【网安】《网络安全》整理内容合集

2019级 网络空间安全专业 吴雨欣 整理

特别鸣谢：dls、sotawhu.cn、以及18级各位提供资料的学长学姐

目录（wyx）

第一章：网络安全概论

CVSS评分表	cjs-第一章-网络安全概论
“安全”的含义	cjs-第一章-网络安全概论
安全的几个要素	cjs-第一章-网络安全概论
安全威胁的来源	cjs-第一章-网络安全概论
安全威胁的几种类型	cjs-第一章-网络安全概论
安全的目标	cjs-第一章-网络安全概论
信息通讯环境	cjs-第一章-信息安全体系
网络通讯的信息安全模型	cjs-第一章-信息安全体系
信息安全体系	cjs-第一章-信息安全体系
Internet网络安全技术	cjs-第一章-信息安全体系
什么是信息保障-PDRR	cjs-第一章-信息系统安全保障体系
补充：P2DR	自己推测
信息保障体系的组成	cjs-第一章-信息系统安全保障体系
信息系统安全管理准则	cjs-第一章-信息系统安全保障体系
信息安全管理的地位	cjs-第一章-信息系统安全保障体系
信息安全管理的层次与内容	cjs-第一章-信息系统安全保障体系
信息安全管理的发展（含其详细内容）	cjs-第一章-信息系统安全保障体系
管理安全等级划分	cjs-第一章-信息系统安全保障体系
IATF V1.0-三个目标十个步骤	cjs-第一章-信息系统安全保障体系
IATF V3.0	cjs-第一章-信息系统安全保障体系

第二章：网络攻击行径分析

黑客与黑客技术	cjs-第二章
攻击事件分类	cjs-第二章
攻击的目的	cjs-第二章
攻击的步骤	cjs-第二章
攻击的基本技巧	cjs-第二章
常用攻击	cjs-第二章

第三章：网络侦察技术

信息收集及其过程	cjs-第三章-常见的网络侦察技术
线下探查手段（社工等）	cjs-第三章-常见的网络侦察技术
离线探查手段-DNS	cjs-第三章-常见的网络侦察技术
离线探查手段——whois	cjs-第三章-常见的网络侦察技术
在线扫描-地址扫描	cjs-第三章-常见的网络侦察技术
ICMP、Ping、Traceroute	cjs-第三章-常见的网络侦察技术
在线扫描-端口扫描	cjs-第三章-常见的网络侦察技术
端口扫描的类型-TCP XXX（）	cjs-第三章-常见的网络侦察技术
端口扫描的类型-UDP XXX（）	cjs-第三章-常见的网络侦察技术
在线扫描-深度扫描	cjs-第三章-常见的网络侦察技术
扫描器的概念和历史	cjs-第三章-常见的网络侦察技术
常用扫描器-nmap	cjs-第三章-常见的网络侦察技术
操作系统辨识和栈指纹技术	cjs-第三章-常见的网络侦察技术
常用扫描器——nessus、xscan、pinger	cjs-第三章-常见的网络侦察技术
网络监听的概念	cjs-第三章-网络监听
以太网的工作原理和工作模式	cjs-第三章-网络监听
共享网络与交换网络	cjs-第三章-网络监听
共享以太网监听技术	cjs-第三章-网络监听
共享以太网抓包应用-Unix下和Windows下	cjs-第三章-网络监听
Unix抓包——Packet socket	cjs-第三章-网络监听
Unix抓包—— BPF	cjs-第三章-网络监听
BPF和libpcap	cjs-第三章-网络监听
Windows抓包——WinPcap	cjs-第三章-网络监听
检测处于混杂模式的节点	cjs-第三章-网络监听
交换技术	cjs-第三章-网络监听
交换以太网监听技术	cjs-第三章-网络监听
ARP	cjs-第三章-网络监听
网络监听-总结	cjs-第三章-网络监听
口令破解方式	cjs-第三章-口令破解
口令破解-分析漏洞	cjs-第三章-口令破解
口令破解-离线破解	cjs-第三章-口令破解
口令破解-在线破解	cjs-第三章-口令破解
口令破解工具	cjs-第三章-口令破解

