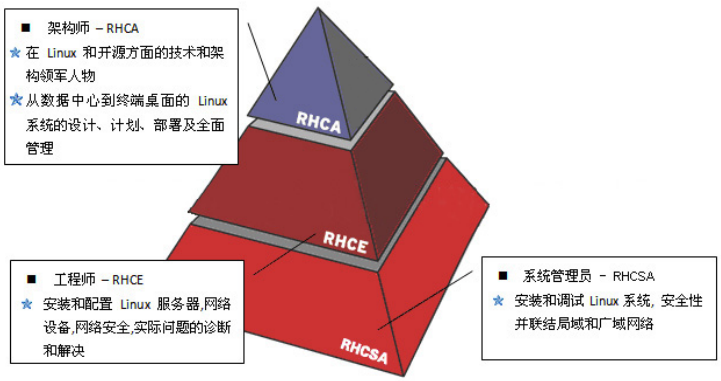
红帽RedHat

`RHCE = 红帽认证工程师` 和 `RHCT = 红帽认证技师`

- `RHCE = Red Hat Certified Engineer = 红帽认证工程师`
    - 是什么：指具备以下能力的 `红帽认证系统管理员 = RHCSA`
        - 自动化红帽企业Linux任务
        - 集成红帽新兴技术

        - 实施自动化来提高效率、促进创新
    - 注意
        - 要想获得 `RHCE` 认证，需要先满足红帽认证系统管理员 (RHCSA) 的要求，然后再通过红帽认证工程师 (RHCE) 考试 (EX300) 才可获得
    - RHCE考试
        - `RHCE` 和 `RHCT` 是以实际操作能力为基础的测试项目，主要考察考生在现场系统中的实际能力
        - 考试内容
            - 第一部分：故障排除和系统维护
                - 时间：2个半小时
            - 第二部分：安装和配置
                - 时间：3个小时
    - 相关
        - 版本
            - RHCE 7版本
            - RHCE 8版本

`RHCSA` 、 `RHCE` 、 `RHCA`

- RHCSA、RHCE、RHCA
    - 名词
        - `RHCA` =红帽认证 `架构师`
        - `RHCE` =红帽认证 `工程师`
        - `RHCSA` =红帽认证 `系统管理员`
    - 阶梯架构
        - 

`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

安全组织

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`
- 主页
  - 中文
    - Welcome to OWASP CHINA — OWASP-CHINA
      - http://www.owasp.org.cn
  - 英文
    - OWASP Foundation | Open Source Foundation for Application Security
      - https://owasp.org/

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

安全标准法规流程

TODO：

网络安全 法规

- 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`
  - 相关流程
- 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

网络安全法和等保

此处整理中国的网络安全法律法规。

1994年 《计算机信息系统安全保护条例》

- 1994年 国务院 颁布 **《计算机信息系统安全保护条例》** = `147号令`
  - 规定**计算机信息系统**实行 `安全等级保护`
    - `安全等级` 的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定

2007年 等保1.0

- 2007年 **等保1.0**
  - **《信息安全等级保护管理办法》=等保1.0**
    - 规定了**信息系统**的安全保护等级划分，及如何开展等级保护的实施与管理工作
    - 等级保护1.0规定了等级保护需要完成的
      - 规定动作
        - 定级备案、建设整改、等级测评和监督检查
    - 为了指导用户完成等级保护的 `规定动作` ，在2008年至2012年期间陆续发布了等级保护的一些主要标准，构成等级保护1.0的标准体系

等级保护1.0 主要标准

- 等级保护1.0时期的主要标准如下
  - 信息安全等级保护管理办法 = = `43号文件` = `上位文件`
  - 计算机信息系统安全保护等级划分准则 = `GB17859-1999` = `上位标准`
  - 信息系统安全等级保护实施指南 = `GB/T25058-2008`
  - 信息系统安全保护等级定级指南 = `GB/T22240-2008`
  - 信息系统安全等级保护基本要求 = `GB/T22239-2008`
    - 业内简称： `等保1.0`
  - 信息系统等级保护安全设计要求 = `GB/T25070-2010`
  - 信息系统安全等级保护测评要求 = `GB/T28448-2012`
  - 信息系统安全等级保护测评过程指南 = `GB/T28449-2012`

