网络攻防技术课程报告

对网络攻防技术课程的全面学习总结

姓名　廖汉钦

学号　2018091620024

课程名称　网络攻防技术

指导老师　赵洋

专业　软件工程互联网安全方向

2020 年 12 月 15 日

摘要

网络攻防作为网络安全概念中的核心概念，有着举足轻重的意义。本学期网络攻防课程的学习将向我们介绍网络攻防中的某些概念、技术和意义。课程将从绪论及概述描述网络攻防大致轮廓，接着将详细分析各网络协议安全性，介绍身份认证技术、访问控制技术、网络隔离技术、网络扫描技术以及各常见漏洞威胁和恶意代码种类。课程向我们详细介绍每一部分内容，每一部分内容都为我们深刻理解网络攻防核心意义打下更为夯实的基础。

第一章 绪论及概述

随着计算机互联网的普遍普及，互联网前景越来越好，全球经济正在以一个极快的速度向着更高级的互联网经济发展，而这其中的信息安全甚至网络安全则显得格外重要。

1.1 何为信息和信息安全?

用香农的话来说就是“信息就是用来消除随机和不确定性的东西”。信息具备有价值性、可传递性、载体依附性、时效性、真伪性、共享性、可处理性等一系列特性。

而信息安全就是“对信息的保密性、完整性和可用性的保持，也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他特征。”

1.2 信息安全的基本属性

一，保密性，信息对未授权的个人、实体或过程不可用或不泄露的特性；二，完整性，信息保持准确和完备的特性；三：可用性：根据授权实体的要求，可以访问和可以使用的特性。以上属性被称为信息安全 CIA 三要素。同时，信息安全还具备如真实性、抗抵赖性、可靠性等多种属性。

1.3 何为网络安全?

从本质上来讲，网络安全就是网络上的信息安全。由于网络系统普遍存在的脆弱性，网络安全无时无刻地存在着各种安全威胁。而当攻击者利用了一个或多个安全威胁进行攻击，则称网络安全受到了安全攻击。

安全攻击分为五种类型：被动攻击、主动攻击、物理临近攻击、内部人员攻击以及配装分发攻击。

被动攻击指被动地监视网络上的信息传递过程或内容，被攻击者无察觉。

主动攻击指避开或破坏安全部件，引入恶意代码，破坏数据或系统完整性，被攻击者有察觉。

物理临近攻击指未授权的个人近距离物理接触，以修改、收集信息或者拒绝对信息的访问。

内部人员攻击指在信息安全处理系统物理边界内的合法人员或者能够直接访问信息安全处理系统的人员发起的攻击。

配装分发攻击指硬件或软件在生产、安装以及运输过程中，被恶意地修改。

1.4 OSI 模型

既然有相关威胁和攻击，就必须提供一个系统的架构，指导可实现的安全标准的设计以及提供一个通用的术语平台。这就是 OSI 参考模型。

OSI 模型提供了五种安全服务：认证服务、访问控制服务、数据保密性服务、数据完整性服务以及不可否认服务和八种安全机制：加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制以及公证。安全服务体现网络信息系统的安全需求，而安全机制是实现安全服务采取的具体技术措施，两者是多对多的关系：安全服务可以用不同的安全机制来实现，安全机制可以用来实现不同的安全服务。

第二章 网络协议的安全性分析

本章将对各网络协议的安全状况进行全面了解，探究其中网络安全威胁产生的原因，掌握常见的网络协议安全威胁的基本工作原理和过程。

2.1 TCP/IP 协议安全概述

互联网设计之初的使用目的是用于科学研究，其基本假设就是节点的诚实性；由于计算机网络的广泛使用，这种假设在今天已经无法成立，因此可能导致各种各样的攻击。安全性问题包括：设计缺陷导致的安全性问题以及实现缺陷导致的安全性问题，前者会一直存在，直至协议更新，而后者会随着软件的更新而消除。而总的安全威胁可分为三类：信息泄漏、消息伪造和拒绝服务。

2.2 网络接口层协议安全分析

2.2.1 网络嗅探

共享环境下的网络嗅探：对网卡进行原始套接字编程，设置为接受来自所有 IP 的包，将网卡设置为混杂模式，来获取网络接口上侦听道德所有数据包。

交换环境下的网络嗅探（交换机毒化）：攻击者发送大量的具有不同伪造源 MAC 地址的帧，由于交换机的自学习功能，这些新的“MAC 地址—接口”映射对会填充整个交换机表，而这些表项都是无效的，结果交换机完全退化为广播模式，攻击者达到窃听数据的目的。