第四章：拒绝服务攻击

拒绝服务攻击概述（定义、攻击思想、实现方式）	cjs-第四章
拒绝服务攻击分类-根据攻击模式分类	cjs-第四章
服务端口攻击-SYN Flooding	cjs-第四章
服务端口攻击-Smurf攻击	cjs-第四章
服务端口攻击-错误处理	cjs-第四章
电子邮件轰炸及应对	cjs-第四章
分布式拒绝服务攻击DDoS	cjs-第四章

第五章：缓冲区溢出攻击

缓冲区溢出的原理	lm-第五章
缓冲区溢出的目标与步骤	lm-第五章
缓冲区溢出的防御技术	lm-第五章
缓冲区溢出攻击防御技术展望	lm-第五章

第六章：程序攻击

逻辑炸弹攻击	lm-第六章
木马的概念	lm-第六章
木马的欺骗手段（名字欺骗、与正常文件进行捆绑）	lm-第六章
木马的实现技术	lm-第六章
后门	lm-第六章
木马 vs 后门	lm-第六章
后门的植入	lm-第六章
木马、后门的安装	lm-第六章
后门的启动	lm-第六章
木马、后门的防御	lm-第六章
ROOTKIT及其原理	lm-第六章
ROOTKIT的分类	lm-第六章
ROOTKIT的技术发展	lm-第六章
Windows RootKit的三种方法	lm-第六章
如何防御Windows用户模式RootKit	lm-第六章
内核模式Rootkit	lm-第六章
Rootkit的技术思路	lm-第六章
检测Rootkit的技术思路	lm-第六章
如何加强Windows内核防护	lm-第六章
进程的隐藏	lm-第六章
用DLL实现Rootkit功能	lm-第六章
代码注入技术	lm-第六章
代码拦截技术	lm-第六章
内核态代码拦截	lm-第六章

第七章：欺骗攻击

DNS欺骗攻击	cjs-第七章
Email欺骗攻击（方法、实现步骤、防护）	cjs-第七章
Web欺骗攻击（概念、动机、形式）	cjs-第七章
Web欺骗的形式（详细）	cjs-第七章
Cookie技术	cjs-第七章
Web服务器端安全性	cjs-第七章
针对Web Server的常见攻击	cjs-第七章
服务器端的安全防护	cjs-第七章
Web客户端的安全性	cjs-第七章
ActiveX control的安全性	cjs-第七章
如何防止Web欺骗	cjs-第七章
IP欺骗	cjs-第七章
IP欺骗的过程	cjs-第七章
如何避免IP欺骗	cjs-第七章
会话(交易)劫持（TCP Session Hijack）	cjs-第七章
TCP ACK Storm	cjs-第七章
TCP ACK Storm 之 如何到达不同步的状态	cjs-第七章
不在一个子网中的劫持(欺骗)手法	cjs-第七章
实施会话劫持的一般性过程	cjs-第七章
Https会话劫持之SSLStrip	cjs-第七章
进行会话劫持的工具	cjs-第七章

第八章：利用处理程序错误攻击

系统漏洞及攻防	lm-第八章
常见Window系统漏洞	lm-第八章
黑客的攻击按如下六个步骤进行	lm-第八章
Web漏洞及攻防	lm-第八章
Web入侵	lm-第八章
Web的三种安全问题	lm-第八章
Web安全问题来源	lm-第八章
常见Web安全问题	lm-第八章

第九章：访问控制技术

操作系统安全等级	cjs-第九章
信息的安全控制技术有3种	cjs-第九章
访问控制技术及其基本任务	cjs-第九章
访问控制技术和信息流控制技术的关系	cjs-第九章
访问控制技术的基本任务与实现方法	cjs-第九章
访问控制技术有效性的前提	cjs-第九章
访问控制技术的概述	cjs-第九章
访问控制技术的类型（DAC、MAC）	cjs-第九章
DAC-访问控制矩阵、实现方法	cjs-第九章
DAC-实现方法-基于行-权限表机制	cjs-第九章
DAC-实现方法-基于行-前缀表机制	cjs-第九章
DAC-实现方法-基于列-保护位机制	cjs-第九章
DAC-实现方法-基于列-访问控制表（ACL）机制	cjs-第九章
DAC-实现方法-基于列-口令机制	cjs-第九章
DAC-面向过程的访问控制	cjs-第九章
DAC-访问许可权与访问操作权	cjs-第九章
DAC-DAC的优缺点	cjs-第九章
MAC-基础	cjs-第九章
MAC-MAC机制的实现方法	cjs-第九章
MAC-木马窃取敏感文件的方法	cjs-第九章
MAC-支持MAC的措施	cjs-第九章
MAC-Bell-La Padual模型	cjs-第九章
MAC-Biba模型	cjs-第九章
新型访问控制技术	cjs-第九章
新型访问控制技术-RABC	cjs-第九章
Linux基本访问控制机制	cjs-第九章
入网认证	cjs-第九章
一次性口令	cjs-第九章
S/Key协议及安全分析	cjs-第九章
Kerberos协议	cjs-第九章
物理隔离措施	cjs-第九章

