教学课题：计算机网络安全体系

教学目的要求：1、明确网络威胁的来源。

2、掌握病毒及黑客的特点及入侵方式。

3、掌握保证网络安全的措施

4、掌握防火墙技术的分类及特点

教学重点：1、计算机病毒的特点及防治

2、黑客入侵的方式及预防

3、防火墙技术

课时：2 课时

教学过程：

计算机网络安全体系

一、计算机病毒

1、计算机病毒的实质：是一段程序代码

2、计算机病毒主要破坏：程序和数据，一般不破坏硬件，（但也有特殊，如 CIH 病毒破坏 BIOS，造成黑屏，号称是第一个破坏硬件的病毒，但实质也是程序，是 ROM 里的程序，不好修）

3、计算机病毒的特征：

1）寄生性（一般不单独存在，寄生在别的程序中，寄主程序运行，则病毒运行）。

2）传染性（传染的很快）。

3）破坏性（一般都具有破坏性）。

4）潜伏性（一开始只传染不发作，只有这样才能传播的更多）。

5）隐蔽性（不易被发现，发现了就不能传播了）。

6）可触发性（条件满足才发作，如黑色星期五病毒）。

4、病毒的产生：都是人有意编写的。

5、病毒会不会变异：会，病毒会有变种，可能是传播中变的，大多还是病毒作者或其他好事的人为了逃避杀毒软件的查杀或为使之破坏能力更强而有意修改的。

6、病毒的传播途径：

1）网络。如不安全的网站，来历不明的电子邮件（附件带毒），有时正规网站也会被人利用而带毒，但毕竟那是极少情况。

2）移动存储介质。如软盘、U 盘、或带毒的光盘（有的盗版游戏光盘中含有病毒）。

7、计算机病毒的分类：

A）依病毒存在的媒体：

（1）文件型病毒（COM、EXE、DOC 文件）

（2）引导型病毒（BOOT，MBR）

（3）混合型。

B）依病毒传染方法：驻留型病毒（感染后驻留在内存）和非驻留型病毒。

C）依病毒的破坏性：良性病毒和恶性病毒。

D）依病毒的链接方式（如何链接在所感染的文件中）：

（1）源码病毒（攻击高级语言的源程序文件，在源程序编译前插入到源程序中，经编译后成为合法程序的一部分）

（2）嵌入型病毒（代码嵌入到现在程序中，难编写，难消除）

（3）外壳型病毒（将自身包围在主程序的四周<首尾>，对原程序不作修改，最常见，易于编写、易于发现，一般测试文件大小即可发现，其实上面两种也比原文件要长）

（4）操作系统病毒（取代操作系统的部分模块进行破坏活动，一般的引导型病毒都是这种）

8、计算机病毒的表现：慢、无故死机、磁盘空间迅速减少、日期时间发生改变、不能启动等。

9、防治：

以预防为主，综合采用多种方法

（1）安装杀毒软件，并及时升级（瑞星、江民、金山、360、卡巴期基、诺顿等，杀毒软件是在病毒出来以后，能过升级病毒库才能新病毒具有查杀能力，故杀毒软件也不能杀灭所有的病毒）

（2）安装防火墙，及时打上系统补丁。

（3）不打开来历不明的邮件。

（4）作好重要资料的备份，最好放在别的电脑，或移动存储器上，也可制成光盘。

（5）不随便点击不安全的陌生网站

（6）升级应用软件到最新版本。

（7）使用移动存储设备要及时杀毒。

（8）安装病毒防护卡（一般是阻止病毒的入侵，现在不常用，不管事，因为病很多，升级的很快，硬件不能及时升级。）

10、恶意病毒“四大家族”

（1）宏病毒（破坏 DOC 文件）

（2）CIH 病毒（这是第一个破坏硬件的病毒，破坏 BIOS 数据，黑屏不能启动）

（3）蠕虫病毒（象虫子一样，大量繁殖自己）

（4）木马病毒（一般通过电子邮件传染，或捆绑在其他程序中，进入你的电脑后，随开机启动，大量发送电脑中有用的信息到特定的网站，往往在你的电脑中开一个后门，以便于放入木马的人对你的电脑进行远程控制）