2017年 网安法

- 2017年 **网安法**
  - 2017年6月1日 **《中华人民共和国网络安全法》**= `网络安全法` = `网安法`
    - 为网络安全等级保护赋予了新的含义，重新调整和修订等级保护1.0标准体系，配合网络安全法的实施和落地，指导用户按照网络安全等级保护制度的新要求，履行网络安全保护义务的意义重大
    - 网络安全法明确

        - 第21条：国家实行网络安全等级保护制度
            - 网络运营者应当按照网络安全等级保护制度的要求，履行一定的安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改
        - 第31条：国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护
    - 作用：网安法为我国有效应对网络安全威胁和风险、全方位保障网络安全提供了上位法依据
    - 法规内容
        - 章节
            - 第一章　总　　则
            - 第二章　网络安全支持与促进
            - 第三章　网络运行安全
                - 第一节 一般规定
                - 第二节 关键信息基础设施的运行安全
            - 第四章　网络信息安全
            - 第五章　监测预警与应急处置
            - 第六章　法律责任
            - 第七章　附　　则
        - 详见
            - 中华人民共和国网络安全法

2018年 网络安全等级保护条例（征求意见稿）

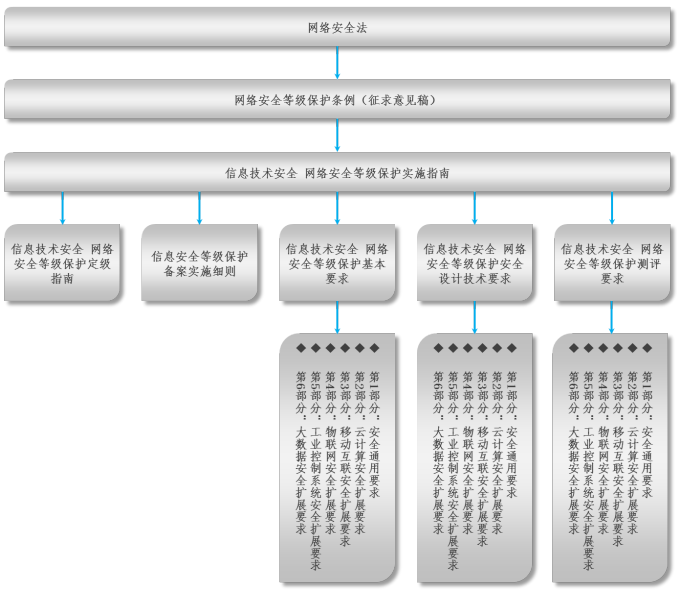
- 2018年 网络安全等级保护条例（征求意见稿）
    - 2018年6月27日，公安部发布
        - **《网络安全等级保护条例（征求意见稿）》**
            - 详见：公安部关于《网络安全等级保护条例（征求意见稿）》 公开征求意见的公告
        - 为深入推进实施国家网络安全等级保护制度，公开征求意见

