第一部分　计算机网络安全基础

第 1 章　计算机网络安全概述

2017 年 5 月，名为“永恒之蓝”的勒索病毒席卷全球。据 360 威胁情报中心监测，我国至少有 29372 个机构遭到这一源自美国国家安全局网络武器库的蠕虫病毒攻击，保守估计超过 30 万台终端和服务器受到感染，覆盖了全国几乎所有地区。勒索病毒不但破坏了很多高价值数据，而且直接导致很多公共服务、重要业务、基础设施无法正常开展，多个国家的高校、加油站、火车站、自助终端、邮政、医院、出入境签证、交通管理等机构陷入瘫痪。该事件是“冲击波”病毒发生以来，14 年一遇的严重网络安全攻击事件，其传播速度之快，后果之严重，防范之难，均为历史罕见。

2017 年 9 月 12 日，中国互联网安全大会（ISC2017）在北京国家会议中心召开。自 2013 年起，中国互联网安全大会已连续举办了 5 届，成为业内规格高、规模大、影响力强的安全盛会。5 年来，大会持续围绕网络安全这一核心议题，就网络安全最新理念与技术进行探讨和交流。在今年的 ISC 大会中更是明确提出了“大安全”这一概念，重新定义了传统意义上的网络安全。

在 ISC 大会主旨演讲环节，中国互联网安全领域领军人物、360 集团董事长兼 CEO 周鸿祎强调：“全球网络安全已经进入大安全时代。网络安全不再仅仅局限于网络本身的安全，更是国家安全、社会安全、基础设施安全、城市安全、人身安全等更广泛意义上的安全。”

一切皆可编程，万物均要互联。在大安全时代，网络安全产业、网络安全形势、网络安全战略都在发生着巨大的改变。事实上，今天互联网跟整个社会已经融为一体，网络世界和现实世界已经深度连接，线上线下的边界已经消失。网络空间的任何安全问题，都会直接映射到现实世界的安全，会深刻影响到社会正常稳定的运转。

1.1　网络安全简介

随着时代的发展，社会的进步，我们的日常生活越来越离不开网络。不论是家庭娱乐，或者是政府办公，都与网络紧密相关。但是，随着网络不断融入我们的生活，网络所带来的威胁也日益严重。我们的私人资料可能随时被窃取，公司的资料也可能随时被窃取，国家的政府网络可能会被恶意攻击者入侵，导致网络瘫痪，对国家、企业、个人造成不可挽回的损失。安全是一个不容忽视的问题，当人们在享受网络带来的方便与快捷的同时，也要时时面对网络开放带来的数据安全方面的新挑战和新危险。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应

用数学、数论、信息论等多种学科的综合性学科，如图 1-1 所示。

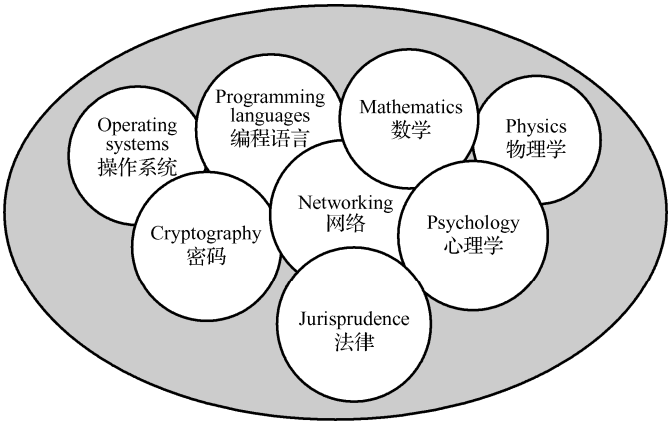

图 1-1　网络安全涉及的范围

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全由于不同的环境和应用而产生了不同的类型，主要有以下几种。

（1）系统安全：是指运行系统安全，即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的消息造成破坏和损失；避免由于电磁泄漏，产生信息泄露，干扰他人或受他人干扰。

（2）网络安全：是指网络上系统信息的安全，包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，计算机病毒防治，数据加密等。

（3）信息传播安全：是指网络上信息传播安全，即信息传播后果的安全，包括信息过滤等。它侧重于防止和控制由非法、有害的信息进行传播所产生的后果，避免公用网络上大量数据自由传播导致的信息失控。

（4）信息内容安全：是指网络上信息内容的安全。它侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，其本质是保护用户的利益和隐私。

