https://github.com/DiaosSama/SCUT_IS_Study

第一章 绪论

1.1 网络空间安全概述

1. 网络空间
    - 定义：构建在信息通信技术基础设施之上的人造空间，用以支撑人们在该空间中开展各类与信息通信技术相关的活动
    - 组成要素：**载体、资源、主体和操作**
2. 网络空间安全：包括网络空间中电磁设备、信息通信系统、运行数据、系统应用中所存在的所有安全问题

1.2 网络安全防护

1. **网络安全属性（*）：**
    - 完整性（integrity）：未经授权不能改变
    - 保密性（confidentiality）：不被泄露给未经授权者
    - 可用性（availability）：
        - 可被授权者访问并按需求使用
        - 即保证合法用户对资源的使用不会被不合理拒绝
    - 可控性（controllability）：对信息的传播及内容具有控制能力
    - 不可否认性（non-repudiation）：
        - 不可抵赖性，及所有参与者都不可能否认或抵赖曾经完成的操作和承诺
        - 发送方不能否认已发送的信息，接收方也不能否认已收到的信息
    - 可靠性（reliability）：信息系统能够在规定时间内和规定条件下完成规定功能
2. 网络安全威胁
    - 广义定义：一切影响网络正常运行的因素
    - 构成威胁的因素：
        - 环境和灾害因素
        - 人为因素：
            - 有意：人为攻击、违法犯罪
            - 无意：工作疏忽造成失误
        - 系统自身因素（硬件、软件、网络和通信协议）
3. 网络安全防护
    - 网络安全防护体系：有机结合组织管理体系、技术标准体系和技术防护体系三个方面
        - 组织管理体系：组织机构、人员编制、职责分工、教育培训
        - 技术标准体系：行政法规、技术标准与规范
        - 技术防护体系：物理安全、信息安全
4. 网络安全防护技术的发展
    - 第一代：以保护为目的：试图在网络边界上阻止非法入侵
    - 第二代：以保障为目的：以检测技术为核心、恢复技术为后端。如果挡不住，至少能发现
    - 第三代：以顽存（可生存）为目的：系统遭受攻击时，仍具有可在一定时间内继续执行关键使命的能力，入侵容忍

1.3 网络攻击技术

1. 网络攻击分类：被动攻击、主动攻击
2. 因特网容易被攻击者利用的特性：
    - 资源共享与分组交换
        - 用户共享所有资源，给予一个用户的服务会受其他用户的影响
        - 攻击数据包在被判断是否恶意之前都会被转发到受害者
        - 路由分散决策，流量无序
    - 认证与可追踪性
        - 缺乏认证机制，一个终端接入即可访问全网
        - 通常路由器不具备数据追踪功能
    - 尽力而为
    - 匿名与隐私
    - 对全球网络基础设施的依赖
3. **网络接口层协议**

- IEEE 802.3以太网：
    - 缺陷：没有提供报文完整性和源地址的认证
    - 攻击：恶意节点以高速率发送大量广播报文，耗尽网络带宽，进行拒绝服务攻击
    - 定位难：可不断变换源MAC地址逃避追踪

4. **网络层协议**

- IPv4协议：
    - 缺陷：无状态、无认证
        - 无认证导致包中的内容几乎都可以伪造，可以用于会话劫持、中间人攻击、伪造攻击等
        - IP无状态，分片功能可用来绕过防火墙和入侵检测，还可以用于攻击不能正确处理分片异常的主机
        - 寻址与协议选项会泄露部分网络拓扑信息，可用于网络侦查
        - 无访问控制和带宽控制
- ICMP协议
    - 目的：提高IP数据包交付成功的机会，允许主机或路由器报告差错情况和提供有关异常情况的报告
    - 分类：ICMP差错报告报文、ICMP询问报文
    - 缺陷：
        - 利用目的站不可到达对目标发起拒绝服务攻击
        - 利用改变路由报文破坏路由表
        - 利用ICMP进行隐蔽通信
        - 利用回送请求或回答报文进行网络扫描或DoS
    - 攻击方法：主机探测、Ping of Death攻击、Smurf攻击、重定向攻击
- ARP协议
    - 用于将计算机的IP地址转化为物理地址
    - 缺陷：缺乏相应的认证机制，导致用户无法辨别ARP报文的真实性
        - 支持不请自来的请求
        - 允许未经请求的ARP广播或单播对缓存条目的更新
        - ARP表可以远程更新并且ARP无法验证更新消息的真实性
        - 代理ARP可以被利用

    - 攻击方法：拒绝服务攻击，中间人攻击，MAC泛洪，网络监听
- RARP协议
    - 缺陷：被上层协议（DHCP、BOOTP）利用，允许主机通过DHCP和BOOTP服务自动配置自己的IP地址，缺乏必要的验证机制
    - 攻击方法：中间人攻击

5. **传输层协议**

- TCP协议
    - 缺陷：缺乏认证机制和报文的完整性检查
    - 攻击方法：通过伪造TCP报文进行各种攻击
        - 网络扫描：利用TCP连接请求
        - SYN Flood攻击：TCP连接数有限，DoS攻击
        - LAND攻击：TCP连接数有限，DoS攻击
        - 序列号猜测：会话劫持
    - UDP协议
        - 缺陷：无连接性，没有任何认证机制和拥塞控制机制，容易伪造数据包
        - 攻击方法：
            - UDP泛洪攻击
            - Fraggle攻击：与Smurf攻击类似
            - Trinoo攻击

6. **应用层协议**
    - POP3协议：用户名密码以明文形式传输，容易被窃听
    - DNS协议：缺乏密码认证机制，可对DNS服务器发动攻击
    - FTP协议：简单的用户名密码认证机制
    - Telnet协议：用户名和口令明文传输
7. 网络攻击过程：
    - 目标踩点
    - 远端扫描
    - 资源列举
    - 权限获取
    - 权限提升
    - 设置后门
    - 毁踪灭迹
8. APT攻击
    - APT，即高级持续性威胁，是一种针对特定对象，长期、有计划、有组织的网络攻击行为

第三章 网络侦查技术

3.1 概述

1. 网络侦查：收集目标主机系统和计算机网络安全相关信息的过程
2. 网络侦查收集的信息：
    - 静态信息：
        - IP地址（段）、名字和域名
        - 联系信息，包括姓名、邮件地址、电话号码
        - DNS、邮件、Web服务器
        - 拓扑结构...

- 动态信息
  - 目标主机是否开机
  - 是否安装了某种你感兴趣的软件
  - 是什么操作系统
  - 是否有某种安全漏洞

3.2 网络侦查方法

1. 搜索引擎信息收集
2. shodan.io、zoomeye.org
3. **Whois数据库查询**
   - 互联网上各类型的Whois数据库充当了互联网白皮书列表的角色，由不同的注册商和特定的互联网基础设施组织所维护
   - 可获取的信息包括：
     - 已注册域名的拥有者信息
     - 域名登记人信息
     - 联系方式
     - 域名注册时间和更新时间
     - 权威DNS的IP地址
   - 查询目标域名的注册机构
     - .com/.net/.org/.edu/.info等站点：查询互联网网络信息中心（InterNIC）的whois数据库
     - 非以上站点：查询Uwhois站点（包含246个国家注册机构）
     - 美国军事组织：http://www.nic.mil/dodnic
     - 美国政府组织：http://www.dotgov.gov/whois.aspx
   - 查询目标域名的详细注册资料
     - 通过注册机构查询，找到目标的具体注册机构的whois库
     - 全球最大的注册机构为Network Solution
4. DNS信息查询
   - 域名查询的解析操作由多个DNS服务器来提供，从而提高可用性和容错性
   - DNS服务器之间采用区传送的机制类同步和复制区内数据
   - 区传送安全问题：传输的域名信息中包含了不该公开的内部主机和服务器的域名信息，从而将内部主机名和IP地址暴露给了攻击者。
   - 区传送查询工具：nslookup
5. 网络拓扑发现
   - 查明目标网络的拓扑结构有利于找出目标网络的关键节点，提高攻击效率
   - 工具：Traceroute
6. **社会工程学**
   - 是一种利用人的弱点（如人的本能反应、好奇心、信任、贪婪等）进行诸如欺骗、伤害等危害手段，获取自身利益的手法
   - 社会工程学的实施者（称为社会工程师）必须掌握心理学、人际关系学和行为学等知识和技能，以便收集和掌握实施入侵所需要的相关资料与信息
   - 常见形式：
     - 伪装：伪造的Web站点
     - 引诱：执行具有诱惑性同时具有危害性的附件
     - 恐吓：散布诸如安全警告、系统风险之类的信息
     - 说服：企业咨询帮助人员为来人来电提供帮助
     - 欺骗：电话欺骗