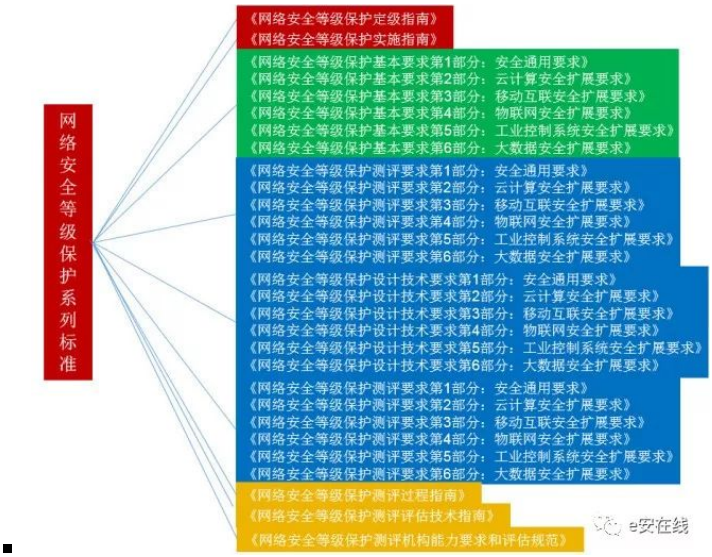
2019年 等保2.0

- 2019年 等保2.0
    - 时间：2019年5月13日正式发布，2019年12月1日开始实施

等级保护2.0标准体系

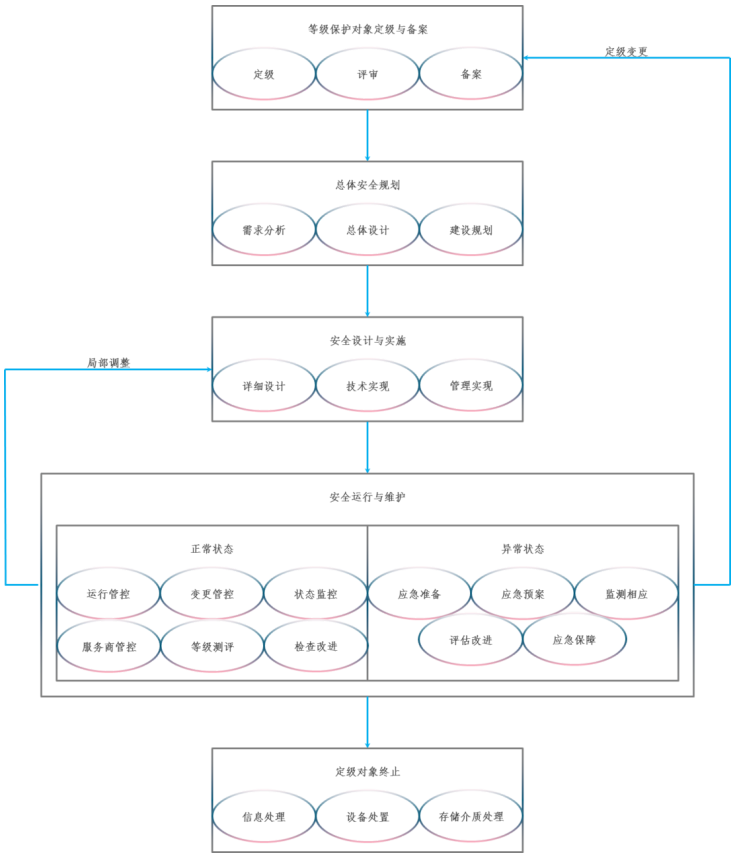
- 等级保护2.0标准体系
    - **等保2.0**是**一系列**标准=法规，称为：**标准体系**
    - 概述
        - 1+N模式
            - 1为通用要求，适用各个行业和各个领域
            - N指具体的一个领域内的扩展要求
                - 目前N为5，分别是

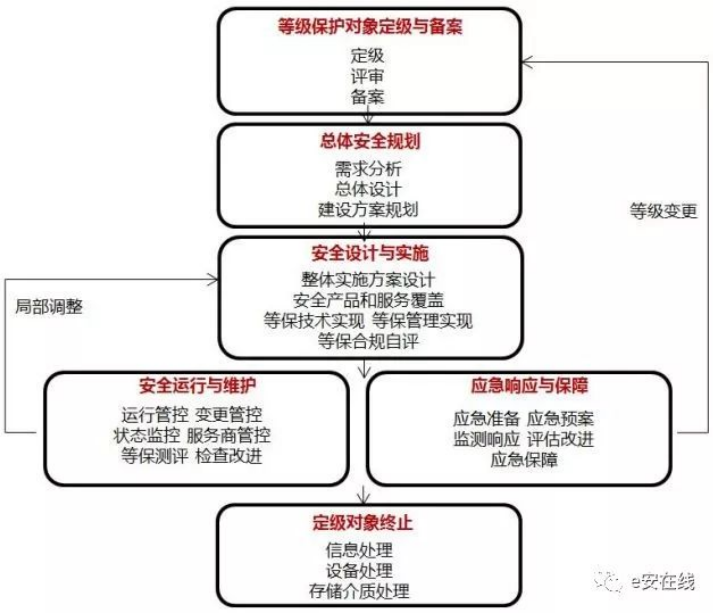
            - 云计算
            - 移动互联
            - 物联网
            - 工业控制
            - 大数据
        - 未来随着技术的发展，N会不断扩展
- 具体包含
    - 其中最核心的是
        - 一个中心，三重防护
            - 一个中心
            - 三重防护
                - 《信息安全技术网络安全等级保护 基本要求》= `GB/T22239-2019`
                - 《信息安全技术网络安全等级保护 测评要求》= `GB/T28448-2019`
                - 《信息安全技术网络安全等级保护 安全设计技术要求》= `GB/T25070-2019`
        - 具体包含
            - 网络安全等级保护条例 = 总要求/上位文件
            - 计算机信息系统安全保护等级划分准则 = 上位标准 = `GB 17859-1999`
            - 网络安全等级保护实施指南 = `GB/T25058-2020`
            - 网络安全等级保护定级指南 = `GB/T22240-2020`
            - 网络安全等级保护基本要求 = `GB/T22239-2019`
                - 业内简称：**等保2.0**
            - 网络安全等级保护设计技术要求 = `GB/T25070-2019`
            - 网络安全等级保护测评要求 = `GB/T28448-2019`
            - 网络安全等级保护测评过程指南 = `GB/T28449-2018`
        - 图 = 等保2.0各标准之间的 关系 = 等保2.0系列标准框架图
            - 



