LM的PPT会标注LM，PPT默认为CY的PPT。

红色为待补充的部分

*蓝色斜体*为PPT中提到的出题类型

# 第二章 网络攻击行径分析

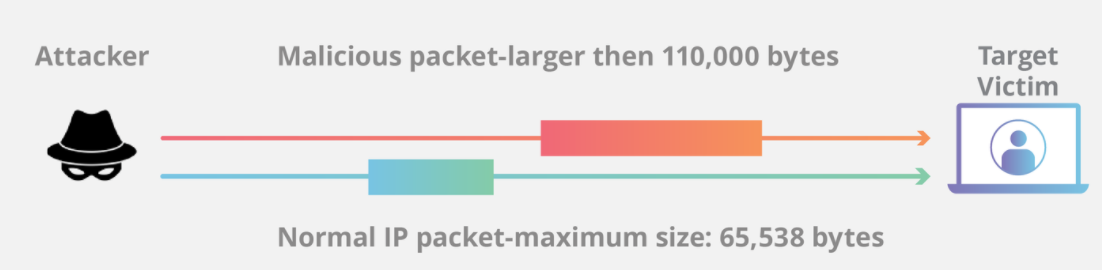
## 破坏型攻击

P9 定义，常见类型（病毒攻击，Dos）

**Dos常见类型和手段**

* Ping of Death

PPT+书上都有原理 *ping -s (设置数据包大小) IP\_Addr*



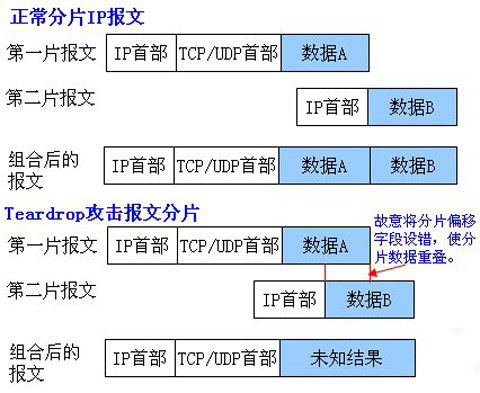
防御方法：对重新组装过程添加检查，以确保在分组重组后不会超过最大数据包大小约束;创建一个具有足够空间的内存缓冲区来处理超过最大准则的数据包。

* IGMP/ICMP Flood

防御方法：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。

* Teardrop

第一个包的偏移量为0，长度为N，第二个包的偏移量小于N。为了合并这些数据段，TCP/IP堆栈会分配超乎寻常的巨大资源，从而造成系统资源的缺乏，甚至机器重新启动。



防御方法：

1. 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。

2. 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。

* UDP Flood

攻击端口为业务端口：根据该业务UDP最大包长设置UDP最大包大小以过滤异常流量。

攻击端口为非业务端口：丢弃所有UDP包；建立UDP连接规则，要求所有去往该端口的UDP包，必须首先与TCP端口建立TCP连接。这种方法需要专业的防火墙或其他防护设备支持。

* SYN Flood

图见PPT

## 利用型攻击

P11

* 口令猜测

首先获得账号（使用Finger命令查询时会保存用户名；社工-email等），然后破译口令。

**网络监听**：很多协议没有采用任何加密或身份认证技术（Telnet、FTP、HTTP、SMTP等传），用户帐户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可很容易收集到帐户和密码。

**缓冲区溢出**：编制有缓冲区溢出错误的SUID程序来获得超级用户权限。

* 特洛伊木马

基于C/S结构的远程控制程序，是一类隐藏在合法程序中的恶意代码，这些代码或者执行恶意行为，或者为非授权访问系统的特权功能而提供后门。

传染方式:通过电子邮件附件发出，捆绑在其他的程序中。

病毒特性:会修改注册表、驻留内存、在系统中安装后门程序、开机加载附带的木马。

　　防范措施:不下载和运行来历不明的程序，不打开不明来历的邮件附件。

* 缓冲区溢出

## 信息收集型攻击

**信息收集方法：**

1. 从一些社会信息入手：通过社工的方式，查找到目标的一些信息。可以参考CYPPT，上面有很多信息收集的内容。

2. 找到网络地址范围：比如通过社交软件获得目标所在地，获得大致ip范围。通过扫描技术，地址扫描

3. 找到关键的机器地址：通过扫描技术，地址扫描

4. 找到开放端口和入口点：端口扫描技术（以上都在课本p12）

5. 找到系统的制造商和版本：体系结构探测（课本p13）

P12 **扫描技术**

Nmap: P35

进行ping扫描，打印出对扫描做出响应的主机,不做进一步测试

*nmap -sP 192.168.1.0/24*

仅列出指定网络上的每台主机，不发送任何报文到目标主机：

*nmap -sL 192.168.1.0/24*

探测目标主机开放的端口，可以指定一个以逗号分隔的端口列表(如-PS22，23，25，80)：

*nmap -PS 192.168.1.234*

使用UDP ping探测主机：

*nmap -PU 192.168.1.0/24*

使用频率最高的扫描选项：SYN扫描,又称为半开放扫描，它不打开一个完全的TCP连接，执行得很快：

*nmap -sS 192.168.1.0/24*

当SYN扫描不能用时，TCP Connect()扫描就是默认的TCP扫描：

*nmap -sT 192.168.1.0/24*

UDP扫描用-sU选项,UDP扫描发送空的(没有数据)UDP报头到每个目标端口:

*nmap -sU 192.168.1.0/24*

确定目标机支持哪些IP协议 (TCP，ICMP，IGMP等):

*nmap -sO 192.168.1.19*

探测目标主机的操作系统：

*nmap -O 192.168.1.19*

*nmap -A 192.168.1.19*

* 地址扫描
* 端口扫描
* 反响映射
* 慢速扫描
* 漏洞扫描

## 网络欺骗攻击

P13 （扩展答）第七章 欺骗攻击

* DNS欺骗攻击
* 电子邮件欺骗
* Web欺骗
* IP欺骗

## 攻击步骤

P17 图2-1

### 准备

* 确定攻击目的 P16 + PPT
* 准备攻击工具 P18
* 收集目标信息 P18 结合扫描技术答

### 实施

* 隐藏自己位置（使用他人IP）
* 登录主机 结合利用型攻击三点答（口令猜测/特洛伊木马/缓冲区溢出）
* 窃取网络资源和特权 （根据具体问题的攻击目的答）

### 善后

Windows-Unix

*为什么要进行善后工作？ P20*

# 第三章 网络侦查技术

## 网络扫描

P30 3.1.1 - **扫描器**的定义、功能（PPT）

### 地址扫描

### 端口扫描

前三个例子PPT上有图，答题时把图画上去。~~P32有代码例子扫一眼~~（LMPPT也有）

* Connect()
* TCP SYN
* TCP Fin

其它的对着PPT看一下特点就行。

### 漏洞扫描

## 网络监听

### 嗅探器

P43

### 交换式以太网

P44 一定程度低于Sniffer攻击。

ARP欺骗（防御方法？）

建立正确的 ARP 映射关系、检测并过滤伪造的 ARP 报文，保证经过其转发的 ARP报文正确合法；

抑制短时间内大量 ARP报文的冲击。

在无线网络中，防御ARP欺骗的有效方法是网络管理员分别在主机或接入点上和路由器或控制器上对**IP和MAC地址进行静态映射绑定**。（ARP欺骗是通过重复应答实现的，那么只需要在主机添加一条静态的ARP映射，这样就不需要询问网关MAC地址了；对于网关欺骗还需要在网关中也添加一条到主机的静态ARP映射。）

### 共享式以太网

P39 共享以太网的四种工作模式：**混杂模式**下可以收听所有报文。

P40 设置为混杂模式的方法，代码扫一眼

### 防范方法

P45

需要基于书上的例子展开答。

* 确保以太网整体安全性
* 采用加密技术（例子？）

如使用RSA加密算法等。缺点是影响数据传输速度以及使用一个弱加密术比较容易被攻破。系统管理员和用户需要在网络速度和安全性上进行折中。

* 交换机（原理？例子？）

**启用并正确配置交换机的安全机制。将交换机物理端口和MAC地址静态绑定，限制交换机单个物理端口可以动态绑定的MAC地址数量。**以交换式集线器代替共享式集线器对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（称为单播包Unicast Packet）还是会被同一台集线器上的其他用户所监听。因此，**应该以交换式集线器代替共享式集线器**，使单播包仅在两个节点之间传送，从而防止非法监听。当然，交换式集线器只能控制单播包而无法控制广播包（Broadcast Packet）和多播包（Multicast Packet）。**但广播包和多播包内的关键信息，要远远少于单播包。**

