目录

信息收集阶段，数据来源可分为四类：

入侵检测的分类
误用检测和异常检测的优缺点
主机数据源和网络数据源的优缺点
基于主机的入侵检测
基于网络的入侵检测系统
入侵检测问题
协同
入侵检测的发展方向（lm PPT p104）
IPS（入侵防御系统）

第一章 概述

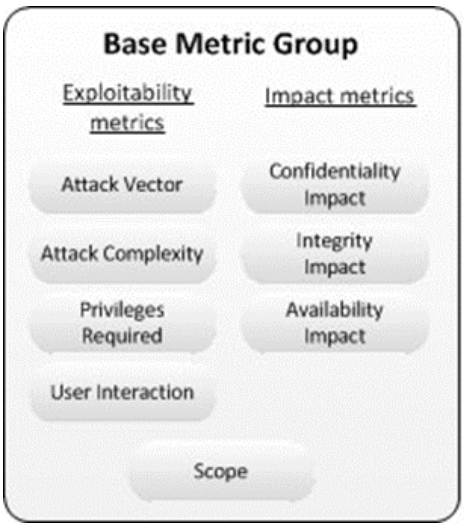
——一些重点的补充

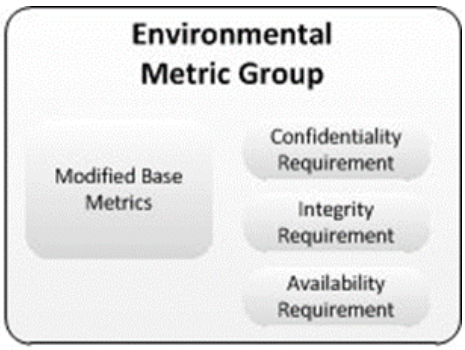
CVSS评分表

CVSS（通用漏洞评分系统），作用是了解CVE漏洞的评分机制，好在以后出现了漏洞的时候利用CVSS标准对该漏洞的实际影响进行评估，从而指导进行下一步操作。

度量指标

CVSS由三个度量组：「基础-Base」，「时间-Temporal」和「环境-Environmental」组成，每一组又由一些度量指标组成，如下：





基础度量组反映了一个漏洞的固有特征——它不随着时间和用户环境的变化而变化。它由两组指标组成：可利用指标和影响指标。包括攻击向量，攻击复杂性，所需权限，用户交互，范围，机密性影响，完整性影响，可用性影响。

可利用指标反映了漏洞可以被利用的简单程度和技术手段。也就是说，它们代表了漏洞易受利用的特征，我们把它称为脆弱的部分。另一方面，**影响指标**反映了成功利用该漏洞可以导致的直接结果，以及受该影响产生的后续结果，我们将其正式称为受影响的组件。

虽然脆弱的组件通常是一个软件应用程序、模块、驱动程序等等(甚至可能是一个硬件设备)，但受影响的组件可能是一个软件应用程序、一个硬件设备或一个网络资源。衡量一个脆弱组件之外的弱点的潜在影响，是CVSS v3.0的一个关键特性。

BaseScore=IF(Scope="C",ROUNDUP(MIN(1.08*(Exp+Impact),10),1),ROUNDUP(MIN(Exp+Impact,10),1))

Impact = IF(Scope="C",7.52*(ISCbase-0.029)-3.25*((ISCbase-0.02)^15), 6.42*ISCbase)

其中：ISCbase = 1 - ((1-C) * (1-I) * (1-A)) ； Exp = 8.22 * AV * AC * PR * UI

时间度量组反映了一个可能随时间而变化的漏洞的特征，但是不跨用户环境。例如，一个易于使用的漏洞利用工具包的出现会增加CVSS分数，而一个官方补丁的创建将会减少它。包括可利用性，补救水平，报告信心。

Temporal = Roundup(BaseScore*E*RL*RC)

环境度量组代表了一个与某个特定用户环境相关且独特的漏洞的特征。这些度量标准允许分析人员合并安全控制，这些控制可以减轻任何后果，也可以根据她的业务风险促进或降低一个脆弱系统的重要性。1包括攻击向量，攻击复杂性，所需权限，用户交互，范围，机密性影响，完整性影响，可用性影响，机密性要求，完整性要求，可用性要求。

Environmental = IF(Scope="C", Roundup(Roundup(Min(1.08*(M.Impact + M.E),10),1),1), Roundup(Min((M.Impact + M.Exp) ,10),1))

M.Impact = IF(Scope="C", 7.52*(M.ISC− 0.029)−3.25*(M.ISC-0.02)^15, 6.42*M.ISC)

其中：M.ISC = Min(1-((1-M.C*CR)*(1-M.I*IR)*(1-M.IA*AR)), 0.915) ； M.Exp = 8.22 * M.AV * M.AC * M.PR * M.UI

P2DR

P2DR模型包括四个主要部分：Policy（安全策略），Protection（防护）、Detection（检测）和Response（响应）。

（lk补充）**感觉这个可信度更高**

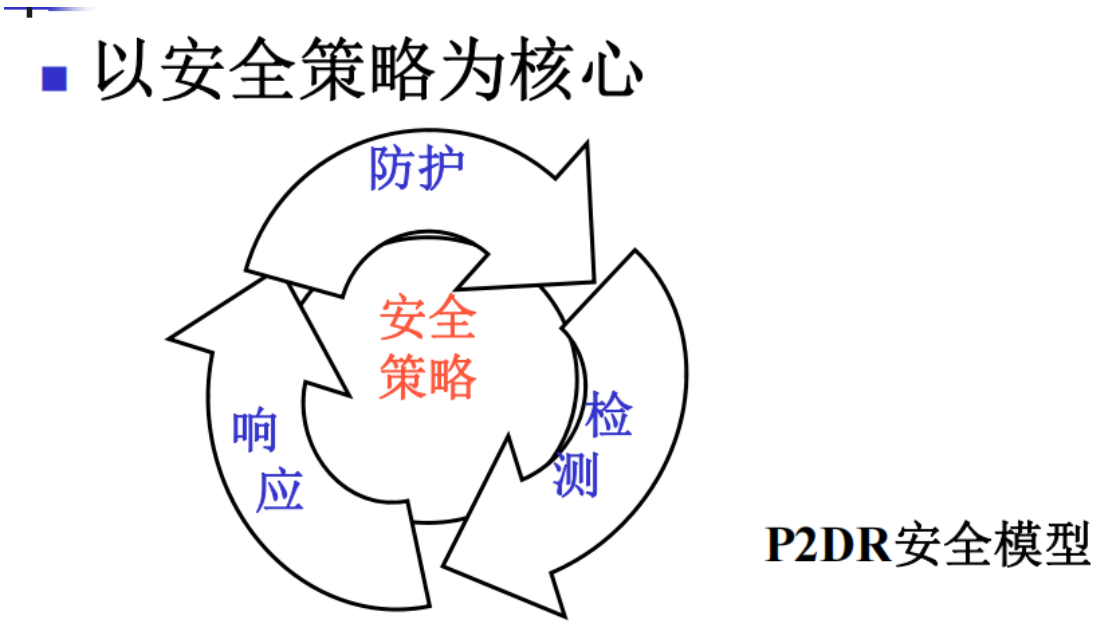
1. 策略：定义系统的监控周期、确立系统恢复机制、制定网络访问控制策略和明确系统的总体安全规划和原则。
2. 防护：通过修复系统漏洞、正确设计开发和安装系统来预防安全事件的发生；通过定期检查来发现可能存在的系统脆弱性；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监视等手段来防止恶意威胁。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。
3. 检测：是动态响应和加强防护的依据，通过不断地检测和监控网络系统，来发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。
4. 响应：系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

P2DR模型是在整体安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认真、加密等）的同时，利用检测工具（如漏洞评估、入侵检测等）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

