**第二章 网络攻击行径分析**

1. **利用向目标主机发送非正常消息而导致目标主机崩溃的攻击方法有哪些**

PingOfDeath、IGMP Flood、Teardrop、UDP flood、SYN flood、Land、Smurf、Fraggle、畸形消息攻击、分布式拒绝服务攻击、目的地不可达攻击、电子邮件炸弹、对安全工具的拒绝服务攻击、拒绝服务攻击、网络远程拒绝服务攻击、本地拒绝服务攻击。

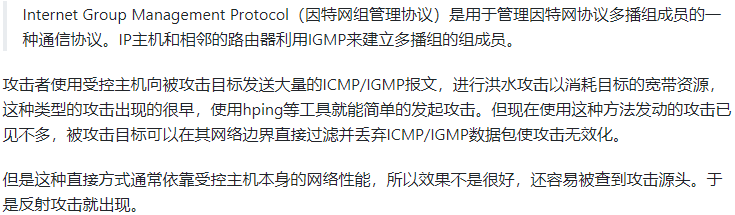
1. **简述破坏型攻击的原理及其常用手段** P9
2. **简述IP欺骗** P14
3. **叙述扫描的作用于并阐述常用的扫描方法** P12
4. **简要叙述攻击的一般过程及注意事项**

攻击的准备阶段、攻击的实施阶段、攻击的善后阶段。*注意*: ①确定攻击目的、准备攻击工具、收集目标信息; ②隐藏自己的位置、利用收集到的信息获取账号和密码，登陆主机、利用漏洞或者其他方法获得控制权并窃取网络资源和特权; ③清理痕迹如Web服务器的日志，事件日志等，可用以下方法:禁止日志审计、清除事件日记、清除IIS服务日记。

1. **为什么要进行攻击善后** P20 如果完成攻击后……留下的痕迹

**资料：**

1. **IGMP flood：**



**第三章 网络侦察技术**

1. **扫描有几种类型？简述它们的功能**

三种：地址扫描、端口扫描、漏洞扫描。功能：P30~35

（端口扫描：判断运行服务的方法就是通过端口扫描，因为常用的服务时使用标准的端口，只要找到相应的端口，就能知道目标主机上运行着什么服务）

1. **什么是网络监听**

是一种见识网络状态、数据流程以及网络上信息传输的管理工具，它可以将网络界面设定成监听模式，并且可以截获网络上锁传输的信息。(或P39)

1. **简述以太网的网络监听**
2. 共享以太网；②Sniffer；③交换式网络上的嗅探器 P40~45
3. **如何防范网络监听** P45~46

**资料：**

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：

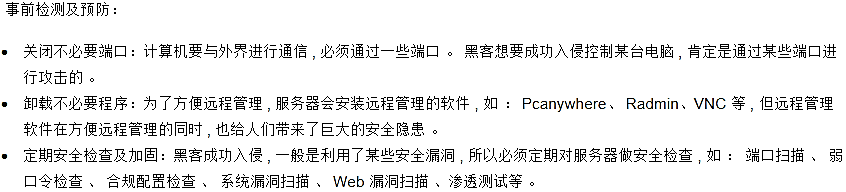
1最理想的防制方法是网络内的每台电脑ARP一律改用静态的方式，不过大型的网络是不可行，因为需要经常更新每台电脑的ARP表。

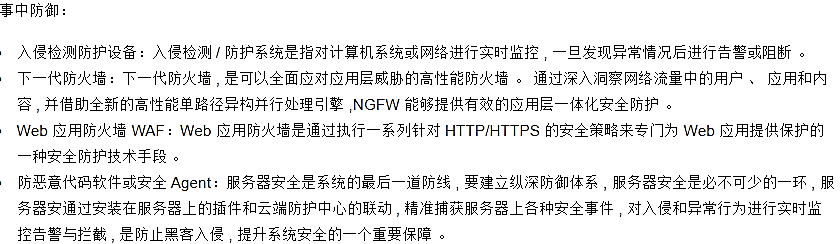
2 使用例如DHCP snooping，网络设备可借DHCP保留网络上各电脑的MAC地址，在伪造的ARP数据包发出时即可侦测到。