1.1.1　网络不安全因素存在的原因

导致网络不安全的因素来自两个方面：一方面是人为因素和自然灾害因素；另一方面是网络体系结构本身存在的安全缺陷。

网络系统是以计算机语言编码和支持软件共同组成的，其设计中的逻辑失误、偏差和缺陷都无法彻底避免。软件威胁可以说是目前网络不安全因素最显著的方面，其中尤以计算机病毒最为普遍。遭到病毒入侵时，计算机操作系统会运行减缓，性能不稳，严重时甚至整个硬件系统崩溃，这是当前世界性的网络安全难题。其他的木马软件、缺少安全措施的联网软件等问题，也可能会导致个人数据遭到大范围的暴露和流失。

人为原因给网络安全带来威胁的有 3 个方面：一是纵横网络的黑客，以编写计算机病毒、

制造网络攻击、侵入局域网系统或网站后台为业，其技术水平往往与网络科技更新同步，甚至超前，是当今世界网络威胁的最大制造者；二是网络维护人员业务能力的不足，管理混乱，甚至有些操作人员利用职权之便窃取用户信息，盗用网络资源；三是计算机或网络用户缺乏网络安全防范意识，保密观念不强，对网络安全风险疏于防范，导致系统遭受攻击，数据被盗。

1.1.2 网络安全事件

1．惊曝淘宝 9900 万账户信息遭窃

2016 年 2 月 1 日，浙江嘉兴平湖警方破获的一起网络黑产案件中，犯罪团伙利用互联网上非法流传的非淘宝用户账号和密码对淘宝账号进行“撞库”匹配，用于抢单等灰黑产行为，涉案金额高达 200 余万元人民币。该团伙于 2015 年 10 月 14 日至 16 日通过租用阿里云服务器进行“撞库”。犯罪团伙利用手中已有的非淘宝账号对淘宝网进行了 9900 多万次比对，匹配后发现有 2059 万账户真实存在。2059 万个账号中，黑产比对后曾尝试利用其他平台密码登录（俗称“撞库”），但绝大多数登录行为遭到淘宝网的拦截，因而未遂。

“撞库”是互联网较常见的黑色行为，以大量的用户数据为基础，利用用户相同的注册习惯（相同的用户名和密码），尝试登陆其他的网站。被“撞库”网站和用户都是黑产行为的受害者，用户在 A 网站被盗的账户密码被用来登陆 B 网站，因为很多用户在不同网站使用的是相同的账号密码，因此可以起到获取用户在 B 网站的用户账户，从而达到目的。因此，一旦某个网站用户数据库泄露，将导致该用户在多个网站的资产受损。

2．OpenSSL 水牢漏洞

2016 年 3 月，全球有 2/3 的网站服务器使用开源的加密工具 OpenSSL，其被曝出新的安全漏洞——“水牢漏洞”，这一漏洞允许黑客攻击网站，并读取密码、信用卡账号、商业机密和金融数据等加密信息，对全球网站产生巨大的安全考验。我国有十万余家网站受到影响。

“水牢漏洞”可以允许攻击者破坏使用 SSLv2 协议进行加密的 HTTPS 网站，读取经加密传输的敏感信息，包括密码、信用卡账号、商业机密、金融数据等。利用“水牢漏洞”难度较高，需要攻击者截获经 HTTPS 加密的通信数据，并破解此数据应送达的服务器的密钥，才可让攻击者对所截获的数据进行解密。破解密钥需要使用一定性能的计算集群，并花费 8 个小时。租用计算集群的成本约 400 美金左右（以租用亚马逊集群的费用为准）。但一旦攻击成功，攻击者就可以破解其截获的所有加密数据。

3．国内部分网站存在 Ramnit 恶意代码攻击

2016 年 4 月，CNCERT 监测发现，一个名为 Ramnit 的网页恶意代码被挂载在境内近 600 个党政机关、企事业单位网站上，一旦用户访问网站就有可能受到挂马攻击，对网站访问用户的 PC 主机构成安全威胁。Ramnit 恶意代码是一个典型的 VBScript 蠕虫病毒，可通过网页挂马的方式进行传播，当用户浏览含有 Ramnit 恶意代码的 HTML 页面时，单击加载 ActiveX 控件，用户主机就很有可能受到恶意代码的感染。

Ramnit 恶意代码主要在用户% TEMP %文件夹中植入了一个名为“svchost.exe”的二进制文件并执行关联的 ActiveX 控件，受感染的用户主机会试图连接到与 Ramnit 相关的一个木

马控制服务器——http://fget-career.com。 根据 CNCERT 监测情况分析，Chrome 和 Firefox 浏览器用户不会受到此恶意代码的影响，而较高版本的 IE 浏览器也会对此类 ActiveX 控件进行告警提示而不是自动执行。所以，受影响的主要是较低版本的 IE 浏览器。IE 浏览器用户在访问互联网站时做好 IE 安全设置（建议设置为中、高安全级别），禁止执行不明来源的 ActiveX 控件。

