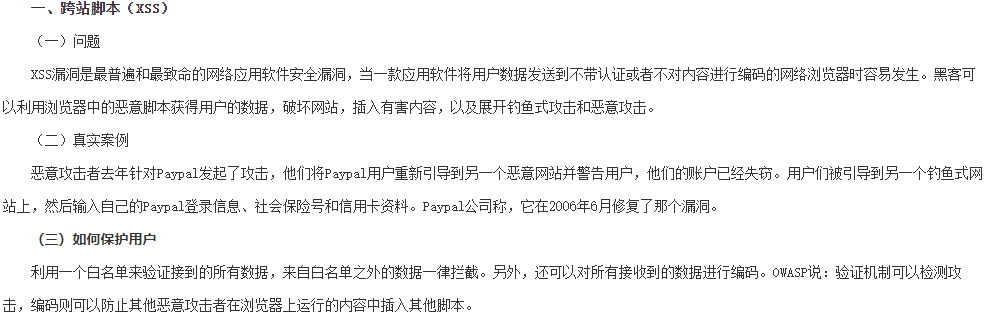
## 一、概述：

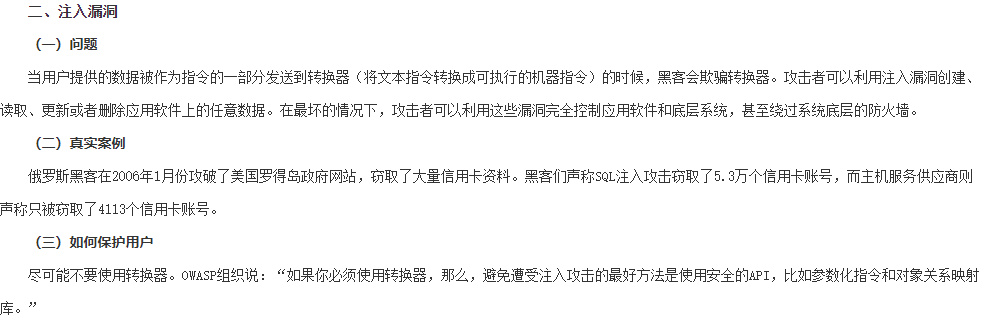
1、硬件软件漏洞例子

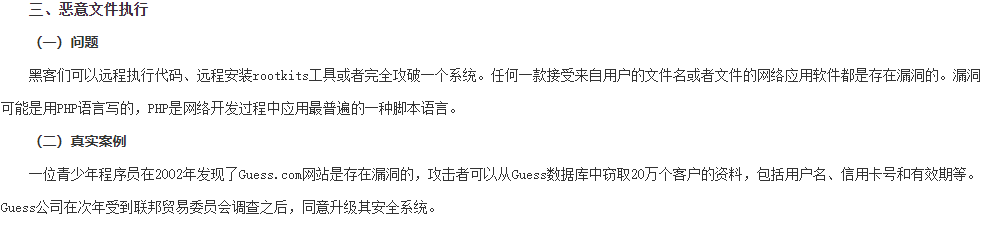
硬件：(芯片漏洞植入为主)

一些网络安全人员给电脑的芯片（CPU）刷入恶意的Firmware固件，使未经许可的攻击者轻易地进入系统，而电脑管理员本身在系统里却无法发觉，用这种攻击方式的人被称为“硬件黑客”。

软件：(xss跨站脚本、注入、跨站指令cookie等)







2、TCP/IP协议栈面临的五大网络安全问题

1. IP欺骗

IP Spoof即IP 电子欺骗，可以理解为一台主机设备冒充另外一台主机的IP地址与其他设备通信。

1. SYN Flooding

SYN Flooding 为DoS攻击形式。它利用TCP三次握手协议的缺陷，向目标主机发送大量的伪造源地址的SYN连接请求，消耗目标主机的资源，从而不能够为正常用户提供服务。

1. ACK Flooding

ACK Flooding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，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。