该理论最基本的的**原理**就是，认为信息相关的所有活动，不管是攻击行为、防护行为、检测行为和响应行为都要消耗**时间**。因此可以用时间来衡量一个体系的安全性和安全能力。

P2DR模型总结：及时的检测和响应就是安全；及时的检测和恢复就是安全。

P2DR缺点：忽略了内在的变化因素，如人员的流动、人员的素质和策略贯彻的不稳定性。实际上，安全问题牵涉面很广，除了涉及到的防护、检测和响应，系统本身的安全“免疫力”增强、系统和整个网络的优化以及人员这个在系统中最重要角色的素质的提升，都是该安全系统没有考虑到的问题。



- 策略（Policy）：是模型的核心，具体的实施过程中，策略意味着网络安全要达到的目标。
- 防护（Protection）：安全规章、安全配置、安全措施
- 检测（Detection）：异常监视、模式发现
- 响应（Reponse）：报告、记录、反应、恢复

PDRR

PDRR模型是一种网络安全模型，由美国国防部提出，它是防护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）四个环节的缩写。该模型旨在改进传统只注重防护的单一安全防御思想，强调信息安全保障的全面性和动态性。

PDRR模型的四个环节包括：

- 保护（Protect）：采用可能采取的手段保障信息的保密性、完整性、可用性、可控性和不可否认性。
- 检测（Detect）：利用高级术提供的工具检查系统存在的可能提供黑客攻击、白领犯罪、病毒泛滥脆弱性。
- 反应（React）：对危及安全的事件、行为、过程及时作出响应处理，杜绝危害的进一步蔓延扩大，力求系统尚能提供正常服务。
- 恢复（Restore）：一旦系统遭到破坏，尽快恢复系统功能，尽早提供正常的服务。

PDRR模型的优点是：

- 全面性：PDRR模型涵盖了保护、检测、反应和恢复这四个关键环节，可以提供全面的安全保护措施，使网络和系统能够有效地应对安全威胁。
- 动态性：该模型强调了安全保障的动态性，不仅关注防护措施，还注重检测、响应和恢复环节，以及持续改进和适应不断变化的安全威胁的能力。

然而，由于PDRR模型的描述比较简略，具体实施过程和细节可能会因组织和具体情境而有所差异。因此，根据具体需求和环境，可能需要进一步细化和定制该模型以确保安全策略的有效性和适应性

第二章 网络攻击行径分析

Teardrop攻击

攻击原理

Teardrop攻击是一种**畸形报文攻击。** 是基于UDP的病态分片数据包的攻击方法。 其工作原理是向被攻击者发送多个分片的IP包（IP分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有**重叠偏移**的伪造分片数据包时将 会出现系统崩溃、重启等现象。

它利用的是系统在实现时的一个错误，即攻击特定的IP协议栈实现片段重组代码存在的缺陷。当网络分组穿越不同的网络时，有时候需要根据网络最大传输单元MTU来把它们分割成较小的片，早期的Linux系统在处理IP分片重组问题时，尽管对片段是否过长进行检查，但对过短的片段却没有进行验证，所以导致了泪滴形式的攻击，会造成系统的死机或重新启动。

防范措施

防御泪滴攻击的最好办法是**升级服务包软件**，如下载操作系统补丁或升级操作系统等。另外，在设置防火墙时对分组**进行重组而不进行转发**，也可以防止这种攻击。

IGMP flood

Internet Group Management Protocol(因特网组管理协议)是用于管理因特网协议多播组成员的一种通信协议。IP主机和相邻的路由器利用IGMP来建立多播组的组成员。

攻击者使用受控主机向被攻击目标发送大量的ICMP/IGMP报文，进行洪水攻击以消耗目标的宽带资源，这种类型的攻击出现的很早，使用hping等工具就能简单的发起攻击。但现在使用这种方法发动的攻击已见不多，被攻击目标可以在其网络边界直接过滤并丢弃ICMP/IGMP数据包使攻击无效化。

但是这种直接方式通常依靠受控主机本身的网络性能，所以效果不是很好，还容易被查到攻击源头。于是反射攻击就出现。

第三章 网络侦察知识点

口令破解

黑客攻击目标时常常把破译普通用户的口令作为攻击的开始

- 分析漏洞破解口令：如果能够得到口令验证代码

- 思路
  - Crack
    - 如果能够修改口令验证代码
  - Vulnerability
    - 如果不能修改代码，但可以构造恶意输入
    - 通过引发代码指针异常，改变控制流绕过口令检查
    - 通过引发数据指针异常，导致任意位置读或写
  - Keygen
    - 如果能够破解口令验证算法
    - 通过口令验证算法漏洞，逆推口令

- 知识点
  - 编译与逆向
    - IDA pro, GHIDRA
    - windbg, ollydbg
  - 加壳与脱壳
    - PE文件格式
    - 反逆向、反跟踪
- 学习资料
  - https://www.kanxue.com/
  - https://www.52pojie.cn/

- 离线破解口令：如果能够得到口令密文

- 在线破解口令：如果能够访问口令验证系统

第四章 拒绝服务知识点

拒绝服务攻击的概念

定义、攻击思想和方法 、分类（PPT+课本）

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。**

同步包风暴 SYN Flooding

攻击原理【课本P63】

黑客通常通过伪造的源IP地址或端口，向服务器发送大量的SYN报文，请求建立TCP连接。由于源IP地址或端口是伪造的，服务器发送的SYN-ACK报文永远不会被真实的客户端接收和回应。极少数情况下，黑客也会使用真实源IP地址，但他们只是通过攻击工具发送海量SYN报文，工具并不会响应来自服务器SYN-ACK报文。无论如何，服务器都接收不到ACK报文，产生了大量的半连接。此时服务器需要维持一张巨大的等待列表，不停地重试发送SYN-ACK报文，同时大量的资源无法释放。当服务器被这些恶意的半连接占满时，就不会再响应新的SYN报文，从而导致正常的用户无法建立TCP连接。

防范措施【课本P66】

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

攻击原理

课本P67

发送伪装的ICMP数据包，目的地址设为某个网络的广播地址，源地址设为要攻击的目的主机，使所有收到此ICMP数据包的主机都将对目的主机发出一个回应，使被攻击主机在某一段时间内收到 成千上万的数据包。

ping 风暴 课本P68

防范措施

（从三个方面回答，课本P68）

被攻击者利用进行攻击的中间网络应采取的措施

被攻击的目标应该采取的措施

攻击者攻击实际发起的网络应采取的措施

利用处理程序错误【课本P69】

- **ping of death**

原理：根据TCP/IP协议的规范，一个包的长度最大为65536字节。尽管一个包的长度最大不能超过65536字节，但是一个包分成的多个片段的叠加却能做到。当一个主机收到了长度大于65536字节的包时，就是受到了Ping of Death攻击，该攻击会造成主机死机。攻击者故意创建一个长度大于65536字节(P协议中规定最天的P包长为65536字节)的Pnig包，并将该包发送到目标受害主机，由于目标主机的服务程序无法处理过大的包，而引起系统崩溃、挂起或重新启动。

**防范*：现在所有的标准TCP/IP实现都已实现对付超大尺寸的包，并且大多数防火墙能够自动过滤这些攻击，包括：从windows98之后的windows,NT(service pack 3之后)，linux、Solaris、和Mac OS都具有抵抗一般ping of death攻击的能力。此外，对防火墙进行配置，阻断ICMP以及任何未知协议，都能防止此类攻击。

- **Teardrop**

检测方法：对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。

防范：网络安全设备将接收到的分片报文先放入缓存中，并根据源IP地址和目的IP地址对报文进行分组，源IP地址和目的IP地址均相同的报文归入同一组，然后对每组IP报文的相关分片信息进行检查，丢弃分片信息存在错误的报文。为了防止缓存溢出，当缓存快要存满时，直接丢弃后续分片报文。