* 划分VLAN

划分VLAN虚拟局域网，可以将以太网通信变为点到点通信，从而防止大部分基于网络监听的入侵。

* 一次性口令
* Kerberos等第三方服务提供认证机制

### 检测手段

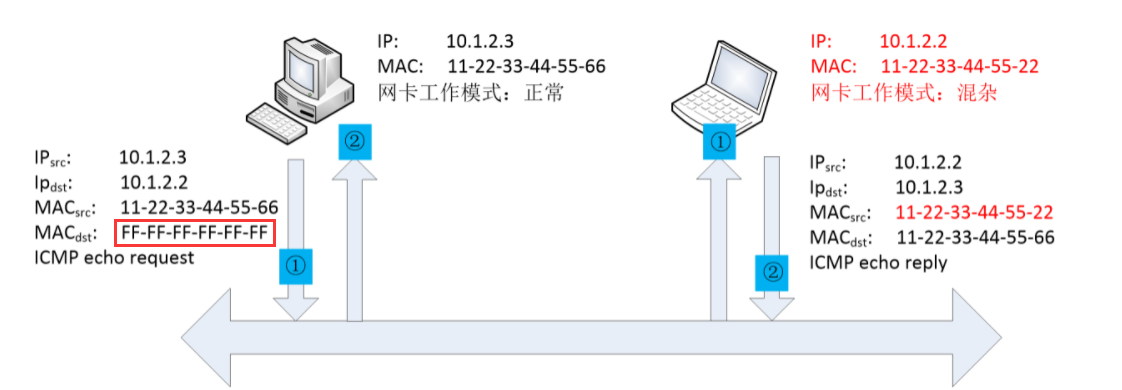
P46

* 反应时间
* DNS测试

地址反向解析：通过IP查域名

* Ping

由于在正常模式下，主机只接收目的 MAC 地址是自己的数据包，其他将一律丢弃；而在混杂模式下，网卡并不检查目的 MAC 地址，对所有的数据包都来者不拒。所以，我们只需要构造并发送一个：疑似待排查为混杂模式目标主机的 IP 目的地址和与其真实 MAC 地址不同的虚假 MAC 目的地址 **ICMP** 回显请求（echo request）数据包，如果收到应答，则说明该被排查的目标主机网卡当前正工作于混杂模式，即当前网络中可能存在监听者。



* ARP数据包 （原理）

首先发送一个 ARP 广播包，这样 ARP 缓存表中便包括了所有在线的主机 IP 到 MAC 地址的映射，随后再发送一个非广播 ARP，接着查看当前 ARP 缓存表，检查两表是否一致，若有异常则说明存在监听。其中arp -a命令用来查看当前 ARP 缓存表。（ARP举例别用FF-FF-FF-FF-FF-FF，那是ARP广播包。原理也是混杂模式不看MAC\_addr）



## 口令破解

P46 + PPT 字典文件通常包含数据内容、类型知道即可。

# 第四章 拒绝服务攻击

## 概述

P56 + PPT 定义

P57 4.1.2 DoS攻击思想和方法要从两个角度答全。

## 分类

P57

### 物理破坏 P60

### 配置文件修改和破坏 P60

### 资源消耗破坏

**消耗网络资源实例：**

* Smurf广播风暴攻击（P67 前年考过）

P58+PPT （ICMP协议的解释见PPT第二章7）

（应对方式需要写详细一点）~~结合P68看一下有什么需要补充的~~

1. 阻断虚假源地址（对应书上3）

2. 阻断WAN广播包（对应书上1）

3. 求助ISP，阻断某IP网段（对应书上2）

* TCP SYN攻击 P61 + LMPPT~~（PPT上提了防御方式，结合P66看一下有什么需要补充）~~
* ACK Flood攻击~~（PPT上提了防御方式，详细一点）~~

僵尸主机多的话怎么办？可以用防范DDoS的思路答。

握手的第二步是 SYN ACK 数据包。通常，服务器在响应来自客户端设备的 SYN 数据包时发送此 SYN ACK 数据包。在 SYN ACK DDoS 攻击中，攻击者使大量 SYN ACK 数据包涌向目标。这些数据包根本不属于三向握手协议的一部分，它们的唯一目的是打断目标的正常运作。

**消耗存储资源实例：**

* TearDrop P70

第二章那里写了防御方式，~~可以再查查~~

* FORK

### 服务中断攻击 P60

## DDoS

### DDoS和DoS区别及DDoS特点

P74 + PPT 三点

### DDoS攻击过程

P75图 + PPT

**攻占代理主机 + 向目标发起攻击**

### 应对方式

P76 + PPT ~~（结合P76看一下有什么需要补充。最好有例子，比如哪些特征字符串等）~~

* 在数据流中搜寻特征字符串
* 利用攻击数据包的特征
* 设置防火墙

1. 监视本地主机端口的使用情况

2. 在防火墙服务器上放置一份 ACL（访问控制列表) 来阻断这些来自一些IP的访问。

* 对通信数据量进行统计

## 反弹技术

利用反弹服务器实现攻击的技术。

区别：PPT上四点 答的时候画图

# 第五章 缓冲区溢出攻击

## 原理概述

P78 + PPT

PPT-危害（~~利用其进行DoS攻击？~~没查到算了）

### 哪些编程习惯会导致

PPT

* 未进行缓冲区越界检查

不知道内存缓冲区的总长度

不能信任来自用户的数据，调用字符串处理函数等库函数时，对数组越界加以检查和限制。（比如下列例子就不知道szName长度）也可以见project1-vul1

　　void Function(char \*szName) {

　　char szBuff[MAX\_NAME];

　　// 复制并使用 szName

　　strcpy(szBuff,szName);

　　 }

由于strcpy不检查内容长度，所以有溢出风险。因此Vul1中需要利用地点就是strcpy()。

* 不安全的库函数调用

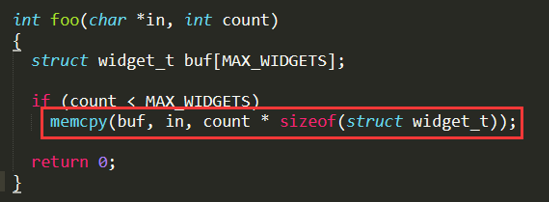
PPT strcpy->strncpy

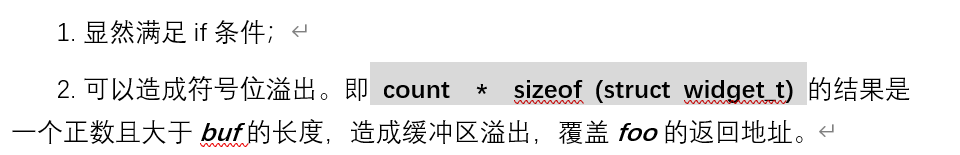
见project1-vul5 格式化字符串

漏洞在snprintf()函数中，因为是将arg作为格式化字符串拷贝（遇到格式化参数之前会先将普通字符拷贝给目标），所以可以从这里下手。除了常见的格式化字符串‘%d’、‘%s’等，%$(如：%20$x)格式输出，可泄漏栈内的数据；%n格式输出，可修改栈中指针指向的任意可写地址。

* 有无符号类型转换

见project1-vul3





* \*多次free() 结合UAF进行攻击

eg. 假设一个对象A前4字节(0x400000)为函数printf，释放后，恶意用户重用这个空间（使用缓冲区溢出等方式），将前4字节改为(0x4a0000)system函数，然后来到漏洞的触发点，程序由于疏忽再次调用A的printf，却调用了system函数

## 方法和步骤

看懂PPT例子和画图形式，答题得画图。可以看LMPPT

**把大作业1的六个例子回顾一下**

## 防御技术

能找到对着抄就行，PPT

## Payload

### 构造流程

P82

* 准备shellcode

### Unix&Windows

P99 地址有/x00

P101 无系统调用

### 构造payload注意事项

* 真实内存地址未知

P94 使用相对IP的偏移地址

* Shellcode中不能存在\x00

P95 使用xor代替mov

* 存在阻断函数\_exit(0)

见project1-vul6，观察\_exit(0)跳转地址，直接修改其为&shellcode

### 绕过防护方式

# ~~第六章 程序攻击~~

## 逻辑炸弹攻击

P109 + PPT 定义了解即可。

## 植入后门

### 后门和木马的区别（~~对照PPT查一下更详细的~~）

在PPT“蠕虫和特洛伊木马”最后

所谓“后门”，就是程序开发人员为了改进自己设计的程序而打开的专用接口（通道），方便自己修改程序，一般具有最高权限，特征在于隐蔽性，没有**欺骗性**。木马是指利用后门或漏洞被发现非法入侵用户电脑，从事侵害用户利益的活动，不一定具有最高权限。

联系在于:都是隐藏在用户系统中向外发送信息,而且本身具有一定权限,以便远程机器对本机的控。

区别在于:木马是一个完整的软件,而后门则体积较小且功能都很单一。

### 后门的隐藏方式（~~对照PPT查一下更详细的~~）

* 应用级隐藏

1. 后门程序和进程隐藏 选择一个隐秘的目录存放后门程序文件

2. 后门程序设置隐藏标记。

3. 定制程序名、修改图标。将自己的服务 端程序图标改成 HTML, TXT, ZIP 等各种文件的图

4. 附着、捆绑或替换合法文件。

5. 修改或替换管理命令。如替换“ ls”“find”“du”可以实现文件和目录隐藏; 替换 “ ps”“top”“ pidof”可以实现进程隐藏; 替换 Netstat, Ifconfig 可 实现网络的连接状态隐藏; 替换 Kill, Killall 可防止删除攻击者 的进程, 替换 Crontab 能隐 藏攻击者的定 时启动信息, 替 换 Tcpd, Syslogd 隐藏攻击者的连接信息等。