2.2.2 ARP 欺骗

互联网上是使用 IP 地址来定位主机，而但在交换机上是通过 MAC—接口映射来实现主机间数据帧的发送，因此需要使用 ARP 协议完成 IP 地址和 MAC 地址的转换。

ARP 协议为改进效率的特殊设计：响应 ARP 请求的主机将请求者的 IP－MAC 映射缓存、主动的 ARP 应答会被视为有效信息接受。这导致 ARP 协议有着以下缺陷：没有认证、无状态以及需要定时更新。

此时攻击者可以，在局域网段发送虚假的 IP/MAC 对应信息，篡改网关 MAC 地址，使自己成为假网关，分析收到的数据包，记录有价值数据，再把数据包转发给真正的网关。这将导致正常主机受到嗅探、中间人攻击以及拒绝服务等攻击的威胁。

2.3 网络层协议安全分析

2.3.1 IP 假冒攻击

由于 IP 协议本身没有验证源 IP 地址真实性的机制，所以攻击者可以构造 IP 地址为随机地址的 IP 报文，从而达到拒绝服务攻击和网络欺骗的目的。

2.3.2 IP 碎片攻击

IP 数据包最长只能为 0xFFFF，就是 65535 字节。如果有意发送总长度超过 65535 的 IP 碎片，或构造畸形的 IP 碎片，部分操作系统在进行碎片重组处理时会导致崩溃或拒绝服务。

Ping of Death 攻击：攻击者发送一个长度超过 65535 的 Echo Request 数据包，目标主机在重组分片的时候会造成事先分配的 65535 字节缓冲区溢出，系统通常会崩溃或挂起。

Teardrop 攻击：攻击者设计一种畸形的碎片，使得这个碎片的长度为一负值，但在计算机系统中该负值被认为一个非常大的正数，这将导致系统崩溃。

2.4 传输层 TCP 协议安全分析

2.4.1 拒绝服务攻击

因为三次握手需要存储连接状态，产生系统开销，所以攻击者向一个特定主机连续不断地发送大量 TCP 连接请求，可以使目标主机因为资源消耗太大而瘫痪。

2.4.2 SYN Flooding 攻击

攻击者向目标主机发送大量带有虚假地址地请求，由于地址是伪造的，所以目标主机在发送回复信息后一直等不到回传的消息，这一过程会消耗大量的资源，所以在攻击者发送大量伪地址请求后，目标主机资源会被耗尽。

SYN Flooding 攻击只需要很少的流量便可产生显著效果，并且攻击来源无法定位。可以通过在防火墙上过滤来自同一主机的后续连接请求或者使用 SYN Cookie 来防御。

2.4.3 其他针对 TCP 协议的攻击

ACK Flooding：向目标主机发送大量 ACK 状态数据包，目标主机会花费大量资源检测数据包包含的连接四元组是否存在。

序列号猜测攻击（会话劫持）：攻击者通过猜测序列号，在 TCP 会话中插入自己构造的数据包。

Land 攻击：构造一个 SYN 包，其源地址和目标地址都被设置成某一个服务器地址，并发送给该服务器。服务器将和自己建立空连接，直至超时。

2.5 传输层 UDP 协议安全分析

2.5.1 UDP 假冒

修改 UDP 报文中的源 IP 地址，即可完成 IP 地址假冒攻击。

2.5.2 UDP 劫持

劫持一个正常 UDP 连接，通过篡改报文中的源 IP 地址，从而起到嗅探的作用。

2.6 应用层 DNS 协议安全分析

2.6.1 DNS 欺骗

攻击者拦截 DNS 服务器向正常客户端发送的响应报文，并修改其中的内容。

2.6.2 DNS 猜测攻击

攻击者向 DNS 服务器发送大量查询请求以及大量猜测 ID 的伪造应答数据包，那么当正常客户端发送正常请求时，就有极大可能 ID 已被攻击者猜测，从而获得一个错误的响应报文。