添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。尽可能采用最新的操作系统，或者在防火墙上设置分段重组功能，由防火墙先接收到同一原包中的所有拆分数据包，然后完成重组工作，而不是直接转发。

- **winnuke**

检测方法：检测数据包目的端口是否为139，并且检查TCP-URG位是否被设置

防范：此类攻击是由于利用软件开发过程中对某种特定类型的报文或请求没有处理，导致软件遇到这类型报文时运行出现异常，软件崩溃甚至系统崩溃。防范此类攻击的方法就是**升级系统或给系统打补丁**，也可以删除NetBIOS协议或关闭137、138、139端口。

- **Land**

检测方法：判断网络数据包的源地址和目标地址是否相同
防范：适当配置防火墙设备或路由器的过滤规则就可以防止这种攻击行为(一般是丢弃该数据包，记录事件发生的时间、源主机和目标主机的MAC地址以及IP地址并对这种攻击进行审计)

第六章 程序攻击知识点

逻辑炸弹攻击

逻辑炸弹攻击是一种利用恶意代码隐藏在程序中，等待特定条件触发后执行恶意操作的攻击。

攻击原理

1. 插入恶意代码：攻击者在目标系统或程序中插入恶意代码，通常是通过软件开发过程中的后门或恶意修改来实现。
2. 触发条件设置：恶意代码会等待特定条件满足，例如特定的日期、时间、文件内容、系统状态等。一旦条件满足，逻辑炸弹将被激活。
3. 执行恶意操作：当逻辑炸弹被触发时，恶意代码会执行预定的恶意操作，例如删除文件、损坏数据、传播恶意软件等。

防范措施

1. 安装更新的防病毒软件：安装最新版本的防病毒软件可以帮助您检测和删除逻辑炸弹。
2. 不要打开来自未知来源的电子邮件附件：不要打开来自未知来源的电子邮件附件，尤其是那些看起来不寻常或不可信的附件。
3. 定期更新操作系统和应用程序：定期更新操作系统和应用程序可以帮助您修补已知的漏洞，从而减少逻辑炸弹攻击的风险。
4. 使用网络安全设备：使用网络安全设备，如防火墙、入侵检测系统和入侵防御系统等，可以帮助您检测和阻止逻辑炸弹攻击。

计算机病毒

计算机病毒是一种恶意软件，通过感染计算机系统或文件来传播并执行恶意代码。不同类型的计算机病毒有不同的攻击原理和防范措施，包括DOS病毒、宏病毒、脚本病毒和PE病毒等。

攻击原理和防范措施如下：

1. DOS病毒（磁盘操作系统病毒）：
    - 攻击原理：DOS病毒感染计算机的引导扇区或主引导记录，以在系统启动时执行恶意代码。它们可以破坏硬盘的分区表或操作系统引导过程。
    - 防范措施：使用安全的引导扇区和引导记录，定期备份数据，并使用可信的杀毒软件进行系统扫描。
2. 宏病毒：
    - 攻击原理：宏病毒利用应用程序中的宏功能，通过感染文档来传播并执行恶意代码。常见的宏病毒存在于办公软件（如Microsoft Office）中。
    - 防范措施：禁用或限制宏的自动执行功能，只允许可信来源的宏执行，及时更新和使用杀毒软件进行扫描。
3. 脚本病毒：
    - 攻击原理：脚本病毒是利用脚本语言（如JavaScript、VBScript）编写的恶意代码。它们可以通过感染网页、电子邮件附件或下载的脚本文件来传播。
    - 防范措施：使用安全的浏览器和电子邮件客户端，禁用自动执行脚本功能，及时更新和使用杀毒软件进行扫描。
4. PE病毒（可执行文件病毒）：
    - 攻击原理：PE病毒感染可执行文件，以在执行时传播并执行恶意代码。它们可以修改程序的执行逻辑或添加恶意功能。
    - 防范措施：使用可信的下载渠道和软件供应商，仔细检查下载的可执行文件的完整性和数字签名，定期更新和使用杀毒软件进行扫描。

防范计算机病毒的常见技术包括：

1. 特征值检测技术：通过检测已知病毒的特征值（如病毒代码或行为模式）来识别和阻止病毒的传播。这需要及时更新病毒特征库。
2. 行为监测技术：监测系统或应用程序的异常行为，如文件的非正常修改、网络通信的异常活动等，以便及时检测和阻止病毒的活动。
3. 启发式扫描技术：通过分析文件的代码和行为模式来检测未知病毒。这种技术可以识别病毒的新变种，但也可能导致误报警情况。
4. 虚拟机技术：使用虚拟机环境来运行可疑文件或应用程序，以隔离和限制病毒的传播和影响范围。这可以提供更安全的环境进行病毒分析。

综上所述，防范计算机病毒需要使用多种技术和措施，包括特征值检测、行为监测、启发式扫描和虚拟机技术等。同时，用户也应保持系统和应用程序的及时更新，避免下载和打开可疑来源的文件，以减少计算机病毒的风险。

RootKit

Rootkit是一种恶意软件，其攻击目标是获取对操作系统的完全控制，常用于隐藏恶意活动和维持持久性访问。下面是Rootkit的攻击原理和防范措施的介绍：

攻击原理

1. 隐藏文件和进程：Rootkit通过修改操作系统的文件系统和进程列表，将恶意文件和进程隐藏起来，使它们在常规检测和监控中不可见。
2. 欺骗系统工具：Rootkit可以修改或欺骗系统工具和API调用的结果，以隐藏恶意活动的痕迹。例如，它可以篡改文件属性、进程状态和网络连接等信息。
3. 欺骗内核：Rootkit可以通过修改内核的数据结构和函数调用来欺骗操作系统的内核部分，从而逃避安全检测和防御机制。
4. 提供后门访问：一些Rootkit可能会创建隐藏的后门，允许攻击者远程访问被感染的系统，并执行恶意操作。

防范措施

1. 定期更新和打补丁：保持操作系统和应用程序的更新，安装最新的安全补丁，以修复已知的漏洞，减少Rootkit的利用机会。
2. 强化访问控制：实施严格的访问控制策略，限制对系统和关键文件的访问权限，确保只有授权的用户和进程可以进行敏感操作。
3. 使用防病毒和反Rootkit软件：定期扫描系统并使用可信赖的防病毒和反Rootkit软件来检测和清除Rootkit的感染。
4. 监控和行为分析：实施实时监控和行为分析，以侦测异常活动和不寻常的行为模式。这些技术可以帮助及早发现Rootkit的存在和活动。
5. 安全启动和固件保护：使用安全启动（Secure Boot）技术，确保系统在启动时只加载经过验证的操作系统和驱动程序。另外，使用固件保护功能，防止Rootkit通过修改固件进行攻击。
6. 审查系统配置和文件完整性：定期检查系统配置文件和关键文件的完整性，以及不明文件或进程的存在。及时发现和处理异常可以减少Rootkit的持续存在。
7. 加强安全意识教育：培养用户对于网络安全的意识，教育用户避免点击可疑链接、下载未经验证的文件或执行不明来源的代码。

综上所述，防范Rootkit的攻击需要综合使用多种技术和措施，包括系统更新、访问控制、防病毒软件、监控和行为分析等。同时，定期审查系统和加强用户的安全意识也是非常重要的。

邮件炸弹

邮件炸弹和垃圾邮件是两种常见的恶意邮件攻击形式，它们的攻击原理和防范措施如下：

邮件炸弹的攻击原理： 邮件炸弹是一种通过发送大量邮件给特定目标邮箱，以使目标邮箱系统过载或崩溃的攻击方式。 攻击者使用自动化脚本或恶意软件，发送大量邮件到目标邮箱，通常是以邮件列表、重复发送或者大附件的形式。这会导致目标邮箱系统资源消耗过多，包括带宽、存储和处理能力，从而导致系统运行缓慢或崩溃。

