网络攻防基础件--课程复习

国家计算机网络入侵防范中心

张玉清

复习纲要

- 课程安排
- 课程内容
- 试卷题型

课程安排

- 课时：60/2
- 内容：课堂讲授 + 实验
- 考核方式：闭卷笔试（40分） + 实验（60分）

课程内容

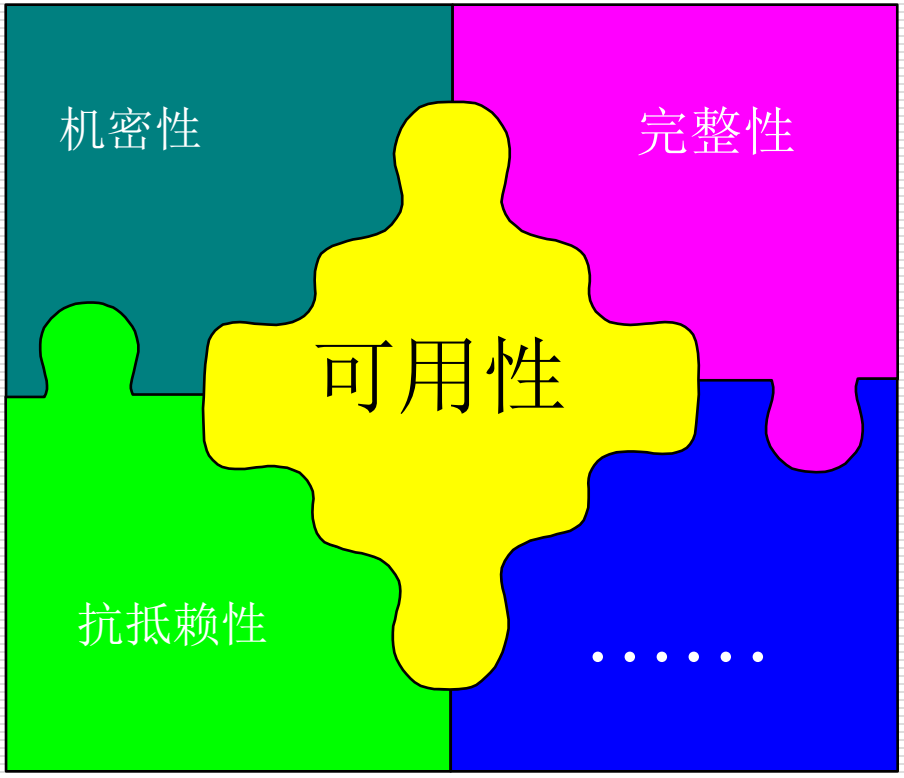
- 第一章　网络安全概述
- 第二章　扫描与防御技术
- 第三章　网络监听及防御
- 第四章　口令破解及防御
- 第五章　欺骗攻击及防御
- 第六章　拒绝服务攻击及防御
- 第七章　缓冲区溢出攻击及防御

第1章 网络安全概述

- 1.1 网络安全基础知识
- 1.2 网络安全的重要性
- 1.3 网络安全的根源
- 1.4 网络攻击过程
- 1.5 网络安全策略及其原则
- 1.6 常用的防护措施

网络安全的基本需求

- 可靠性
- 可用性
- 保密性
- 完整性
- 不可抵赖性
- 可控性
- 可审查性
- 真实性

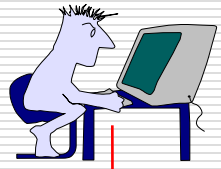


安全漏洞简介

- 漏洞也叫脆弱性（**Vulnerability**），是计算机系统在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷和不足。
- 漏洞一旦被发现，就可使用这个漏洞获得计算机系统的额外权限，使攻击者能够在未授权的情况下访问或破坏系统，从而导致危害计算机系统安全。