6. 进程动态注入。将后门程序可执行代码注入正在运 行的进程中, 可以极大地提高后门的生存能力。此项技术可以 很好地隐藏后门程序, 并且植入后门代理程序后

* 通信状态隐藏

1. 通信端口隐藏

2. 将后门隐藏在合法端口,

3. 通信连接隐藏

检测方式：通信端口检查、通信特征匹配、植入痕迹查找和完整性检查

* 内核级隐藏

LKM( Loadable Kernel Modules) 内核加载模块隐藏

检测方式：内核级后门是在内核级隐藏目录、文件、进程和通信连接等, 它不修改程序二进制文件, 因此 MD5 校验无法检测。内核级隐藏的一种方法是通过修改系统调用表来实现系统调用重定向从而隐藏文件、进程和通信连接, 所以通过检查系统调用的内存地址就可能发现是否被植入了后门

常用查杀工具：rkhunter，chkrookit

## 蠕虫和特洛伊木马

蠕虫的其他方法 P125

**病毒 蠕虫 木马的区别（**整合一下答案即可，cy说是送分题）

首先病毒，木马，蠕虫统称为电脑病毒。病毒（包含蠕虫）的共同特征是**自我复制、传播、破坏电脑文件，对电脑造成数据上不可逆转的损坏**。而木马独有特征是**伪装成正常应用骗取用户信任而入侵，潜伏在电脑中盗取用户资料与信息**。

病毒：编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能**自我复制**的一组计算机指令或者程序代码。

1、它必须能自行执行。它通常将自己的代码置于**另一个程序的执行路径中**。

2、它必须能**自我复制**。例如，它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染桌面计算机也可以感染网络 服务器。

木马：木马也称木马病毒，是指通过特定的程序来控制另一台计算机。与一般的病毒不同，**它不会自我繁殖**，也专并不“刻意”地去感染其他文件，它通过将自身伪装**吸引用户下载执行**，向施种木马者提供打开被种主机的门户，使施属种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。

蠕虫病毒：蠕虫病毒一种能够**利用系统漏洞通过网络进行自我传播的恶意程序**。它**不需要附着在其他程序上**，而是独立存在的。当形成规模、传播速度过快时会极大地消耗网络资源导致大面积网络拥塞甚至瘫痪。通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等等，同时具有自己的一些特征，如**不利用文件寄生(有的只存在于内存中)， 对网络造成拒绝服务，以及和黑客技术相结合**。普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫**不使用驻留文件即可在系统之间进行自我复制**，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。

按照传输方式分类 P130

# 第七章 欺骗攻击

**PPT上的例子着重关注一下**

## DNS欺骗攻击

P159 例子原理看懂 防御机制查一下

前提条件 P159

危害 P158

防护和检测见补充部分。

## Email欺骗攻击

### 步骤

P162 + ppt

SMTP服务器需要关注的点？书+PPT 查一下详细一点

### 应对方式

基于PPT详细一点即可

## Web欺骗攻击

### 步骤

P163 + ppt 看懂例子

### 应对方式

基于PPT详细一点即可

## IP欺骗攻击

P171看书和PPT例子吧 我累了 他讲了好久 我感觉要考

不在一个子网中的欺骗方法？

# ~~第八章 利用程序错误攻击~~

把书上的实例思路总结一下

# 第九章 访问控制技术

## 访问控制模式

三个维度答

### 争用

### 定时

### \*物理空间~~（视频中提了一下，可以大概查一下是什么维度）~~

## 自主访问控制 DAC

定义可以看LMPPT

方法：P219 一般是基于行的

类型：220

优缺点：LMPPT

## 强制访问控制 MAC

P221 + PPT定义解释 定义可以看LMPPT

DAC和MAC的区别以及结合？结合LMPPT和PPT总和一下答案

## 基于角色的访问控制技术RBAC

P225 书上过一遍概念

P228 + PPT 相对于DAC和MAC的优点和不足

## 物理隔离

~~把PPT上最后“物理隔离的未尽之处”详细化~~

P213 图9-3

P215 网络安全隔离卡 过渡区

网络隔离卡和网卡的区别？ 见补充部分

### 隔离网闸

P216 和防火墙的区别见PPT

# 第十章 防火墙

## 概述

P230 静态安全技术

P231 图10-2抽象模型在防火墙中的实际应用

## 分类

P237 两种方式对比 扫一眼就行

### 术语

* 堡垒机
* 双重宿主主机
* 周边网络

### 体系结构

P239

* 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

## 构建

* 选择体系 P251 + PPT LMPPT
* 安装堡垒机 P254 + PPT
* 数据包过滤规则 P256 + PPT

**看书上例子**

注意路由器的向内/向外，内部接口和外部接口的向内都是向路由器本身。

# 第十一章 入侵检测

## 概述

P287 + PPT 定义:动态网络安全技术

~~为什么具有实时性和自适应性？结合后面内容详细解释~~

具体问题可以对照P288图和PPT的原理图答

## 分类和评估

P290 每种分类方式都需要了解

LMPPT有更详细点

集中式/分布式看LMPPT

IDS评估标准 P293 + PPT 误报&漏报 其他扩充答一下就行

* 准确性，指系统正确识别入侵行为的能力；
* 可靠性，指系统的容错能力和可持续运行能力；
* 可用性，指系统开销大小，对网络性能影响的大小；
* 可测试，指系统能够通过模拟攻击进行检测测试；
* 适应性，指系统易于开发和扩展；
* 实时性，指系统能够及早发现入侵企图；
* 安全性，指系统可确保自身的安全。

# 第十二章 VPN

## 概述

P305 + PPT 定义和优点（按照PPT示例答即可）

P306 组成和基本结构

~~VPN为什么需要两个服务器，VPN工作原理？整理一下~~

## 协议与实现

### 身份验证

P309 + PPT验证过程了解即可

### 隧道协议

P310 +PPT 隧道的定义：针对VPN协议重新**打包**

重点了解PPTP和L2TP区别 P315 + PPT + P319的表格

PPTP和L2TP都属于第二层隧道协议，使用PPP协议对数据进行封装，然后添加附加包头用于数据在互联网络上的传输。

* **PPTP** 点对点隧道协议
* **L2TP** 第二层隧道协议

和PPTP本质区别就是可以从MAC层封装，从数据链路层开始数据包就是安全的。

* **IPSec** IP安全协议

定义和优势看PPT就行

PPT 封装方法 常用模式Tunnel Mode1

加密过程细节都不用关注。

### 数据加密

# 盲猜一手

## 简答题

### 攻击步骤

### 交换式以太网和共享式以太网

* *简述以太网网络监听？*工作原理、扫描方式等
* *如何防范网络监听？*ARP欺骗例子及防御方法

### DoS

* *外部用户针对网络连接发动拒绝服务攻击有哪几种模式？*

DoS分类 P57

### 缓冲区溢出

* *缓冲区溢出的一般目标？*

提权；

* *要让程序跳转到安排好的地址空间执行 一般有哪些方法？*

### 病毒 蠕虫 木马的区别

### 访问控制

* DAC和MAC的区别以及如何结合

### VPN

* PPTP和L2TP区别

## 综合题

### DDoS实例

不知道会怎么出，可能会结合攻击步骤知识点，写一个完整的攻击思路？

### 缓冲区溢出

方法和步骤，会偏技术

* *Printf()有哪些漏洞？*举例说明

### 欺骗攻击

* 给图解释DNS欺骗过程
* ***IP欺骗，他讲了很久，感觉很有可能考***

### 防火墙

重点在 数据包过滤规则 给拓扑图写过滤规则

但其他流程答全即可

### \*入侵检测

HIDS&NIDS区别

# 补充

**一、Teardrop防御方法**：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。为了防止缓存益处，当缓存快要存满是，直接丢弃后续分片报文。

**二、信息收集的过程，结合经验和理解**

1. 从一些社会信息入手：通过社工的方式，查找到目标的一些信息。可以参考CYPPT，上面有很多信息收集的内容。

2. 找到网络地址范围：比如通过社交软件获得目标所在地，获得大致ip范围。通过扫描技术，地址扫描

3. 找到关键的机器地址：通过扫描技术，地址扫描

4. 找到开放端口和入口点：端口扫描技术（以上都在课本p12）

5. 找到系统的制造商和版本：体系结构探测（课本p13）

**三、网络监听—交换式以太网**

**1.其中的安全问题**

1.交换机缓冲区溢出攻击

　　 交换机大多使用存贮转发技术，工作时维护着一张MAC地址与端口的映射表，这个表中记 录着交换机每个端口绑定的MAC地址。他的工作原理是对某一段数据包进行分析判别寻址， 并进行转发，在发出前均存贮在交换机的缓冲区内。但是，交换机缓冲区是有限的。如用大 量无效IP包，包含错误MAC地址的数据帧对交换机进行攻击。该交换机将接收到大量的不符 合分装原则的包，造成交换机处理器工作繁忙，从而导致数据包来不及转发，进而导致缓 冲区溢出产生丢包现象。这时交换机就会退回到HUB的广播方式，向所有的端口发送数据包 。这样，监听就变得非常容易了。