2.6.3 DNS 缓存毒化

攻击者通过假冒 DNS 服务器或者篡改 DNS 服务器中的缓存内容，从而导致

正常客户端或者正常 DNS 服务器向攻击者服务器发送请求时得到的是被篡改过的错误记录。

2.6.4 基于 DNS 的拒绝服务攻击

攻击者向 DNS 服务器发送大量请求，其中的源地址为目标主机的 IP 地址，则目标主机将会收到大量来自 DNS 服务器的应答报文，从而消耗大量资源至崩溃。

2.7 应用层 HTTP 协议安全分析

2.7.1 HTTP 钓鱼攻击

攻击者通过编写一个页面与正常网站页面一摸一样的网站，从而获得用户输入的内容（如用户名和密码等）。

2.7.2 跨站攻击

浏览器对网页的展现是通过解析 HTML 代码实现的，如果传入的参数含有代码，浏览器会解析它而不是原封不动的展示。此时如果攻击在页面中注入了恶意代码，浏览器将解析它们从而执行一些攻击者期望的操作。

第三章 身份认证技术

3.1 身份认证技术概述

身份认证是指证实主体的真实身份与其所声称的身份是否相符的过程。身份认证可分为用户（代表用户的进程）与主机间的认证和主机与主机之间的认证。身份认证可用于验证用户对抗假冒、依据身份实施控制以及明确责任便于审计。

身份认证可按认证因子数量分为单因子认证、双因子认证和多因子认证，可按认证因子状态分为静态认证和动态认证。

3.2 基于口令的身份认证

为系统中所有合法用户分配一个唯一的身份标识 ID（用户名、账号名），并由用户设置或系统分配一个与 ID 关联的口令（Password）。认证时，用户通过出示凭据｛ID，Password｝来完成身份认证。

3.2.1 口令猜测与穷举攻击

原理：利用用户信息安全意识不高，口令质量不高，实施的口令猜测或穷举攻击。

防范：可以通过设置安全口令、强化口令安全策略以及增加认证信息量来防范。

3.2.2 口令嗅探攻击

原理：利用网络协议采用明文或简单编码方式传输口令，通过网络嗅探方式获取用户口令。

防范：采用加密方式进行口令传输。

3.2.3 口令窃取攻击

原理：如果口令以明文方式存储，攻击者可以通过攻击存储口令的服务器或者通过木马监听用户键盘输入获取用户口令。

防范：使用基于单向函数的口令认证以及使用安全控件对关键数据进行加密。

3.2.4 口令重放攻击

原理：通过网络嗅探获取包含口令等认证信息的数据包，在随后的验证过程中使用该数据包发起身份认证请求，欺骗认证服务器。

防范：使用动态口令。

3.3 基于对称密码的身份认证

ISO/IEC9798-2 协议：使用对称共享密钥对时间戳或者一次性随机数进行加密，从而进行身份认证。

使用第三方的认证协议：通过可信第三方实现会话密钥的建立，实现身份认证。

3.4 基于公钥密码的身份认证

通信的一方想要认证另一方的身份，就必须使用公钥密码算法生成数字签名，通过验证这个数字签名来进行身份认证。

第四章 访问控制技术

4.1 访问控制技术概述

访问控制就是通过某种途径显式地准许或限制访问能力及范围的一种方法。

通过限制对关键资源的访问，防止非法用户侵入或因合法用户的不慎操作而造成的破坏，从而保证网络资源受控地、合法地使用，它是针对越权使用资源的防御措施。

访问控制三元组：主体，发出访问指令、存取要求的主动方；客体，被访问的对象；访问控制策略，用以确定一个主体是否对客体拥有访问能力的规则集。

访问控制工作流程：确权、审核、决策。

4.2 访问控制应用模型

所谓访问控制应用模型就是用来描述主体、客体间授权关系的一种形式化方式。

4.2.1 自主访问控制

根据访问者的身份和授权来决定访问模式，对访问进行限定的一种控制策略。

与业务和应用场景无关，灵活性较高。但是存在以下问题：不能实现全局性访问控制、不能区分所有权和访问权以及不能体现严格的组织架构。

4.2.2 强制访问控制

由安全管理员统一对主体和客体的安全标签赋值，普通用户不能改变。客体的安全级表现了客体中所含信息的敏感程度，而主体的安全级别则反映了主体对敏感信息的可信程度。根据访问者的安全等级和被访问客体的安全等级来决定访问模式，可以提供严格的访问控制策略保障。分为 BLP 模型和 Biba 模型。