1. UDP flooding

UDP Flooding是日渐猖厥的流量型DoS攻击，利用大量UDP小包冲击DNS服务器，或Radius认证服务器、流媒体视频服务器

1. Connection Flooding

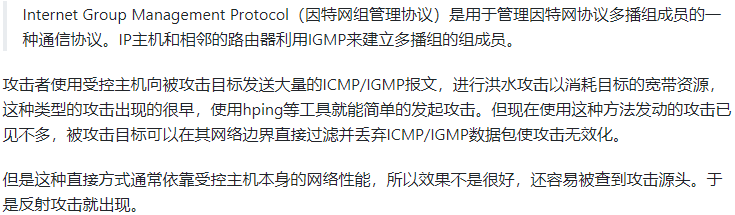
Connection Flooding是利用小流量冲击大带宽网络服务的攻击方式。利用真实的IP地址向服务器发起大量的连接，建立连接之后很长时间不释放，占用服务器的资源，造成服务器上残余连接(WAIT状态)过多，效率降低，甚至资源耗尽，无法响应其他客户所发起的连接。

3、U盘双击容易中毒原理

就是“autorun.inf文件”。病毒首先把自身复制到u盘,然后创建一个autorun.inf，当你在插入U盘或者双击u盘时，autorun.inf中的设置会运行u盘中的病毒。

## 二、攻击行径

1、IGMP flood



## 三、网络扫描/侦察技术

1、ARP欺骗的破绽特征？/防护

ARP欺骗的特征就是不断的发arp包，让被攻击主机相信并修改arp表。

使用wireshark开启混杂模式后，只需抓取arp类型的包，看密集程度。一旦出现攻击态势，就可以快速对攻击和被攻击双方进行定位。

防护时：

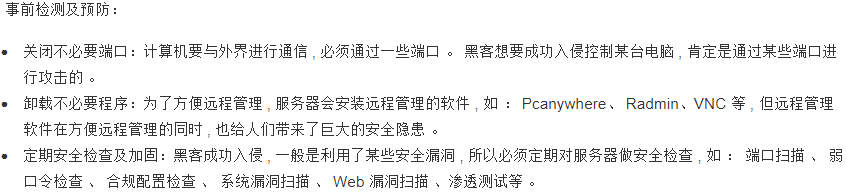
1最理想的防制方法是网络内的每台电脑ARP一律改用静态的方式，不过大型的网络是不可行，因为需要经常更新每台电脑的ARP表。

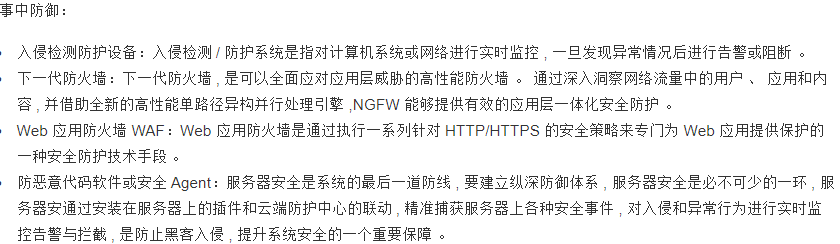
2 使用例如DHCP snooping，网络设备可借DHCP保留网络上各电脑的MAC地址，在伪造的ARP数据包发出时即可侦测到。

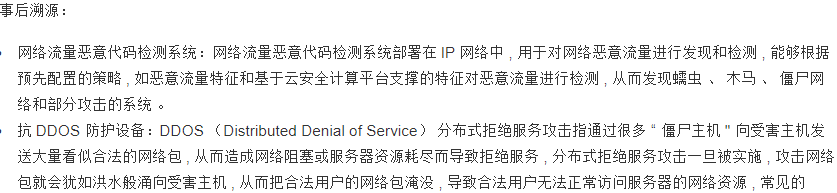
2、僵尸主机多怎么办？

僵尸主机(沦为肉鸡)是指感染僵尸程序病毒，从而被黑客程序控制的计算机设备。其可以随时按照黑客的命令与控制指令展开DoS攻击或发送垃圾信息。一般被侵占的电脑只是僵尸网络里面众多中的一个，会被用来去运行一连串的或远端控制的恶意程序

解决/检测：(特征 发动攻击时突然产生大量网络流量)