        - 渗透：表面上看起来毫无用处的信息都会被他们利用来进行系统渗透

3.3 网络侦查防御

1. 防御搜索引擎和基于Web的侦查
    - Web服务器建立信息披露策略（不在Web站点上放置敏感信息）
    - 要求职工不在公共渠道发布系统配置、商业计划和其他敏感话题信息
    - 发现搜索引擎把一个不期望公开的URL或页面进行了索引，可以要求搜索引擎将它们移出
2. 防御WHOIS检索
    - 保证记录中没有额外可供攻击者使用的信息，例如管理员的账户名
    - 对员工进行培训，避免误中社会工程学攻击诡计
3. 防御基于DNS的侦查
    - 确保没有通过DNS服务器泄露额外的信息
    - 限制DNS区域传送
    - 使用DNS分离技术（指在两台不同服务器上分离DNS的功能，外部用户和内部用户分贝使用不同的DNS服务），减少可公开获得的基础设施的DNS信息

第四章 网络扫描技术

4.1 网络扫描的基本概念

1. 网络扫描：使用网络扫描软件对特定目标进行各种试探性通信，以获取目标信息的行为

4.2 主机发现

1. 概念：向目标主机发送探测数据包，根据是否收到响应来推断主机的工作状态
2. 方式：
    - 利用ICMP协议进行主机发现（Echo、Non-Echo）
    - 利用IP协议进行主机发现（异常的IP数据报首部、错误的分片）
3. 基于ICMP协议的主机发现
    - Echo扫描：发送ICMP询问报文，等待回复
    - Non-Echo扫描：发送其他类型的ICMP询问报文
    - 问题：
        - 很多防火墙会对ICMP回送报文请求进行过滤，使其无法到达目标主机
4. 基于IP协议的主机发现
    - 主机在收到首部异常的IP数据报时应当返回“参数问题”的ICMP报文
    - 主机由于缺少分片而无法完成IP数据报重组时，主机回应“分片重组超时”的ICMP报文

4.3 端口扫描

1. 端口扫描技术分类：
    - 开放扫描：会产生大量的审计数据，容易被对方发现，但可靠性高
    - 隐蔽扫描：能有效避免入侵检测系统和防火墙的检测，但这种扫描使用的数据包在通过网络时容易被丢弃从而产生错误探测信息
    - 半开放扫描：隐蔽性和可靠性介于两者之间
2. 方法：
    - 开放扫描：TCP Connect扫描（TCP全连接扫描）
    - 半开放扫描：TCP SYN扫描
    - 隐蔽扫描：

        - TCP FIN扫描
        - TCP Xmas扫描
        - TCP Null扫描
        - FTP proxy扫描
3. TCP Connect扫描
    - 尝试同目标端口建立正常的TCP连接（直接调用系统connect()函数）
    - 优点：稳定可靠，不需要特殊的权限
    - 缺点：扫描方式不隐蔽，服务器会记录下客户机的连接行为，容易被溯源
4. TCP SYN扫描
    - 利用三次握手建立TCP连接的原理，发送SYN包初始化一个连接，但并不建立完整的TCP连接
    - 优点：隐匿性好，很少有系统会记录这样的行为
    - 缺点：需要管理员权限才能构造这样的SYN数据包
5. TCP FIN扫描
    - 发送FIN位为1的数据报，若端口关闭，会返回RST报文段，否则无响应
    - 优点：不是TCP建立连接的过程，比较隐蔽
    - 缺点：
        - 与SYN扫描类似，也需要构造专门的数据包
        - 只适用于Unix系统的目标主机，Windows系统总是发送RST报文段
6. Xmas扫描和Null扫描
    - Xmas扫描打开FIN、URG、ACK、PSH、RST、SYN标记，即全部置1
    - Null扫描关闭所有标记，即全部置0
    - 优缺点与TCP FIN扫描相同
7. FTP proxy扫描
    - FTP代理选项允许客户端控制一个FTP服务器向另一个服务器传输数据
    - 利用这一特点可以实现端口扫描的功能
    - 优点：不但难以跟踪，而且可以穿越防火墙
    - 缺点：一些FTP服务器禁止这种特性
8. UDP扫描
    - UDP在通信过程中没有复杂的交互过程，判断主机UDP端口工作状态比较难
    - 方式：主机向目标主机的UDP端口发送UDP数据包，如果目标窗口处于监听状态，将不会作出响应，否则会返回ICMP_PORT_UNREACH错误
    - 优点：目标端口状态不同，对扫描数据包响应不同，区分度很好
    - 缺点：
        - UDP和ICMP数据包通信中可能丢失，判断出错
        - RFC1812：对ICMP错误信息的比例限制
9. **端口扫描的隐蔽性策略：**
    - 调整扫描次序（端口随机扫描）
    - 减缓扫描速度（慢扫描）
    - 对数据包中一些字段进行随机化处理（数据包随机化扫描）
    - 利用虚假的源地址（诱骗）
    - 采用分布式的方法进行扫描（分布式协调扫描）

4.4 操作系统识别

1. 为什么要进行操作系统识别
    - 操作系统不同，可能存在的漏洞也不同
    - 操作系统检测旨在确定目标主机所运行的操作系统，便于采取最有效的攻击方法和手段
2. 操作系统检测方法：
    - 获取旗标信息
    - 利用端口信息
    - 分析TCP/IP协议栈指纹
3. 旗标信息识别
    - 旗标（Banner）：客户端向服务端提出连接请求时服务端所返回的欢迎信息
    - 通过旗标可间接推断主机操作系统
4. 利用端口信息识别
    - 不同操作系统通常会有一些默认开放的服务
    - 例如Windows XP/2003等默认开放TCP135、139、445，而Linux系统通常不使用
5. TCP/IP协议栈指纹识别
    - 根据采集指纹信息的方式分为：主动扫描、被动扫描
    - 主动扫描：
        - 采用向目标系统发送构造的特殊包并监控其应答的方式来识别操作系统类型
        - 优点：速度快、可靠性高
        - 缺点：严重依赖于目标系统网络拓扑结构和过滤规则
        - 分类：
            - FIN探测
            - BOGUS标记探测
            - TCP ISN取样
            - 不分段指示位
            - TCP初始化窗口值
            - ACK值
            - ICMP错误信息终结
            - ICMP消息引用
            - SYN泛洪限度
    - 被动扫描：
        - 通过监听工具收集数据包，再对数据包的不同特征（TCP Window-size、 IP TTL、 IP TOS、DF位等参数）进行分析，来识别操作系统。
        - 优点：基本不具备攻击特征，具有很好的隐蔽性
        - 缺点：其实现严格依赖扫描主机所处的网络拓扑结构；和主动探测相比较，速度慢、可靠性不高