邮件炸弹的防范措施：

1. 邮件服务器配置：配置邮件服务器的反垃圾邮件功能，设置阈值来限制每个邮箱的邮件数量和频率。这可以帮助检测和阻止大量的邮件流量。
2. 流量监控和限制：监控邮件服务器的网络流量和资源消耗情况，及时检测异常流量并采取限制措施，如限制特定IP地址或域名的连接数或带宽。
3. 安全过滤和识别：使用安全软件或服务来过滤和识别垃圾邮件和邮件炸弹。这些工具可以根据特定的规则、黑名单、白名单或机器学习算法来检测和阻止恶意邮件。

垃圾邮件

垃圾邮件的攻击原理： 垃圾邮件是指大量发送给广泛目标的无用或欺诈性的邮件。攻击者发送垃圾邮件的目的可能是推销产品、传播恶意软件、进行钓鱼或欺诈行为等。

垃圾邮件的防范措施：

1. 垃圾邮件过滤：使用垃圾邮件过滤技术和工具，例如基于规则、内容分析、黑名单、白名单和机器学习算法等方法来识别和过滤垃圾邮件。这些技术可以检测垃圾邮件的特征、关键词、发送者的信誉等信息。
2. 反垃圾邮件政策：制定并实施反垃圾邮件政策，明确组织的邮件使用规范和限制，包括禁止发送垃圾邮件、限制外部邮件发送权限等。这可以帮助组织减少垃圾邮件的传播和影响。
3. 用户教育和安全意识：加强用户对垃圾邮件的识别和防范意识，教育用户避免打开垃圾邮件附件、点击垃圾邮件中的链接或提供个人信息等。用户的谨慎和警惕可以减少垃圾邮件攻击的成功率。
4. 邮件服务器配置和限制：对邮件服务器进行适当的配置和限制，限制每个用户的邮件发送量和频率。这可以减少恶意用户或恶意软件利用邮件服务器进行大规模垃圾邮件发送。

综上所述，防范邮件炸弹和垃圾邮件攻击需要使用合适的技术和策略，包括邮件服务器配置、流量监控、安全过滤、垃圾邮件过滤、反垃圾邮件政策和用户教育等。

IE攻击

IE（Internet Explorer）攻击是指针对Internet Explorer浏览器的安全漏洞进行的恶意攻击。攻击者利用这些漏洞来执行恶意代码、植入恶意软件、窃取用户信息等。以下是IE攻击的攻击原理和防范措施的介绍：

攻击原理

1. Exploit利用：攻击者通过发现或购买已知或未知的IE浏览器漏洞，开发相应的Exploit工具或恶意代码。这些Exploit利用浏览器的漏洞，将恶意代码注入到用户的计算机上。
2. 社交工程：攻击者可能利用社交工程技术，通过诱导用户点击恶意链接、下载恶意附件或访问感染的网站，来触发IE浏览器的漏洞并进行攻击。
3. 恶意广告和插件：攻击者可能通过恶意广告或恶意插件来感染用户的IE浏览器。这些广告或插件可能利用浏览器漏洞，执行恶意代码或将用户重定向到恶意网站。

防范措施

1. 及时更新和打补丁：确保IE浏览器及其相关组件（如ActiveX控件）始终处于最新版本，并及时应用官方发布的安全补丁。这可以修复已知的漏洞，减少攻击者利用的机会。
2. 安全配置：加强IE浏览器的安全配置，例如限制网站对ActiveX和插件的使用、禁用自动运行功能、启用强密码保护、设置安全级别等。这可以减少恶意代码的执行和恶意网站的访问。
3. 安全软件：使用可信赖的安全软件（如防病毒软件、防火墙、反间谍软件等），定期进行系统扫描和实时监测，以检测和阻止恶意代码和攻击。
4. 用户教育：加强用户的安全意识和教育，教导用户避免点击可疑链接、下载未经验证的文件、访问不信任的网站等。用户的警惕性可以减少IE攻击的成功率。
5. 多浏览器策略：在可能的情况下，使用多个浏览器并定期更新它们。这样，即使某个浏览器存在漏洞，其他浏览器也可以提供额外的安全保护。

综上所述，防范IE攻击需要综合使用多种技术和措施，包括及时更新和打补丁、安全配置、安全软件、用户教育和多浏览器策略等。同时，定期关注官方安全公告和最新威胁情报，以及加强网络安全意识和实践，也是重要的防范措施。

第七章 欺骗攻击知识点

DNS欺骗攻击

攻击原理

DNS 欺骗攻击，是**攻击者冒充域名服务器**，把用户查询的域名地址更换成攻击者的 IP 地址，然后攻击者将自己的主页取代用户的主页，这样访问用户主页的时候只会显示攻击者的主页，这就是DNS欺骗的原理。DNS欺骗并不是“黑掉”了真正的服务器的主页，而是替换成攻击者的主页，将真正的服务器主页隐藏起来无法访问而已。

DNS欺骗的实现，是利用了DNS协议设计时的一个安全缺陷：在一个局域网内，攻击者首先**使用ARP欺骗，使目标主机的所有网络流量都通过攻击者的主机。**之后攻击者通过**嗅探目标主机发出的DNS请求分组**，分析数据分组的ID和端口号后，向目标主机发送**攻击者构造好的 DNS 返回分组**，目标主机收到 DNS 应答后，发现 ID和端口号全部正确，即把返回的数据分组中的域名和对应的IP地址保存进DNS缓存，而后到达的真实DNS应答分组则被丢弃。

防范措施

首先，DNS攻击存在一定的局限性：

- 攻击者不能替换缓存中已存在的记录，这也就是我们为什么要在实验开始时刷新受害机的DNS缓存的原因
- DNS服务器缓存时间的刷新（每隔一段时间电脑中DNS缓存会重新刷新）

防范措施：

(from openWHU)

- 在DNS欺骗之前一般需要使用ARP攻击来配合实现，因此，首先可以做好**对ARP欺骗的防御工作**，如设置静态ARP映射、安装ARP防火墙等。

- 使用**代理服务器**进行网络通信，本地主机对通过代理服务器的所有流量都可以加密，包括DNS信息。
- 尽量访问带有https标识的站点，带有https标识的站点因为有SSL证书，难以伪造篡改，如果浏览器左上角的https为红色叉号，需要提高警惕。
- 使用DNSCrypt等工具，DNSCrypt是OpenDNS发布的加密DNS工具，可加密DNS流量，阻止常见的 DNS 攻击，如重放攻击、观察攻击、时序攻击、中间人攻击和解析伪造攻击。DNSCrypt支持Mac OS和Windows，是防止DNS污染的绝佳工具，如图5所示。DNSCrypt使用类似于SSL的加密连接向DNS服务器拉取解析，所以能够有效对抗DNS劫持、DNS污染以及中间人攻击。
- 关闭DNS服务器的递归功能（这个我没懂为什么，有懂的可以点击这一个block左边六饼的comment留言）
- 使用最新版本的DNS服务器软件，及时安装补丁
- 保护内网设备，DNS攻击一般都是从内网中发起的，如果你的内网设备很安全，那么也就不存在被感染的风险

（from ChatGPT)

- 使用可信赖的DNS解析器：选择受信任的DNS解析器，避免使用未经验证的公共DNS服务器。
- 配置防火墙：配置防火墙以限制对DNS服务器的访问，只允许来自受信任的IP地址的查询和响应。
- 使用DNSSEC：DNSSEC是一种安全扩展协议，可以验证域名解析的完整性和身份验证，防止DNS响应被篡改。
- 定期更新和监控：定期更新DNS服务器的软件和配置，并监控网络流量以检测异常的DNS响应。
- 加密通信：使用安全的传输层协议（如HTTPS）来保护DNS查询和响应的机密性，防止中间人攻击。
- 增加安全意识：教育用户如何警惕钓鱼网站和恶意链接，以减少受到DNS欺骗攻击的风险