4．2.7 亿 Gmail、雅虎和 Hotmail 账号遭泄露

2016 年 5 月，俄罗斯黑客成功地组织了一场大规模的网络攻击。在此次网络攻击中，黑客盗取了 2.723 亿个账号，以俄罗斯最受欢迎的电子邮件服务 Mail.ru 用户为主，此外还有 Gmail 地址、雅虎及微软电邮 Hotmail 用户。路透社称，数以亿计的数据目前正在“俄罗斯的地下黑市”出售。

5．全美互联网瘫痪

2016 年 10 月 21 日，黑客挟持成千上万物联网设备对美国 DNS 服务商 Dyn 发动了 3 波流量攻击，使得 Dyn 多个数据中心服务器受到影响，导致美国大部分网站都出现无法访问情况，包括亚马逊、Etsy、GitHub、Shopify、Twitter 、Netflix、Airbnb 等热门网站，此次的 DDoS 攻击让很多人觉得整个互联网都陷入了瘫痪。

Dyn 是美国主要域名服务器（DNS）供应商。域名是网友访问互联网的起点和入口，也是全球互联网通信的基础。而 DNS 作为承载全球亿万域名正常使用的系统，则是互联网重要的基础设施。造成本次大规模网络瘫痪的原因是 Dyn 公司的服务器遭到了 DDoS 攻击。DDoS 攻击又称拒绝服务攻击。最基本的 DDoS 就是黑客利用合理的服务请求去占用尽可能多的服务资源，从而使得用户无法得到服务响应。

随着万物互联，也即所谓的物联网必将引发大量网络安全问题，这场攻击只是未来安全问题的一个缩影。目前，互联网感染僵尸木马的 iot 设备约在 60 万左右，这些设备如果一起攻击，可以轻松发起接近 1T（相当于中国一个省流量）的攻击。

6．5 家俄罗斯银行遭遇 DDoS 攻击

2016 年 11 月 10 日，俄罗斯 5 家主流大型银行遭遇长达两天的 DDoS 攻击。来自 30 个国家 2.4 万台计算机构成的僵尸网络持续不间断发动强大的 DDoS 攻击。卡巴斯基实验室提供的分析表明，超过 50%的僵尸网络位于以色列、台湾地区、印度和美国。每波攻击持续至少一个小时，最长的不间断持续超过 12 个小时。攻击的强度达到每秒发送 66 万次请求。

DDoS 攻击已成为互联网安全面临的最严峻的威胁，自 2015 年，以 P2P、比特币为代表的互联网金融最火，同时也成为 DDoS 攻击的重灾区，许多公司更是前脚刚刚发布融资成功的新闻，后脚就被黑客攻击得无法登录，而 2016 年，无论是国外还是国内，DDoS 攻击向着各个不同行业蔓延。今天，DDoS 攻击已转化为一个完善的产业链，从攻击肉鸡的贩卖，到发动敲诈勒索，甚至是雇凶攻击，这背后都是利益的驱动。

7．希拉里邮件门影响美国大选

2016 年 11 月，希拉里因“邮件门”最终落败美国总统竞选。希拉里在 2009 年至 2013 年担任国务卿的 4 年里，使用个人电子邮件账户来处理政府事务，违反了“政府官员之间的通信应作为机构档案加以保留”的联邦政府规定。希拉里被美国联邦调查局（FBI）调查，

民众支持率节节下降。

8．电信诈骗导致高中生徐玉玉身亡

2016 年高考，徐玉玉以 568 分的成绩被南京邮电大学录取。2016 年 7 月 19 日下午 4 点 30 分左右，她接到了一通陌生电话，对方声称有一笔 2600 元人民币助学金要发放给她。在这通陌生电话之前，徐玉玉曾接到过教育部门发放助学金的通知。“18 日，女儿接到了教育部门的电话，让她办理了助学金的相关手续，说钱过几天就能发下来。”徐玉玉的母亲李自云告诉记者，由于前一天接到的教育部门电话是真的，所以当时他们并没有怀疑这个电话的真伪。按照对方要求，徐玉玉将准备交学费的 9900 元人民币打入了骗子提供的账号……发现被骗后，徐玉玉万分难过，当晚就和家人去派出所报了案。在回家的路上，徐玉玉突然晕厥，不省人事，虽经医院全力抢救，但仍没能挽回她 18 岁的生命。