第十章：防火墙技术

防火墙技术概述	cjs-第十章
状态检测	cjs-第十章
防火墙的结构	cjs-第十章
构建防火墙	cjs-第十章
包过滤防火墙的设置	cjs-第十章

第十一章：

传统的安全技术	cjs-第十一章
预防的局限性	cjs-第十一章
动态安全模型P2DR	cjs-第十一章
信息安全两态论	cjs-第十一章
入侵检测技术概述	cjs-第十一章
入侵分析-信息收集	cjs-第十一章
入侵分析-误用检测、异常检测、完整性分析	cjs-第十一章
入侵检测的分类	cjs-第十一章
异常检测	cjs-第十一章
NT审计	cjs-第十一章
系统日志	cjs-第十一章
主机源与网络源	cjs-第十一章
基于主机的入侵检测（集中式、分布式）	cjs-第十一章
基于网络的入侵检测	cjs-第十一章
入侵检测产品	cjs-第十一章
入侵检测问题	cjs-第十一章
协同	cjs-第十一章
数据挖掘	cjs-第十一章
报警信息融合	cjs-第十一章
网络流量异常检测	cjs-第十一章
攻击源追踪	cjs-第十一章
入侵检测的发展方向	cjs-第十一章
IPS（入侵防御系统）	cjs-第十一章

第十二章：VPN 技术

VPN概述	cjs-第十二章
VPN的分类	cjs-第十二章
VPN使用的协议与实现	cjs-第十二章
PPTP	cjs-第十二章
IPSEC	cjs-第十二章

目录（wyw）

网络安全复习

1-概述

网络安全概论

- 什么是安全
  - 看ppt的15页
- 信息安全的级别
  - 第一级为计算机安全
  - 第二级网络安全
  - 第三级为信息系统安全
- 安全的要素
  - 可用性
  - 机密性
  - 完整性
  - 可控性
  - 可审查性
- 安全威胁的来源
  - 外部渗入
  - 内部渗入者
  - 滥用职权者
- 安全威胁的几种类型
  - 线缆连接
  - 身份鉴别
  - 编程
  - 系统漏洞
  - 物理威胁
- 安全的目标

    - 安全保护能力
    - 隐患发现能力
    - 应急反应能力
    - 信息对抗能力

信息安全概况

信息安全体系

信息系统安全保障体系

- 信息保障
    - 保护
    - 检测
    - 反应
    - 恢复
- 信息保障体系的组成
    - 法律和政策体系
    - 标准与规范体系
    - 人才培养体系
    - 产业支撑体系
    - 技术保障体系
    - 组织管理体系
- 信息系统安全管理准则
- 信息安全管理的层次与内容
    - 宏观管理
    - 微观管理

2-网络攻击行径分析

攻击事件

- 安全威胁

    - 外部攻击
    - 内部攻击
    - 行为滥用
- 攻击事件分类
    - 破坏型攻击
    - 利用型攻击
    - 信息收集型攻击
    - 网络欺骗型攻击
    - 垃圾信息攻击

攻击目的

- 动机
    - 恶作剧
    - 恶意破坏
    - 商业目的
    - 政治军事
- 性质
    - 破坏
    - 入侵
- 目的
    - 破坏目标工作
    - 窃取目标信息
    - 控制目标机器
    - 利用假消息欺骗对方