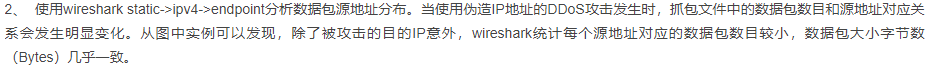
## 四、DOS攻击

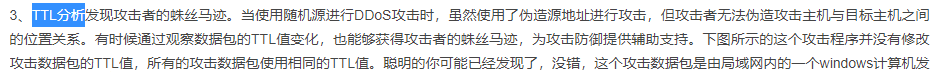
1、怎么应对DDos攻击(属于黑客中的暴力犯罪)，利用数据包的哪些特征？

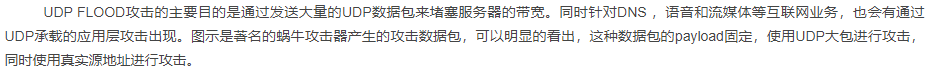
攻击发生时的cap文件(wireshark抓包)进行仔细的分析，找出攻击者忽略的地方，找出攻击数据包与正常业务流量中有区别的地方。

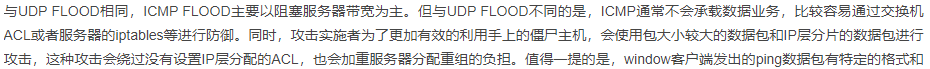
例子：

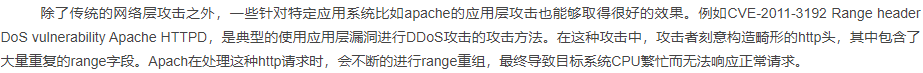










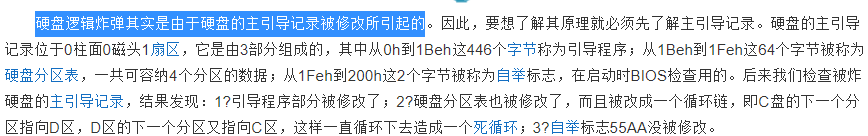


## 六、处理程序错误攻击

1、如何存放/投放逻辑炸弹？

逻辑炸弹可以以软件和硬件形态存在，如操作系统、应用软件、主板、CPU、FPGA等。例子：

逻辑：硬盘启动/装载时触发 死循环 装载不了



## 七、欺骗攻击

1、如何识别服务器应答包与虚假包

2、针对Email应用，除了Email欺骗，还有哪种攻击方式？

Email电子邮件轰炸攻击，见书P161 P72 存储资源消耗Dos攻击

3、TCP会话劫持 监听者如何猜测序列号

书P170

## 九、访问控制

1、DAC和MAC结合

通常MAC与DAC结合使用，并实施一些附加的、更强的访问限制。一个主体只有通过自主与强制性访问限制检查后，才能访问其客体。用户可利用DAC来防范其他用户对自己客体的攻击，由于用户不能直接改变强制访问控制属性，所以强制访问控制提供了一个不可逾越的、更强的安全保护层，以防范偶然或故意地滥用DAC。