4.5 漏洞扫描

1. 漏洞存在的原因：设计方案或具体实现存在缺陷、配置不当
2. 漏洞扫描的意义：
    - 管理员：及时发现计算机的安全漏洞，以便针对性加固
    - 攻击者：发现目标服务程序或系统可能存在的漏洞，以便发动攻击
3. **扫描方式：向目标发送特定报文，根据响应判断是否存在漏洞**
4. 分类：根据扫描方法不同，漏洞扫描可以分为
    - 基于主机的漏洞扫描

    - 基于网络的漏洞扫描
5. 基于主机的漏洞扫描
    - 在目标系统上安装扫描程序
    - 赋予管理员权限，以确保访问操作系统内核、系统配置文件以及系统中的各类应用程序
    - 扫描程序依据规则对系统进行分析以发现漏洞
    - 对发现的漏洞给出描述信息和补丁方法
6. 基于网络的漏洞扫描
    - 扫描主机和被扫描的目标系统通过网络连接
    - 利用端口扫描结果
    - 模拟简单攻击活动，对目标系统进行具有攻击性的测试
7. **基于网络的漏洞扫描组成**
    - 扫描控制台
    - 漏洞库：核心、经常更新
    - 扫描引擎

第五章 拒绝服务攻击

5.1 概述

1. 拒绝服务攻击
    - 定义：攻击者通过某种手段，有意地造成计算机或网络不能正常运转从而不能向合法用户提供所需要的服务或者使服务质量降低
    - 服务：系统提供的，用户在对其使用中会受益的功能
    - 拒绝服务：任何对服务的干涉如果使得其可用性降低或者失去可用性称为拒绝服务，如：计算机系统崩溃；带宽耗尽；硬盘被填满
    - 攻击方式：消耗系统或网络资源；更改系统配置
2. 分布式拒绝服务攻击
    - 定义：如果处于不同位置的多个攻击者同时向一个或多个目标发起拒绝服务攻击,或者一个或多个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施拒绝服务攻击
    - 特点：攻击来源的分散性、协同性，攻击力度的汇聚性
    - 主要攻击对象：
        - 网站
        - 路由器
        - DNS服务器等网络基础结构
3. 分类
    - 按攻击机制分类，拒绝服务攻击可分为：
        - 剧毒包或杀手包型
        - 风暴型
        - 重定向型

5.2 剧毒包型拒绝服务攻击

1. 概念：利用协议本身或其软件实现中的漏洞，通过一些畸形的数据包使受害者系统崩溃，也称为“漏洞攻击”或“协议攻击”
2. 泪滴攻击（Teardrop）
    - 原理：利用异常的数据分片导致接收方在处理分片数据时崩溃，也称为碎片攻击。
        - 利用Window95/NT/3.1和低版本Linux中处理IP分片的漏洞，发送偏移地址重叠的UDP数据包分片，使目标及其在将分片重组时出现异常错误

- 利用数据报分片的其他攻击
  - 小片段攻击（变种一）
    - 目的不是DoS，而是用于穿透防火墙
    - 原理：通过很小的片段使得防火墙需要检测的信息进入到下一个片段中
  - 重叠分片攻击（变种二）
    - 目的不是DoS，而是用于穿透防火墙
    - 原理：**防火墙在处理重叠分片时与目标主机系统（受害者主机）之间可能存在差异： 当收到重叠分片时，有的系统是以先到的数据为主，有的系统则是用后到的数据覆盖先前的数据**
  - 通过分片导致防火墙或IDS的拒绝服务（变种三）
    - 原理：有些防火墙或IDS为了检测碎片攻击或其他类型的利用分片的攻击而设置了碎片重组：当收到分片数据包时并不单独检测，而是等待所有的分片都到达（必须缓存已到的分片），重组完成后再检测。
    - 攻击：攻击者伪造并发送大量的分片，但却不让这些分片构成完整的数据报以此占用防火墙或IDS的CPU和存储单元，构成DoS攻击

3. Ping of Death攻击
   - 原理：利用协议实现漏洞[CVE-1999-0128]，向受害者发送超长的Ping数据包（超过65507B的ICMP数据包），导致受害者系统异常
   - 66607B怎么来的?
     - IP数据包最大不超过64KB（65535B）
     - IP报头>=20B，ICMP报头>=8B，数据部分<=65535-20-8=65507B
4. Land攻击
   - 原是一段C程序，其功能是向受害者发送TCP SYN包，这些包的源IP地址和目的IP地址被伪造成受害者的IP地址，源端口和目的端口也是相同的，目标系统在收到这样的包以后可能会挂起、崩溃或重启
5. 循环攻击
   - 也称为振荡攻击或乒乓攻击
   - 原理：当两个都会产生输出的端口(可以是一个系统 / 一台机器的两个端口，也可以是不同系统 / 机器的两个端口)之间建立连接以后，第一个端口的输出成为第二个端口的输入，导致第二个端口产生输出，同时第二个端口的输出又成为第一个端口的输入，如此，一两个端口间将会有大量的数据包产生，导致拒绝服务

5.3 风暴型拒绝服务攻击（*）

1. 概念：通过大量“无用”数据包占用过多的资源以达到拒绝服务的目的，也称为“带宽攻击”
2. 分类：
   - 直接风暴型攻击
   - 反射攻击
3. 风暴型拒绝服务攻击一般包含3个步骤：
   - 攻击者使用扫描工具探测扫描寻找一台或多台主机作为入侵目标，安装攻击handler
   - 攻击者在handler上使用扫描工具扫描大量主机寻找入侵目标，并设法通过handler入侵有安全漏洞的主机并获取控制权。在被攻陷的系统中安装并运行DoS的攻击代理（Agent）
   - 攻击者通过handler通知agent攻击的目标和类型，在收到攻击指令后，Agent发起真正的攻击
4. 风暴型攻击所使用的分组
   - TCP洪流（Floods）：向目标主机发送大量设置了不同标志的TCP分组，常被利用的标志包括：SYN，ACK，RST
   - ICMP Echo请求/响应报文（如Ping Floods）：向目标主机发送大量的ICMP分组
   - UDP洪流：向目标主机发送大量各种基于UDP协议的应用协议包（如NTP，SSDP，DNS等）

5. 直接风暴型攻击
    - Ping风暴攻击
        - 原理：利用控制的大量主机向受害者发送大量ICMP回应请求消息，使受害者忙于处理而降低性能
        - 优点：简单有效
        - 缺点：需要大规模僵尸网络的支持，大多防火墙会过滤ICMP包
    - SYN Flood攻击
        - 原理：发送大量SYN报文，但对服务器的应答报文不做应答，造成服务器维护大量的半连接列表，小号服务器半连接资源的攻击方式
        - 需要伪造地址，一方面逃避追踪，另一方面为了攻击能成功
    - TCP连接耗尽型攻击
        - 原理：通过众多TCP连接耗尽受害者资源
        - 与SYN Flood攻击的区别：不需要不停地向受害者发起连接
    - UDP风暴攻击
        - 原理：向目标主机连续发送大量较长的UDP数据包，占用网络带宽，达到阻塞网络的目的
        - **典型：Trinoo攻击**
    - HTTP风暴型攻击
        - 原理：用HTTP协议对网页进行语义上合法的请求，不停地从受害者处获取数据，占用连接的同时占用带宽
        - 缺点：一般需要使用真实的IP地址
    - 对邮件系统的DoS攻击
        - 邮件炸弹：往一个邮件地址或邮件服务器发送大量相同或不同的邮件，耗尽其存储空间
        - 垃圾邮件：不请自来的邮件，目的在于宣传，而不是攻击，但由于数量众多，常常造成与DoS同样的效果
6. 反射型拒绝服务攻击
    - 原理：攻击者利用应用层协议，向互联网上大量开放特定服务的服务器发送请求数据包，其中源IP地址被伪造成攻击目标的IP地址，这些开放特定服务的服务器在此攻击过程中也被称为反射节点，当反射节点收到请求数据包后，则将应答数据包发送给攻击目标，当大量应答数据包到达时，即形成对攻击目标的DDoS攻击
    - NTP反射式拒绝服务攻击
        - NTP： Network Time Protocol，网络时间协议，用于计算机间时间同步（利用UDP 123端口）
    - **Smurf攻击：**
        - 原理：发送ICMP Echo请求分组，包中源IP地址为目的IP地址，目的IP地址为广播地址
    - **Fraggle攻击：**
        - 与Smurf的区别在于：采用的是UDP Echo（Fraggle）消息而不是PING消息
7. 僵尸网络
    - 定义：僵尸网络（Botnet）是**僵尸主人（BotMaster）**通过命令与控制信道（C&C）控制具有协调性的恶意计算机群
        - 被控制的计算机称为**僵尸主机（Zombie，肉鸡）**
        - 僵尸主人用来控制僵尸主机的计算机称为**僵尸程序（Bot）**
        - 一对多的控制关系使得攻击者以极低的代价高效控制大量资源为其服务
    - 分类：**IRC僵尸网络和P2P僵尸网络**
    - IRC僵尸网络结构：
        - 基于标准IRC协议**在IRC聊天服务器上构建命令与控制信道**，控制者通过它实现对大量受控主机的僵尸程序版本更新、发动攻击等