Email攻击

防范：

为了防范这些攻击，用户和组织可以采取一些措施，如：

- 教育用户，提高他们对电子邮件安全的意识，教授他们如何识别和应对垃圾邮件、钓鱼邮件和其他欺诈行为。
- 谨慎点击和下载附件，确保其来源可信，避免打开未知的文件或链接。
- 使用强密码，并定期更改密码。同时，启用多因素身份验证（MFA）来增加账户的安全性。
- 定期更新和维护电子邮件应用程序和防病毒软件，以及其他安全工具，以确保及时防御新的威胁。
- 部署反垃圾邮件和反钓鱼技术，以帮助过滤和阻止潜在的恶意邮件。
- 对于企业和组织，建立安全策略和流程，包括培训员工、监控网络流量和实施安全审核等措施，以确保电子邮件系统的安全性。

通过采取这些措施，可以增强对电子邮件应用的安全防御，减少受到攻击的风险。

Web欺骗攻击

攻击原理

攻击者通过伪造某个WWW站点的影像拷贝，使该Web的入口进入到攻击者的Web影像服务器，并经过攻击者机器的过滤作用，从而达到攻击者监控受攻击者的任何活动以获取有用信息的目的。

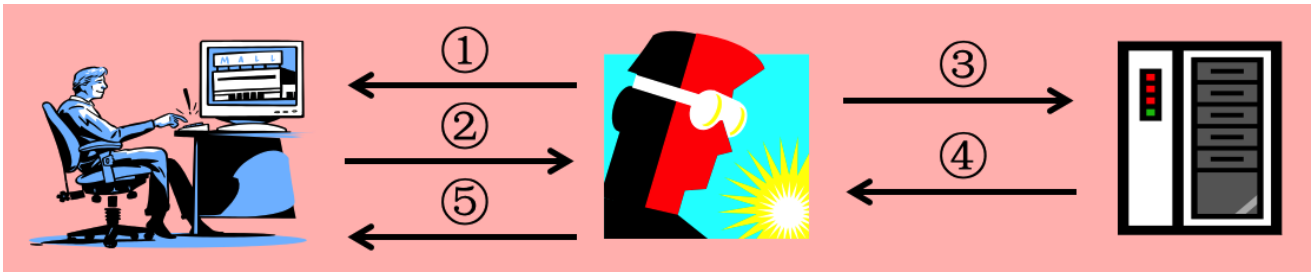
攻击者能够监视被攻击者的网络信息，记录他们访问的网页和内容。当被攻击者填完一个表单并发送后，这些数据将被传送到Web服务器，Web服务器将返回必要的信息，但不幸的是，攻击者完全可以截获并使用这些信息。在得到必要的数据后，攻击者可以通过修改受害者和Web服务器两方任何一方数据，来进行破坏活动。攻击者可以修改受害者的确认数据，攻击者还可以修改Web服务器返回的数据。

Web欺骗能够成功的关键是在受害者和真实Web服务器之间插入攻击者的Web服务器，这种攻击常被称为“中间人攻击“。攻击者改写Web页中的所有URL地址，使它们指向攻击者的Web服务器不是真正的Web服务器。

Web欺骗的形式：

- 使用相似的域名
- 改写URL
- 劫持Web会话

改写URL的工作流程：



- 用户访问伪造过的http://www.hacker.net/；
- http://www.hacker.net/向http://www.dhs.com/请求文档；
- http://www.dhs.com/向http://www.hacker.net/返回文档；
- http://www.hacker.net/改写文档中的所有URL；
- http://www.hacker.net/向用户返回改写后的文档

劫持Web会话 会话劫持（Session hijacking），这是一种通过获取用户Session ID后，使用该Session ID登录目标账号的攻击方法，此时攻击者实际上是使用了目标账户的有效Session。会话劫持的第一步是取得一个合法的会话标识来伪装成合法用户，因此需要保证会话标识不被泄漏。

- 目标用户需要先登录站点；
- 登录成功后，该用户会得到站点提供的一个会话标识SessionID；
- **攻击者通过某种攻击手段捕获Session ID；（攻击的要点）**
- 攻击者通过捕获到的Session ID访问站点即可获得目标用户合法会话。

HTTP协议不支持会话(无状态)，Web会话如何实现？（ppt上提到Cookie、用url记录会话、用表单中的隐藏元素记录会话；目前有三种广泛使用的在Web环境中 维护会话\传递Session ID 的方法：URL参数，隐藏域和Cookie。）

- 基于 server 端 session 的管理方式
- cookie-base 的管理方式
- token-base 的管理方式

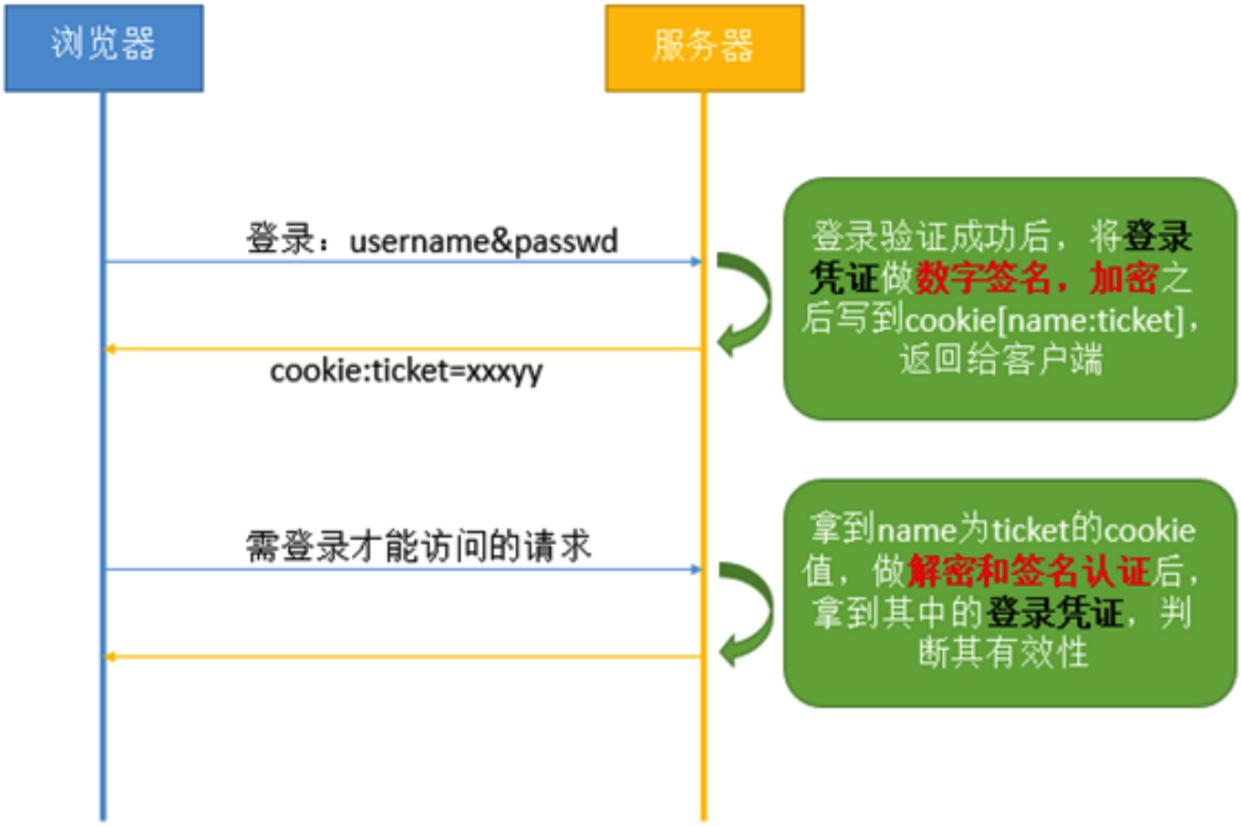
Web Session 是建立在 HTTP 层之上的服务管理机制，在实现 Session 机制时，必然会用到 HTTP 的某些特性，比如 cookie， 当然也可以实现不依赖于 cookie 的 Session 机制，尤其是 cookie 有可能会被人为的禁止；另一种技术是 URL 重写技术，就是把 session id 直接附加在 URL 路径的后面。