2、设置客户端物理隔离过渡区？

双硬盘：一个对应一个网络

单硬盘：单个硬盘上磁道的读写控制技术，在一个硬盘上分隔出两个工作区间 网络安全隔离卡(物理方式PC物理层) 在任何时候，数据只能通往一个分区。

数据交换/过渡区：在两个分区以外，在硬盘上另外设置一个功能区，用于不同的状态转换，表现为硬盘的D盘，各个分区可以通过功能区作为一个过渡区来交换数据。

3、网卡、隔离卡区别？

网卡 链路层 类似一个系统 通过不同的网卡 连接不同网段 上内外网

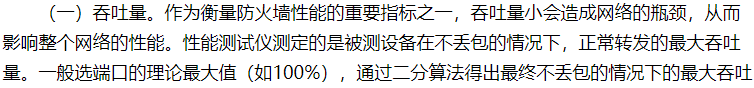
隔离卡 物理层 每次换内外网 需要重启系统 类似双系统

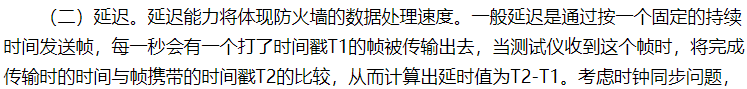
4、思考题

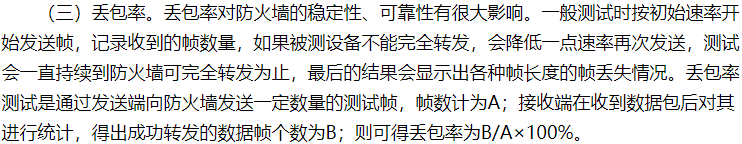
## 十、防火墙

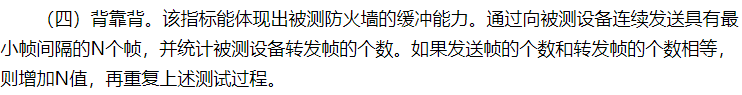
1、防火墙指标 内网控制 稳定性 工作原理

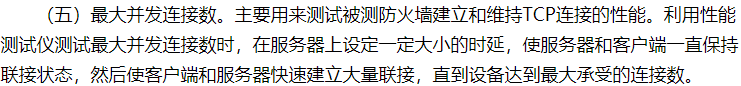
防火墙性能衡量：

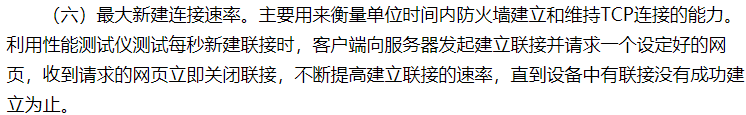






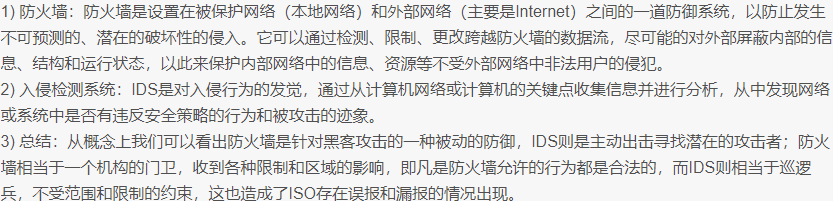




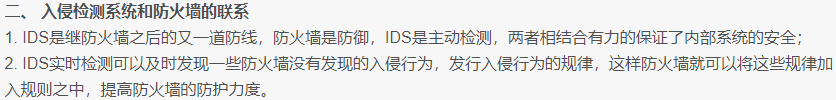


## 十一、入侵检测

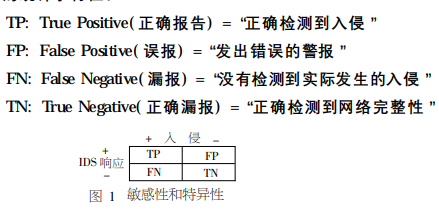
1、和防火墙不同？

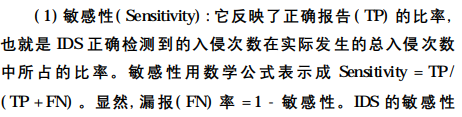
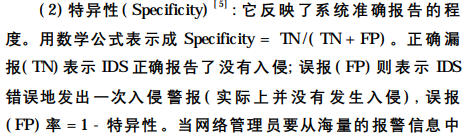


防火墙只是被动防御为主，通过防火墙的数据便不再进行任何操作，IDS则进行主动实时的检测，发现入侵行为即可做出反应，是对防火墙弱点的修补，但可能误报等；防火墙可以允许内部的一些主机被外部访问，IDS则没有这些功能，只是监视和分析用户和系统活动。

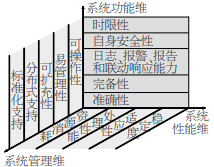


2、IDS评估标准



准确性：所有检测结果的正确率



系统功能维：反映IDS的攻击检测、报告、审计、报警 等能力。

系统性能维：主要是检验IDS 在不同环境下的承受强度，包括检测引擎的吞吐量、过滤的效率等指标

系统可管理维：主要评估系统用户界面的可用性、完整性、扩充性以及平台的兼容性。