网络安全等级保护实施指南 = `GB/T25058-2020`

- 网络安全等级保护实施指南 = `GB/T25058-2020`
  - 安全等级保护工作实施的基本流程 = 等级保护2.0工作流程图





各国家行业主管或监管部门的监管权力和职责

- 各国家行业主管或监管部门的监管权力和职责具体如下表

序号	具体部门单位	工作职责
1	中央网络安全和信息化领导机构	统一领导网络安全等级保护工作
2	国家网信部门	统筹协调网络安全等级保护工作
3	国务院公安部门	主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫工作
4	国家保密行政管理部门	主管涉密网络分级保护工作，负责网络安全等级保护工作中有关保密工作的监督管理
5	国家密码管理部门	负责网络安全等级保护工作中有关密码管理工作的监督管理
6	国务院其他有关部门	在各自职责范围内开展网络安全等级保护相关工作
7	县级以上地方人民政府	依照本条例和有关法律法规规定，开展网络安全等级保护工作

等保1.0 vs 等保2.0

- 等保1.0 vs 等保2.0 == 等保2.0的主要变化
  - 名称变化
    - `等保1.0`：《信息安全技术 信息系统安全等级保护基本要求》
    - `等保2.0`：《信息安全技术 网络安全等级保护基本要求》
      - 与《网络安全法》保持一致

- 定级对象变化
  - `等保1.0`： (狭义的)**信息系统**
  - `等保2.0`： 更广
    - 概述
      - 扩展成了等级保护对象（信息系统、通信网络设施和数据资源等）
      - 

    - 包含
      - 信息系统
      - 基础信息网络 = **网络基础设施**
        - 广电网、电信网、专用通信网络等
      - 云计算平台 = **云计算平台/系统**
      - 大数据平台 = **大数据平台/系统**
      - 物联网系统
      - 工业控制系统
      - 采用移动互联技术的网络
    - 评价
      - 基于新技术和新手段提出新的分等级的技术防护机制和完善的管理手段是等级保护2.0标准必须考虑的内容
- 各级技术要求
  - `等保1.0`： `物理安全` 、 `网络安全` 、 `主机安全` 、 `应用安全` 和 `数据安全和备份与恢复`
  - `等保2.0`： `安全物理环境` 、 `安全通信网络` 、 `安全区域边界` 、 `安全计算环境` 和 `安全管理中心`
- 各级管理要求
  - `等保1.0`： `安全管理制度` 、 `安全管理机构` 、 `人员安全管理` 、 `系统建设管理` 和 `系统运维管理`
  - `等保2.0`： `安全管理制度` 、 `安全管理机构` 、 `安全管理人员` 、 `安全建设管理` 和 `安全运维管理`
- `等保2.0`
  - 新标准强化了密码技术和可信计算技术的使用
    - 把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求，强调通过密码技术、可信验证、安全审计和态势感知等建立主动防御体系的期望
  - 取消了原来安全控制点的S、A、G标注
  - 增加一个附录A
    - `关于安全通用要求和安全扩展要求的选择和使用`
  - 描述等级保护对象的定级结果和安全要求之间的关系
    - 说明如何根据定级的S、A结果选择安全要求的相关条款，简化了标准正文部分的内容
  - 增加附录
    - 附录C：描述等级保护安全框架和关键技术
    - 附录D：描述云计算应用场景