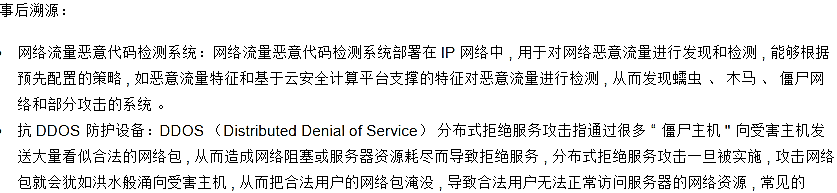
1. **僵尸主机多怎么办？**

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)







**第四章 拒绝服务攻击**

1. **外部用户针对网络连接发动拒绝服务攻击有哪几种模式？举例说明** P57
2. **如何对抗TearDrop攻击？**

TearDrop攻击原理P70。*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。

1. **如何发现自己正在受到消耗网络资源的DoS攻击？**

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。

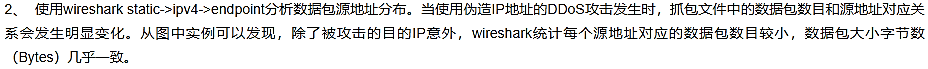
1. **对付分布式拒绝服务攻击的方法有哪些？举例说明** P76~77

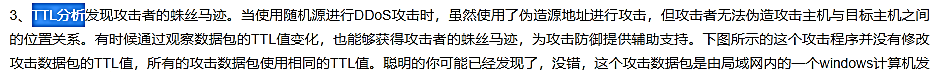
**资料：**

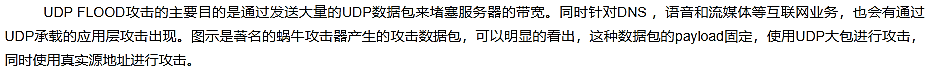
1. **怎么应对DDos攻击(属于黑客中的暴力犯罪)，利用数据包的哪些特征？**

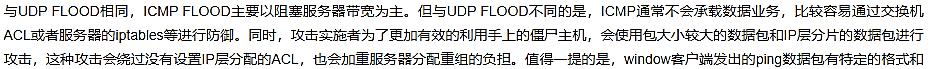
攻击发生时的cap文件(wireshark抓包)进行仔细的分析，找出攻击者忽略的地方，找出攻击数据包与正常业务流量中有区别的地方。

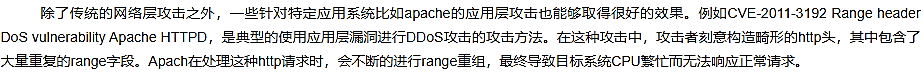












**第五章 缓冲区溢出攻击**

1. **什么程序会发生缓冲区溢出**

➢ 代码在操作缓冲区时，没有对缓冲区边界进行检查

➢ 使得写入缓冲区的数据量超过缓冲区能够容纳的范围，从而导致溢出的数据改写了与该缓冲区相邻存储单元的内容。

➢ C语言中许多字符串处理函数如：Strcpy、Strcat、Gets、Sprintf等都没有对数组越界加以检测和限制

1. **缓冲区溢出攻击的一般目标是什么**

（修改程序的返回地址，让它去执行一段精心准备的程序。）

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的控制权。如果该程序具有足够的权限，那么整个主机就被控制了。攻击者必须达到如下的两个目标：

①在程序的地址空间里安排适当的代码；②通过适当的初始化寄存器和内存，让程序跳转到入侵者安排的地址空间执行。

1. **要让程序跳转到安排好的地址空间执行，一般有哪些方法** P83

**第六章 程序攻击**

1. **逻辑炸弹与病毒有哪些相同点与不同点？**

共同点：1）都具有隐蔽性，用户一般不会察觉；2）具有攻击性，发作后会干扰屏幕显示，或降低电脑运行速度，或删除程序，或破坏数据。

不同点：1）病毒具有“传染性”，而逻辑炸弹是没有“传染性”的；2）逻辑炸弹的逻辑条件具有不可控制的意外性，逻辑炸弹本身虽然不具备传播性，但是诱因的传播是不可控的，由于逻辑炸弹还原和清除更加困难。