11、病毒是不是一般会使文件变长（对）

12、文件加密能不能防病毒，能

13、采用多种方法能不能特底防毒，不受任何病毒的侵染（不能）

14、磁盘染毒最彻底的杀毒方法：格式化磁盘，但不提倡，因为什么都没有了。

二、黑客

（一）黑客与入侵者

严格意义上来说，黑客和入侵者是有区别的。

一般来说，黑客的行为没有恶意，他们是计算机狂的代名词，他们的水平都很高，热衷于研究计算机的各种奥秘，善于发出系统中的漏洞，并分享他们的发现，并没有恶意破坏数据。

入侵者和行为是有恶意的，他们利用获得的非法访问权，破坏数据。入侵者的水平可能很高，也可能只是一个初学者。

而现实网络世界里，根本也分不清谁是真正意义上的黑客，谁是真正意义上的入侵者，所以现在黑客的概念发生了变化。

黑客：所谓黑客就是利用系统安全漏洞，对网络上的电脑进行攻击破坏或窃取资料的人，也就是未经授权远程登录到别人计算机上的人。（QQ 远程协助，是授权了，不是黑客）。

（二）黑客攻击的目的：

1、窃取信息。这是最直接的目的。

2、获取口令。获取口令的目的，还是窃取更重要的信息。

3、控制中间站点。利用中间站点，攻击其它主机，黑客可以隐藏自己。

4、获得超级用户权限。获得超级用户权限后，可以在系统中埋伏后门，为以后出入提供方便；还可以修改系统配置，为所欲为（成为黑客的肉鸡）。

（三）黑客攻击的三个阶段：

（1）确定目标。或者是某个自己感兴趣的站点，也或者是具有敌对观点的宣传站点，等等。

（2）搜集与攻击目标相关的信息，并找出系统的安全漏洞。搜集信息的目的是进行攻击，只有找到系统或某些软件的安全漏洞和安全弱点，才能攻击。这里好多系统或软件漏洞并不是什么秘密，并且相关网站也提供了漏洞修复补丁，只是用户并不一定及时修复这些补丁，使黑客有了可乘之机，所以我们平时应养成及时修复系统及软件补丁的习惯。

（3）实施攻击。黑客攻击成功后，在被攻击的系统上植入木马，即黑客自己在目标系统上安装的一些后门程序及探测软件，后门程序是为了黑客出入方便，探测软件用来窥探所在系统的活动，收集黑客感兴趣的一切信息，如 QQ 帐号密码，支付宝帐号密码，甚至银行的帐号密码等等。黑客攻击目标电脑后，最初只是窃取目标电脑中的信息，如果获取了一系列口令，那么被攻击对像的损失就大了。如果黑客再获取了目标电脑的超级用户权限，那就可以为所欲为了，目标电脑也就沦为肉鸡了，损失惨重不说，还可以利用目标电脑，再攻击其他系统，栽赃陷害目标电脑，而隐藏自己。

（四）黑客攻击的手段。

（1）使用扫描软件。扫描目标电脑的漏洞，寻找可乘之机。

（2）使用工具软件，利用目标电脑的漏洞，植入木马程序和探测软件，木马程序再

在系统中设置大大小小的漏洞，为自己大开方便之后门。

（3）使用监听程序。利用监听程序窃取各种口令。

三、防火墙技术（保证网络安全的措施之一，用于保护内网）

（一）防火墙简介

防火墙（Firewall）是一种保障信息安全的设备或软件，它依照特定的规则，允许或是禁止传输的数据通过。防火墙可以是一台专门的硬件，也可以是运行在硬件上的软件。

防火墙安装在内网和外网之间，目的是实施访控制策略，以允许或阻止外网的访问。防火墙的功能有两个：一是允许，另一个是阻止。

通常意义上的防火墙是指硬件防火墙，价格较贵，效果也好。软件防火墙是通过软件的方式来达到，价格便宜，效果也差些。目前路由器中也有防火墙的部分功能，功能不是很大。

（一）防火墙的功能

1、保护那些易受攻击的服务。防火墙可以过滤那些不安全的服务，只有预先被允许的服务才能通过防火墙，这样降低了受到非法攻击的风险。

2、控制对特殊站点的访问。有些关键站点可以设置为不允许外网访问。如通常情况下，内网中只有 main 服务器（电子邮件服务器）、FTP 服务器和 WWW 服务器允许外网访问，而其它服务器而在防火墙中设置为禁止访问。

3、对网络访问进行记录和统计。当发生可疑操作时，防火墙能够报警并提供详细记录，以便用户追踪攻击源。

（三）防火墙的类型：

防火墙大致可划分为包过滤防火墙、应用网关防火墙、状态监视防火墙、复合型防火墙。代理服务器技术（应用网关防火墙）是防火墙技术中最受推崇的一种安全技术。

1、包过滤防火墙（工作在网络层）

包过滤防火墙是最简单的防火墙。检查数据流中每个数据包的源地址、目的地址、通信的 TCP 端口号和 TCP 链路状态等要素，依据一组预定义的规则，允许的通过，不允许的丢弃。如看到可疑 IP 地址的数据包丢弃。

优点是价格便宜，对用户透明，速度快，对网络性能影响很小，缺点是配置起来比较复杂，对 IP 欺骗式攻击比较敏感（无效）。这种防火墙没有用户的使用记录。

2、应用网关防火墙（也称代理服务器防火墙）（工作在应用层）

前面我们讲过代理服务器，代理服务器介于内网和外网之间，内网有访问外网的请求，首先把请求发给代理服务器，代理服务器替我们访问外网，然后再把访问得到的信息传给内网。代理服务器有防火墙的作用。在这里代理服务器将防火墙功能进一步强化，而其它功能有所弱化，而形成一种防火墙技术，即称为代理防火墙技术，也称应用网关防火墙。代理服务器技术（应用网关防火墙）是防火墙技术中最受推崇的一种安全技术。