9．Wanna Cry 勒索病毒席卷全球

2017 年 5 月 12 日晚，一款名为 Wanna Cry 的蠕虫勒索软件袭击全球网络，这被认为是迄今为止最巨大的勒索交费活动，影响到近百个国家上千家企业及公共组织。之所以能产生如此大的影响力，还得“归功于”NSA 泄漏的 0 day 黑客工具的加持。在该事件爆发不久后，美国国会便提出了一项法案，以阻止政府存储网络武器的行为。

10．雅虎 30 亿用户数据被盗

2013 年，雅虎遭到了黑客的攻击，盗走了用户的电子邮件地址、密码、生日、电话号码等大量信息。2016 年，雅虎披露称，在那次黑客袭击当中，他们旗下的 30 亿个账户中有超过 10 亿个账户的信息被泄露出去。在 2017 年 10 月 5 日，雅虎宣布，在 2013 年的那次数据泄漏事件当中，所有 30 亿雅虎用户的个人信息被泄露。

1.1.3　网络安全的基本要求

网络安全的 5 个属性为：可用性、可靠性、完整性、保密性和不可抵赖性。

1．可用性（Availability）

得到授权的实体在需要时可访问资源和服务。可用性是指无论何时，只要用户需要，信息系统必须是可用的，也就是说信息系统不能拒绝服务。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的（话音、数据、文字和图像等），有时还要求时效性。网络必须随时满足用户通信的要求。攻击者通常采用占用资源的手段阻碍授权者的工作。可以使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害（战争、地震等）造成的系统失效。

2．可靠性（Reliability）

可靠性是指系统在规定条件下和规定时间内完成规定功能的概率。可靠性是网络安全最基本的要求之一，网络不可靠，事故不断，也就谈不上网络的安全。目前，对于网络可靠性的研究基本上偏重于硬件可靠性方面。研制高可靠性元器件设备，采取合理的冗余备份措施仍是最基本的可靠性对策，然而有许多故障和事故都与软件可靠性、人员可靠性和环境可靠性有关。

3．完整性（Integrity）

完整性是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被篡改，即信息的内容不能被未授权的第三方修改，信息在存储或传输时不被修改、破坏，不出现信息包的丢失、乱序等。

4．保密性（Confidentiality）

保密性是指确保信息不暴露给未授权的实体或进程，即信息的内容不会被未授权的第三方所知。这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，个人的秘密和个人私密（如浏览习惯、购物习惯）。防止信息失窃和泄露的保障技术称为保密技术。

5．不可抵赖性（Non-Repudiation）

不可抵赖性又称不可否认性。不可抵赖性是面向通信双方（人、实体或进程）信息真实同一的安全要求，它包括收、发双方均不可抵赖。一是源发证明，它提供给信息接收者以证据，这将使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞；二是交付证明，它提供给信息发送者以证明，这将使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

1.2 黑客与攻击方法

1.2.1 黑客概述

黑客是“Hacker”的音译，源于动词 Hack，其引申意义是指“干了一件非常漂亮的事”。这里说的黑客是指那些精于某方面技术的人，对于计算机而言，黑客就是精通程序设计、网络、系统及软硬件技术的人。

白帽子描述的是正面的黑客，网络安全的守卫者。他可以识别计算机系统或网络系统中的安全漏洞，但并不会恶意去利用，而是公布其漏洞。这样，系统将可以在被其他人（如黑帽子）利用之前进行修补漏洞；白帽子发现和报告安全问题，企业修复并披露安全问题，用户了解信息安全，从而对企业提出信息安全要求。

世界著名黑客有：

- Kevin Mitnick

Mitnick 也许就是黑客的代名词。美国司法部仍然指责他为“美国历史上头号计算机犯罪通缉犯”。他的所作所为被记录在两部好莱坞电影当中：《Takedown》和《Freedom Downtime》。Mitnick“事业”的起点是成功破解了洛杉矶公交车打卡系统，并因此可以免费乘坐。然后和苹果的 Steve Wozniak 一样，Mitnick 开始尝试盗打电话。Mitnick 第一次被判有罪，是因为进入数码设备公司的计算机网络并且窃取软件。 稍后 Mitnick 开始了两年半的黑客行为，他声称自己侵入计算机、穿行于电话网络、窃取公司的秘密，并且进入了国防部的预警系统。他的落马源于其入侵计算机专家和黑客 Tsutomu Shimomura 的家用计算机。在 5 年 8 个月的监禁之后，Mitnick 现在的身份是一个计算机安全专家、顾问。