网络安全主要威胁来源

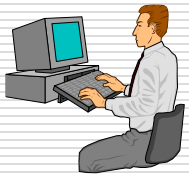
特洛伊木马



黑客攻击

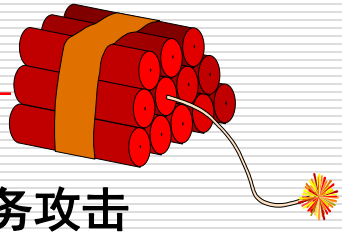
后门、隐蔽通道

计算机病毒

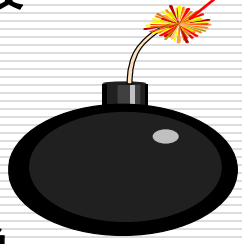


信息丢失、篡改、销毁

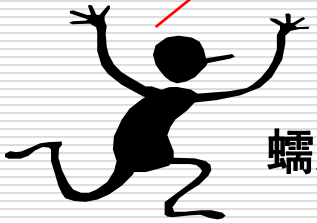
网络



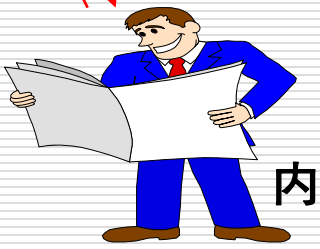
拒绝服务攻击



逻辑炸弹



蠕虫



内部、外部泄密

黑客分类

白帽子创新者
- 设计新系统
- 打破常规
- 精研技术
- 勇于创新

没有最好，
只有更好

MS -Bill Gates
GNU -R.Stallman
Linux -Linus

灰帽子破解者
- 破解已有系统
- 发现问题/漏洞
- 突破极限/禁制
- 展现自我

计算机
为人民服务

漏洞发现 - Flashsky
软件破解 - 0 Day
工具提供 - Glacier

黑帽子破坏者
- 随意使用资源
- 恶意破坏
- 散播蠕虫病毒
- 商业间谍

人不为己，
天诛地灭

入侵者 -K.米特尼克
CIH -陈盈豪
攻击Yahoo -匿名

网络攻击过程

- 入侵一般可以分为本地入侵和远程入侵
- 在这里我们主要讲的是远程的网络入侵：
  - 网络攻击准备阶段
  - 网络攻击的实施阶段
  - 网络攻击的善后阶段

第2章 扫描与防御技术

- 2.1 扫描技术基础
- 2.2 常见的扫描技术
- 2.3 扫描工具赏析
- 2.4 扫描的防御

什么是网络扫描器

- 网络扫描器可以通过执行一些脚本文件来模拟对网络系统进行攻击的行为并记录系统的反应，从而搜索目标网络内的服务器、路由器、交换机和防火墙等设备的类型与版本，以及在这些远程设备上运行的脆弱服务，并报告可能存在的脆弱性。