应用网关防火墙会像一堵墙那样挡在内部网络和外部网络之间。当应用网关接收到内网用户的上网请求后，会检查用户请求的站点是否允许访问，如果允许，应用网关就会去那个站点取回所需信息再转发给客户。从外部只能看到应用网关而看不到任何内部资源，如用户的 IP 地址，故可以保护内网。

应用网关防火墙优点是：可以将被保护的网络内部结构屏蔽起来，增强网络的安全性，防止攻击内网；也可以实施较强的数据流监控、过滤、记录和报告等。缺点是，访问速度变慢（解释：代理服务器防火墙，主要目的是防火墙功能，故不再有较大的 chace，不仅中转需要时间，同时每一种特定的 internet 服务都需要安装相应的应用网关软件，如果尚未安装，安装软件也需要时间），应用网关防火墙不能支持所有的 internet 访问类型。

3、状态监视防火墙（工作在数据链路层和网络层之间）

就是在防火墙上运行一个实现网络安全策略的软件引擎，称之为检测模块。状态监视防火墙优于前两种防火技术，比前两种应用范围还要广。缺点是配置非常复杂；会降低网络速度。

4、复合型防火墙

复合型防火墙集防火墙、入侵检测、安全评估、虚拟专用网 4 大功能模块于一体，以防火墙功能为基础平台，以其它的安全模块为多层次应用环境，构筑一套完整的、立体的网络安全解决方案。

防火墙的弱点和不足：

1、防火墙不能防范不经过防火墙的攻击；2、防火墙不能防止来自网络内部的攻击和安全问题；3、防火墙不能防止安全策略配置不当或者错误所引起的威胁；4、防火墙不能防病毒（并不检查数据包内容）；5、防火墙本身也会有安全漏洞。

Windows 防火墙是在 windows 操作系统中系统自带的软件防火墙。

四、例题分析：

1、网络上的计算机为了防御黑客或网络病毒的入侵，应该（）

A. 使用网络防火墙

B. 使用病毒防火墙

C. 安装最新的操作系统漏洞补丁

D. 以上全是

标准答案:d

解析:这里不仅防御黑客，还要防御病毒。所以即使用网络防火墙（主要防黑客），还需要使用病毒防火墙（主要防病毒），另外安装最新的操作系统漏洞补丁、安装各种应用软件补丁也可以防黑客和病毒。

2. 以下哪一项不是预防计算机病毒的措施？ （ ）

A). 专机专用 B). 不上网 C). 建立备份 D). 定期检查

标准答案:b

解析：

建立备份，一旦发中毒，可以恢复备份，减少损失。

专机专用，没有交叉感染，可以减少中毒机会

定期检查，及早发现清除减少损失。

不上网那叫因噎废食，怕中毒，就不上网了，干脆别用电脑了。

3. 在桌面办公系统中，什么类型的软件能够阻止外部主机对本地计算机的端口扫描

（）

A). 个人防火墙　　B). 反病毒软件

C). 基于 TCP/IP 的检查工具　　D). 加密软件

标准答案:a

解析:防火墙是一种特殊编程的路由器，安装在内网和外网之间，目的是实施访控制策略，以允许或阻止外网的访问。

4. 防火墙应该能够确保满足的功能中，不包括以下()。

A). 实现安全策略　　B). 创建检查点

C). 记录 Internet 活动　　D). 保护外部网络

标准答案:d

解析:防火墙保护内网不受外网的攻击，是单向的。是保护自己的，不是保护别人的。

5. 网上“黑客”是指(　　)的人。

A). 总在晚上上网　　B). 匿名上网

C). 在网上私闯他人计算机系统并进行攻击、破坏。　　D). 不花钱上网

标准答案:c

6. 用浏览器浏览台湾的某个中文网站，出现许多乱码，但图片能显示正常，原因是（）

A). 浏览器被该网站破坏了　　B). 浏览器的汉字编码设置不对

C). 网络协议不同　　D). 该网站被黑客破坏了

标准答案:b

7. 下列行为不属于黑客行为的是

A). 利用现成的软件后门，获取网络管理员的密码

B). 非法进入证券交易系统，修改用户口令。

C). 进入自己的计算机，并修改数据

D). 利用电子窃听技术，获取要害部门的口令

标准答案:c

解析:

8. 为使发送方不能否认自己发出的签名消息，应该使用（ ）技术

A). 数据加密　　B). 防火墙　　C). 链路加密　　D). 数字签名

标准答案:d

9、防火墙是指隔离在本地网络与外界网络之间的一道防御系统

正确

错误

标准答案:a