- 附录E：描述移动互联应用场景
- 附录F：描述物联网应用场景
- 附录G：描述工业控制系统应用场景
- 附录H：描述大数据应用场景

安全保护的等级划分

等级	《信息安全等级保护管理办法》	《网络安全等级保护条例（征求意见稿）》
第一级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。	一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络。
第二级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。	一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络。
第三级	信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。	一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。
第四级	信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。	一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络。
第五级	信息系统受到破坏后，会对国家安全造成特别严重损害。	一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络。

网络安全保护等级（共五级）

安全等级 / 划定因素	一旦受到破坏 会对相关公民、法人和其他组织的合法权益造成损害的严重程度	对国家安全、社会秩序和公共利益的危害程度	网络类型
第一级	损害	不会危害	一般网络
第二级	严重损害	对社会秩序和公共利益危害 / 不会危害国家安全	一般网络
第三级	特别严重损害	严重危害	重要网络
第四级		社会秩序和公共利益特别严重危害 / 对国家安全造成严重危害	特别重要网络
第五级		对国家安全造成特别严重危害	极其重要网络

等保2.0 主要标准的框架和内容

- 等保2.0 主要标准的框架和内容
  - 主要标准的框架和内容
    - 标准的框架结构
      - 《GB/T 22239-2019》、《GB/T 25070-2019》和《GB/T28448-2019》三个标准采取了统一的框架结构
      - 安全通用要求细分为技术要求和管理要求。其中技术要求包括 `安全物理环境` 、 `安全通信网络` 、 `安全区域边界` 、 `安全计算环境` 和 `安全管理中心` ；管理要求包括 `安全管理制度` 、 `安全管理机构` 、 `安全管理人员` 、 `安全建设管理` 和 `安全运维管理`
    - 安全通用要求
      - 安全通用要求针对共性化保护需求提出，无论等级保护对象以何种形式出现，需要根据安全保护等级实现相应级别的安全通用要求。安全扩展要求针对个性化保护需求提出，等级保护对象需要根据安全保护等级、使用的特定技术或特定的应用场景实现安全扩展要求。等级保护对象的安全保护需要同时落实安全通用要求和安全扩展要求提出的措施
        - 安全物理环境
          - 针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护
        - 安全通信网络
          - 针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网等；涉及的安全控制点包括网络架

构、通信传输和可信验证。
    - 安全区域边界
        - 针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证
    - 安全计算环境
        - 针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护
    - 安全管理中心
        - 针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控
    - 安全管理制度
        - 针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订
    - 安全管理机构
        - 针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查
    - 安全管理人员
        - 针对人员管理提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理
    - 安全建设管理
        - 针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理
    - 安全运维管理
        - 针对安全运维过程提出的安全控制要求，涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理
- 安全扩展要求
    - 安全扩展要求是采用特定技术或特定应用场景下的等级保护对象需要增加实现的安全要求。《GB/T 22239-2019》提出的安全扩展要求包括云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求
        - 云计算安全扩展要求是针对云计算平台提出的安全通用要求之外额外需要实现的安全要求。主要内容包括 基础设施的位

置 、 虚拟化安全保护 、 镜像和快照保护 、 云计算环境管理 和 云服务商选择 等

- 移动互联安全扩展要求是针对移动终端、移动应用和无线网络提出的安全要求，与安全通用要求一起构成针对采用移动互联技术的等级保护对象的完整安全要求。主要内容包括 无线接入点的物理位置 、 移动终端管控 、 移动应用管控 、 移动应用软件采购 和 移动应用软件开发 等
- 物联网安全扩展要求是针对感知层提出的特殊安全要求，与安全通用要求一起构成针对物联网的完整安全要求。主要内容包括 感知节点的物理防护 、 感知节点设备安全 、 网关节点设备安全 、 感知节点的管理 和 数据融合处理 等
- 工业控制系统安全扩展要求主要是针对现场控制层和现场设备层提出的特殊安全要求，它们与安全通用要求一起构成针对工业控制系统的完整安全要求。主要内容包括 室外控制设备防护 、 工业控制系统网络架构安全 、 拨号使用控制 、 无线使用控制 和 控制设备安全 等