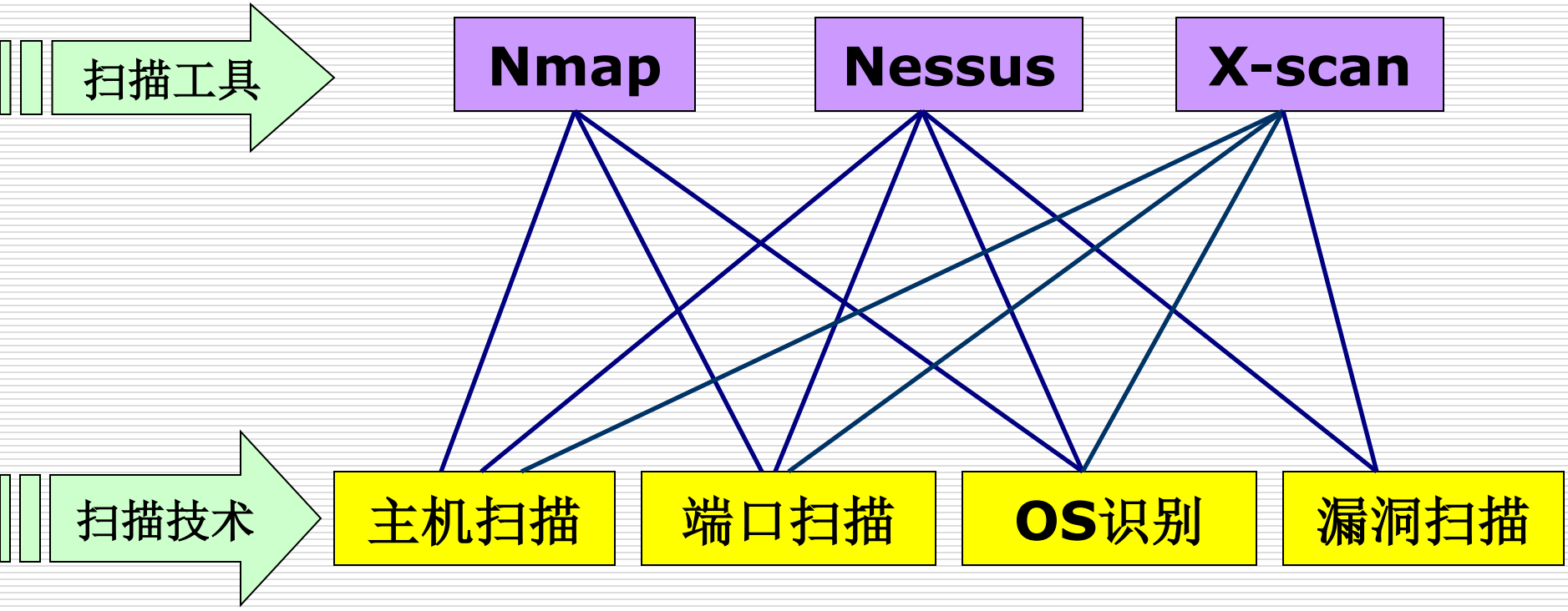
扫描三步曲

- 一个完整的网络安全扫描分为三个阶段：
  - 第一阶段：发现目标主机或网络
  - 第二阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务以及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息
  - 第三阶段：根据收集到的信息判断或者进一步测试系统是否存在安全漏洞

常见的扫描技术

- 主机扫描
- 端口扫描
  - 全扫描
  - 半扫描
  - 秘密扫描
- 远程主机OS指纹识别
- 漏洞扫描

常用扫描工具比较



第3章 网络监听及防御

- 3.1 网络监听概述
- 3.2 监听技术
- 3.3 监听的防御

基础知识

网络监听的概念

- 网络监听技术又叫做网络嗅探技术，顾名思义这是一种在他方未察觉的情况下捕获其通信报文或通信内容的技术。
- 在网络安全领域，网络监听技术对于网络攻击与防范双方都有着重要的意义，是一把双刃剑。
- 网络监听技术的能力范围目前只限于局域网，它是主机的一种工作模式，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。

基础知识

- 网卡的四种工作模式

（1）广播模式：该模式下的网卡能够接收网络中的广播信息。

（2）组播模式：该模式下的网卡能够接受组播数据。

（3）直接模式：在这种模式下，只有匹配目的MAC地址的网卡才能接收该数据帧。

（4）混杂模式：（Promiscuous Mode）在这种模式下，网卡能够接受一切接收到的数据帧，而无论其目的MAC地址是什么。

网络监听防御的通用策略

- 由于嗅探器是一种被动攻击技术，因此非常难以被发现。
- 完全主动的解决方案很难找到并且因网络类型而有一些差异，但我们可以先采用一些被动但却是通用的防御措施。
- 这主要包括采用安全的网络拓扑结构和数据加密技术两方面。

第4章 口令破解及防御

- 4.1 口令的历史与现状
- 4.2 口令攻击方式
- 4.3 典型的口令破解工具
- 4.4 口令攻击的综合应用
- 4.5 口令攻击的防御

词典攻击

- 因为大多数人都会使用普通词典中的单词作为口令，发起词典攻击通常是一个比较好的开端。
- 词典攻击使用的是一个包含大多数词典单词的文件，利用这些单词来猜测口令。

强行攻击

- 如果有速度足够快的计算机能尝试字母、数字、特殊字符所有的组合，将最终能破解所有的口令。这种攻击方式叫做强行攻击（也叫做暴力破解）。
- 使用强行攻击，先从字母**a**开始，尝试**aa**、**ab**、**ac**等等，然后尝试**aaa**、**aab**、**aac** **……**。

组合攻击

- 词典攻击虽然速度快，但是只能发现词典单词口令；强行攻击能发现所有口令，但是破解的时间长。而且在很多情况下，管理员会要求用户的口令是字母和数字的组合，而这个时候，许多的用户就仅仅会在他们的口令后面添加几个数字，例如，把口令从**ericgolf**改成**ericgolf2324**。
- 而实际上这样的口令是很弱的，有一种攻击是在使用词典单词的基础上为单词的串接几个字母和数字，这种攻击就叫做组合攻击。

第5章 欺骗攻击及防御

- 5.1 概述
- 5.2 IP欺骗及防御技术
- 5.3 ARP欺骗及防御技术
- 5.4 电子邮件欺骗及防御技术
- 5.5 DNS欺骗及防御技术
- 5.6 Web欺骗及防御技术

IP欺骗

- 最基本的IP欺骗技术有三种：
  - 基本地址变化
  - 使用源站选路截取数据包
  - 利用Unix机器上的信任关系
- 这三种IP欺骗技术都是早期使用的，原理比较简单，因此效果也十分有限。
- IP欺骗高级应用—TCP会话劫持。

ARP欺骗原理

- **ARP欺骗攻击**是利用**ARP**协议本身的缺陷进行的一种非法攻击，目的是为了在全交换环境下实现数据监听。
- 通常这种攻击方式可能被病毒、木马或者有特殊目的攻击者使用。
- 原理：主机在实现**ARP**缓存表的机制中存在一个不完善的地方，当主机收到一个**ARP**的应答包后，它并不会去验证自己是否发送过这个**ARP**请求，而是直接将应答包里的**MAC**地址与**IP**对应的关系替换掉原有的**ARP**缓存表里的相应信息。