Cookie 由于前一种方式（基于 server 端 session 的管理方式）会增加服务器的负担和架构的复杂性，所以后来就有人想出直接把用户的登录凭证直接存到客户端的方案，当用户登录成功之后，把登录凭证写到cookie里面，并给cookie设置有效期，后续请求直接验证存有登录凭证的cookie是否存在以及凭证是否有效，即可判断用户的登录状态。使用它来实现会话管理的整体流程如下：

1）用户发起登录请求，服务端根据传入的用户密码之类的身份信息，验证用户是否满足登录条件，如果满足，就根据用户信息创建一个登录凭证，这个登录凭证简单来说就是一个对象，最简单的形式可以只包含用户id，凭证创建时间和过期时间三个值。

2）服务端把上一步创建好的登录凭证，先对它做数字签名，然后再用对称加密算法做加密处理，将签名、加密后的字串，写入cookie。cookie的名字必须固定（如ticket），因为后面再获取的时候，还得根据这个名字来获取cookie值。这一步添加数字签名的目的是防止登录凭证里的信息被篡改，因为一旦信息被篡改，那么下一步做签名验证的时候肯定会失败。做加密的目的，是防止cookie被别人截取的时候，无法轻易读到其中的用户信息。

3）用户登录后发起后续请求，服务端根据上一步存登录凭证的cookie名字，获取到相关的cookie值。然后先做解密处理，再做数字签名的认证，如果这两步都失败，说明这个登录凭证非法；如果这两步成功，接着就可以拿到原始存入的登录凭证了。然后用这个凭证的过期时间和当前时间做对比，判断凭证是否过期，如果过期，就需要用户再重新登录；如果未过期，则允许请求继续。



防范措施

防范改写URL手段：

- 配置网络浏览器使它总能显示目的URL，并且习惯查看它。
- 检查源代码，如果发生了URL重定向，就一定会发现。不过，检查用户连接的每一个页面的源代码对普通用户来说是不切实际的想法。
- 使用反网络钓鱼软件。
- 禁用JavaScript、ActiveX或者任何其他在本地执行的脚本语言。
- 确保应用有效和能适当地跟踪用户。无论是使用cookie还是会话ID，都应该确保要尽可能的长和随机。
- 培养用户注意浏览器地址线上显示的URL的好习惯。培养用户的安全意识和对开发人员的安全教育。

防范劫持Web会话

目前有三种广泛使用的在Web环境中维护会话（传递Session ID）的方法：URL参数，隐藏域和Cookie。其中每一种都各有利弊，Cookie已经被证明是三种方法中最方便最安全的。从安全的观点，如果不是全部也是绝大多数针对基于Cookie的会话管理机制的攻击对于URL或是隐藏域机制同样适用，但是反过来却不一定，这就让Cookie成为从安全考虑的最佳选择。

1、 更改Session名称。PHP中Session的默认名称是PHPSESSID，此变量会保存在Cookie中，如果攻击者不分析站点，就不能猜到Session名称，阻挡部分攻击。

2、 关闭透明化Session ID。透明化Session ID指当浏览器中的Http请求没有使用Cookie来存放Session ID时，Session ID则使用URL来传递。

3、 设置HttpOnly。通过设置Cookie的HttpOnly为true，可以防止客户端脚本访问这个Cookie，从而有效的防止XSS攻击。

4、 关闭所有phpinfo类dump request信息的页面。

5、验证HTTP头部信息

6、养成显式注销的习惯

7、使用长的会话ID

防范使用类似的域名

- 注意观察URL地址栏的变化
- 不要信任不可靠的URL信息

（from ChatGPT)

Web欺骗攻击的目的通常是窃取用户的敏感信息、进行金融欺诈、传播恶意软件或执行其他恶意操作。为了防范Web欺骗攻击，用户和网站管理员可以采取以下防护措施：

- 提高用户的安全意识，教育用户如何辨别可疑的网站和URL，避免点击来路不明的链接;
- 注意域名和URL的细微差别，仔细检查拼写错误或类似字符，尤其是在访问敏感网站时。
- 使用HTTPS协议，确保与网站之间的通信加密，以防止中间人攻击和数据篡改。
- 定期更新和修补Web应用程序的安全漏洞，以减少攻击者利用漏洞的机会。
- 防止跨站点脚本（XSS）漏洞，对用户输入的数据进行适当的过滤和验证，避免恶意脚本的注入。
- 实施会话管理和身份验证的最佳实践，包括使用强密码、多因素身份验证和定期的会话失效。
- 部署Web应用程序防火墙（WAF）和入侵检测系统（IDS）等安全工具来检测和阻止恶意活动。

综合使用这些防护措施可以增强Web应用程序和用户的安全性，并降低受到Web欺骗攻击的风险。

IP欺骗攻击

攻击原理

IP 欺骗攻击指攻击行动产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。这是一种黑客的攻击形式，黑客使用一台计算机上网，而借用另外一台机器的 IP 地址，从而冒充另外一台机器与服务器进行交互。

防范措施

(lm PPT p24)

- 主机保护，两种考虑
  - 保护自己的机器不被用来实施IP欺骗
    - 物理防护、登录口令
    - 权限控制，不允许修改配置信息
  - 保护自己的机器不被成为假冒的对象
    - 无能为力
- 网络防护
  - 路由器上设置欺骗过滤器
    - 入口过滤，外来的包带有内部IP地址
    - 出口过滤，内部的包带有外部IP地址
- 保护免受源路由攻击
  - 路由器上禁止这样的数据包

(from ChatGPT)

避免IP欺骗是确保网络安全的重要一环。以下是从主机保护、网络防护和保护免受源路由攻击三个方面的建议：

1. 主机保护：

- 使用防火墙：配置和使用防火墙来限制进入和离开主机的网络流量。防火墙可以过滤和监视网络数据包，阻止未经授权的访问和IP欺骗尝试。
- 定期更新和维护：确保主机操作系统和应用程序始终处于最新状态，并及时应用安全补丁和更新。这有助于修复已知漏洞，提高主机的安全性。
- 安全设置和授权：限制主机的网络服务和端口的访问权限，只允许必要的服务和端口开放，并设置强密码和身份验证措施，以防止未经授权的访问。

2. 网络防护：

- 使用网络入侵检测系统（IDS）和入侵防御系统（IPS）：部署IDS和IPS来监测和阻止恶意的IP欺骗行为。这些系统可以分析网络流量，并根据预定义的规则或异常行为来检测和防止IP欺骗攻击。
- 网络流量监控和日志记录：定期监控网络流量和日志记录，识别异常或可疑的IP活动。及时检测并响应异常行为可以防止IP欺骗攻击的成功。
- VPN使用：对于涉及远程访问或敏感数据传输的情况，使用虚拟私人网络（VPN）来建立加密的隧道连接，确保数据的机密性和完整性，并防止IP欺骗的影响。