- P2P僵尸网络结构：
  - 网络中每台僵尸主机都与该僵尸网络中的某一台或某几台僵尸主机存在连接

5.5 拒绝服务攻击的检测及响应技术（*）

1. DoS攻击检测技术
   - 依据DDoS攻击的特征标志检测
     - 特定端口：trinoo使用TCP端口27655，UDP端口27444和31335；NTP是123端口
     - 标志位：Shaft攻击所用的TCP分组的序列号都为0x28374839
     - 特定数据内容
   - 依据异常流量来检测
     - 大量目标主机域名解析
     - 极限通信流量：DDoS攻击一个站点时，会出现明显超出该网络正常工作时极限通信流量的现象
     - 特大型的ICMP和UDP数据包
     - 不属于正常连接通信的TCP和UDP数据包
     - 数据段内容特征：只包含文字和数字字符
2. DoS攻击响应技术

   现有的对付DDoS攻击的方案主要有四种
   - 分组过滤：通过丢弃恶意分组的方法保护网络
     - 对特定流量进行过滤丢弃
     - 输入诊断：与ISP配合
   - 源端控制：在源端控制DDoS攻击
     - 过滤假冒的IP地址
   - 追溯：追溯攻击的源端，然后阻止它发起新的攻击
     - 追溯攻击源
   - 路由器动态检测和控制：路由器动态监测流量并进行控制
     - 流量清洗

第六章 特洛伊木马

6.1 恶意代码

1. 恶意代码（又称恶意软件）
   - 定义：指在不为人知的情况下侵入用户的计算机系统，破坏系统、网络、信息的保密性、完整性和可用性的程序或代码
   - 形式：计算机病毒、蠕虫、木马程序、逻辑炸弹、Rootkit、后门
2. 计算机病毒：
   - 定义：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者损坏数据、影响计算机使用，并能自我复制的一组计算机指令或者程序代码。
   - **特征（*）：**
     - 传染性
     - 潜伏性
     - 触发性
     - 寄生性：一般寄生在两类地方：文件或硬盘引导扇区
     - 非授权执行性特征
     - 破坏性
   - **结构（*）：**

计算机病毒一般由引导模块、搜索模块、感染模块和标识模块五个模块组成

- 引导模块：负责完成病毒运行所需请求内存、修改系统中断等准备工作
- 搜索模块：发现或定位病毒的感染对象，决定病毒的扩散能力
- 感染模块：是计算机病毒的核心模块，实现自我繁殖
- 表现模块：设定触发条件以及病毒触发后执行的具体操作
- 标识模块：设置病毒签名，避免重复感染

3. 计算机蠕虫：
   - 定义：一种可以独立运行，并通过网络传播的恶意代码
   - 与计算机病毒的比较

项目	病毒	蠕虫
存在形式	代码片段	独立个体
复制机制	插入到宿主程序	自身的复制
传染机制	宿主的运行	系统存在漏洞
攻击目标	本地文件系统	网络上的计算机
使用者角色	病毒传播的关键	无关
防治措施	从宿主文件中清除	打系统补丁

   - **结构（*）：**
     - 搜索模块：自动运行，寻找满足感染条件的目标
     - 攻击模块：自动攻击搜索模块找到的对象，取得权限，建立传输通道（如远程Shell）
     - 传输模块：负责蠕虫程序复制
     - 负载模块：搜集信息、清理现场和攻击破坏等
     - 控制模块：调整蠕虫行为，控制被感染主机，执行蠕虫编写者下达的指令
   - 影响传播速度的因素
     - 潜在脆弱目标的数量
     - 漏洞主机被发现的速度
     - 蠕虫自身复制的速度
4. 特洛伊木马：
   - 定义：特洛伊木马是一段能实现有用的或必须的功能的程序，但是同时还完成一些不为人知的功能
   - 分类：
     - 密码窃取型木马
     - 投放器型木马
     - 下载型木马
     - 监视型木马
     - 代理型木马
     - 点击型木马
     - 远程控制型木马
   - **远程控制木马的入侵（*）**
     1. 配置木马
        - 定制木马：定制端口，确定木马在哪个端口监听
        - 信息反馈：设置信息反馈的方式
        - 隐蔽性设置：文件名称、隐藏手段
     2. 传播木马

传播途径主要有：

- Email捆绑、欺骗
- 网页挂马
- 应用软件捆绑、欺骗
- 利用漏洞攻击
- 即时通讯软件捆绑、欺骗

3. 运行木马
   - 触发条件
   - 启动木马
   - 进入内存
   - 开启端口
4. 信息反馈

   反馈相关信息给配置和传播木马的控制者，包括：
   - 受害主机的IP地址
   - 系统软硬件信息
   - 口令信息
   - 共享资源信息
5. 建立连接
   - 正向连接：客户端连接服务端
   - **反向连接：由木马的服务端主动连接客户端**
     - 优点：
       - 解决动态IP地址的问题
       - 解决内网地址的问题
       - 绕过防火墙的限制
     - 缺点：
       - 容易暴露控制端
   - **改进的反向连接：通过代理服务器获取客户端IP端口，并非保存在服务端上**
6. 远程控制

- 木马植入技术
  - 主动植入：包括本地安装和远程安装
  - 被动植入：网页挂马、钓鱼邮件、软件捆绑下载....
- **木马的隐藏技术（*）**
  1. 木马在加载时的隐藏
     - 目标：在用户不知情的情况下运行木马程序
     - 手段：捆绑欺骗、网页挂马、漏洞攻击...
  2. 木马在存储时的隐藏
     - 隐藏扩展名
     - 修改文件图标
     - Hook截获查看文件的指令
  3. 木马在运行时的隐藏
     - 木马在运行时更容易被发现，所以木马程序格外重视运行阶段的隐藏
     - 手段：
       - 进程列表欺骗（Hook）
       - 利用DLL实现木马隐藏（因为DLL不会出现在进程列表中，使用Rundll或Rundll32方法）

        - 通信隐藏（利用IP协议族中的其他协议进行通讯，比如ICMP）
            - 利用ICMP的潜伏：ICMP协议由内核或进程直接处理，不通过端口
            - 端口复用技术：多个应用在同一合法端口监听，利用合法端口掩护通信（木马程序优先接收，决定自己处理或转发）
            - 端口反弹技术：反向连接、改进的反向连接