**2. ARP协议和欺骗**

**1. ARP欺骗的原理**

在每台主机都有一个ARP缓存表，缓存表中记录了IP地址与MAC地址的对应关系，而局域网数据传输依靠的是MAC地址。

假设主机 A 192.168.1.2,B 192.168.1.3,C 192.168.1.4; 网关 G 192.168.1.1; 在同一局域网，主机A和B通过网关G相互通信，就好比A和B两个人写信，由邮递员G送信，C永远都不会知道A和B之间说了些什么话。但是并不是想象中的那么安全，在ARP缓存表机制存在一个缺陷，就是当请求主机收到ARP应答包后，不会去验证自己是否向对方主机发送过ARP请求包，就直接把这个返回包中的IP地址与MAC地址的对应关系保存进ARP缓存表中，如果原有相同IP对应关系，原有的则会被替换。

这样C就有了偷听A和B的谈话的可能，继续思考上面的例子：

C假扮邮递员，首先要告诉A说：“我就是邮递员” （C主机向A发送构造好的返回包，源IP为G 192.168.1.1，源MAC为C自己的MAC地址），愚蠢的A很轻易的相信了，直接把“C是邮递员”这个信息记在了脑子里；

C再假扮A，告诉邮递员：“我就是A” （C向网关G发送构造好的返回包，源IP为A 192.168.1.2，源MAC地址为自己的MAC地址），智商捉急的邮递员想都没想就相信了，以后就把B的来信送给了C，C当然就可以知道A和B之间聊了些什么

上面ABCG的故事就是ARP双向欺骗的原理了

ARP单向欺骗就更好理解了，C只向A发送一个返回包，告诉A：G 192.168.1.1 的MAC地址为 5c-63-bf-79-1d-fa（一个错误的mac地址），A把这个信息记录在了缓存表中，而G的缓存表不变，也就是说，A把数据包给了C，而G的包还是给A，这样就是ARP单向欺骗了。

**2. 防范ARP欺骗的方法**

建立正确的 ARP 映射关系、检测并过滤伪造的 ARP 报文，保证经过其转发的 ARP报文正确合法；

抑制短时间内大量 ARP报文的冲击。

在无线网络中，防御ARP欺骗的有效方法是网络管理员分别在主机或接入点上和路由器或控制器上对**IP和MAC地址进行静态映射绑定**。（ARP欺骗是通过重复应答实现的，那么只需要在主机添加一条静态的ARP映射，这样就不需要询问网关MAC地址了；对于网关欺骗还需要在网关中也添加一条到主机的静态ARP映射。）

1.主机级被动检测

  当系统接收到来自局域网上的ARP请求时，系统检查该请求发送端的IP地址是否与自己的IP地址相同。如果相同，则说明该网络上另有一台机器与自己具有相同的IP地址。

2.主机级主动检测

  主机定期向所在局域网发送查询自己IP地址的ARP请求报文。如果能够收到另一ARP响应报文，则说明该网络上另有一台机器与自己具有相同的IP地址。

3.服务器级检测

  当服务器收到ARP响应时，为了证实它的真实性，根据反向地址解析协议(RARP)就用从响应报文中给出的 地 MAC址再生成一个RARP请求，它询问这样一个问题：“如果你是这个MAC地址的拥有者，请回答你的IP地址”。这样就会查询到这个MAC地址对应的IP地址，比较这两个IP地址，如果不同，则说明对方伪造了ARP响应报文。

4.网络级检测

  配置主机定期向中心管理主机报告其ARP缓存的内容。这样中心管理主机上的程序就会查找出两台主机报告信息的不一致，以及同一台主机前后报告内容的变化。这些情况反映了潜在的安全问题。或者利用网络嗅探工具连续监测网络内主机硬件地址与IP地址对应关系的变化。

**3. 网络监听的防范**

1.网络分段

　　网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是防范网络监听的一 项重要措施。将网络划分为不同的网段，其目的是将非法用户与敏感的网络资源相互隔离， 从而防止可能的非法监听。

2.以交换式集线器代替共享式集线器

　　 对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络最终 用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包(单播包)还是会被同一 台集线器上的其他用户监听。因此，应该以交换式集线器代替共享式集线器，使 单播包仅在两个节点之间传送，从而防止非法监听。

3.使用加密技术

　　数据经过加密后，通过监听仍然可以得到传送的信息,但显示的是乱码。使用加密技术的 缺点是影响数据传输速度以及使用一个弱加密术比较容易被攻破。

4.划分VLAN

　　运用VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，VLAN子网隔离了广播风暴 ，可以防止大部分基于网络监听的侵入，对一些重要部门实施了安全保护。且当某一部门物 理位置发生变化时，只需对交换机进行设置，就可以实现网络的重组，非常方便、快捷，同 时节约了成本。为保证不同职能部门管理的方便性和安全性以及整个网络运行的稳定性，可 采用VLAN技术进行虚拟网络划分。

**四、拒绝服务攻击—ACK Flood攻击**

1.原理：

ACK Flood攻击是在TCP连接建立之后，所有的数据传输TCP报文都是带有ACK标志位的，主机在接收到一个带有ACK标志位的数据包的时候，需要检查该数据包所表示的连接四元组是否存在，如果存在则检查该数据包所表示的状态是否合法，然后再向应用层传递该数据包。如果在检查中发现该数据包不合法，例如该数据包所指向的目的端口在本机并未开放，则主机操作系统协议栈会回应RST包告诉对方此端口不存在。

这里，服务器要做两个动作：查表、回应ACK/RST。这种攻击方式显然没有SYN Flood给服务器带来的冲击大，因此攻击者一定要用大流量ACK小包冲击才会对服务器造成影响。按照我们对TCP协议的理解，随机源IP的ACK小包应该会被Server很快丢弃，因为在服务器的TCP堆栈中没有这些ACK包的状态信息。但是实际上通过测试，发现有一些TCP服务会对ACK Flood比较敏感，比如说JSP Server，在数量并不多的ACK小包的打击下，JSP Server就很难处理正常的连接请求。对于Apache或者IIS来说，10kpps的ACK Flood不构成危胁，但是更高数量的ACK Flood会造成服务器网卡中断频率过高，负载过重而停止响应。可以肯定的是，ACK Flood不但可以危害路由器等网络设备，而且对服务器上的应用有不小的影响。

如果没有开放端口，服务器将直接丢弃，这将会耗费服务器的CPU资源。如果端口开放，服务器回应RST。

2 ACK Flood防护

利用对称性判断来分析出是否有攻击存在。所谓对称型判断，就是收包异常大于发包，因为攻击者通常会采用大量ACK包，并且为了提高攻击速度，一般采用内容基本一致的小包发送。这可以作为判断是否发生ACK Flood的依据，但是目前已知情况来看，很少有单纯使用ACK Flood攻击，都会和其他攻击方法混合使用，因此，很容易产生误判。

一些防火墙应对的方法是：建立一个hash表，用来存放TCP连接“状态”，相对于主机的TCP stack实现来说，状态检查的过程相对简化。例如，不作sequence number的检查，不作包乱序的处理，只是统计一定时间内是否有ACK包在该“连接”(即四元组)上通过，从而“大致”确定该“连接”是否是“活动的”。

（每建立一个监听套接字，就将套接字挂入监听哈希表的某个表项链表中。则在内核收到连接请求的SYN或ACK等包传到TCP层时，要根据请求包的请求连接地址与端口号到哈希表中查找对应的服务器监听套接字是否存在）

**五、DoS攻击的防范方法**

1. 确保服务器的系统文件是最新的版本,并及时更新系统补丁。

要定期扫描现有的网络主节点,清查可能存在的安全漏洞,对新出现的漏洞及时进行清理。骨干节点的计算机因为具有较高的带宽,是黑客利用的最佳位置,因此对这些主机本身加强主机安全是非常重要的。而且连接到网络主节点的都是服务器级别的计算机,所以定期扫描漏洞就变得更加重要了。

1. 关闭不必要的服务

过滤不必要的服务和端口.可以使用Inexpress、Express、Forwarding等工具来过滤不必要的服务和端口,即在路由器上过滤假IP。比如Cisco公司的 CEF(Cisco Express Forwarding)可以针对封包Source IP和Routing Table做比较,并加以过滤。只开放服务端口成为目前很多服务器的流行做法,例如WWW服务器那么只开放80而将其他所有端口关闭或在防火墙上做阻止策略。