攻击步骤

- 准备阶段
    - 确定攻击目的
    - 准备攻击工具
    - 收集目标信息

- 实施阶段
  - 隐藏自己的位置
  - 利用收集到的信息获取账号和密码，登录主机
  - 利用漏洞或者其他方法获得控制权并窃取网络资源和特权
- 善后阶段
  - 日志
  - Windows
    - ...
  - Unix
    - ...
  - 为了下次攻击的方便，攻击者都会留下一个后门，充当后门的工具种类非常多，最典型的是木马程序

攻击诀窍

3-网络侦察技术

信息收集：nslookup

- 关于DNS
  - 是一个全球分布式数据库，对于每一个DNS节点，包含有该节点所在的机器的信息、邮件服务器的信息、主机CPU和操作系统等信息
  - Nslookup是一个功能强大的客户程序
- 熟悉nslookup，就可以把DNS数据库中的信息挖掘出来
  - 分两种运行模式
    - 非交互式，通过命令行提交命令
    - 交互式：可以访问DNS数据库中所有开放的信息
- UNIX/LINUX环境下的host命令有类似的功能

DNS & nslookup

- 通过nslookup可以做什么?
  - 区域传送：可以列出DNS节点中所有的配置信息
    - 这是为了主DNS和辅DNS之间同步复制才使用的
  - 查看一个域名，根据域名找到该域的域名服务器
  - 反向解析，根据IP地址得到域名名称
- 从一台域名服务器可以得到哪些信息?
  - 如果支持区域传送，不用客气，拿下来看一看
  - 否则的话，至少可以发现以下信息
    - 邮件服务器的信息，在实用环境中，邮件服务器往往在防火墙附近，甚至就在同一台机器上
    - 其他，比如ns、www、ftp等，这些机器可能被托管给ISP
- 需注意的地方
  - 关闭未授权区域传送功能
    - 或者，在防火墙上禁止53号TCP端口，DNS查询请求使用53号UDP端口
  - 区分内部DNS和外部DNS
    - 内部信息不出现在外部DNS中
  - DNS中该公开的信息总是要公开的，否则，域名解析的功能就无效了，没有MX记录就不能支持邮件系统

网络扫描

- 扫描器
  - 扫描器是一种自动检测远程或本地主机安全性弱点的程序
  - 通过使用扫描器可以发现远程服务器是否存活、它对外开放的各种TCP端口的分配及提供的服务、它所使用的软件版本(如操作系统或其他应用软件的版本)、所存在可能被利用的系统漏洞
- 扫描的类型
  - 地址扫描

- Ping & Traceroute
    - Ping
        - 用来判断远程设备可访问性最常用的方法
        - 原理：发送ICMP Echo消息，然后等待ICMPReply消息
    - Traceroute
        - 用来发现实际的路由路径
        - 原理：给目标的一个无效端口发送一系列UDP，其TTL依次增一，中间路由器返回一个ICMP Time Exceeded消息

- 端口扫描
    - 端口扫描技术
        - 基本的TCP connect()扫描
            - 做法
                - 扫描器调用socket的connect()函数发起一个正常的连接
                    - 如果端口是打开的，则连接成功
                    - 否则，连接失败
            - 优点
                - 简单，不需要特殊的权限
            - 缺点
                - 服务器可以记录下客户的连接行为，如果同一个客户轮流对每一个端口发起连接，则一定是在扫描
        - TCP SYN扫描(半开连接扫描, half open)
            - 做法
                - 向目标主机的特定端口发送一个SYN包
                    - 如果应答包为RST包，则说明该端口是关闭的
                    - 否则，会收到一个SYN|ACK包。于是，发送一个RST，停止建立连接
                - 由于连接没有完全建立，所以称为“半开连接扫描”

- 优点
  - 很少有系统会记录这样的行为
- 缺点
  - 在UNIX平台上，需要root权限才可以建立这样的SYN数据包

- TCP Fin扫描(秘密扫描，stealth)
  - 做法
    - 扫描器发送一个FIN数据包
      - 如果端口关闭的，则远程主机丢弃该包，并送回一个RST包
      - 否则的话，远程主机丢弃该包，不回送
    - 变种，组合其他的标记
  - 优点
    - 不是TCP建立连接的过程，所以比较隐蔽
  - 缺点
    - 与SYN扫描类似，也需要构造专门的数据包
    - 在Windows平台无效，总是发送RST包