BLP 模型：主体可以读取低安全级以及修改高安全级的客体，不能读取高安全级以及修改低安全级客体。系统中的信息流程单向不可逆的，保证了信息流总是由低安全级的实体流向高安全级的实体。

BiBa 模型：主体可以读取高安全级以及修改低安全级的客体，不能读取低安全级以及修改高安全级客体。系统中信息流总是由高安全级的实体流向低安全级的实体，有效地保护了数据的完整性。

4.2.3 基于角色的访问控制

管理员创建角色，给角色分配权限，让用户关联角色，角色所属的用户可以执行相应的权限。实现了用户和权限的分离，具有支持权限的继承，与实际应用密切关联等特点。

基于角色的访问控制基本安全原则：最小权限、责任分离和数据抽象。

主要分类为：基本 RBAC、分及 RBAC、静态责任分离和动态责任分离。

4.3 访问控制实现机制

访问控制的实现机制是指在具体系统中采用何种方式来记录主体与客体间的授权关系。

4.3.1 访问控制矩阵（ACM）

行表示客体，列表示主体，而行和列的交叉表示某个主体对客体的访问权限。

4.3.2 访问控制能力表（ACCL）

从主体（行）出发，用链表形式表达矩阵某一行的信息。

4.3.3 访问控制列表（ACL）

从客体（列）出发，用链表形式表达矩阵某一列的信息。

4.3.4 访问控制授权关系表（ACARL）

每一行（或称一个元组）表示了主体和客体的一个权限关系。

4.3.5 访问控制安全标签列表（ACSSL）

分别标记主体和客体的安全等级标签的列表。

第五章 网络扫描技术

5.1 网络扫描技术概述

网络扫描技术是一种用于发现 Internet 远程目标网络或本地主机安全性脆弱点的技术，可以获取各种 TCP/IP 端口的分配、开放的服务、Web 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞 。

网络扫描的过程：发现目标主机或网络、收集目标信息以及判断或进一步测试目标是否存在安全漏洞。

5.2 主机扫描技术

确定在目标网络上的主机是否可达，同时尽可能多映射目标网络的拓扑结构，主要利用 ICMP 协议向目标主机发送 ICMP Echo Request 数据包，等待 ICMP Echo Reply 包。

高级主机扫描技术：利用被探测主机产生的 ICMP 错误报文来进行复杂的主机探测。

5.3 端口扫描技术

发现远程主机开放的端口以及服务。

5.3.1 TCP Connect 扫描（开放扫描）

向目标系统的目标端口发起连接，能建立连接，则表示端口开启，反之不然。

5.3.2 TCP SYN 扫描（半开放扫描）

扫描主机向目标主机的选择端口发送 SYN 数据段。如果应答是 RST，那么说明端口是关闭的，按照设定就探听其它端口；如果应答中包含 SYN 和 ACK，说明目标端口处于监听状态，扫描主机传送一个 RST 给目标机从而停止建立连接。

5.3.3 秘密扫描

非正常 TCP 连接过程，通常不记录，隐蔽性最强。

5.4 操作系统扫描技术

许多安全漏洞都是操作系统特定的，可以根据扫描获取的特征判别操作系统，同时也方便攻击者快速锁定攻击目标。

通过系统服务获取标识信息：用来获得某些服务的标识信息，如 Telnet, FTP,

HTTP。

协议栈查询技术：通过测量远程主机的 TCP/IP 协议栈对不同请求的响应来探测系统。协议规范具有一定的弹性，在某些操作系统中一些选择性的特性被使用，而其他的一些系统则可能没有使用；协议规范可能被修改，某些对 IP 协议的自主改进也可能被实现，这就成为了某些操作系统的特性。

第六章 网络隔离技术

6.1 网络隔离技术概述

隔离技术是指通过对具有不同安全需求的应用系统进行分类保护，从而有助于将风险较大的应用系统与其他需要更多安全保护的应用系统隔离，达到保护的目的。本质就是既要信息交换或共享资源，又要通过隔离提高安全性保障。分为物理隔离和逻辑隔离。

6.2 交换机与网络隔离

6.2.1 交换机直接隔离

子网 1 和子网 2 分属不同的网段，可抑制广播数据的传播和监听。

6.2.2 虚拟子网（Vlan）的隔离

连接在同一交换机上的主机可以通过 VLAN 划分到不同的虚拟子网，将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现隔离。