➢ Adrian Lamo

Lamo 专门找大的组织下手，如破解进入微软和《纽约时报》。Lamo 喜欢使用咖啡店、Kinko 店或者图书馆的网络来进行他的黑客行为，因此得了一个诨号：不回家的黑客。Lamo 经常发现安全漏洞，并加以利用。通常他会告知企业相关的漏洞。 在 Lamo 攻击过的名单上有雅虎、花旗银行、美洲银行和Cingular等，白帽黑客这么干是合法的，因为他们受雇于公司，但是 Lamo 这么做却是犯法的。 由于侵入《纽约时报》内部网络，Lamo 成为顶尖的数码罪犯之一。也正是由于这一罪行，Lamo 被处以 65 000 美元的罚款，并被处以 6 个月的家庭禁闭和两年的缓刑。

➢ Jonathan James

16 岁的时候，James 就已经恶名远播，因为他成为第一个因为黑客行径被捕入狱的未成年人。他稍后承认自己喜欢开玩笑、四处闲逛和迎接挑战。 James 攻击过的高度机密组织包括国防威胁降低局，这是国防部的一个机构。他的入侵使其获得了可以浏览高度机密邮件的用户名和密码。在 James 的“功劳簿”上，他还入侵过NASA的计算机，并且窃取了价值超过 170 万美元的软件。美国司法部有这样的一段描述：James 窃取的软件可以支持国际空间站的物理环境，包括温度和湿度控制。发现这次入侵之后，NASA 不得不立刻关闭了整个计算机系统，造成的损失达到 41000 美元。现在 James 立志开办一家计算机安全公司。

➢ Robert Morris

Morris 的父亲是前美国国家安全局的一名科学家。Morris 是首个被以计算机欺骗和滥用法案起诉的人，他是 Morris蠕虫病毒的创造者，这一病毒被认为是首个通过互联网传播的蠕虫病毒。

Morris 在康奈尔大学上学期间，创造的蠕虫病毒是为了探究当时的互联网究竟有多大。然而，这个病毒以无法控制的方式进行复制，造成很多计算机的死机。专家声称有 6000 台计算机被毁。Morris 最后被判处 3 年缓刑，400 小时的社区服务和 10 500 美元的罚金。

Morris 现在担任麻省理工计算机科学和人工智能实验室的教授，其研究方向是计算机网络的架构。

➢ Kevin Poulsen

Poulsen 的另一个经常被提及的名字是 Dark Dante，他受到广泛关注是因为他采用黑客手段进入洛杉矶电台的 KIIS-FM 电话线，这一举动为他赢得了一辆保时捷。此后，FBI 开始追查 Poulsen，因为他闯入了 FBI 的数据库和用于敏感窃听的联邦计算机系统。Poulsen 的专长就是闯入电话线，他经常占据一个基站的全部电话线路。Poulsen 还会重新激活黄页上的电话，并提供给自己的伙伴进行出售。Poulson 留下了很多未解之谜，最后在一家超市被捕，判处以 5 年监禁。在狱中，Poulson 干起了记者的行当，并且被推举为 Wired News 的高级编辑。在他最出名的文章里面，通过详细比对 Myspace 的档案，识别出了 744 名性罪犯。

➢ Barnaby Jack

Jack 是出生于新西兰的黑客、程序员和计算机安全专家。他曾花了两年时间研究如何破解自动提款机。2010 年 7 月 28 日，在美国拉斯维加斯举行的一年一度的“白帽”黑客会议上，Jack 将两台 ATM 搬到“黑帽”会场上，他刚一执行破解程序，自动提款机便不断吐出钞票，在地上堆成一座小山。这段“提款机破解秀”堪称 2010 年“白帽”黑客会议上最为轰动的精彩好戏。

1.2.2 黑客攻击的一般过程

随着网络业的迅猛发展，网络安全问题日趋严重，黑客攻击活动日益猖獗，黑客攻防技术也成为人们关注的焦点。在因特网上，黑客站点随处可见，黑客工具可以任意下载，对网络的安全造成了极大的威胁。总体来说，一个有预谋的黑客攻击包括以下几个步骤，如图 1-2 所示