- TCP ftp proxy扫描(bounce attack)
  - FTP bounce attack
  - 做法
    - 在ftp协议中，数据连接可以与控制连接位于不同的机器上
    - 让ftp server与目标主机建立连接，而且目标主机的端口可以指定
    - 如果端口打开，则可以传输否则，返回"425 Can't build data connection: Connection refused."
    - Ftp这个缺陷还可以被用来向目标(邮件,新闻)传送匿名信息
  - 优点：这种技术可以用来穿透防火墙
  - 缺点：慢，且有些ftp server禁止这种特性

- 用IP分片进行SYN/FIN扫描(躲开包过滤防火墙)

        - 它本身并不是一种新的扫描方法，而是其他扫描技术的变种，特别是SYN扫描和FIN扫描
        - 思想是，把TCP包分成很小的分片，从而让它们能够通过包过滤防火墙
            - 注意，有些防火墙会丢弃太小的包
            - 而有些服务程序在处理这样的包的时候会出现异常，或者性能下降，或者出现错误
    - UDP recvfrom扫描
        - 非root用户不能直接读取ICMP Port Unreach消息，但是Linux提供了一种方法可以间接通知到
        - 做法
            - 第二次对一个关闭的UDP端口调用write()总是会失败
            - 经验：在ICMP错误到达之前，在UDP端口上调用recvfrom()会返回EAGAIN(重试)，否则会返回ECONNREFUSED(连接拒绝)
    - UDP ICMP端口不可达扫描
        - 利用UDP协议
        - 做法
            - 开放的UDP端口并不需要送回ACK包，而关闭的端口也不要求送回错误包，所以利用UDP包进行扫描非常困难
            - 有些协议栈实现的时候，对于关闭的UDP端口，会送回一个ICMP Port Unreach错误
        - 缺点
            - 速度慢，而且UDP包和ICMP包都不是可靠的
            - 需要root权限，才能读取ICMP Port Unreach消息
        - 一个应用例子
            - Solaris的rpcbind端口(UDP)位于32770之上，这时可以通过这种技术来探测
    - Reverse-ident扫描
        - Ident协议使得攻击者可以发现任何一个通过TCP连接的进程的所有者的用户名，即使该进程并没有发起该连接

        - 只有在TCP全连接之后才有效
        - TCP端口113
    - 例如
        - 可以先连接到80端口，然后通过identd来发现服务器是否在root下运行
    - 建议关闭ident服务，或者在防火墙上禁止，除非是为了审计的目的
- 漏洞扫描
    - 概述
        - 漏洞扫描是指使用漏洞扫描程序对目标系统进行信息查询
        - 漏洞扫描器是一种自动检测远程或本地主机安全性弱点的程序
        - 外部扫描 与 内部扫描
    - 操作系统辨识
        - 动机
            - 许多漏洞是系统相关的，而且往往与相应的版本对应
            - 从操作系统或者应用系统的具体实现中发掘出来的攻击手段都需要辨识系统
            - 操作系统的信息还可以与其他信息结合起来，比如漏洞库，或者社会诈骗(社会工程，social engineering)
        - 如何辨识
            - 端口服务提供的信息
            - 栈指纹识别技术
- 常用的网络扫描器

信息收集：扫描技术

- Port scanning: 找出网络中开放的服务
- 基于TCP/IP协议，对各种网络服务，无论是主机或者防火墙、路由器都适用
- 端口扫描可以确认各种配置的正确性，避免遭受不必要的攻击
- 用途，双刃剑

    - 管理员可以用来确保自己系统的安全性
    - 黑客用来探查系统的入侵点
- 端口扫描的技术已经非常成熟，目前有大量的商业、非商业的扫描器
- 扫描器的重要性
    - 扫描器能够暴露网络上潜在的脆弱性
    - 无论扫描器被管理员利用，或者被黑客利用，都有助于加强系统的安全性
        - 它能使得漏洞被及早发现，而漏洞迟早会被发现的
    - 扫描器可以满足很多人的好奇心
    - 扫描器除了能扫描端口，往往还能够
        - 发现系统存活情况，以及哪些服务在运行
        - 用已知的漏洞测试这些系统
        - 对一批机器进行测试，简单的迭代过程
        - 有进一步的功能，包括操作系统辨识、应用系统识别