1. 限制同时打开的SYN半连接数目,缩短SYN半连接的timeout时间,限制SYN/ICMP流量

用户应在路由器上配置SYN/ICMP的最大流量来限制SYN/ICMP封包所能占有的最高频宽,这样,当出现大量的超过所限定的SYN/ICMP流量时,说明不是正常的网络访问,而是有黑客入侵。早期通过限制SYN/ICMP流量是最好的防范DOS的方法,虽然目前该方法对于Ddos效果不太明显了, 不过仍然能够起到一定的作用。

1. 正确设置防火墙

禁止对主机的非开放服务的访问；限制特定IP地址的访问，（过滤所有RFC1918 IP地址RFC1918 IP地址是内部网的IP地址,像10.0.0.0、192.168.0.0和172.16.0.0,它们不是某个网段的固定的IP地址,而是Internet内部保留的区域性IP地址,应该把它们过滤掉。此方法并不是过滤内部员工的访问,而是将攻击时伪造的大量虚假内部IP过滤,这样也可以减轻Ddos的攻击。）启用防火墙的防DDoS的属性；严格限制对外开放的服务器的向外访问；运行端口映射程序祸端口扫描程序,要认真检查特权端口和非特权端口。

1. 认真检查网络设备和主机/服务器系统的日志。只要日志出现漏洞或是时间变更,那这台机器就可能遭到了攻击。
2. 限制在防火墙外与网络文件共享。这样会给黑客截取系统文件的机会,主机的信息暴露给黑客,无疑是给了对方入侵的机会。
3. 充分利用网络设备保护网络资源

所谓网络设备是指路由器、防火墙等负载均衡设备,它们可将网络有效地保护起来。当网络被攻击时最先死掉的是路由器,但其他机器没有死。死掉的路由器经重 启后会恢复正常,而且启动起来还很快,没有什么损失。若其他服务器死掉,其中的数据会丢失,而且重启服务器又是一个漫长的过程。特别是一个公司使用了负载 均衡设备,这样当一台路由器被攻击死机时,另一台将马上工作。从而最大程度的削减了Ddos的攻击。

1. 用足够的机器承受黑客攻击

如果用户拥有足够的容量和足够的资源给黑客攻击,在它不断访问用户、夺取用户资源之时,自己的能量也在逐渐耗失,或许未等用户被攻死,黑客已无力支招儿了。不过此方法需要投入的资金比较多,平时大多数设备处于空闲状态,和目前中小企业网络实际运行情况不相符。

1. 检查访问者的来源

使用Unicast Reverse Path Forwarding等通过反向路由器查询的方法检查访问者的IP地址是否是真,如果是假的,它将予以屏蔽。许多黑客攻击常采用假IP地址方式迷惑用户, 很难查出它来自何处。因此,利用Unicast Reverse Path Forwarding可减少假IP地址的出现,有助于提高网络安全性。

**六、DoS与DDoS攻击的原理和区别**

**DOS攻击的原理**：首先攻击者向被攻击的服务器发送大量的虚假ip请求，被攻击者在收到请求后返回确认信息，等待攻击者进行确认，（此处需要拥有HTTP协议工作方式和tcp三次握手的基本知识）该过程需要TCP的三次握手，由于攻击者发送的请求信息是虚假的，所以服务器接收不到返回的确认信息，在一段时间内服务器会处与等待状态，而分配给这次请求的资源却被有被释放。当被攻击者等待一定的时间后，会因连接超时而断开，这时攻击者在次发送新的虚假信息请求，这样最终服务器资源被耗尽，直到瘫痪。

**DDOS的原理**，它是在DOS基础上进行的大规模，大 范围的攻击模式，DOS只是单机和单机之间的攻击模式，而DDOS是利用一批受控制的僵尸主 机向一台服务器主机发起的攻击，其攻击的强度和造成的威胁要比DOS严重很多，更具破坏 性。首先DDOS攻击者要寻找僵尸主机，在互联网上寻找一些有后门漏洞的主机，然后入侵系 统安装控制程序，入侵的越多，控制的僵尸主机就越多，攻击源就更多，然后把入侵的主机 分配，一部分充当攻击的主要控制端，一部分充当攻击源，各负其责，在攻击者统一指挥下 对被攻击的服务器发起攻击，由于这个攻击模式是在幕后操作，所以很难被监控系统跟踪， 身份不容易被发现。

**七、反弹技术—DRDoS**

　DRDoS分布反射式拒绝服务攻击这是DDoS攻击的变形,它与DDoS的不同之处就是DrDoS不需要在攻击之前占领大量的“肉鸡”。它的攻击原理和Smurf攻击原理相近,不过DRDoS是可以在广域网上进行的,而Smurf攻击是在局域网进行的。它的作用原理是基于广播地址与回应请求的。一台计算机向另一台计算机发送一些特殊的数据包如ping请求时,会接到它的回应;如果向本网络的广播地址发送请求包,实际上会到达网络上所有的计算机,这时就会得到所有计算机的回应。这些回应是需要被接收的计算机处理的,每处理一个就要占用一份系统资源,如果同时接到网络上所有计算机的回应,接收方的系统是有可能吃不消的,就象遭到了DDoS攻击一样。不过是没有人笨到自己攻击自己,不过这种方法被黑客加以改进就具有很大的威力了。黑客向广播地址发送请求包,所有的计算机得到请求后,却不会把回应发到黑客那里,而是发到被攻击主机。这是因为黑客冒充了被攻击主机。黑客发送请求包所用的软件是可以伪造源地址的,接到伪造数据包的主机会根据源地址把回应发出去,这当然就是被攻击主机的地址。黑客同时还会把发送请求包的时间间隔减小,这样在短时间能发出大量的请求包,使被攻击主机接到从被欺骗计算机那里传来的洪水般的回应,就像遭到了DDoS攻击导致系统崩溃。骇客借助了网络中所有计算机来攻击受害者,而不需要事先去占领这些被欺骗的主机,这就是Smurf攻击。而DRDoS攻击正是这个原理,黑客同样利用特殊的发包工具,首先把伪造了源地址的SYN连接请求包发送到那些被欺骗的计算机上,根据TCP三次握手的规则,这些计算机会向源IP发出SYN+ACK或RST包来响应这个请求。同Smurf攻击一样,黑客所发送的请求包的源IP地址是被攻击主机的地址,这样受欺骗的主机就都会把回应发到被攻击主机处,造成被攻击主机忙于处理这些回应而瘫痪。

**八、DNS欺骗**

**DNS欺骗检测和防范思路**

发生DNS欺骗时，Client最少会接收到两个以上的应答数据报文，报文中都含有相同的ID序列号，一个是合法的，另一个是伪装的。据此特点，有以下两种检测办法：

(1)被动监听检测。即监听、检测所有DNS的请求和应答报文。通常DNS Server对一个请求查询仅仅发送一个应答数据报文(即使一个域名和多个IP有映射关系，此时多个关系在一个报文中回答)。因此在限定的时间段内一个请求如果会收到两个或以上的响应数据报文，则被怀疑遭受了DNS欺骗。

(2)主动试探检测。即主动发送验证包去检查是否有DNS欺骗存在。通常发送验证数据包接收不到应答，然而黑客为了在合法应答包抵达客户机之前就将欺骗信息发送给客户，所以不会对DNS Server的IP合法性校验，继续实施欺骗。若收到应答包，则说明受到了欺骗攻击。

**防范思路**

在侦测到网络中可能有DNS欺骗攻击后，防范措施有：①在客户端直接使用IP Address访问重要的站点，从而避免DNS欺骗; ②对DNS Server和Client的数据流进行加密，Server端可以使用SSH加密协议，Client端使用PGP软件实施数据加密。

对于常见的ID序列号欺骗攻击，采用专业软件在网络中进行监听检查，在较短时间内，客户端如果接收到两个以上的应答数据包，则说明可能存在DNS欺骗攻击，将后到的合法包发送到DNS Server并对DNS数据进行修改，这样下次查询申请时就会得到正确结果。

**防护方法：**

1 进行IP地址和MAC地址的绑定

 (1)预防ARP欺骗攻击。

 (2)DNS信息绑定。

2 使用Digital Password进行辨别

3.优化DNS SERVER的相关项目设置

4.直接使用IP地址访问

5.对DNS数据包进行监测

**九、访问控制技术—DAC**

主体是用户的身份，客体是资源或者说是文件（切记：一切皆文件）。由客体的属主对自己的客体进行管理，由主体自己决定是否将自己的客体访问权限或部分访问权限授予其他主体，这种控制方式是自主的。也就是说，**在自主访问控制下，用户可以按自己的意愿，有选择地与其他用户共享他的文件**。

DAC系统有两个至关重要的标准：

1.**文件的所有权**：系统中的每个文件（一些特殊文件可能没有，如块设备文件等）都有所有者。在DAC系统中，文件的所有者是创建这个文件的计算机的使用者（或事件，或另一个文件）。那么此文件的自主访问控制权限由它的创建者来决定如何设置和分配；