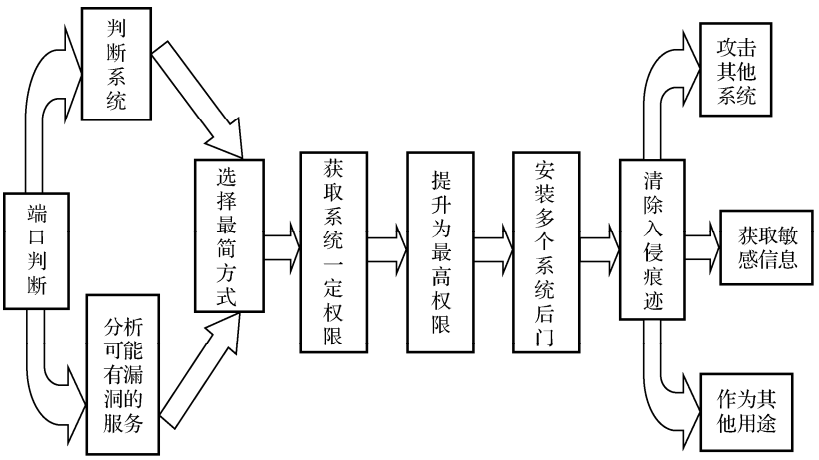

图 1-2　黑客攻击的步骤

1．锁定目标

攻击的第一步就是要确定目标的位置，在互联网上，就是要知道这台主机的域名或者 IP 地址。知道了要攻击目标的位置还不够，还要了解系统类型、操作系统、所提供的服务等全面的资料。

2．信息收集

扫描系统进一步了解目标的系统类型、操作系统、提供的服务等。黑客一般会利用下列的公开协议或工具来收集目标的相关信息。

（1）SNMP：该协议用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。

（2）TraceRoute 程序：用该程序获得到达目标主机所要经过的网络数和路由器数。

（3）Whois 协议：该协议的服务信息能提供所有有关的 DNS 域和相关的管理参数。

（4）DNS 服务器：该服务器提供了系统中可以访问的主机 IP 地址表和它们所对应的主机名。

（5）Finger 协议：用来获取一个指定主机上的所有用户的详细信息（如注册名、电话号码、最后注册时间及有没有读邮件等）。

（6）ping：可以用来确定一个指定的主机的位置。

3．端口扫描

当一个黑客锁定目标之后，黑客就开始扫描分析系统的安全弱点了。黑客一般可能使用

下列方式来自动扫描驻留在网络上的主机。

1）自编入侵程序

对于某些产品或者系统，已经发现了一些安全漏洞，该产品或系统的厂商或组织会提供一些“补丁”程序来进行弥补。但是，有些系统常常没有及时打补丁，当黑客发现这些“补丁”程序的接口后就会自己编写能够从接口入侵的程序，通过这个接口进入目标系统，这时系统对于黑客来讲就变得一览无余了。

2）利用公开的工具

各种端口扫描软件：Nmap、Nessues、X-Scan 等，可以对整个网络或子网进行扫描，寻找安全漏洞。这些工具都有两面性，就看是什么人在使用它们了。系统管理员可以使用它们来帮助发现其管理的网络系统内部隐藏的安全漏洞，从而确定系统中哪些主机需要用“补丁”程序去堵塞漏洞，从而提高网络的安全性能。而如果被黑客所利用，则可能通过它们来收集目标系统的信息，发现漏洞后进行入侵并可能获取目标系统的非法访问权。

4．获取访问权

完成了对目标的扫描和分析，找到系统的安全弱点或漏洞后，那就“万事俱备，只欠攻击了”，接下来是黑客们要做的关键步骤——发动攻击。对 Windows 系统采用的主要攻击技术有密码猜测、窃听、攻击 Web 服务器及缓冲区溢出等。

5．权限提升

获得普通用户的访问权限后，攻击者就会试图将普通用户权限提升至超级用户权限，以便完成对系统的完全控制。这种从一个较低权限开始，通过各种攻击手段得到较高权限的过程称为提权。

6．攻击过程

黑客一旦获得了对系统的访问权后，可能有下述多种选择。

（1）试图毁掉攻击入侵的痕迹，并在受到损害的系统上建立另外的新的安全漏洞或后门，以便在先前的攻击点被发现之后，继续访问这个系统，掩盖踪迹的方法有禁止系统审计、清空事件日志、隐藏作案工具等。

（2）在系统中安装一些后门及陷阱，包括木马等，用以掌握受害者的一切活动，能以特权用户的身份控制整个系统并获取比较感兴趣的信息，如电子银行账号和密码之类。

（3）如果是在一个局域网中，黑客就可能会利用此台计算机作为对整个网络展开攻击的大本营。

1.3　网络安全实训平台的搭建实训

【实训目的】

目前，虚拟化技术已经非常成熟，相关的产品如雨后春笋般地出现，如 VMware、Virtual PC、Xen、Parallels、Virtuozzo 等，但非常流行和常用的当属 VMware 了。VMware Workstation 是 VMware 公司的专业虚拟机软件，可以虚拟任何现有的操作系统，而且使用简单，容易掌握。