网络监听

- 网络监听的目的是截获通信的内容
- 监听的手段是对协议进行分析
- 当黑客成功地登录进一台网络上的主机，并取得了root权限之后，而且还想利用这台主机去攻击同一网段上的其它主机时，这时网络监听是一种最简单而且最有效的方法，它常常能轻易地获得用其他方法很难获得的信息
- 以太网的监听
- 交换式网络上的嗅探器
    - 交换以太网中，交换机能根据数据帧中的目的MAC地址将数据帧准确地送到目的主机的端口，而不是所有的端口。所以交换式网络环境在一定程度上能抵御Sniffer攻击
    - 在交换环境中，Sniffer的简单的做法就是伪装成为网关
    - ARP欺骗
- 网络监听的防范方法
- 检测网络监听的手段

以太网

- 工作原理
- 工作模式

共享网络和交换网络

- 共享式网络
- 交换式网络
- 交换技术
    - 二层交换技术
    - 三层交换技术
    - 四层交换技术

应用程序抓包的技术

- Packet socket
- BPF
    - BSD抓包法
    - Libpcap(一个抓包工具库)支持BPF
        - 关于Libpcap
    - BPF是一种比较理想的抓包方案
- WinPcap

检测处于混杂模式的节点

口令破解

- 字典文件
- 口令攻击类型
    - 字典攻击
    - 强行攻击
    - 组合攻击

- 口令破解器
- 注册码
- Windows口令破解
- Unix口令破解

4-拒绝服务攻击

拒绝服务攻击概述

- DoS定义
    - 拒绝服务攻击DoS（Denial of Service）是阻止或拒绝合法使用者存取网络服务器的一种破坏性攻击方式
- 从某种程度上可以说，DoS攻击永远不会消失
- 而且从技术上，目前还没有根本的解决办法
- DoS攻击思想及方法
    - 服务器的缓冲区满，不接收新的请求
    - 使用IP欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。这也即是DoS攻击实施的基本思想
- DoS攻击的实现方式
    - 资源消耗、服务中止、物理破坏等

拒绝服务攻击分类

- 攻击模式
- 发起方式

服务端口攻击

- SYN Flooding
    - 同步包风暴攻击的本质是利用TCP/IP协议集的设计弱点和缺陷
    - 只有对现有的TCP/IP协议集进行重大改变才能修正这些缺陷

    - 目前还没有一个完整的解决方案，但是可以采取一些措施尽量降低这种攻击发生的可能性
    - 应对
        - 优化系统配置
        - 优化路由器配置
        - 使用防火墙
        - 主动监视
        - 完善基础设施
- Smurf攻击
- 利用处理程序错误的拒绝服务攻击
    - Ping of Death
    - Teardrop
    - Winnke攻击
    - Land攻击

电子邮件轰炸

分布式拒绝服务攻击DDos

5-缓冲区溢出攻击

缓冲区溢出概述

- 缓冲区定义
- 缓冲区溢出的定义
- 溢出的危害
- 造成溢出的根本原因

缓冲区溢出攻击的原理

- 攻击模式
    - 找到可利用的缓冲区溢出隐患.....
- 溢出可能发生的位置

    - 堆栈
    - 堆
    - 数据段
    - BSS段
- 常见的溢出缓冲区的途径
    - 利用C的标准函数库
    - 利用数组下标的越界操作
    - 利用有符号整数与无符号整数的转换
    - 恶意代码（注入）
- 恶意代码（已在内存）

缓冲区溢出攻击的防御技术

- 黄金规则
    - 要求代码传递缓冲区长度
    - 检查内存
    - 采取防御措施
- 基于软件的防御技术
    - 类型安全的编程语言
    - 相对安全的函数库
    - 修改的编译器
    - 内核补丁
    - 静态分析方法
    - 动态检测方法
- 基于硬件的防御技术
    - 处理器结构方面的改进

6-程序攻击

逻辑炸弹攻击

- 定义

- 特征
    - 隐蔽性
    - 攻击性

植入后门

- 后门是一个允许攻击者绕过系统中常规安全控制机制的程序，他按照攻击者自己的意图提供通道
- 后门的重点在于为攻击者提供进入目标计算机的通道
- 攻击方法
- 隐藏
- 后门的启动