1. **为什么后来的木马制造者制造出反弹式木马，反弹式木马的工作原理是什么？画出反弹式木马的工作流程图** P134

为什么：随着……反弹式木马；原理：它利用……目的；流程图：图6-6

1. **嵌入式木马不同于主动型木马和反弹式木马的主要特点是什么？为什么这种木马更厉害，更不易被清除？** 主要特点P135、137

因为嵌入式木马隐藏于常用的网络程序中，不像另两者会建立新的Socket连接，所以杀毒软件难以发现、清除和隔离，多数情况只能手工清除。

1. **木马技术包括哪些，这些技术有什么特点？**

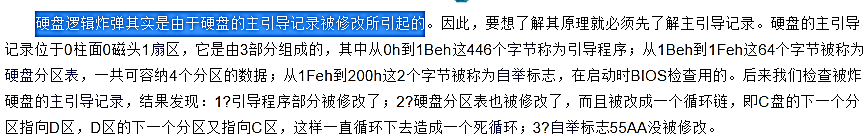
①自动启动技术，木马程序第一次运行需要用户来执行，以后会启动系统时候自动装在服务端程序。②隐藏技术，木马程序不同于普通程序的最大特定就是想尽一切办法隐藏自己。③远程监控技术，木马的最主要功能，也是木马的最终目的。 P140~144

**资料：**

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



**第七章 欺骗攻击**

1. **请简述DNS的工作原理，并指出在整个DNS解析过程中，可能存在的被欺骗攻击的地方**

工作原理P156（DNS实现……域名服务器）。

可能存在的被欺骗：在当提交给某个域名服务器的域名解析请求的数据包被捕获，然后按截获者的意图将一个虚假的IP地址作为应答信息返回给请求者。

1. **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**

（①直接用IP访问重要的服务，从而避开DNS欺骗攻击。②使用自定义的DNS服务器并刷新DNS解析缓存）

注意MAC地址和IP地址是否遭到了替换和修改。如果确认MAC地址为真，可打开路由器，通过相互对应的MAC查找IP地址，或将MAC地址添加到路由器的安全地址过滤功能当中进行处理并启用，这样有问题的电脑会自动断线。若安装了ARP防火墙，一般情况下能够防御大部分攻击，但如果在拥有防火墙的情况下遭到攻击，首先要做的是查出攻击来源，然后将主机系统重新设置并重启。

1. **Web欺骗攻击有哪些具体形式？请简述其原理。** P165~168
2. **TCP/IP是否存在考虑其安全的地方？哪些建议？**

TCP/IP的层次不同提供的安全性也不同，例如，在网络层提供虚拟私用网络，在传输层提供安全套接服务。

物理层安全问题是指由网络环境及物理特性产生的网络设施和线路安全性，致使网络系统出现安全风险，如设备问题、意外故障、信息探测与窃听等。

网络层的主要功能主要用于数据包的网络传输，其中IP协议是整个TCP/IP协议体系结构的重要基础。IPv4在设计之初根本没有考虑到网络安全问题，IP包本身不具有任何安全特性，从而导致在网络上传输的数据包很容易泄漏或受到攻击（如伪造IP包地址、拦截、窃取、篡改、重播等）。IPv6简化了IPv4中的IP头结构，并增加了对安全性的设计。

传输层主要包括传输控制协议TCP和用户数据报协议UDP,其安全措施主要取决于具体的协议.传输层的安全主要包括:传输与控制安全、数据交换与认证安全、数据保密性与完整性等。为了保证传输层的安全设计了安全套接层协议SSL，此协议提供了身份验证、完整性检验和保密性服务。