本书中的所有实训无须配备特殊平台，均在计算机中搭建虚拟环境，即在自己已有的系统中，利用虚拟机再创建一个内在的系统，该系统可以与外界独立，但与已经存在的系统建立网络关系，从而方便使用某些黑客工具进行模拟攻击。这样一来即使有黑客工具对虚拟机造成了破坏，也可以很快恢复，不会影响自己原有的计算机系统，因此具有更普遍的意义。本实训的目的是在虚拟机 VMware 中搭建实训平台。

【场景描述】

在虚拟机环境下配置 3 个 Win XP 虚拟系统“Win XP1” 、“Win XP2”和“Win XP3”，使得 3 个系统之间能够相互通信，并在 3 个系统上更新 VMware Tools，网络拓扑如图 1-3 所示。这里使用 Windows XP 系统是为了节省实体机的 CPU 资源，如果主机的运行速度足够，可以使用 Windows 7 等系统来进行实验。虚拟镜像可以从网上下载，也可以自己安装。

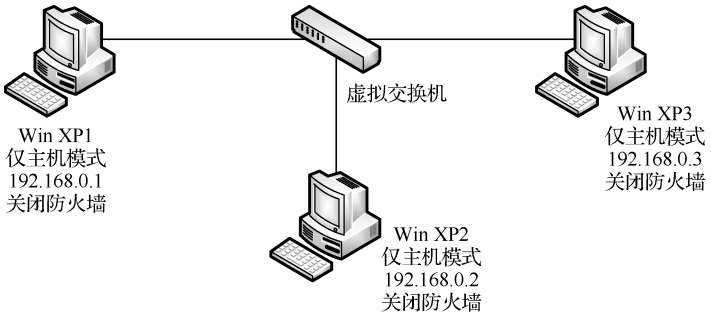

图 1-3　网络拓扑

【实训步骤】

（1）打开虚拟机 VMware Workstation 软件，创建 3 台 Win XP 的虚拟系统，分别命名为“Win XP1”、“Win XP2”和“Win XP3”，如图 1-4 所示。

图 1-4　创建虚拟系统

（2）由于 Win XP2 和 Win XP3 都是复制了 Win XP1 的虚拟镜像，为了不发生网络重名的系统错误，我们要分别修改计算机名为“vmwarexp1”、“vmwarexp2”、“vmwarexp3”，如图 1-5 所示。

（3）修改网络连接方式为“仅主机模式”，为了避免 MAC 地址冲突错误，我们需要修改 Win XP2 和 Win XP3 的 MAC 地址，确保 3 台计算机的 MAC 地址不一致，如图 1-6 所示。

（4）设置 3 台虚拟机的 IP 地址分别为“192.168.0.1” 、“192.168.0.2” 和“192.168.0.3”，子网掩码均为“255．255．255．0”，如图 1-7 所示。