第七章 口令攻击技术

7.1 概述

1. 口令
    - 定义：最常用的认证方式，俗称为“密码”
    - 分类：静态口令和动态口令
2. 静态口令
    - 主要原理：用户在注册阶段生成用户名和初始口令，系统在其用户文件或数据库中保存用户的信息（用户名和口令）。
    - 优点：用户定期改变口令，以保证安全性。这种口令因实现简单、使用方便，得到了广泛的应用
    - 攻击方式：
        - 口令监听
        - 截取/重放
        - 简单口令猜测
        - 字典攻击
        - 穷举攻击
        - 伪造服务器攻击
        - 口令泄露
        - 直接破解口令文件
3. 动态口令
    - 也称为一次性口令
    - 基本原理：在用户登录过程中，基于用户口令加入不确定因子，对用户口令和不确定因子进行单向散列函数变换，所得结果作为认证数据提交给认证服务器。认证服务器接收到用户的认证数据后，把用户的认证数据和自己用同样的散列算法计算出的数值进行比对，从而实现对用户身份的认证
    - 动态口令按生成原理可分为非同步和同步两种认证技术
        - 非同步技术生成的动态口令主要是依据**挑战-响应原理**来实现
        - 同步认证技术包括与时间有关的**时钟同步认证技术**和与时间无关的**事件同步认证技术**

7.2 操作系统口令破解

1. Windows口令
    - Windows中的**本地安全授权子系统LSASS**（Local Security Authority Subsystem Service）负责有关安全方面的功能
    - 该子系统将用户登录过程中输入的用户名和密码信息发送给**安全账号管理器（SAM，Security Account Manage**以决定登录尝试是否合法
    - SAM中的SAM数据库记录了每一个用户账号的密码Hash值
    - SAM文件中每个用户账号有两条密码记录：LM密码表示和NT哈希表示（Windows7开始去掉了LM密码）

      （用户名：ID：LM密码：NT哈希）

        - NT哈希是使用MD-4哈希算法3次产生密码的哈希值
    - 破解工具：L0phtCrack5
2. Unix/Linux系统口令
    - 以前，Unix/Linux系统使用/etc/passwd文件管理账户
    - 现在的系统把账户信息和口令密文分开存放。/etc/passwd文件用于保存账户信息，加密过后的密码保存在/etc/shadow或/etc/secure这个影子口令文件中，只有root用户能够读取
    - 破解软件：Crack，JohnTheRipper
3. 跨域拓展攻击（脱库-洗库-撞库）
    - 脱库：窃取数据库
    - 洗库：对用户数据分类，通过技术手段或黑色产业链变现
    - 撞库：用得到的用户账号信息在其他网站进行尝试登陆

7.4 常用文件口令破解

1. Office口令破解
    - 工具：Advanced Office Password Recovery
2. 存档文件口令破解
    - 工具：Advanced Archive Password Recovery
3. PDF文件口令破解
    - 工具：Advanced PDF Password Recovery

7.5 口令防御

1. 强壮的密码策略
    - 不包含用户账户名
    - 至少8个字符长
    - 包含4类字符中的3类字符：英文大写字母、英文小写字母、基本数字、非字母字符
    - 禁止使用易被他人获取的信息
2. 用户意识
    - 不要在不同系统上使用同一口令
    - 不要选取显而易见的信息作口令
    - 不要将口令写下来或存储于文件中
    - 定期更改口令
    - 不要使用重复口令
    - 不要让人知道、看见自己在输入口令
    - 公共场所确认系统是否安全

第八章 网络监听技术

交换式环境的网络流量劫持（端口镜像、MAC攻击、端口盗用、ARP欺骗）

1. 网络流量劫持：
    - 使监听目标的网络流量经过攻击者控制的监听点（主机）
    - 主要通过各种地址欺骗或流量定向的方法来实现
2. 网络环境分类：
    - 共享网络：同一网段的所有网络接口都能访问在物理媒体上传输的数据
    - 交换网络：一个端口的输入交换到指定端口
3. 共享式网络监听

- 广播特性的总线：所有都能收到，但只有地址对了，才处理，从而实现了一对一的通信

4. **交换式网络监听（*）**
    - 端口镜像：把交换机一个或多个端口的数据镜像到某个端口的方法
    - MAC攻击（MAC泛洪）
        - 攻击思路
            - 在局域网中发送带有欺骗性MAC地址源的数据
            - CAM（内容可寻址存储器）表中将会填充伪造的MAC地址记录，随着记录增多，与CAM表相关的交换机内存将被耗尽，这时交换机以类似于集线器的模式工作，向其他所有的物理端口转发数据
        - 成功原因：
            - 对源MAC地址缺乏认证机制
            - 交换机内存有限，MAC地址表不能无限增长
            - 交换机自学习模式：新的虚假映射淘汰真实记录信息，找不到时即广播
    - ARP欺骗
        - 攻击思路
            - 攻击者向主机A和B发送ARP欺骗报文
            - 攻击者从网络接口上嗅探受害主机发过来的数据帧
            - 攻击者将嗅探到的数据发送回原本应该接收的主机
        - 成功原因
            - ARP协议设计之初没有考虑安全问题，任何计算机都可以发送虚假的ARP数据包
            - ARP协议的无状态性
            - ARP缓存需要定时更新
    - 端口盗用
        - 攻击思路
            - 发送伪造以太网帧：源MAC为受害者的MAC，目的MAC为攻击者的MAC
            - 受害主机将数据帧发送给攻击者，攻击者从网络接口嗅探数据
            - 攻击者将数据缓存，让网络正常后，再将数据转交。然后再开始新一轮的攻击
5. 网络监听的检测
    - 采用Ping主机方法：随机填入MAC，ping可疑主机，是否响应
    - 发送垃圾数据包的方法：发伪造MAC垃圾数据包，测试发送前后ping响应速度变化
    - 利用ARP数据包进行检测：虚假地址的ARP请求，响应与否
    - 观察DNS服务器的解析请求：不存在IP地址发ping数据包，是否请求反向DNS解析
6. 网络监听的防范
    - 从逻辑或物理上对网络分段
    - 采用交换机取代集线器
    - 采用加密技术
    - 防范与网络监听有关的黑客技术（例如：静态绑定ARP）

第10章 Web网站攻击技术

10.2 Web应用体系结构脆弱性分析

1. Web客户端的脆弱性
2. Web服务器的脆弱性
3. Web应用程序的脆弱性
4. HTTP的脆弱性
5. Cookie的脆弱性
6. 数据库的安全脆弱性

10.3 SQL注入攻击

1. 概述：SQL注入攻击以网站数据库为目标，一般利用Web应用程序对特殊字符串过滤不完全的缺陷，通过精心构造的SQL语句达到非法访问网站数据库内容或在数据库中执行命令的目的。大多数SQL注入攻击发生在Web应用程序使用用户提供的输入内容来拼接动态SQL语句以访问数据库的情形
2. 攻击流程：
    - Web程序提供了用户输入的表单
    - 攻击者通过填写表单数据发起攻击
    - Web程序通过SQL语句的形式将攻击递交给数据库
    - 数据库执行SQL语句，将执行结果加密后返回给应用程序
    - 应用程序解密数据，将结果发送给用户
3. 防范：

    由于SQL注入攻击发生在应用层，大多数防火墙无法防范此类攻击，问题的解决依赖于完善编程

    - 对用户输入进行检查，确保输入数据的安全性
    - 在构造动态SQL语句时，使用类型安全的参数编码机制
    - 禁止将敏感性数据以明文存放在数据库中，即使被SQL注入攻击，减少泄密风险
    - 遵循最小特权原则
    - 尽量不要使用动态拼接的SQL语句，可以使用参数化的SQL或者使用存储过程进行数据查询
    - 尽量少给出异常信息的提示