网络安全性问题主要重点解决的常用应用系统（协议），包括HTTP、FTP、SMTP、DNS、Telnet等。

*建议*：对物理层，由于以太网上存在交换设备并采用广播方式,可能在某个广播域中侦听、窃取并分析信息。为此，保护链路上的设施安全极为重要,物理层的安全措施相对较少，最好采用“隔离技术”将每两个网络保证在逻辑上能够连通，同时从物理上隔断，并加强实体安全管理与维护；对应用层，应注意不下载未经过检验的程序，SMTP服务器应增加过滤、扫描及设置拒绝指定邮件等功能，可采用防火墙保护DNS服务器并阻止各种区域传输。

1. **假如你负责开发、维护和管理某商业网站，面对潜在的Web欺骗攻击，你将采取哪些手段避免你的网站受到攻击？** P168

**资料：**

1. **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

1. **TCP会话劫持 监听者如何猜测序列号**

书P170

**第八章 漏洞攻击/利用处理程序错误**

**1. 跳板的作用是什么？**

跳板的作用是进行攻击源的隐藏。为了更好地隐蔽自己，一些网络攻击者通常并不直接从自己的系统向目标发动攻击，而是先攻破若干中间系统,让它们成为“跳板”，再通过这些“跳板系统”完成攻击行动。

1. **如何避免多个服务系统之间的连带关系？**
2. **简述用ASP编写的网站的常见攻击方式有哪些？** P200~206

**第九章 访问控制技术**

**1. 什么是自主访问控制？方法有哪些？** P218/P219

1. **为什么自主访问控制无法抵御特洛伊木马攻击？** P221
2. **口令认证技术的认证方法。哪些方法可提高口令认证技术安全性？**P209

口令认证也成通行字认证，是一种根据已知事物验证身份的方法。需要考虑和规定选择方法，使用期限，字符长度，分配和管理及在计算机系统内的保护等。

提高安全性：每个用户需分配有专用的同行字，系统可知道哪些用户在联机、采用随时间变化的通行字、采用通行短语代替通行字、在通行字后填充随机数。

1. **网络的物理隔离技术包含哪几方面？各自采用了什么样的技术？** P212
2. **什么是基于角色的访问控制技术？它与传统的访问控制技术有何不同？**

*什么是*：（P226）。*不同*：和DAC、MAC相比，优点在于：它是一种策略无关的访问控制技术，具有自管理的能力，使得安全管理更贴近应用领域的机构或组织的实际情况。缺点在于：技术不够成熟、较复杂、RBAC的策略无关性需要用户自己定义适合本领域的安全策略。（P228）

**资料：**

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。

1. **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。

1. **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

**第十章 防火墙技术**

1. **防火墙体系结构**

（经典）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、（扩展）合并内部和外部路由器、合并堡垒主机和外部路由器、多台内/外部路由器、多个周边网络（见PPT）

1. **使用应用层代理访问外部Web站点时，会出现访问某些经典网站的响应速度较快，而其他站点响应速度较慢，原因何在？**

因为代理有缓存功能。会把常用的网站页面缓存下来,所以速度快。不常用的网页要远程读取,所以慢些。

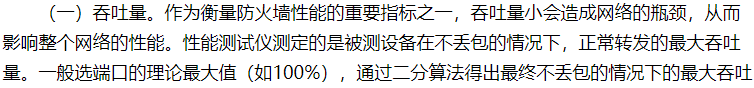
1. **若防火墙允许周边网络上的主机访问内部网络上的任何基于TCP协议的服务，而禁止外部网络访问周边网络上的任何基于TCP的服务，给出实现思路？**