6.3 路由器与网络隔离

路由器作为唯一安全组件：相对交换机，能提供更高层次的安全功能。

路由器作为安全组件的一部分：在一个全面安全体系结构中，常用作屏蔽设备，执行包过滤功能，而防火墙对能够通过路由器的数据包进行检查。

6.4 防火墙与网络隔离

防火墙是用一个或一组网络设施，在两个或多个网络间加强访问控制，以保护一个网络不受到另一个网络攻击的安全技术。

逻辑上防火墙是一个分离器，一个限制器，也是一个分析器。

防火墙可以过滤掉不安全的服务协议，强化网络安全策略，阻止内部信息泄漏以及提供实现某些网络功能的便利平台。

但是防火墙有其弊端：无法检测不经过防火墙的流量，如通过内部提供拨号服务接入公网的流量；不能防范来自内部人员恶意的攻击；不能阻止被病毒感染的和有害的程序或文件的传递，如木马；不能防止数据驱动式攻击，如一些缓冲区溢出攻击。

6.4.1 分组过滤

基于源地址和目的地址、应用、协议类型以及每个 IP 包的端口来做出通过与否的判断。

过滤依据主要是 IP 报头里面的信息，不能对应用层数据进行处理。

分组过滤规则设置基本原则：双向性原则、内外性原则和默认拒绝原则。

分组过滤防火墙由于看不到内层数据，所以处理效率较高，容易实现，但是过滤风险较大，不能进行深度检查。

6.4.2 应用代理

应用代理逻辑位置在 OSI 7 层协议的应用层上，所以主要采用协议代理服务(proxy services)。

应用代理可以对数据包的数据区进行分析，并以此判断数据是否允许通过。

因为可以看到内层数据，所以可以提供更为细致的应用级过滤，并能提供诸如身份验证等功能，但是开销较大，对用户不透明。

6.4.3 状态检测

状态检测可以结合前后数据包里的数据信息进行综合分析决定是否允许该包通过。这是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。

其比分组过滤技术安全性高，比应用代理技术效率高。

6.4.4 链路层代理

链路层代理可以对客户端连接请求进行分析，依据客户身份和请求此判是否否允许建立连接。

可以支持不同的应用层协议，且支持用户级的认证，但是对客户端不透明，无法针对特定的应用协议进行安全管理。

6.5 地址转换与虚拟专网

6.5.1 网络地址转换 NAT

隐藏了内部网络结构，而且内部网络可以使用私有 IP 地址，在公开地址不足的网络可以使用这种方式提供 IP 复用功能。

静态转换（Static NAT）：将内部网络的私有 IP 地址与公有 IP 地址进行一一对应的转换。

动态转换(Dynamic NAT)：将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址是不确定的，是随机的。

网络地址端口转换（NAPT）：改变外出数据包的源端口并进行端口转换，内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。

6.5.2 虚拟专网 VPN

VPN（Virtual Private Network）技术是指在公共网络中建立专用网络，数据通过安全的“加密管道”在公共网络中传播。

保证数据的完整性：接收到的数据必须与发送时的一致。

保证通道的机密性：提供强有力的加密手段。

提供动态密钥交换功能：提供密钥中心管理服务器，防止数据重演(Replay)，通道不能被重演。

提供安全防护措施和访问控制：要有抵抗黑客通过 VPN 通道攻击企业网络的能力，并且可以对 VPN 通道进行访问控制(Access Control)。

6.6 物理隔离

指内部网在任何情况下不得直接或间接地连接公共网。物理安全的目的是保护路由器、工作站、各种网络服务器等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击。