10.4 跨站脚本攻击

1. 定义：跨站脚本攻击指攻击者利用Web程序对用户输入过滤不足的缺陷，把恶意代码（包括HTML代码和客户端脚本）注入到其他用户浏览器显示的页面上执行，从而窃取用户敏感信息、伪造用户身份等恶意行为的攻击方式
2. 危害：
    - 盗取用户账号
    - 控制企业数据
    - 非法转账
    - 发送电子邮件
    - 网站挂马
    - 控制受害计算机向其他计算机发起攻击
    - ...
3. 原理：输入嵌有JavaScript或其他恶意脚本的HTML标签代码
4. 问题根源：不当的服务器端输入检查，从而允许用户输入可被客户端浏览器解释的脚本命令
5. **攻击前提（*）：**
    - **Web程序接受用户输入**
    - **Web程序重新显示用户输入的内容**
6. 主要攻击形式：
    - 反射式跨站脚本攻击（非持久性）
    - 本地脚本漏洞攻击/DOM式跨站脚本攻击
    - 存储式跨站脚本攻击
7. 防范
    - 服务端
        - 黑名单过滤
        - 白名单过滤
        - 字符转换

- 客户端
    - 浏览器设置禁止动态脚本
    - 谨慎点击链接
    - 防止访问已知的恶意网站

第十三章 网络防火墙技术

13.1 概述

1. 定义：防火墙是在两个网络之间执行访问控制策略的一个或一组安全系统。它是一种计算机硬件和软件系统的集合，是实现网络安全策略的有效工具之一，被广泛地应用到内部网络与外部网络的边界位置。
    - 防火墙本身必须具有很强的抗攻击能力，以确保其自身的安全性
    - 防火墙简单的可以只用路由器实现，复杂的可以用主机、专用硬件设备及软件甚至一个子网来实现
2. 主要功能
    - 保护脆弱和有缺陷的网络服务
    - 实施安全策略，加强对网络系统的访问控制
    - 防止内网信息暴露，加强隐私
    - 对内外网之间的通信进行监控审计
3. 分类：
    - 按照软、硬件形式划分
        - 软件防火墙
        - 硬件防火墙
        - 芯片级防火墙
    - 从防火墙监控的网络协议层次划分
        - 网络防火墙/包过滤
        - 应用级防火墙/应用网关
    - 从防火墙组成结构划分
        - 单一主机防火墙
        - 路由器集成防火墙
        - 分布式防火墙
    - 从保护的对象划分
        - 单机/个人防火墙
        - 网络防火墙

13.2 防火墙的工作原理

1. 包过滤防火墙
    - 原理：包过滤防火墙根据数据包的包头信息，依据事先设定的过滤规则，决定是否允许数据包通过
    - 核心：过滤规则是防火墙的核心，其作用是执行系统的网络访问策略
    - 两种默认规则：
        - 拒绝访问一切未允特许的服务——限制性原则
        - 允许访问一切未被特别拒绝的服务——连通性原则
    - 包过滤技术的工作对象是数据包
    - 必须仔细考虑规则的顺序，防止出现系统漏洞
    - **优点：**

        - **将包过滤防火墙部署在网络的边界上即可实现对整个网络的保护，实现简单、快速，很多路由器可以作数据包过滤，不需专门添加设备。**
        - **包过滤技术的检查规则相对简单，因此检查操作耗时极短，执行效率非常高，不会给用户的网络性能带来不利的影响。**
        - **包过滤防火墙对用户和应用都透明，内网用户无需对主机进行特殊设置**
    - **缺点：**
        - **安全判决的信息不足，仅依赖网络层和传输层信息。由于缺少信息，一些协议如RPC、UDP难以有效过滤**
        - **支持规则的数量有限，规则过多则会降低网络效率**
        - **正确制定规则并不容易**
        - **不可能引入认证机制**
2. 状态检测包过滤防火墙
    - 原理：根据连接的"状态"进行检查。当一个连接的初始数据报文到达执行状态检测的防火墙时，首先检查该报文是否符合过滤规则规定。如果报文与规定相符合，则将该连接的信息记录下来并自动添加一条允许该连接通过的过滤规则，然后向目的地转发该报文。以后凡是属于该连接的数据防火墙一律予以放行，包括从内向外的和从外向内的双向数据流。

      通信结束、释放该连接以后，防火墙将自动删除关于该连接的过滤规则
    - **优点：**
        - **安全性相比静态包过滤技术要高**
        - **与静态包过滤技术相比，提升了防火墙的性能**
    - **缺点：**
        - **主要工作在网络层和传输层，对报文的数据部分检查很少，安全性还不够高**
        - **检查内容多，对防火墙性能提出了更高的要求**
3. 应用网关防火墙
    - 定义：应用网关防火墙是代理内部网络用户与外部网络服务器进行信息交换的程序。
    - 原理：它将内部用户的请求确认后送达外部服务器，同时将外部服务器的响应再回送给用户。
    - 优点：
        - 相对于包过滤技术而言，代理技术能够提供更高的安全等级
        - 实现了网络隔离，降低了用户网络受到直接攻击的风险。而且对外网隐藏了内网的结构以及用户，进一步降低了用户网络遭受探测的风险。
        - 包过滤技术通常由路由器实现。若过滤机制被破坏，则内网将毫无遮拦地直接与外网接触，不可避免地出现网络攻击和信息泄露的现象。而代理服务器要是损坏的话，只是内网与外网的连接中断，但无法出现网络攻击和信息泄漏的现象。从这个角度看，代理技术比包过滤技术安全。
    - 缺点：
        - 对每一类应用，都需要专门的代理。大多数代理服务器只能处理相对较少的应用
        - 应用代理往往比包过滤防火墙性能要差
        - 成本更加昂贵
        - 不能使用户免于协议本身缺点的限制
        - 有些服务要求建立直接连接，无法使用代理

13.3 防火墙体系结构

1. **防火墙体系结构一般有四种：**
    - **屏蔽路由器结构**
    - **双宿主机结构**
    - **屏蔽主机结构**
    - **屏蔽子网结构**

2. 屏蔽路由器结构
    - 定义：屏蔽路由器防火墙作为内外连接的唯一通道，要求所有报文都必须在此通过检查
    - 屏蔽路由器结构是最简单的防火墙结构
    - 优点：硬件成本低、结构简单、易于部署等
    - 缺点：
        - 核心组件是包过滤防火墙，如果规则配置不当，可能对内网构成威胁
        - 依靠一个单一的部件来保护网络系统，一旦部件出现问题，会对内网失去保护作用
        - 没有或仅有很简单的日志记录功能，网络管理员很难确定网络系统是否正在被攻击或已经被入侵
3. 双宿主机结构
    - 堡垒主机：允许外网主机访问，向外网提供网络服务，易遭受外网攻击，必须具有很强的安全性
        - 堡垒主机常常充当内部网络或防火墙中应用代理的角色
        - 堡垒主机是最显露的主机，因此应当是最安全的主机
    - 定义：所有通信必须经过堡垒主机，禁止内外网络之间直接通信
    - 优点：
        - 双宿主机网关优于屏蔽路由器的地方是堡垒主机，可以监视内外网之间的通信，可进行详细的日志记录，对日后的安全检查非常有用
    - 缺点：
        - 一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网上用户均可以随便访问内部网络
4. 屏蔽主机结构
    - 结构：
        - 一个包过滤路由器连接外部网络，再通过一个堡垒主机与内部网络相连
        - 通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络唯一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击
    - 优点：
        - 无论内网如何变化都不会对包过滤防火墙和堡垒主机配置产生影响
        - 安全风险主要只限制在堡垒主机和屏蔽路由器
    - 缺点：
        - 一旦包过滤路由器被攻破，整个内网和堡垒主机与外网之间就没有任何阻挡
        - 一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网上用户均可以随便访问内部网络
5. 屏蔽子网结构
    - 定义：在外界网络和内部网络之间建立一个双方都可以访问的独立网络（屏蔽子网）用**两台分组过滤路由器**将这一子网分别于内部网络和外部网络分开
    - 特点：
        - 屏蔽子网也常常被称为DMZ区，他可以只包含堡垒主机，也可以增加需要对外提供服务的服务器
        - 屏蔽子网不提供外部网络和内部网络之间的通路