3. 保护免受源路由攻击：

- 使用反源路由过滤（Reverse Path Filtering）：反源路由过滤是一种网络防护技术，用于验证网络流量的源IP地址是否可达。通过配置反源路由过滤规则，可以防止源路由攻击，确保接收到的数据流量来自预期的源IP地址。
- BGP安全设置：对于使用边界网关协议（BGP）的网络，配置和实施BGP安全措施，如路由策略过滤、BGP加密、BGP消息认证等，以防止源路由攻击。

综上所述，通过主机保护、网络防护和保护免受源路由攻击三个方面的措施，可以减少IP欺骗的风险，并提升网络的

安全性。

（？不知道是什么）ActiveX control的安全性

- 下载ActiveX control
  - 通过数字签名来识别control的受信任程度
    - 验证数字签名，PKI中的可信任根CA
- 安装和注册ActiveX control
  - 已经在调用ActiveX control的代码了
  - 并且，它可以自己声明自己是安全的
    - 操纵注册表
- 对象的初始化
  - 创建对象，并且对对象进行初始化，ActiveX control是一个永久对象
- 对象的脚本操作
  - 通过脚本调用对象的方法
- -〉Active Document

TCP Session Hijack

我们可以把会话劫持攻击**分为两种类型**：

1）中间人攻击(Man In The Middle，简称MITM)（这也就是我们常说的“中间人攻击”，在网上讨论比较多的就是SMB会话劫持，这也是一个典型的中间人攻击。要想正确的实施中间人攻击，攻击者首先需要**使用ARP欺骗**或**DNS欺骗**，将会话双方的通讯流暗中改变，而这种改变对于会话双方来说是完全透明的。）

2）注射式攻击（Injection）（它不会改变会话双方的通讯流，而是在双方正常的通讯流插入恶意数据。在注射式攻击中，需要实现两种技术：1）IP欺骗；2）预测TCP序列号）

并且还可以把会话劫持攻击**分为两种形式**：

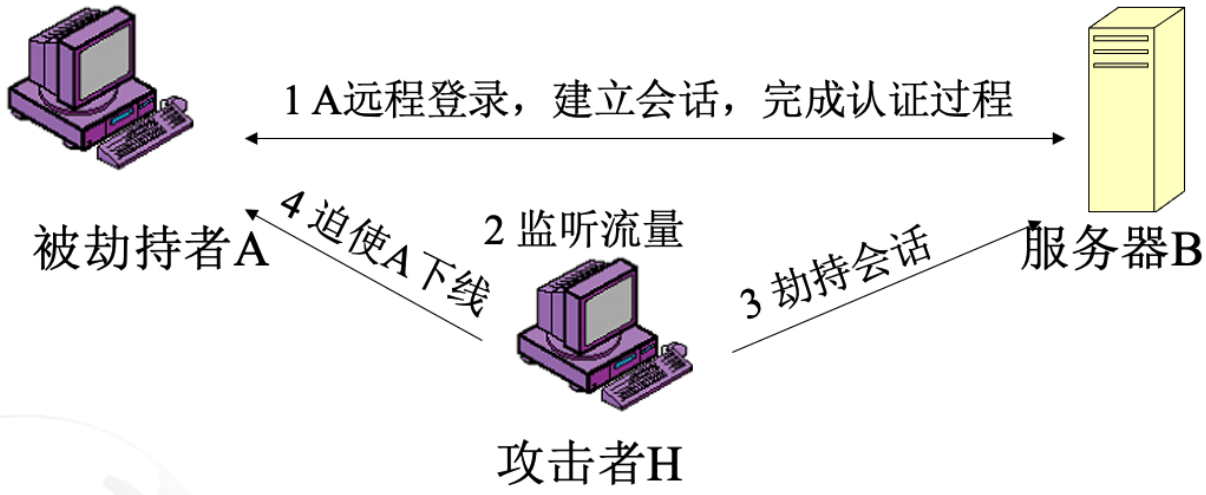
1）被动劫持，被动劫持实际上就是在后台监视双方会话的数据流，从中获得敏感数据

2）主动劫持，而主动劫持则是将会话当中的某一台主机“踢”下线，然后由攻击者取代并接管会话，这种攻击方法危害非常大，攻击者可以做很多事情

会话劫持（Session Hijack）: 就是结合了嗅探以及欺骗技术在内的攻击手段。例如，在一次正常的会话过程当中，攻击者作为第三方参与到其中，他可以在正常数据包中插入恶意数据，也可以在双方的会话当中进行监听，甚至可以是代替某一方主机接管会话。

（欺骗是伪装成合法用户，以获得一定的利益；劫持是积极主动地使一个在线的用户下线，或者冒充这个用户发送消息，以便达到自己的目的）

会话劫持示意图：



攻击原理

lm PPT p31

防范措施

- 部署共享式网络，用交换机代替集线器
- TCP会话加密
- 防火墙配置：限制尽可能少量的外部许可连接的IP地址
- 检测：ACK包的数量明显增加

第十章 防火墙技术知识点

（彭佳琳ver 不足再加）

- 防火墙
  - 模型-经典安全模型（书p231第一二段）
  - 概念-书p230概述的一二段；
  - 规则

    处理方式-ACCEPT，REJECT，DROP；注意REJECT和DROP的区别（ppt有）；

    基本原则-默认允许or默认拒绝

    默认拒绝安全性更好，在配置无误的情况下，通过的一定安全，但是安全的不一定能通过；

    默认允许服务性更强，在配置无误的情况下，通过的一定不安全，但是不安全的也可能通过；
  - 匹配条件

    网络层：源ip，目的ip，网络层（ICMP）以及传输层的协议号（例如标识了TCP，UDP等），匹配是否源路由数据报（指定必须经过某几个路由器的数据报）

    传输层：源端口，目的端口

    应用层：各个应用不一样；比如拒绝ftp的PORT命令之类的。

    信息流向：向外，向内（根据网络环境设定的）
  - 分类

    实现技术（同防火墙技术方案）-数据包过滤&应用层代理（ppt我觉得够了）

    防范领域-个人防火墙&网络防火墙（ppt有提到设置的要点）

    按照实现的方式-软件&硬件（突然发现书上有，p238，包括安装在哪里和提供的服务，硬件包含一个芯片架构的名字）
  - 两种技术方案的对比

    ppt上挺全的分点。
- 防火墙结构

  ppt蛮全的；

  就双重宿主主机，被屏蔽主机，被屏蔽子网三大架构
- 构建实例(最后的部分)

  ppt上有一个针对WWW，FTP，BBS，EMAIL，DNS进行配置的，不想蒙题了，对着仿写吧

第十一章 入侵检测技术

入侵检测系统是什么

入侵检测是一种动态的网络安全技术：

- 利用各种不同类型的引擎，实时地或定期地对网络中相关的数据源进行分析，依照引擎对特殊的数据或事件的认识，将其中具有威胁性的部分提取出来，并触发响应机制。
- 入侵检测的动态性反映在入侵检测的实时性、对网络环境的变化具有一定程度上的自适应性，这是以往静态安全技术无法具有的

入侵检测技术原理

书p288

入侵分析

在一个环境中，审计信息必须与它要保护的系统分开来存储和处理

- 防止入侵者通过删除审计记录来使入侵检测系统失效
- 防止入侵者通过修改入侵检测器的结果来隐藏入侵的存在
- 要减轻操作系统执行入侵检测任务带来的操作负载

信息收集阶段，数据来源可分为四类：

- 来自主机的：基于主机的监测收集通常在操作系统层的来自计算机内部的数据，包括操作系统审 计跟踪信息和系统日志
- 来自网络：检测收集网络的数据
- 来自应用程序：监测收集来自运行着的应用程序的数据，包括应用程序事件日志和其它存储在应 用程序内部的数据
- 来自目标机：使用散列函数来检测对系统对象的 修改。