不同等级网络运营者的安全保护义务

不同等级网络运营者的安全保护义务		
所有等级的网络运营者	一般安全保护义务 （第二十条）	确定网络安全等级保护工作责任人，建立网络安全等级保护工作责任制等
	自查工作 （第二十五条）	每年对本单位落实网络安全等级保护制度情况和网络安全状况至少开展一次自查
	数据和信息安全保护 （第三十一条）	建立并落实重要数据和个人信息安全保护制度、建立异地备份恢复等技术措施等
	新技术新应用风险管控（第三十三条）	采取措施，管控云计算等新技术、新应用带来的安全风险，消除安全隐患
第三级以上网络的运营者	特殊安全保护义务 （第二十一条）	对网络安全管理负责人和关键岗位的人员进行安全背景审查，落实持证上岗制度等
	等级测评 （第二十三条）	每年开展一次网络安全等级测评，并将测评结果等向公安机构报告
	产品服务采购使用的安全要求 （第二十八条）	应当采用与其安全保护等级相适应的网络产品和服务等
	技术维护要求 （第二十九条）	应当在境内实施技术维护，不得境外远程技术维护
	监测预警和信息通报 （第三十条）	建立健全网络安全监测预警和信息通报制度，向同级公安机关和行业主管部门报送监测预警信息，报告网络安全事件
	应急处置要求 （第三十二条）	制定网络安全应急预案，定期开展网络安全应急演练等
新建的第二级网络	上线检测 （第二十二条第一款）	按照网络安全等级保护有关标准规范进行测试
新建的第三级以上网络	上线检测 （第二十二条第二款）	委托网络安全等级测评机构按照网络安全等级保护有关标准规范进行等级测评

网络安全法相关解析

网络安全法明确等级保护工作重点

- 网络安全法 中 等级保护 相关解析
  - 《网络安全法》第二十一条说明如下：
    - > 第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

    - 解读：本条规定的是网络运营者的义务。条款提到的网络安全等级保护制度与公安部运营多年的信息系统安全等级保护制度（即等级保护1.0）有非常大的关联，也说明国家会修订和出台相关 `网络安全等级保护` 的相关配套制度（即等级保护2.0），目前等级保护2.0标准体系的修订工作已基本完成，近期即将出台。
    - > （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
    - 解读：一般第一主要责任人是单位一把手，厅长、局长、院长、校长等领导，第二主要责任人是单位具体分管信息化、分管网络安全的领导，副厅长、副局长、副院长、副校长或总工等
    - > （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施
    - 解读：一般来说 `防火墙` 、 `IDS` 、 `IPS` 、 `防病毒网关` 、 `杀毒软件` 和 `防DDOS攻击系统` 等属于这类技术措施
    - > （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月
    - 解读：网络审计、行为审计、运维审计、日志管理分析、安全管理平台和态势感知平台等都属于这类技术措施
    - > （四）采取数据分类、重要数据备份和加密等措施
    - 解读：数据安全越来越重要，等保方案需要充分考虑数据备份、数据传输和数据存储安全等内容
    - > （五）法律、行政法规规定的其他义务
    - 通过以上解读，了解了网络安全法明确等级保护工作的重点，接下来再聊聊网络安全法如何明确等级保护工作的核心

网络安全法明确等级保护工作核心

- 关键信息基础设施标准体系框架如下
  - 关键信息基础设施保护条例（征求意见稿）（总要求/上位文件）
  - 关键信息基础设施安全保护要求（征求意见稿）
  - 关键信息基础设施安全控制要求（征求意见稿）
  - 关键信息基础设施安全控制评估方法（征求意见稿）

1. 关键信息基础设施的定义

- > 第三十一条 国家公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定
- 解读：等级保护工作的核心是关键信息基础设施，本条首先定义了什么是关键信息基础设施。国家互联网信息办公室已于2017年7月发布《关键信息基础设施安全保护条例（征求意见稿）》，参照网络安全法和关键信息基础设施安全保护条例等法律法规要求
- 关键信息基础设施的认定可参照下表