其工作模式为单向隔离、协议隔离和网闸隔离。

物理隔离的哲学是要安全就不连网，要绝对保证安全。

逻辑隔离的哲学是在保证网络正常使用下，尽可能安全。

第七章 入侵检测技术

7.1 入侵检测技术概述

入侵事件：绕过系统安全机制的非授权行为。

入侵检测：一种对计算机系统或网络事件进行监测并分析这些入侵事件特征的过程。

误报率：在检测时出现把系统的正常行为判为入侵行为的错误的概率。

漏报率：在检测时出现把某些入侵行为判为正常行为的错误的概率。

入侵检测系统的主要功能：监测功能、分析识别和预警功能。

入侵检测系统处于防火墙之后，不仅能检测来自外部的入侵行为，同时也监督内部用户的未授权活动。

按数据检测方法分类：异常检测模型（Anomaly Detection)和误用检测模型（Misuse Detection)。

按系统结构分类：集中式和分布式。

按时效性分类：离线入侵检测系统（off-line IDS）和在线入侵检测系统（On-line IDS)。

按数据来源分类：基于主机的入侵检测系统（HIDS)、基于网络的入侵检测系统(NIDS)、混合型入侵检测系统(Hybrid IDS)、网络节点入侵检测系统(NNIDS)和文件完整性检测系统。

7.2 通用入侵检测框架

IDWG 通用 IDS 模型：一个或多个下列组建的组合：传感器、分析器和管理器。

CIDF 通用入侵检测框架：包括：IDS 的体系结构，通信机制，描述语言和应用程序接口 API。

7.3 入侵检测技术原理

7.3.1 基于误用的检测

运用已知攻击方法，根据已定义好的入侵模式，通过判断这些入侵模式是否出现来检测；通过分析入侵过程的特征、条件、排列以及事件间关系能具体描述入侵行为的迹象。

专家系统:指示入侵的具体条件放在规则的左边(if 侧),当满足这些规则时,规则执行右边（then 侧）的动作。

模式匹配：根据知识建立攻击脚本库，每一脚本都由一系列攻击行为组成。

检测准确度很高，但是无法检测未知入侵。而且对于系统内部攻击者的越权行为，很难检测。

7.3.2 基于异常的检测

前提：入侵是异常活动的子集。

用户轮廓(Profile): 通常定义为各种行为参数及其阀值的集合，用于描述正常行为范围。

对正常用户建立行为模式，对入侵者的行为产生的异常性进行比对，从而对入侵进行检测。能有效检测出冒充合法用户的入侵，但是实现较为困难，并且某些入侵者能缓慢改变自身行为，从而逐步变为合法。

第八章 网络攻击与防御（一）缓冲区溢出攻击

8.1 缓冲区溢出相关概念

如果用户输入的数据长度超出了程序为其分配的内存空间，这些数据就会覆盖程序为其它数据分配的内存空间，形成所谓的缓冲区溢出.

攻击者制造溢出的目的:

制造程序运行错误。随意制造数据溢出只会使得程序运行错误，但是不能对其实施攻击。

执行 shellcode。通过制造缓冲区溢出使程序运行一个用户 shell，再通过 shell 执行其他命令，从而使得程序的运行流程被攻击者所控制。

8.2 缓冲区溢出攻击原理

8.2.1 栈溢出

在程序调用过程中，会保存返回地址，新建局部变量等数据，若对栈空间实施栈溢出攻击，那么就可以对其利用使程序转到 shellcode 进行执行。

8.2.2 Shellcode

Shellcode 实际是一段代码，是用来在程序发生溢出后，程序将要执行的代码。Shellcode 的作用就是实现漏洞利用者想要达到的目的，一般看到的 Shellcode 都是用来安装木马或者提升权限的。

在执行溢出攻击时，只需将编写的 Shellcode 的地址覆盖到栈空间中的返回地址处，即可将程序转到 Shellcode 处执行。进一步地，程序地跳转处不必精确地是 shellcode 地址，只需在 shellcode 地址代码之前写入大量的 NOP 代码，再将程序跳转到这部分 NOP 代码中，便可达成目的。

编制 Shellcode 的方法:

方法一：直接汇编语言编制后编译，提取二进制可执行代码。

方法二：C 语言+汇编混合编制，再编译后提取二进制编码。

8.2.3 整型溢出与格式化字符串溢出

整型溢出：当计算机试图保存一个比它可以表示的最大值还大的数时，就会发生整数溢出。

格式化字符串溢出：使用某些格式化函数时，由于参数 format 的使用错误，导致出现内存数据被泄漏或修改。

8.3 缓冲区溢出保护技术

人—代码作者：学习安全编程、软件质量控制、使用源码级纠错工具。

编译器：数组边界检查、编译时加入条件。

语言：使用安全类语言（如 Java，C#）

RunTime 保护：二进制重写保护技术，强制对重要的栈在使用之前进行检测；Hook 危险函数技术，拦截所有已知有问题的库函数调用来分析缓冲区溢出的存在性。

操作系统：执行内存修改-执行分离策略，使得可执行的内存区域不可修改，可修改的内存区域不可执行。

第九章 网络攻击与防御（二）恶意代码原理与防治

9.1 恶意代码基本概念与技术原理

恶意代码（程序）是指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码。最常见的恶意代码有计算机病毒（简称病毒）、特洛伊木马（简称木马）、计算机蠕虫（简称蠕虫）、后门、逻辑炸弹等。