2.**访问权限**：文件的所有者拥有访问权限，并且可以将访问权限分配给自己及其他用户。

上述两个标准说明：

1.文件的所有权的优先级高于访问权限

1)文件的所有者即便没有任何权限，也可以在为自己分配权限之后获得访问文件的能力。

2)非文件的所有者即便已经获得了访问权限，也可能会被所有者随时收回，从而导致无权访问该文件。

2.权限是文件访问的关键

1)无论是不是文件的所有者，关系到使用者能否访问文件的最直接的因素是其所对应的用户是否获得了可访问该文件的权限

2)使用者被分配的何种权限，就只能以该权限所规定的操作来访问文件，无法越权。

**强制访问控制MAC**

MAC是利用策略将访问控制规则“强加”给访问主体的，即系统强制主体服从访问控制策略。MAC的主要作用对象是所有主体及其所操作的客体（如：进程、文件等）。**MAC为这些主体及其所操作的客体提供安全标记**，这些标记是实施强制访问控制的依据。

**系统通过比较主体和客体的安全标记来判断一个主体是否能够访问其要操作的客体。用户发起的进程无法改变其自身及其它客体的安全标记，利用这样的机制，系统可以比较有效地防止特洛伊木马攻击以及root身份冒用或盗用等安全威胁**。

MAC一般与DAC共同使用，两种访问控制机制的过滤结果将累积，以此来达到更佳的访问控制效果。也就是说，**一个主体只有通过了DAC限制检查与MAC限制检查的双重过滤装置之后，才能真正访问某个客体。一方面，用户可以利用DAC来防范其它用户对那些所有权归属于自己的客体的攻击；另一方面，由于用户不能直接改变MAC属性，所以MAC提供了一个不可逾越的、更强的安全保护层以防止其它用户偶然或故意地滥用DAC**。

**DAC与MAC的对比**

**1. DAC（Discretionary Access Control，自主访问控制）**

① DAC是传统的Linux的访问控制方式，DAC可以对文件、文件夹、共享资源等进行访问控制。

② 在DAC这种模型中，文件客体的所有者（或者管理员）负责管理访问控制。

③ DAC使用了ACL（Access Control List，访问控制列表）来给非管理者用户提供不同的权限，而root用户对文件系统有完全自由的控制权。

**2. MAC（Mandatory Access Control，强制访问控制）**

① SELinux在内核中使用MAC检查操作是否允许。

② 在MAC这种模型中，系统管理员管理负责访问控制，用户不能直接改变强制访问控制属性。

③ MAC可以定义所有的进程（称为主体）对系统的其他部分（文件、设备、socket、端口和其它进程等，称为客体）进行操作的权限或许可。

**3. DAC和MAC的其它区别**

① DAC的主体是真实有效的用户和组ID，MAC的主体是安全上下文，两者的UID是各自独立的。

② DAC的访问控制模式是rwxrwxrwx，MAC的访问控制模式是user:role:type。

**十、网卡与网络隔离卡的区别**

网路隔离卡见课本

网卡是工作在链路层的网络组件，是局域网中连接计算机和传输介质的接口，不仅能实现与局域网传输介质之间的物理连接和电信号匹配，还涉及帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据缓存的功能等。

专网专用，连系统也必须各是各的，内网是内网系统、外网是外网系统，不能一个系统可以同时连接两个网络（双网卡既是一个系统可以同时连接两个网络）.

**十一、网闸与防火墙的区别**

网闸与防火墙的区别是：1、防火墙首先保证网络连通性，然后考虑安全问题，网闸在保证安全的基础上进行数据交换；2、防火墙是单主机架构，网闸是双主机架构；3、网闸相对于防火墙同步类功能安全性更高。

**1、应用场景区别**

防火墙：防火墙首先要保证网络的连通性，其次才是安全问题；

网闸：网闸是保证安全的基础上进行数据交换。网闸是两个网络已经存在，现在两个网络不得不互联，互联就要保证安全，网闸是现在唯一最安全的网络边界安全隔离的产品，只有网闸这种产品才能解决这个问题，所以必须用网闸。

**2、硬件区别**

防火墙是单主机架构，早期使用包过滤的技术，网闸是双主机2+1架构，通过私有的协议摆渡的方式进行数据交换，基于会话的检测机制，由于网闸是双主机结构，即使外网端被攻破，由于内部使用私有协议互通，没办法攻击到内网，防火墙是单主机结构，如果被攻击了，就会导致内网完全暴露给别人。

**3、功能区别**

网闸主要包含两大类功能，访问类功能和同步类功能，访问类功能类似于防火墙，网闸相对于防火墙安全性更高的是同步类功能。



**十二、防火墙—代理技术**

**1.代理的执行流程（两种情况）**

1.代理服务器监听内联网络中主机的请求，当请求到达代理服务器后，代理服务器根据安全策略对数据包的首部和数据部分信息进行检查，检查之后将内联网络中的主机源地址改为自己的地址之后将这个数据包发给外部的目的主机，这样外部的主机接到的信息是来自于代理服务器而不是源主机。目的主机应答的数据包也将发送到代理服务器，经过代理服务器检查允许通过后，代理服务器将数据包的目的地址改为内联主机的地址，之后发往目的主机。类似于在内联网络和外联网络之间设置一个中转，外联网络并不清楚内联网络的拓补结构。

2.内部的主机只接受代理服务器的信息而不接收任何外部地址主机发来的信息，外部主机只能讲信息发往代理服务器，之后由代理服务器将信息转发给内联网路中的主机。代理服务器负责监控整个通信过程来保证通信过程的安全性。

**十、入侵检测系统—评价指标**

**1. 测试评估IDS性能的标准**

根据Porras等的研究，给出了评价IDS性能的三个因素：

1. **准确性**：指IDS从各种行为中正确地识别入侵的能力，当一个IDS的检测不准确时，就有可能把系统中的合法活动当作入侵行为并标识为异常（虚警现象）。
2. **处理性能**：指一个IDS处理数据源数据的速度。显然，当IDS的处理性能较差时，它就不可能实现实时的IDS，并有可能成为整个系统的瓶颈，进而严重影响整个系统的性能。
3. **完备性**：指IDS能够检测出所有攻击行为的能力。如果存在一个攻击行为，无法被IDS检测出来，那么该JDS就不具有检测完备性。也就是说，它把对系统的入侵活动当作正常行为（漏报现象）。由于在一般情况下，攻击类型、攻击手段的变化很快，我们很难得到关于攻击行为的所有知识，所以关于IDS的检测完备性的评估相对比较困难。

在此基础上，Debar等又增加了两个性能评价测度：

1. **容错性**：由于IDS是检测入侵的重要手段／所以它也就成为很多入侵者攻击的首选目标。IDS自身必须能够抵御对它自身的攻击，特别是拒绝服务（Denial-of-Service）攻击。由于大多数的IDS是运行在极易遭受攻击的操作系统和硬件平台上，这就使得系统的容错性变得特别重要，在测试评估IDS时必须考虑这一点。
2. **及时性**：及时性要求IDS必须尽快地分析数据并把分析结果传播出去，以使系统安全管理者能够在入侵攻击尚未造成更大危害以前做出反应，阻止入侵者进一步的破坏活动，和上面的处理性能因素相比，及时性的要求更高。它不仅要求IDS的处理速度要尽可能地快，而且要求传播、反应检测结果信息的时间尽可能少。

按照数据分析发生的时间不同，IDS可以分为**脱机分析和联机分析**

**脱机分析：**就是在行为发生后，对产生的数据进行分析，而不是在行为发生的同时进行分析。如对日志的审核、对系统文件的完整性检查都属于这种。一般而言，脱机分析也会间隔很长时间，脱机只是相对于联机而言的。

**联机分析**：就是在数据产生或者发生改变的同时对其进行检查，以发现攻击行为。这种方式一般用于对网络数据的实时分析，对系统资源要求比较高。

**HIDS和NIDS的对比分析：**（罗敏PPT加对比分析）

HIDS和NIDS的区别如下：

**1. HIDS（Host-based Intrusion Detection System，基于主机的入侵检测系统）**

① HIDS将代理安装在受保护的系统中，它要求与操作系统内核和服务紧密捆绑在一起，监控各种系统事件，如对内核或API的调用，以此来进行防御。

② HIDS还可以监测特定的系统文件和可执行文件调用，以及Windows NT下的安全记录和Unix环境下的系统记录。

③ HIDS能对检测的入侵行为、事件给予积极的反应，比如断开连接、封掉用户账号、杀死进程、提交警报等。

④ HIDS技能要求非常高，要求开发HIDS的企业对有关的操作系统非常了解，而且安装在主机上的代理必须非常可靠，系统占用小，自身安全性要好，否则将会对系统产生负面影响。