后门VS特洛伊木马

- 差异
    - 如果一个程序仅仅提供远程访问，那么它只是一个后门
    - 如果攻击者将这些后门伪装成某些其他良性程序，那么那就变成真正的特洛伊木马
    - 木马是披着羊皮的狼！！它对用户个人隐私造成极大威胁
- 如何防御木马、后门

病毒攻击

- 详见第13章 网络病毒防治

特洛伊木马攻击

- 木马通常用来控制目标主机，通常由两端组成
- 反弹型木马
- 嵌入式木马
- 欺骗手段
    - 名字欺骗
    - 与正常文件进行捆绑
- 木马的实现技术

其他程序攻击

Rootkit(恶意程序)

- 什么是Rootkit
- Rootkit的宗旨
    - 隐蔽
- 按内核模式分类
    - 用户级Rootkit
    - 内核级Rootkit
- 技术发展
- Windows用户模式Rootkit
    - 不盛行的原因
    - Rootkit的三种方法
    - 如何防御
- 内核模式Rootkit
    - 采用的手段
    - 技术思路
    - 如何检测
- Rootkit技术篇
    - NT进程的隐藏
        - 思路
            - 第一是让系统管理员看不见（或者视而不见）你的进程
            - 第二是不使用进程
                - DLL
        - 用DLL实现Rootkit功能
            - RUNDLL32

        - 特洛伊DLL
            - 函数转发器forward
            - 弱点
        - 动态嵌入技术
            - 创建远程线程
            - 插入ＤＬＬ
            - 地址跳转
    - 代码拦截

7-欺骗攻击

DNS欺骗攻击

- DNS欺骗原理

Email欺骗攻击

- 欺骗方法
- 实现步骤
- 防护

Web欺骗攻击

- 攻击原理
- Web是应用层上提供的服务，直接面向Internet用户，欺骗的根源在于
- 动机
- 形式
    - 使用相似的域名
    - 改写URL
    - 劫持Web会话
- 如何防止

IP欺骗攻击

- 动机
- 形式
    - 单向IP欺骗：不考虑回传的数据包
    - 双向IP欺骗：要求看到回传的数据包
    - 更高级的欺骗：TCP会话劫持
        - 会话(交易)劫持
            - 在现实环境中，比如对于银行一笔交易
            - 原理
            - 方法
- 成功的要诀
- 欺骗的过程
- 如何避免

8-利用处理程序错误的攻击

系统漏洞及攻防

- Windows的经典漏洞
    - 输入法登录漏洞
    - 远程过程调用（RPC）漏洞
- UPnP拒绝服务漏洞
- 其它Windows漏洞
- Windows的防护
- Unix漏洞
- 入侵总计
    - 攻击的六个步骤

Web漏洞及攻防

- Web入侵
- Web的三种安全问题
- Web安全问题的来源
- 常见Web安全问题
- CGI
    - CGI的安全问题
    - CGI的漏洞
- ASP及IIS的安全性

9-访问控制技术

访问控制技术概述

- 访问控制内容包括
- 访问控制的类型
    - 自主访问控制（DAC）
        - 实现方法
            - 基于行的DAC
                - 权限表机制
                - 前缀表（profiles）机制
                - 口令（password）机制
            - 基于列的DAC
                - 保护位机制
                - 访问控制表（ACL）机制
        - 面向过程的访问控制
        - 访问许可权与访问操作权
            - 在DAC策略下，访问许可(accesspermission)权和访问操作权是两个有区别的概念

        - 在DAC模式下，有3种控制许可权手段
            - 层次型的（hierarchical）
            - 属主型的（owner）
        - DAC的优点和缺点
    - 强制访问控制（MAC）
        - MAC机制的实现方法
        - Bell-La Padual模型
            - 简单安全规则
            - 星规则
        - Biba模型
            - 简单完整规则
            - 完整性制约规则（星规则）
    - 木马窃取敏感文件的方法
    - 支持MAC的措施

入网认证

- 身份认证
    - 身份认证的依据
    - 身份认证的评价标准
- 口令认证
    - 口令认证的一般过程
    - 通行字的选择原则
    - 需要考虑的方面
    - 认证方式
    - 一次性口令
        - 不确定因子选择方式