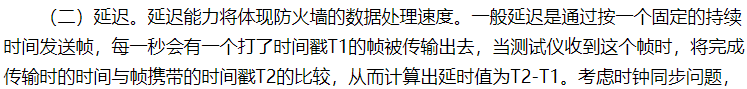
P284~285，图10-27，编辑规则然后防火墙按要求对数据包进行过滤。

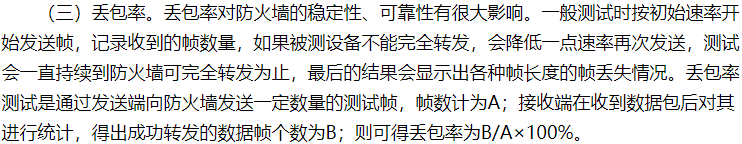
**资料：**

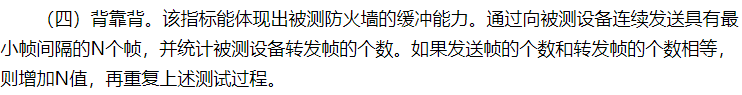
1. **防火墙指标 内网控制 稳定性 工作原理**

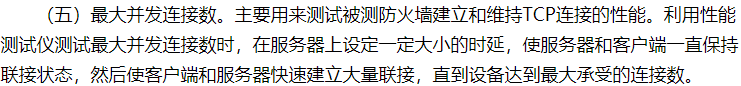
防火墙性能衡量：

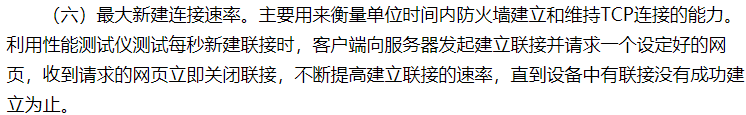










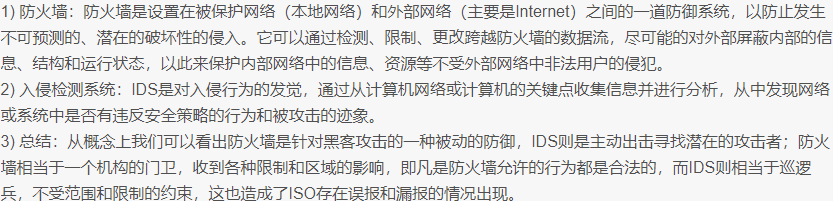


**第十一章 入侵检测技术**

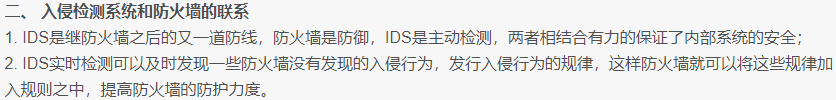
1. **某用户平均每天登录3次，但是某日突然登录30次** 异常检测
2. **运行程序后不测试超级用户密码，绑定端口....** 模式匹配

**资料：**

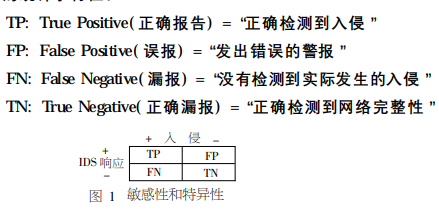
1. **和防火墙不同？**

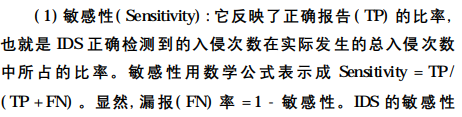
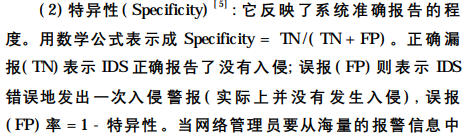


防火墙只是被动防御为主，通过防火墙的数据便不再进行任何操作，IDS则进行主动实时的检测，发现入侵行为即可做出反应，是对防火墙弱点的修补，但可能误报等；防火墙可以允许内部的一些主机被外部访问，IDS则没有这些功能，只是监视和分析用户和系统活动。

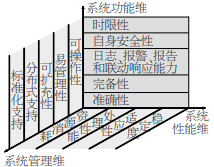


1. **IDS评估标准**



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。

**第十二章 VPN**

1. 简述IPSec中AH协议的功能

AH协议包头可以保证信息源的可靠性和数据的完整性.

2. 简述IPSec中ESP协议的功能

ESP可以提供数据的完整性和可靠性.

3. 比较PPTP与L2TP