入侵分析

- 误用检测
- 异常检测
- 完整性分析，往往用于事后分析

入侵检测的分类

离线和在线检测系统、误用检测和异常检测

按照分析方法（检测方法）

- 异常检测模型（Anomaly Detection)：首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵 。
- 误用检测模型（Misuse Detection)：收集非正常操作的行为特征，建立相关的特征库，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 。

误用检测和异常检测的优缺点

误用检测：

优点：

- 模式匹配具有很强的可分割性、独立性
- 能提供更有效的入侵检测引擎
- 模式匹配具有很强的针对性，对已知的入侵方法检测效率很高

缺点：

- 可测量性与性能都和模式数据库的大小体系结构有关；
- 可扩展性差
- 需要及时更新模式数据库
- 通常不具备自学习能力
- 攻击行为转化为模式比较困难

异常检测：

优点：

- 符合数据的异常变化理论，适合事务的发展规律
- 对变量的跟踪不需要大量的内存
- 异常检查对模式匹配发现不了的某些新的攻击具有检测与响应的能力

缺点：

- 数据假设可能不合理，加权算法在统计意义上可能不准确；
- 对突发性正常事件容易引起误判断“对长期、稳定的攻击方法灵敏度太低

主机数据源和网络数据源的优缺点

主机数据源（lm PPT p45）：

优点：

- 可利用操作系统本身提供的功能，因此检测效率 高，速度快
- 可结合操作系统和应用程序的行为特征，得出更为准确的报告
- 可检测针对本机的入侵行为

缺点

- 依赖于系统的可靠性
- 主机提供的信息有限
- 对网络层的入侵无能为力
- 必须为不同操作系统开发不同的程序
- 增加系统负荷

网络数据源（lm PPT p50）：

优点：

- 可以对整个子网进行检测
- 不影响现存的数据源，不改变系统和网络的工作模式
- 不影响主机性能和网络性能
- 被动接收方式，隐蔽性好
- 对基于网络协议的入侵手段有较强的分析能力

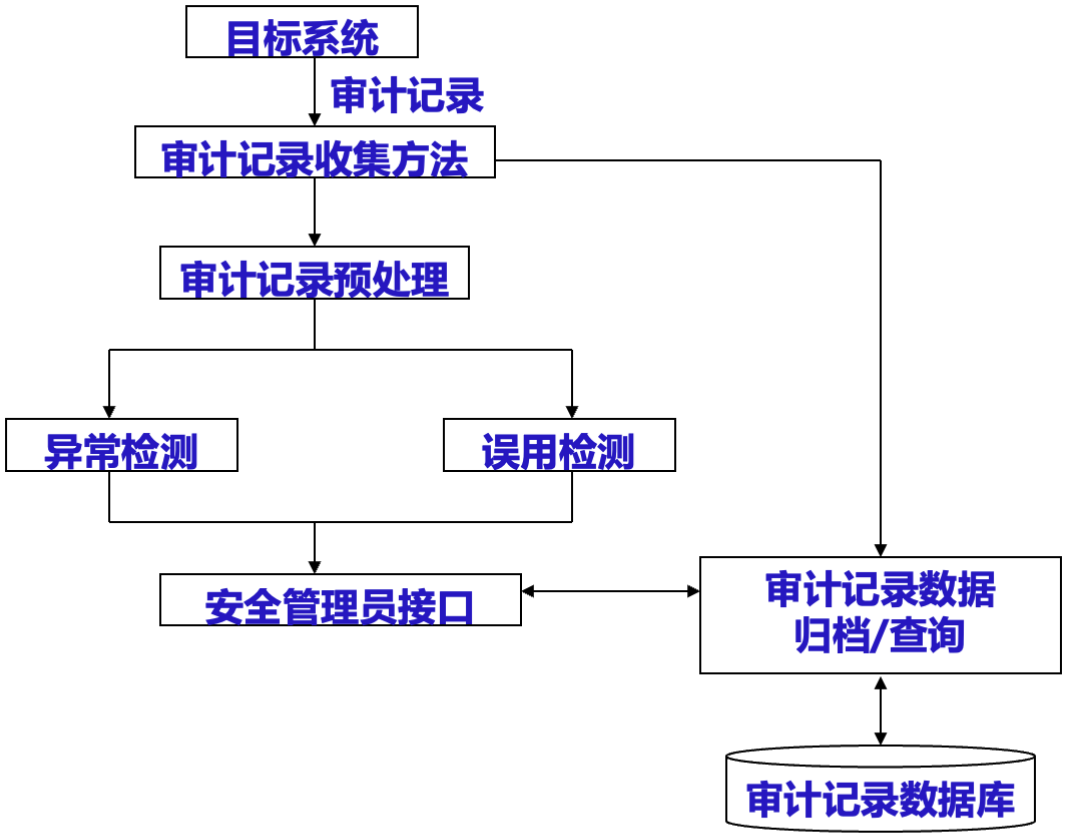
缺点：

- 检测效率
- 网络流量日益增大的挑战
- 虚警和漏警的平衡
- 应用于交换环境出现的问题

基于主机的入侵检测

优点：威慑内部人员；检测；通告及响应；毁坏情况评估；攻击预测；诉讼支持；行为数据辨析

面临的问题：性能：降低是不可避免的；部署/维护；欺骗：审计源



基于主机的入侵检测系统结构示意图

基于网络的入侵检测系统

入侵检测问题

协同

目前DDS实现的功能是相对初级的

IDS也需要充分利用数据信息的相关性 IDS作为网络安全整体解决方案的重要部分， 与其他安全设备之间应该有着紧密的联系 IDS需要一种新的系统体系来克服自身的不足并将IDs的各个功能模块与其他安全产品有机地融合起来，这就需要引入协同的概念

- 数据采集协同
- 数据分析协同
- 数据挖掘
- 响应协同

IDS的不足：

1. 误报：把本来不是入侵的访问判断成入侵
2. 把实际的入侵判断为正常的访问

入侵检测的发展方向（lm PPT p104）

1. 体系结构方面进一步研究分布式入侵检测与通用入侵检测框架
2. 应用层入侵检测
3. 智能的入侵检测
4. 提供高层统计与决策
5. 响应策略与恢复研究
6. 入侵检测的评测方法
7. 和其他网络安全部件的协作、与其他安全技 术的结合

IPS（入侵防御系统）

入侵防御系统（Intrusion Prevention System，IPS）是一种网络安全设备或软件，旨在监测和防止网络中的入侵行为和安全漏洞。IPS通过实时监控网络流量、分析和识别潜在的入侵行为，并采取相应的措施来阻止或防御这些入侵。

以下是入侵防御系统的一些关键特点和功能：

1. 实时监测：IPS对网络流量进行实时监测和分析，通过检查数据包的源、目的地、协议、内容等信息来识别潜在的入侵行为。
2. 入侵检测：IPS使用各种技术和算法来检测已知的入侵行为模式，例如基于规则的检测、基于签名的检测、行为分析等，以识别和报告可能的安全威胁。
3. 实时响应：当IPS检测到入侵行为时，它可以立即采取相应的措施来阻止或防御入侵，例如阻止恶意流量、断开连接、发送警报等。
4. 漏洞管理：IPS可以监测并报告系统和应用程序中的安全漏洞，并提供建议和措施来修补这些漏洞，以防止潜在的攻击。
5. 入侵预防：除了检测和响应入侵行为外，IPS还可以采取主动措施来防止潜在的入侵。它可以通过网络阻断、安全策略强制执行、访问控制等技术来阻止未经授权的访问和恶意活动。
6. 日志和报告：IPS记录和存储有关入侵事件、安全事件和网络流量的详细信息，并生成报告和日志，以便进行后续的安全分析、审计和调查。

入侵防御系统（IPS）在提供实时的入侵检测和防御能力方面起着重要作用。它帮助组织识别并应对网络中的安全威胁，提高网络的安全性和保护敏感数据免受未经授权的访问和恶意活动的影响。