- Kerberos协议

物理隔离措施

- 网络物理隔离方案
  - 客户端的物理隔离
  - 集线器级的物理隔离
  - 服务器端的物理隔离

自主访问控制

强制访问控制

新型访问控制技术

- 基于角色的访问控制技术
  - RBAC（ Role-Based Access Control）
  - NIST（National Institute of Standard Technology）
- 基于任务的访问控制技术
  - TBAC （Task-Based Access Control）
  - 基于组机制的访问控制技术

10-防火墙技术

TCP/IP基础

防火墙

- 防火墙技术概述
  - 经典安全模型
  - 防火墙规则
  - 匹配条件
  - 防火墙分类

        - 按实现的方式分类
        - 按实现技术分类
            - 数据包过滤
            - 应用层代理
    - 状态检测
- 防火墙的结构
    - 经典防火墙体系结构
        - 双重宿主主机体系结构
        - 被屏蔽主机体系结构
        - 被屏蔽子网体系结构
    - 其他体系结构
        - 合并内部和外部路由器
        - 合并堡垒主机和外部路由器
        - 合并堡垒主机和内部路由器
        - 多台内部路由器
        - 多台外部路由器
        - 多个周边网络
- 构建防火墙
    - 选择防火墙体系结构
    - 安装外部路由器
    - 安装内部路由器
    - 安装堡垒主机
    - 设置数据包过滤规则
    - 设置代理系统
    - 检查防火墙运行效果
- 防火墙技术的发展

11-入侵检测

传统的安全技术

- 预防(prevention)、防护（protection)
- 遵循 “正确的安全策略 → 正确的设计 →正确的开发 → 正确的配置与使用

动态安全模型

- P2DR安全模型
    - 策略（Policy）
    - 防护（Protection）
    - 检测（Detection）
    - 响应（Reponse）

入侵检测系统

- 基于主机的入侵检测系统
    - 基于主机的检测威胁
        - 特权滥用
        - 关键数据的访问及修改
        - 安全配置的变化
- 基于网络的入侵检测系统
    - 基于网络的检测威胁
        - 非授权访问
        - 数据/资源的窃取
        - 拒绝服务

入侵检测技术

- 公共入侵检测框架
- 入侵分析——信息收集
- 入侵分析
    - 误用检测（模式匹配）
    - 异常检测（统计分析）
    - 完整性分析，往往用于事后分析
- 入侵检测的分类

    - 按照分析方法（检测方法）
        - 异常检测模型
        - 误用检测模型
- 入侵检测系统分类
    - 离线和在线检测系统
    - 误用检测和异常检测
- 检测数据源
- NT审计机制

入侵检测产品

入侵检测问题

- 新的入侵模式
- 大量的报警信息
- 分布式攻击
- 黑客跟踪

协同

- 数据采集协同
- 数据分析协同
    - 数据挖掘
- 响应协同

其他

- 报警信息融合
- 网络流量异常检测
- 攻击源追踪
- 基于主机的攻击源追踪
- 基于网络的攻击源追踪

入侵检测的发展方向

12-VPN

VPN概述

- 概念
    - 虚拟专用网
- 组成

VPN的分类

- 远程访问虚拟网（Access VPN）
- 企业内部虚拟网（Intranet VPN）
- 企业扩展虚拟网（Extranet VPN）

VPN使用的协议与实现

- VPN使用三个方面的技术保证了通信的安全性
    - 身份验证
    - 隧道协议
    - 数据加密
- VPN的一般验证流程
- 隧道
    - VPN的核心是被称为“隧道”的技术
- 隧道协议
    - 点对点隧道协议
    - 第2层隧道协议
    - IP安全协议
        - IPSec的保护技术
            - AH
            - ESP
        - 工作方式

        - Transmission mode
        - Tunnel mode

16-取证技术

取证的基本概念

- 定义
- 目的
- 电子证据
    - 证据的特点
    - 电子证据的特点
    - 电子证据的优点
    - 电子证据的来源

取证的原则与步骤

- 一般原则
- 计算机取证过程
    - 数据获取
    - 数据分析
    - 证据陈述
- 计算机取证相关技术
    - 数据获取技术
    - 数据分析技术
    - 数据获取、保全、分析技术

蜜罐技术

- 蜜罐概述
    - 主要功能
    - 优点
    - 缺点

- 蜜罐作用
- 分类
- 配置方式
- 发展趋势

取证工具

XMind - Trial Version