按照传播方式分类可分为：网络病毒、文件病毒、引导型病毒和混合型病毒。

恶意代码的基本特性：传染性、潜伏性、可触发性以及破坏性。

其基本结构为：感染模块、触发模块、引导模块以及破坏模块。由感染模块传播感染，触发模块触发执行，引导模块将病毒引导到指定目标，最后由破坏模块执行破坏。

9.1.1 引导型病毒

引导型病毒由引导扇区中的引导程序引导至内存以及硬盘中，从而实现感染传播。

9.1.2 计算机病毒

传染机理基于文件型病毒，可通过被动传染和主动传染等多种方式进行传染，破坏对象有系统数据区、文件、内存、系统运行速度、磁盘、CMOS、主板和网络等众多对象。

9.2 特洛伊木马技术原理

特洛伊木马(Trojan Horse)，是一种恶意程序，是一种基于远程控制的黑客工具。一旦侵入用户的计算机，就悄悄地在宿主计算机上运行，在用户毫无察觉的情况下，让攻击者获得远程访问和控制系统的权限。

9.3 计算机蠕虫技术原理

蠕虫是一种通过网络自动传播它自身功能的拷贝或它的某些部分到其他的计算机系统中的恶意代码，可利用系统缺陷进行自动传播，并且不需要宿主。

总结

本课程一共 28 个课程学时以及 12 个实验学时，通过长达 40 个学时的网络攻防技术学习历程，我收益良多，收获匪浅。

课程首先对自信息安全概念诞生到现在的整体信息安全现状进行了初步的介绍，对信息安全和网络安全相关概念进行了学习。第二章中，对网络协议栈中的各层常用协议进行了安全性分析，包括 ARP、IP、TCP、UDP、HTTP、DNS 等常用协议。在第三章中，介绍了身份认证技术的产生原因和必要性作用，介绍了常见的几种身份认证技术，包括基于口令的身份认证、基于公钥密码的身份认证以及基于对称密码的身份认证，并对集中身份认证技术进行全方面的安全性分析。在第四章中，对访问控制技术的产生原因和作用进行了概述，并详细介绍了三种基本访问控制模型并对其安全性进行了全面分析，包括自主访问控制、强制访问控制以及基于角色的访问控制，接着对五种访问控制实现机制进行了介绍，包括访问控制矩阵（ACM）、访问控制能力表（ACCL）、访问控制列表（ACL）、访问控制授权关系表（ACARL）以及访问控制安全标签列表（ACSSL）。在第五章中，对网络扫描技术进行概述，并对三种主要网络扫描技术进行了详细的原理介绍和作用分析，包括主机扫描技术、端口扫描技术和操作系统扫描技术。在第六章中，对网络隔离技术的应用需求与分类进行了一个概述，并对主流网络隔离技术的各个类别的原理进行探究和对其实现细节进行了介绍，包括交换机隔离、路由器隔离、防火墙隔离与网络地址转换技术。在第七章中，首先对入侵事件、入侵检测、相关指标以及入侵检测技术分类进行大致的概述，再入侵检测技术的框架和与原理进行详细地分析和介绍。在第八章中，对一种常见却又危害性极大的安全漏洞——缓冲区溢出漏洞进行了详细的学习和分析，并对其产生和利用原理进行了剖析。在第九章中，对恶意代码的相关概念进行了初步介绍，并对常见的几类恶意代码进行了从原理上的分析，以及对它们相对应的防范和解决办法进行了探究。

至此，整个网络攻防技术部分的学习就告一段落，通过这一阶段的学习，加强了我对当今社会整体的网络安全和信息安全现状的认识，我深刻地理解到网络空间安全和信息安全对整个社会和国家的极大重要性，更加强了我对这一领域的技术学习的决心。