13.5 防火墙评价标准

1. 并发连接数
    - 定义：并发连接数是指内网和外网之间穿越防火墙能够同时建立的最大连接数量
    - 并发连接数的差异主要取决于三方面的因素：
        - 并发连接数取决于防火墙内并发连接表的大小
        - 并发连接数的增大应充分考虑CPU的处理能力
        - 物理链路的实际承载能力将影响防火墙发挥其对海量并发连接的处理能力
2. 吞吐量
    - 定义：吞吐量是指在保证不丢失数据帧的情况下，防火墙能够达到的最大数据帧转发速率
3. 时延
    - 定义：指数据包的第一个比特进入防火墙，到最后一个比特从防火墙输出的时间间隔
4. 丢包率
    - 定义：指在正常稳定的网路状态下，应当被转发但由于防火墙缺少资源而没有转发、被防火墙丢弃的数据包在全部发送数据包中所占的比例
5. 背靠背缓冲
    - 定义：指防火墙接收到以最小数据帧间隔传输的数据帧时，在不丢弃数据的情况下，能够处理的最大数据帧数目
6. 最大TCP连接建立速率
    - 定义：指所有TCP连接成功建立的前提下，防火墙能够达到的最大连接建立速率
7. 防火墙的不足：
    - 防火墙不能防范不经过防火墙的攻击
    - 由于防火墙性能上的限制，因此它通常不具备实时监控入侵的能力
    - 防火墙不能防止策略配置不当或错误配置引起的安全威胁
    - 防火墙不能防止受病毒感染的文件的传输
    - 防火墙不能防止利用服务器系统和网络协议漏洞所进行的攻击
    - 防火墙不能防止数据驱动式的攻击
    - 防火墙不能防止内部的泄密行为
    - 防火墙不能防止本身的安全漏洞的威胁

第十四章 入侵检测技术

14.1 概述

1. 为什么需要入侵检测
    - 防火墙存在许多不足
        - 无法发现和阻止对合法服务的攻击
        - 无法发现和阻止源自其他入口的攻击
        - 无法发现和阻止来自内部网络的攻击
        - 无法发现和阻止来自特洛伊木马的威胁
2. 入侵检测定义：通过从计算机系统或网络的关键点收集信息并进行分析，从中发现系统或网络中是否有违反安全策略的行为和被攻击的迹象
3. 入侵检测系统（IDS）定义：指实施入侵检测的软件与硬件的组合
4. 入侵防御系统（IPS）定义：入侵检测+主动防御
    - 主动防御：预先对入侵活动和攻击性网络流量进行拦截，而不是简单的在恶意流量传送时发出警报
    - 问题：由于增加了主动阻断能力，检测准确程度的高低对应IPS非常关键，误报会导致合法数据被阻塞

5. **通用入侵检测框架（CIDF）**
    - **CIDF将入侵检测系统分为四个基本组件**
        - **事件产生器：负责采集原始数据，转换为具有标准格式的事件，并提供给其他组件**
        - **事件分析器：分析事件产生器输出的事件，将分析结果输出给响应单元**
        - **响应单元：根据事件分析器输出的结果做出反应**
        - **事件数据库**

14.2 入侵检测系统的信息源

1. IDS是数据驱动的系统，它的数据源主要分为三类：
    - 来自主机的数据
    - 来自应用的数据
    - 来自网络的数据
2. 来自主机的数据
    - 主要包括操作系统审计记录、系统日志文件等
    - 优点：具有较高的可靠性、安全性和可信性
    - 缺点：
        - 不同操作系统的审计格式存在差异
        - 冗余信息过多，分析处理负担较重
        - 如果审计记录中没有需要的事件信息，需要通过其他渠道获取
3. 来自应用的数据
    - 主要包括程序日志和应用程序的运行记录
    - 优点：精确度高、完整性强、开销低
    - 缺点：
        - 缺乏保护机制，可能被篡改和删除
        - 一些应用程序无日志功能或者日志不够详尽
        - 由于资源限制，应用程序可能停止记录日志
4. 来自网络的数据
    - 优点：
        - 网络数据的收集分析不会影响业务主机的性能
        - 以被动监听方式获取数据包，不会降低网络性能
        - 不易遭受攻击
        - 相比主机数据源，可更快速有效监测网络攻击
        - 标准化程度高，易兼容不同系统
    - 缺点：
        - 加密数据包无法分析
        - 数据流量大，处理开销高
        - 保护精确度不如来自主机的数据

14.3 入侵检测系统的分类

1. 根据数据源分：
    - 基于主机的入侵检测系统
    - 基于应用的入侵检测系统
    - 基于网络的入侵检测系统
    - 混合的入侵检测系统
2. 根据检测方法来分：

- 基于特征的入侵检测
- 基于异常的入侵检测
- 混合入侵检测

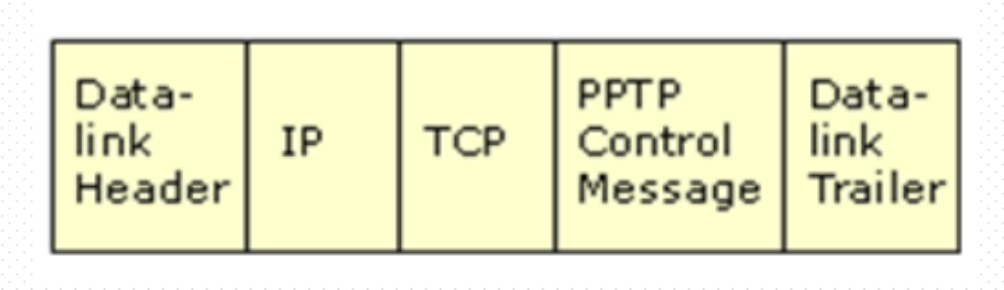
14.4 入侵检测方法

1. 特征检测
    - 定义：收集非正常操作的行为特征，建立相关特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵
    - 特征：
        - 静态特征：比如Land攻击数据包源地址目标地址，源端口目标端口相同
        - 动态特征：网络统计数据、审计记录、日志、文件、硬盘、内存大小的变化
        - 特征描述：描述语言
    - 实现方式
        - **模式匹配法**：将收集到的入侵特征转换成模式，存放在模式数据库中。检测过程中将收集到的数据信息与模式数据库进行匹配，从而发现攻击行为。
        - **专家系统法**：入侵活动被编码成专家系统的规则。入侵检测系统根据收集到的数据，通过条件匹配判断是否出现了入侵并采取相应动作
        - **状态迁移法**：利用状态转换图描述并检测已知的入侵模式。入侵检测系统保存入侵相关的状态转换图表，并对系统的状态信息进行监控，当用户动作驱动系统状态向入侵状态迁移时触发入侵预警
2. 异常检测
    - 定义：首先总结正常操作应该具有的特征，当用户与正常行为有重大偏离时即被认为是入侵
    - 实现方式
        - **统计分析法**：以统计理论为基础建立用户或者系统的正常行为模式。主体的行为模式常常由测量参数的频度、概率分布、均值、方差等统计量来描述。将用户的短期特征轮廓与长期特征轮廓进行比较，如果偏差超过设定的阈值，则认为存在异常
        - **神经网络法**：向神经网络提交标识用户正常行为的训练数据，神经网络可以通过自学建立用户或者系统活动的正常特征模式
        - **聚类分析法**：采用聚类分析法进行异常检测，是希望在描述用户行为或者系统行为的数据中发现不同类别的数据集合。需要采用用户行为或者系统行为的一些属性描述被监控主体的行为特征
        - **人工免疫**：将非法程序及非法应用与合法程序、合法数据区分开来，与人工免疫系统对自体和非自体进行类别划分相类似
    - 优点：
        - 无需更新特征库，管理开销较小
        - 不依赖具体的、已知的攻击特征检测，可以判别未知的攻击
    - 缺点：
        - 不能准确告知攻击类型
        - 准确度没有特征检测高
3. Snort入侵检测系统
    - 规则编写