关键信息基础设施种类	认定标准	网络安全事件的潜在影响
网站类	1）县级(含)以上党政机关网站。 2）重点新闻网站。 3）日均访问量超过 100 万人次的网站。 4）一旦发生网络安全事故，可能造成右边列影 响之一的。 5）其他应该认定为关键信息基础设施。	1）影响超过 100 万人工作、生活； 2）影响单个地市级行政区 30%以上人口的工作、生活；3）造成超过 100 万人个人信息泄露； 4）造成大量机构、企业敏感信息泄露； 5）造成大量地理、人口、资源等国家基础数据泄露； 6）严重损害政府形象、社会秩序，或危害国家安全。
平台类	1）注册用户数超过 1000 万，或活跃用户(每 日至少登陆一次)数超过 100 万。 2）日均成交订单额或交易额超过 1000 万元。 3）一旦发生网络安全事故，可能造成右边列 影响之一的。 4）其他应该认定为关键信息基础设施。	1）造成 1000 万元以上的直接经济损失； 2）直接影响超过 1000 万人工作、生活； 3）造成超过 100 万人个人信息泄露； 4）造成大量机构、企业敏感信息泄露； 5）造成大量地理、人口、资源等国家基础数据泄露； 6）严重损害社会和经济秩序，或危害国家安全。
生产业务类	1）地市级以上政府机关面向公众服务的业务 系统，或与医疗、安防、消防、应急指挥、 生产调度、交通指挥等相关的城市管理系统。 2）规模超过 1500 个标准机架的数据中心。 3）一旦发生网络安全事故，可能造成右边列影响之一的。 4）其他应该认定为关键信息基础设施。	1）影响单个地市级行政区 30%以上人口的工作、生活； 2）影响 10 万人用水、用电、用气、用油、取暖或交通出行等；3）导致 5 人以上死亡或 50 人以上重伤； 4）直接造成 5000 万元以上经济损失； 5）造成超过 100 万人个人信息泄露； 6）造成大量机构、企业敏感信息泄露； 7）造成大量地理、人口、资源等国家基础数据泄露； 8）严重损害社会和经济秩序，或危害国家安全。

2．关键信息基础设施的安全保护义务

- > 第三十四条 运营者设置专门机构和负责人、网络安全教育培训、容灾备份、应急预案和演练等
- 解读：本条款说明关键信息基础设施的保护要求高于网络安全等级保护制度的一般要求，从制度、培训、灾备、应急等方面提出了进一步要求
- > 第五十九条 运营者拒不改正或导致危害网络安全的，罚款10-100万元，直接责任人罚款1-10万元 3．敏感信息保存
- > 第三十七条 境内收集产生的个人信息和重要数据应当在境内存储。确需向境外提供的，应进行安全评估
- 解读：本条是外企和有海外业务的国内企业很关注的一条。主要是关于数据境内存储和境外数据流动的问题。核心是数据安全。这里有两个关键词，一个是 `重要数据` ，什么是重要数据，相关的常见提法还有 `业务数据` 、 `运营数据`` 、`服务数据` 、 `个人数据` 、 `企业数据` 、 `国家数据` ，专家认为，重要数据是从影响因子的权重来区分数据，是一种新的数据分类方式，而不是从用途和归属的角度去分类。另一个关键词是 `安全评估` ，这个安全评估的方式是将来要出台的配置制度。相关问题也并不清晰，例如评估对象的问题，是对要流向境外的数据进行评估?还是对业务的模式进行评估?还有谁来评估的问题，是主管单位来评估，还是运营者自己进行评估? 本条说明了将来会出台 `向境外提供关键信息基础设施重要数据的安全评估办法` 。
- > 第六十六条 运营者违反规定的，没收违法所得，罚款5-50万元，吊销执照，直接责任人罚款1-10万元 4．风险检测评估
- > 第三十八条 运营者每年至少组织一次安全风险检测评估，并评估情况和改进措施报相关部门