⑤ HIDS关注的是到达主机的各种安全威胁，并不关注网络的安全。

⑥ HIDS由于采取的是对事件和系统调用的监控，衡量它的技术指标非常少。

**2. NIDS（Network Intrusion Detection System，网络入侵检测系统）**

① NIDS最大的特点在于不需要改变服务器等主机的配置，它不需在业务系统的主机中安装额外的软件。

② NIDS不是系统中的关键路径，即使发生故障也不会影响正常业务的运行。

③ NIDS是以网络包作为分析数据源。它通常运用一个工作在混杂模式下的网卡来实时监视并分析通过网络的数据流。

④ NIDS的分析模块通常运用模式匹配、统计分析等技能来识别攻击行为，一旦检测到了攻击行为，NIDS的响应模块就作出适当的响应，比如报警、切断有关用户的网络连接等。

⑤ NIDS收集的是网络中的动态流量信息，因此，攻击特征库数目多少以及数据处理能力，就决定了NIDS识别入侵行为的能力。

⑥ 部署一个NIDS，比HIDS的风险与成本相对较低。

⑦ NIDS采取的基本上都是模式匹配的形式，所以衡量NIDS的技术指标可以数量化。

⑧ 在NIDS的应用过程中，最大的敌人就是误警和漏警。漏警不影响应用环境的可用性，只是用户的投资失误；而误警则有可能导致警报异常、网络紊乱，甚至应用的瘫痪。

**十三、VPN—工作原理**

1、通常情况下，VPN网关采取双网卡结构，外网卡使用公网IP接入Internet。

　　2、网络一（假定为公网internet）的终端A访问网络二（假定为公司内网）的终端B，其发出的访问数据包的目标地址为终端B的内部IP地址。

　　3、网络一的VPN网关在接收到终端A发出的访问数据包时对其目标地址进行检查，如果目标地址属于网络二的地址，则将该数据包进行封装，封装的方式根据所采用的VPN技术不同而不同，同时VPN网关会构造一个新VPN数据包，并将封装后的原数据包作为VPN数据包的负载，VPN数据包的目标地址为网络二的VPN网关的外部地址。

　　4、网络一的VPN网关将VPN数据包发送到Internet，由于VPN数据包的目标地址是网络二的VPN网关的外部地址，所以该数据包将被Internet中的路由正确地发送到网络二的VPN网关。

　　5、网络二的VPN网关对接收到的数据包进行检查，如果发现该数据包是从网络一的VPN网关发出的，即可判定该数据包为VPN数据包，并对该数据包进行解包处理。解包的过程主要是先将VPN数据包的包头剥离，再将数据包反向处理还原成原始的数据包。

　　6、网络二的VPN网关将还原后的原始数据包发送至目标终端B，由于原始数据包的目标地址是终端B的IP，所以该数据包能够被正确地发送到终端B。在终端B看来，它收到的数据包就和从终端A直接发过来的一样。

　　7、从终端B返回终端A的数据包处理过程和上述过程一样，这样两个网络内的终端就可以相互通讯了。

　　通过上述说明可以发现，在VPN网关对数据包进行处理时，有两个参数对于VPN通讯十分重要：原始数据包的目标地址（VPN目标地址）和远程VPN网关地址。根据VPN目标地址，VPN网关能够判断对哪些数据包进行VPN处理，对于不需要处理的数据包通常情况下可直接转发到上级路由；远程VPN网关地址则指定了处理后的VPN数据包发送的目标地址，即VPN隧道的另一端VPN网关地址。由于网络通讯是双向的，在进行VPN通讯时，隧道两端的VPN网关都必须知道VPN目标地址和与此对应的远端VPN网关地址。

**十四、PPTP和L2TP**

**L2TP/IPSec 和 PPTP 在以下方面类似：**

它们提供了一种逻辑传输机制来发送 PPP 有效载荷。

它们提供隧道或封装，以便基于任何协议的 PPP 有效载荷可以通过 IP 网络发送。

它们依靠 PPP 连接过程来执行用户认证和协议配置。

**L2TP/IPSec 和 PPTP 在以下方面有所不同：**

使用 PPTP，数据加密在 PPP 连接过程（因此，PPP 身份验证）完成后开始。使用 L2TP/IPSec，数据加密在 PPP 连接过程之前开始。

PPTP 连接使用 MPPE，这是一种基于 Rivest-Shamir-Aldeman RC-4 加密算法并提供 40、56 或 128 位加密密钥的流密码。流密码将数据加密为比特流。L2TP/IPSec 连接使用数据加密标准 (DES)，它是一种分组密码，它使用 56 位的 DES 密钥或三个 3-DES 的 56 位密钥。块密码以离散块（64 位块，在 DES 的情况下）中加密数据。

PPTP 连接仅需要通过基于 PPP 的身份验证协议进行用户级身份验证。L2TP/IPSec 连接需要相同的用户级身份验证，此外还需要通过计算机证书进行计算机级身份验证。

（主要是PPTP和L2TP的工作原理LMPPT + 课本P315）

**如何对抗Teardrop攻击**

Teardrop攻击是攻击者A给受害者B发送一些分片IP报文，并且故意将“13位分片偏移”字段设置成错误的值(既可与上一分片数据重叠，也可错开)，B在组合这种含有重叠偏移的伪造分片报文时，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。利用UDP包重组时重叠偏移（假设数据包中第二片IP包的偏移量小于第一片结束的位移，而且算上第二片IP包的Data，也未超过第一片的尾部，这就是重叠现象。）的漏洞对系统主机发动拒绝服务攻击，最终导致主机菪掉；对于Windows系统会导致蓝屏死机，并显示STOP 0x0000000A错误。

Teardrop攻击防御方法：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。为了防止缓存益处，当缓存快要存满是，直接丢弃后续分片报文。

反攻击方法：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。

**如何发现自己正在受到消耗网络资源的DoS攻击（可参考课本p75）**

1、服务器主机上有大量等待的TCP连接；

2、检查网站后台服务器发现大量无用的数据包；

3、一段时期中IP请求异常且源地址虚假；

4、网络流量出现异常变化突然暴涨；

5、当发现Ping超时或丢包严重时，注意连接错误。假如遇到无法访问网站这种情况，并看到类似于“无法访问站点”之类的错误，且无法访问其他Internet服务，则可能是DoS攻击带来的影响。

6、查看自己的邮箱里是否突然收到大量的垃圾邮件。

具体地，可使用netstat命令：

netstat -n -p | grep SYN\_REC | sort -u

列出所有连接过的IP地址。

netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n

使用netstat命令计算每个主机连接到本机的连接数。

netstat -na

该命令将显示所有活动的网络连接。

netstat -n -p | grep SYN\_REC | awk '{print $5}' | awk -F: '{print $1}'

列出所有发送SYN\_REC连接节点的IP地址。

netstat -an | grep :80 | sort

显示所有80端口的网络连接并排序。这里的80端口是http端口，所以可以用来监控web服务。如果看到同一个IP有大量连接的话就可以判定单点流量攻击了。

netstat -ntu | grep ESTAB | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr

检查 ESTABLISHED 连接并且列出每个IP地址的连接数量。

netstat -plan|grep :80|awk {'print $5'}|cut -d: -f 1|sort|uniq -c|sort -nk 1

列出所有连接到本机80端口的IP地址和其连接数。80端口一般是用来处理HTTP网页请求。

netstat -anp |grep 'tcp|udp' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n

列出所有连接到本机的UDP或者TCP连接的IP数量。

**netstat -n -p|grep SYN\_REC | wc -l**

**这个命令可以查找出当前服务器有多少个活动的 SYNC\_REC 连接。正常来说这个值很小，最好小于5。 当有Dos攻击或者邮件炸弹的时候，这个值相当的高。**尽管如此，这个值和系统有很大关系，有的服务器值就很高，也是正常现象。

如何通过netstat命令缓解DDOS攻击呢？一旦获得攻击服务器的IP地址就可以使用以下命令拒绝此IP的所有连接。

iptables -A INPUT 1 -s $IPADRESS -j DROP/REJECT

注意，你需要将 $IPADRESS 替换成需要拒绝连接的IP地址。执行完以上命令后，使用以下命令结束所有的httpd连接以清理系统。

killall -KILL httpd

然后执行以下命令重启httpd服务。

service httpd start           #RedHat 系统

/etc/init/d/apache2 restart   #Debian 系统

当然通过netstat命令只能缓解部分DDoS攻击，而且还很有可能造成大量误封正常访客。所以墨者安全还是建议最好通过专业的网络安全公司部署DDoS高防IP，对恶意攻击流量进行清洗，隐藏服务器源IP，确保源站稳定运行。

**对付分布式拒绝服务攻击的方法有哪些？举例说明（参考课本p77）**

**企业网管理员**

网管员做为一个企业内部网的管理者，往往也是安全员、守护神。在他维护的网络中有一些服务器需要向外提供WWW服务，因而不可避免地成为DDoS的攻击目标，他该如何做呢？可以从主机与网络设备两个角度去考虑。