ARP欺骗攻击的防范

- MAC地址绑定，使网络中每一台计算机的IP地址与硬件地址一一对应，不可更改。
- 使用静态ARP缓存，用手工方法更新缓存中的记录，使ARP欺骗无法进行。
- 使用ARP服务器，通过该服务器查找自己的ARP转换表来响应其他机器的ARP广播。确保这台ARP服务器不被黑。
- 使用ARP欺骗防护软件，如ARP防火墙。
- 发现正在进行ARP欺骗的主机并将其隔离。

电子邮件欺骗原理及实现方法

- 执行电子邮件欺骗有三种基本方法，每一种有不同难度级别，执行不同层次的隐蔽。它们分别是：
  - 利用相似的电子邮件地址
  - 修改邮件客户软件设置
  - 远程登录到25号端口

DNS欺骗的原理及实现步骤

- 当客户主机向本地DNS服务器查询域名的时候，如果服务器的缓存中已经有相应记录，DNS服务器就不会再向其他服务器进行查询，而是直接将这条记录返回给用户。
- 而入侵者欲实现DNS欺骗，关键的一个条件就是在DNS服务器的本地Cache中缓存一条伪造的解析记录。

Web欺骗

- Web欺骗是一种电子信息欺骗，攻击者创造了一个完整的令人信服的Web世界，但实际上它却是一个虚假的复制。
- 虚假的Web看起来十分逼真，它拥有相同的网页和链接。然而攻击者控制着这个虚假的Web站点，这样受害者的浏览器和Web之间的所有网络通信就完全被攻击者截获。
- 实例：网络钓鱼

第6章 拒绝服务攻击及防御

- 6.1 拒绝服务攻击概述
- 6.2 典型拒绝服务攻击技术
- 6.3 分布式拒绝服务攻击
- 6.4 拒绝服务攻击的防御
- 6.5 分布式拒绝服务攻击的防御

拒绝服务攻击的概念

- “拒绝服务”这个词来源于英文**Denial of Service**（简称**DoS**），它是一种简单的破坏性攻击，通常攻击者利用**TCP/IP**协议中的某个弱点，或者系统存在的某些漏洞，对目标系统发起大规模的进攻，致使攻击目标无法对合法的用户提供正常的服务。
- 简单的说，拒绝服务攻击就是让攻击目标瘫痪的一种“损人不利己”的攻击手段。

典型拒绝服务攻击技术

- 死亡之Ping（Ping of Death）
- “泪滴”（teardrop）
- IP欺骗DoS攻击
- UDP“洪水”
- SYN“洪水”
- Land攻击

典型拒绝服务攻击技术(Cont.)