- 解读：本条主要是关于对关键信息基础设施年度检测评估的问题。这里提到了网络安全服务机构，就是我们常说的提供风险评估等各类安全服务的机构，这些机构以后又多了一项业务了
- > 第五十九条 运营者拒不改正或导致危害网络安全的，罚款10-100万元，直接责任人罚款1-10万元

其他数据和信息保护相关法规

- 2019年版《**个人信息安全规范**（征求意见稿）》
- 2019年5月28日，国家互联网信息办公室发布 《**数据安全管理办法**（征求意见稿）》
- 2017年4月11日，国家互联网信息办公室发布 《**个人信息出境安全评估办法**（征求意见稿）》
  - 借鉴了
    - 2018年5月25日，欧盟发布的 `GDPR` = `General Data Protection Regulation` **=通用数据保护条例**
- 2019年8月22日国家互联网信息办公室发布 《**儿童个人信息网络保护规定**》

安全标准

ISO27001

TODO:

【整理】信息安全管理体系 ISO27001

安全流程

SDL

TODO:

【整理】SDL 安全

附录

下面列出相关参考资料。

参考资料

- Web安全攻防流程和常用概念 | ProcessOn免费在线作图
-
- 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
- 为什么要换掉传统Web应用防火墙 (WAF)？ - 安全内参 | 决策者的网络安全知识库 (secrss.com)
- Application firewall - Wikipedia
- Web application firewall - Wikipedia
- 360浏览器：中国为什么没有自主研发的浏览器内核？|浏览器|360|自主研发*新浪科技*新浪网 (sina.com.cn)
- 用户研究之「用户画像」的建立 | 产品壹佰 (chanpin100.com)
- 【绿盟大讲堂】渗透测试流程解析 – 绿盟科技技术博客
- 未知的未知：九大模糊测试工具 - 安全牛
- 谷歌开源模糊测试工具 ClusterFuzz 尝鲜记录 (进行中) · TesterHome
- 《网络安全法》实施：实现网络安全的法治保障-中共中央网络安全和信息化委员会办公室
- 中华人民共和国网络安全法
- 2019年《网络安全法》立法进展与执法重点回顾 | China Law Insight
- 网络安全等级保护2.0标准解读
- 网络安全法与等级保护二者关系浅析
- 《网络安全等级保护条例（征求意见稿）》之重点解读 - 专业文章 - 锦天城律师事务所
- 网络安全之等保2.0与等保1.0的区别解读 - 知乎
- 等保合规安全解决方案-安全等级保护-阿里云
- 《网络安全等级保护条例（征求意见稿）》解读-深信服

- OWASP Top Ten Web Application Security Risks | OWASP
- OWASP Foundation | Open Source Foundation for Application Security
- 第十一章 蜜罐和蜜网 · 网络安全
- 第九章 入侵检测 · 网络安全
- IETF RFCs: RFC4765 The Intrusion Detection Message Exchange Format (IDMEF). H. Debar, D. Curry, B. Feinstein. March 2007.
- IETF RFCs: RFC4766 Intrusion Detection Message Exchange Requirements. M. Wood, M. Erlinger. March 2007.
- IETF RFCs: RFC4767 The Intrusion Detection Exchange Protocol (IDXP). B. Feinstein, G. Matthews. March 2007.
- 网络安全 黄玮
- 国家标准 - 全国标准信息公共服务平台
- 第八章 防火墙 · 网络安全
- Kali Metapackages | Penetration Testing Tools
- 为什么招聘单位都要求你有ITIL证书，你知道吗？ - 知乎
- 为什么拥有ITIL证书，招聘单位抢着要你？ - 华为云
- ITIL认证有几种？哪些人可以进行ITIL认证?
- ITIL Certifications | AXELOS
- ITIL 4: ITSM gets agile | InsiderPro
- ITIL certification guide: Costs, requirements, levels and paths | CIO
- ITIL® 4 Foundation Certification Training Course
- What is ITIL V3? | ITIL Framework | Try Freshservice
- AXELOS announces discontinuation of ITIL v3
- 红帽认证工程师
- 关于RHCE认证的简介 - 华为云
- 深度评解红帽RHCSA、RHCE、RHCA认证。 | 《Linux就该这么学》
- 红帽认证工程师常见问题解答