主机上的设置  
几乎所有的主机平台都有抵御DoS的设置，总结一下，基本的有几种：

* 关闭不必要的服务
* 限制同时打开的Syn半连接数目
* 缩短Syn半连接的time out 时间
* 及时更新系统补丁

网络设备上的设置  
企业网的网络设备可以从防火墙与路由器上考虑。这两个设备是到外界的接口设备，在进行防DDoS设置的同时，要注意一下这是以多大的效率牺牲为代价的，对你来说是否值得。

１.防火墙

* 禁止对主机的非开放服务的访问
* 限制同时打开的SYN最大连接数
* 限制特定IP地址的访问
* 启用防火墙的防DDoS的属性
* 严格限制对外开放的服务器的向外访问

第五项主要是防止自己的服务器被当做工具去害人。

２.路由器  
以Cisco路由器为例

* Cisco Express Forwarding（CEF）
* 使用 unicast reverse-path
* 访问控制列表（ACL）过滤
* 设置SYN数据包流量速率
* 升级版本过低的ISO
* 为路由器建立log server

其中使用CEF和Unicast设置时要特别注意，使用不当会造成路由器工作效率严重下降，升级IOS也应谨慎。路由器是网络的核心设备，与大家分享一下进行设置修改时的小经验，就是先不保存。Cisco路由器有两份配置startup config和running config，修改的时候改变的是running config，可以让这个配置先跑一段时间（三五天的就随意啦），觉得可行后再保存配置到startup config；而如果不满意想恢复原来的配置，用copy start run就行了。

**假如你的主机正在面临DNS欺骗攻击，你打算采取什么解决策略和方案？**

**DNS欺骗检测和防范思路**

**3.1 检测思路**

      发生DNS欺骗时，Client最少会接收到两个以上的应答数据报文，报文中都含有相同的ID序列号，一个是合法的，另一个是伪装的。据此特点，有以下两种检测办法：

      (1)被动监听检测。即监听、检测所有DNS的请求和应答报文。通常DNS Server对一个请求查询仅仅发送一个应答数据报文(即使一个域名和多个IP有映射关系，此时多个关系在一个报文中回答)。因此在限定的时间段内一个请求如果会收到两个或以上的响应数据报文，则被怀疑遭受了DNS欺骗。

      (2)主动试探检测。即主动发送验证包去检查是否有DNS欺骗存在。通常发送验证数据包接收不到应答，然而黑客为了在合法应答包抵达客户机之前就将欺骗信息发送给客户，所以不会对DNS Server的IP合法性校验，继续实施欺骗。若收到应答包，则说明受到了欺骗攻击。

**3.2 防范思路**

      在侦测到网络中可能有DNS欺骗攻击后，防范措施有：①在客户端直接使用IP Address访问重要的站点，从而避免DNS欺骗; ②对DNS Server和Client的数据流进行加密，Server端可以使用SSH加密协议，Client端使用PGP软件实施数据加密。

      对于常见的ID序列号欺骗攻击，采用专业软件在网络中进行监听检查，在较短时间内，客户端如果接收到两个以上的应答数据包，则说明可能存在DNS欺骗攻击，将后到的合法包发送到DNS Server并对DNS数据进行修改，这样下次查询申请时就会得到正确结果。

**四、DNS防护方案**

**4.1 进行IP地址和MAC地址的绑定**

      (1)预防ARP欺骗攻击。因为DNS攻击的欺骗行为要以ARP欺骗作为开端，所以如果能有效防范或避免ARP欺骗，也就使得DNS ID欺骗攻击无从下手。例如可以通过将Gateway Router 的Ip Address和MAC Address静态绑定在一起，就可以防范ARP攻击欺骗。

      (2)DNS信息绑定。DNS欺骗攻击是利用变更或者伪装成DNS Server的IP Address，因此也可以使用MAC Address和IP Address静态绑定来防御DNS欺骗的发生。由于每个Network Card的MAC Address具有唯一性质，所以可以把DNS Server的MAC Address与其IP Address绑定，然后此绑定信息存储在客户机网卡的Eprom中。当客户机每次向DNS Server发出查询申请后，就会检测DNS Server响应的应答数据包中的MAC Address是否与Eprom存储器中的MAC Address相同，要是不同，则很有可能该网络中的DNS Server受到DNS欺骗攻击。这种方法有一定的不足，因为如果局域网内部的客户主机也保存了DNS Server的MAC Address，仍然可以利用MAC Address进行伪装欺骗攻击。

**4.2 使用Digital Password进行辨别**

      在不同子网的文件数据传输中，为预防窃取或篡改信息事件的发生，可以使用任务数字签名(TSIG)技术即在主从Domain Name Server中使用相同的Password和数学模型算法，在数据通信过程中进行辨别和确认。因为有Password进行校验的机制，从而使主从Server的身份地位极难伪装，加强了Domain Name信息传递的安全性。

      安全性和可靠性更好的Domain Name Service是使用域名系统的安全协议(Domain Name System Security, DNSSEC))，用Digital Signature的方式对搜索中的信息源进行分辨，对DATA的完整性实施校验，DNSSEC的规范可参考RFC2605。因为在设立Domain时就会产生Password，同时要求上层的Domain Name也必须进行相关的Domain Password Signature，显然这种方法很复杂，所以InterNIC域名管理截至目前尚未使用。然而就技术层次上讲，DNSSEC应该是现今最完善的Domain Name设立和解析的办法，对防范Domain Name欺骗攻击等安全事件是非常有效的。

**4.3 优化DNS SERVER的相关项目设置**

      对于DNS Server的优化可以使得DNS的安全性达到较高的标准，常见的工作有以下几种：①对不同的子网使用物理上分开的Domain Name Server,从而获得DNS功能的冗余;②将外部和内部Domain Name Server从物理上分离开并使用Forwarders转发器。外部Domain Name Server可以进行任何客户机的申请查询，但Forwarders则不能，Forwarders被设置成只能接待内部客户机的申请查询;③采用技术措施限制DNS动态更新;④将区域传送(zone transfer)限制在授权设备上;⑤利用事务签名对区域传送和区域更新进行数字签名;⑥隐藏服务器上的Bind版本;⑦删除运行在DNS服务器上的不必要服务，如FTP、telnet和Http;⑧在网络外围和DNS服务器上使用防火墙,将访问限制在那些DNS功能需要的端口上。

**4.4 直接使用IP地址访问**

      对个别信息安全等级要求十分严格的WEB站点尽量不要使用DNS进行解析。由于DNS欺骗攻击中不少是针对窃取客户的私密数据而来的，而多数用户访问的站点并不涉及这些隐私信息，因此当访问具有严格保密信息的站点时，可以直接使用IP地址而无需通过DNS解析，这样所有的DNS欺骗攻击可能造成的危害就可以避免了。除此，应该做好DNS Server的安全配置项目和升级DNS软件，合理限定DNS Server进行响应的IP地址区间，关闭DNS Server的递归查询项目等。

**4.5 对DNS数据包进行监测**

      在DNS欺骗攻击中，Client会接收到至少两个DNS的数据响应包，一个是真实的数据包，另一个是攻击数据包。欺骗攻击数据包为了抢在真实应答包之前回复给Client，它的信息数据结构与真实的数据包相比十分简单，只有应答域，而不包括授权域和附加域。因此，可以通过监测DNS响应包，遵循相应的原则和模型算法对这两种响应包进行分辨，从而避免虚假数据包的攻击。

**TCP/IP的安全性隐患？改进措施？**

**1、链路层上的攻击**

在TCP/IP网络中，链路层这一层次的复杂程度是最高的。其中最常见的攻击方式通常是网络嗅探组成的TCP/IP协议的以太网。

以太网卡有两种主要的工作方式，一种是一般工作方式，另一种是较特殊的混杂方式。这一情况下，很可能由于被攻击的原因而造成信息丢失情况，且攻击者可以通过数据分析来获取账户、密码等多方面的关键数据信息。

**2、网络层上的攻击**

如果ARP识别链接错误，这样的话ARP直接应用可疑信息，那么可疑信息就会很容易进入目标主机当中。ARP协议没有状态，不管有没有收到请求，主机会将任何受到的ARP相应自动缓存。

如果信息中带有病毒，采用ARP欺骗就会导致网络信息安全泄露。因此，在ARP识别环节，应加大保护，建立更多的识别关卡，不能只简单通过IP名进行识别，还需充分参考IP相关性质等。

**3、传输层上的攻击**

在传输层还存在网络安全问题。如在网络安全领域中，IP欺骗就是隐藏自己的有效手段，主要是通过将自身IP地址进行伪造，并向目标主机发送恶意的请求，攻击主机，而主机却因为IP地址被隐藏而无法准确确认攻击源。或者通过获取目标主机信任而趁机窃取相关的机密信息。

**4、应用层上的攻击**

对于因特网而言，IP地址与域名均是一一对应的，这两者之间的转换工作，被称为域名解析。而DNS就是域名解析的服务器。DNS欺骗指的是攻击方冒充域名服务器的行为，使用DNS欺骗能将错误DNS信息提供给目标主机。所以说，通过DNS欺骗可误导用户进入非法服务器，让用户相信诈骗IP。