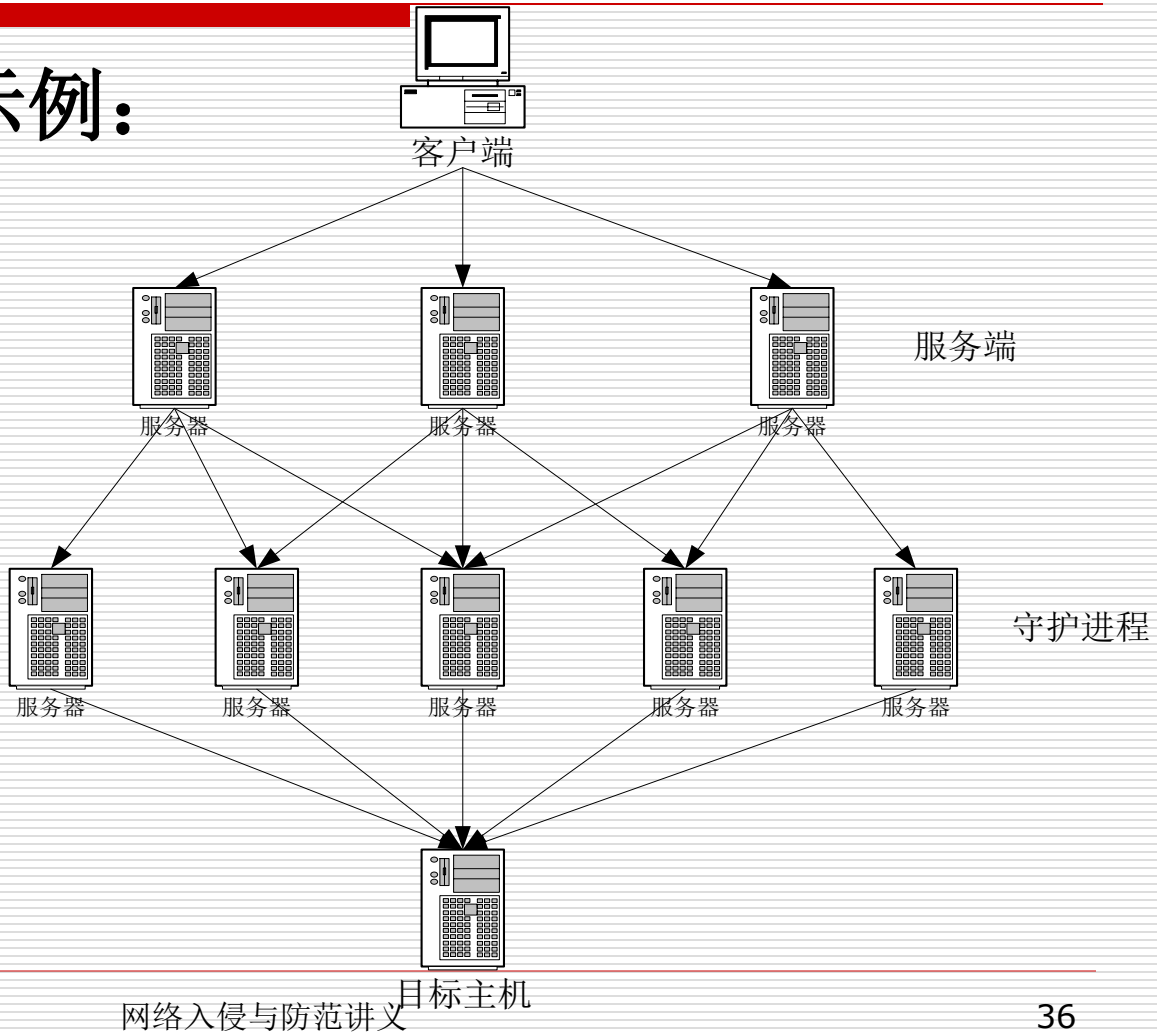
- **Smurf**攻击
- **Fraggle**攻击
- 分布式反射拒绝服务攻击
- 电子邮件炸弹
- 畸形消息攻击
- **Slashdot effect**
- **WinNuke**攻击

分布式拒绝服务攻击

- 分布式拒绝服务**DDoS (Distributed Denial of Service)**攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动**DoS**攻击，从而成倍地提高拒绝服务攻击的威力。
- 利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

分布式拒绝服务攻击(Cont.)

- **DDoS攻击示例：**



第7章 缓冲区溢出攻击及防御

- 7.1 缓冲区溢出概述
- 7.2 缓冲区溢出危害
- 7.3 缓冲区溢出分析
- 7.4 常见的溢出形式
- 7.5 实例：ida溢出漏洞攻击
- 7.6 缓冲区溢出的防御

缓冲区溢出概述

- 什么是缓冲区？它是指程序运行期间，在内存中分配的一个连续的区域，用于保存包括字符数组在内的各种数据类型。
- 所谓溢出，其实就是所填充的数据超出了原有的缓冲区边界，并非法占据了另一段内存区域。
- 两者结合进来，所谓缓冲区溢出，就是由于填充数据越界而导致原有流程的改变，黑客借此精心构造填充数据，让程序转而执行特殊的代码，最终获取控制权。

堆

- 堆(Heap)，用于存储程序运行过程中动态分配的数据块。
- 堆的大小并不固定，可动态扩张或缩减。当进程调用**malloc**等函数分配内存时，新分配的内存就被动态添加到堆上（堆被扩张）；当利用**free**等函数释放内存时，被释放的内存从堆中被剔除（堆被缩减）。
- 随着系统动态分配给进程的内存数量的增加，**Heap(堆)** 一般来说是向内存的高地址方向增长的。

栈(Cont.)

- 函数被调用的时候，栈中的压入情况如下：

缓冲区溢出的原理

- 如果在堆栈中压入的数据超过预先给堆栈分配的容量时，就会出现堆栈溢出，从而使得程序运行失败；如果发生栈溢出的是大型程序还有可能会导致系统崩溃。

试题类型

- 本试卷卷面分共40分（闭卷），本课程其余60分来自实验部分。
- 一 选择题
- 二 判断题
- 三 简答题
- 四 论述题

考试事宜

- 闭卷笔试
- 2025年1月7日晚上18:10-20:10
- 地点：教1-305

100 X 100

感谢!