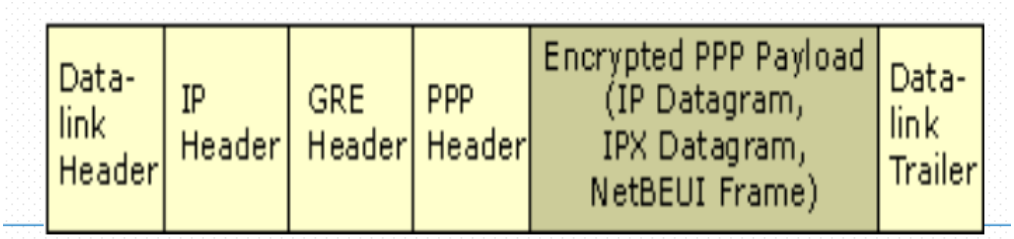
虚拟专用网

1. 定义：指通过在公用网络中建立一条安全、专用的虚拟通道，连接异地的两个网络，构成逻辑上的虚拟子网
2. 优点：
    - 安全可靠

    - 易于部署
    - 成本低廉
3. 分类：
    - 按应用范围划分
        - 远程访问VPN
        - 企业内部VPN
        - 企业外部VPN
    - 按VPN网络结构划分
        - 基于VPN的远程访问：单机连接到网络
        - 基于VPN的网络互连：网络连接到网络
        - 基于VPN点对点通信：单机到单机
    - 按接入方式划分
        - 专线VPN：通过固定线路连接到ISP
        - 拨号接入VPN（简称VPDN）：使用拨号连接连接到ISP
    - 按隧道协议划分
        - 第二层隧道协议VPN：PPTP VPN、L2TP VPN
        - 第三层隧道协议VPN：IPSec VPN
        - 第四层隧道协议VPN：SSL VPN
    - 按隧道建立方式划分
        - 自愿隧道：以客户端计算机或路由器为端点的隧道，使用客户软件发送VPN请求来创建
        - 强制隧道：用户端的计算机不作为隧道端点，而是由远程接入服务器的NAS作为隧道的一个端点
          （用户计算机只能使用由NAS创建的隧道，所以称之为强制隧道）
4. 关键技术：
    - 隧道技术：通过对数据进行封装，在公共网络上建立一条数据通道，让数据包通过这条隧道传输
    - 隧道协议：封装数据、管理隧道的通信标准
    - **隧道协议组成（*）**：无论何种隧道协议，其数据包格式都是由**乘客协议**、**封装协议**和**传输协议**三部分组成的
        - **乘客协议：指用户要传输的数据，也就是被封装的数据，它们可以是IP、PPP、SLIP等**
        - **封装协议：用于建立、保持和拆卸隧道，如L2F、PPTP、L2TP属于封装协议**
        - **传输协议：乘客协议被封装之后应用传输协议，以使数据包顺利通过包交换网络（如Internet），抵达目的地，如用UDP协议对L2TP协议数据包进行传输**
5. PPTP协议
    - 希望通过拨入当地ISP进入Internet，再连接企业的VPN网关，避免长途电话的费用
    - PPTP包封装在IP数据包中，通过IP网络进行传输，只要网络层连通，就可运行PPTP协议
    - 使用一个TCP连接对隧道进行维护
    - PPTP通信时，客户机和服务器间有2个通道
        - 一个通道是TCP 1723端口的控制连接，另一个通道用于传输数据，是传输PPP数据包的IP隧道
    - PPTP有两种报文
        - 控制报文：用于PPTP隧道的建立、维护和断开，采用TCP控制



- 数据报文：先封装在PPP协议中，然后在用GRE协议（通用路由封装协议）封装成标准IP包，通过IP网络进行发送



6. L2TP协议
    - L2TP使用IPSec对通信数据进行加密和鉴别
        - L2TP客户端需支持L2TP隧道协议和IPSec安全协议
        - 客户端和服务器进行VPN通信的前提是二者之间有连通且可用的IP网络
    - L2TP主要由**LAC（L2TP接入集中器）**和**LNS（L2TP网络服务器）**构成
        - LAC用于发起呼叫，接受呼叫和建立隧道
        - LNS是所有隧道的终点
    - 包括两种类型的报文：**控制报文**和**数据报文**
        - 两种报文均采用UDP协议封装和传送PPP帧
        - PPP帧的有效载荷（即用户传输数据）可以经过加密或压缩
        - L2TP控制报文：用于隧道的建立与维护
            - 与PPTP的区别：
                - PPTP通过TCP协议进行隧道的维护，L2TP则是采用UDP协议
                - PPTP的控制报文没有经过加密，而L2TP的控制报文应用IPSec ESP进行了加密
            - 由于UDP提供的是无连接的数据包服务，因此L2TP采用报文序列化的方式来保证L2TP报文按序提交
                - L2TP控制报文中，*Next Received*字段和*Next Sent*字段用于维持控制报文的序列化，无序报文将被丢弃
                - 这两个字段同样用于用户传输数据的按序提交

        - L2TP数据报文：
            - L2TP数据报文和控制报文有相同的包格式

7. GRE协议
    - 封装过程：
        - 在原始数据包的外面增加一个GRE头部构成GRE报文
        - 再为GRE报文增加一个新IP头，从而构成最终的IP包
    - 优点：
        - 可以利用公共IP网络连接非IP网络
        - 通过GRE，可以使用保留地址进行网络互连
        - 扩大了网络的工作范围
        - GRE只提供封装，不提供加密，对路由器的性能影响较小，设备要求相对较低
    - 缺点：
        - 不提供加密
8. IPSec
    - 三个主要协议：
        - 鉴别报头Authentication Header，AH协议：只涉及认证，不涉及加密
        - 封装安全载荷Encapsulating Security Payload，ESP协议：主要用来处理对IP数据包的加密
        - 密钥管理与交换协议Internet Key Exchange，IKE协议：对使用的协议、加密算法和密钥进行协商
    - 两种工作模式：
        - 传输模式
        - 隧道模式
9. SSL
    - 协议过程通过3个元素来完成：
        - 握手协议
        - 记录协议
        - 警告协议

蜜罐技术

1. 蜜罐是一类安全资源。其价值就在于被探测、被攻击及被攻陷
2. 蜜罐技术的分类
    - 按部署目的分：
        - 产品型
        - 研究型
    - 按交互度等级分：
        - 低交互蜜罐（产品型蜜罐一般属于低交互蜜罐）
            - 一般仅仅模拟操作系统和网络服务
        - 高交互蜜罐（研究型蜜罐一般都是高交互蜜罐）
            - 完全提供真实的操作系统和网络服务，没有任何的模拟
            - 在提升黑客活动自由度的同时，自然地加大了部署和维护的复杂度及风险的扩大

3. 优点：
    - 收集到的数据大可能就是黑客攻击造成的，减少了漏报率和误报率
    - 能够收集到新的攻击工具和攻击方法
    - 不需要强大的资源支持
4. 缺点：
    - 需要较多的时间和精力投入
    - 只能对针对蜜罐的攻击行为进行监视和分析，其视图较为有限
    - 不能直接防护有漏洞的信息系统
    - 会带来一定的安全风险
5. 蜜罐技术实例——Honeyd
    - 是一种针对UNIX系统设计、开源、低交互的Honeypot，用于对可疑活动的检测、捕获和预警
    -