图 1-5　修改计算机名

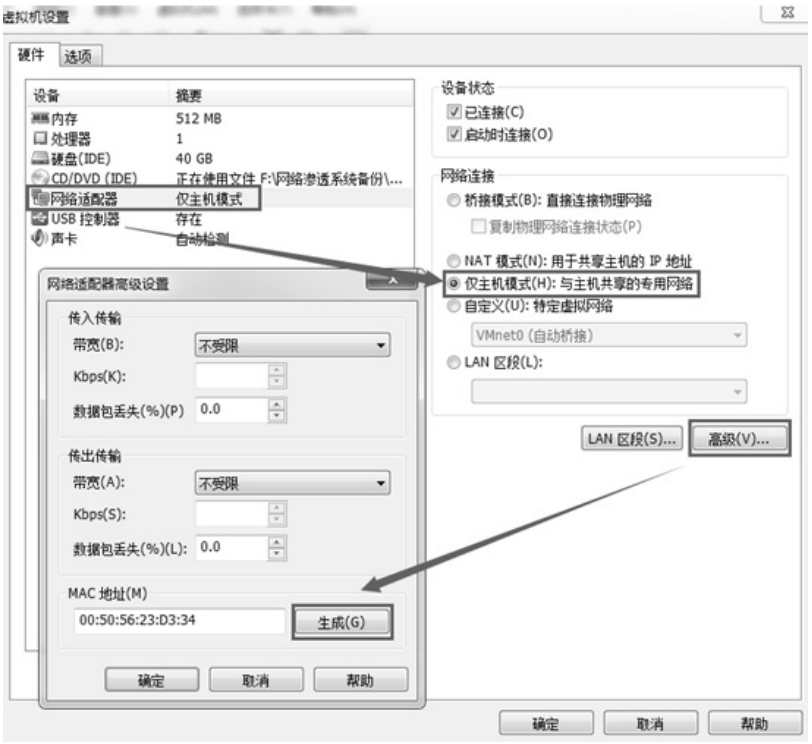

图 1-6　修改网络连接方式和 MAC 地址

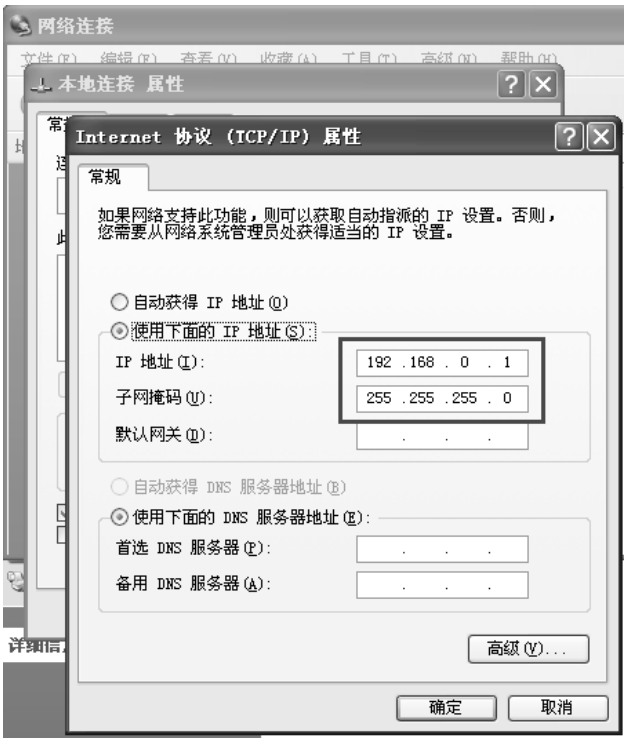

图 1-7　设置 IP 地址

（5）关闭 3 个系统的防火墙，如图 1-8 所示。

图 1-8　关闭防火墙

（6）进行连通性测试，使得 3 台系统都能相互通信，如图 1-9 所示。

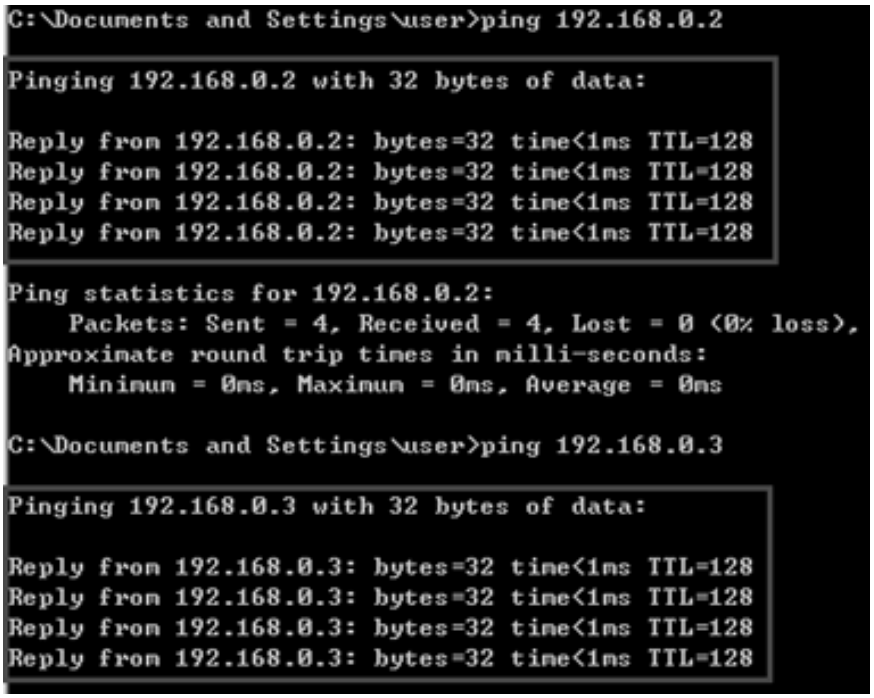

图 1-9　连通性测试

（7）为了使得实体机与虚拟机之间能够传输文件，我们要更新 VMware Tools。先把 Win XP 安装光盘的 ISO 镜像文件放到虚拟机的光驱上，如图 1-10 所示，然后单击“更新 VMware Tools”，如图 1-11 所示，安装完毕后重启计算机，便可实现实体机与虚拟机之间传输文件。

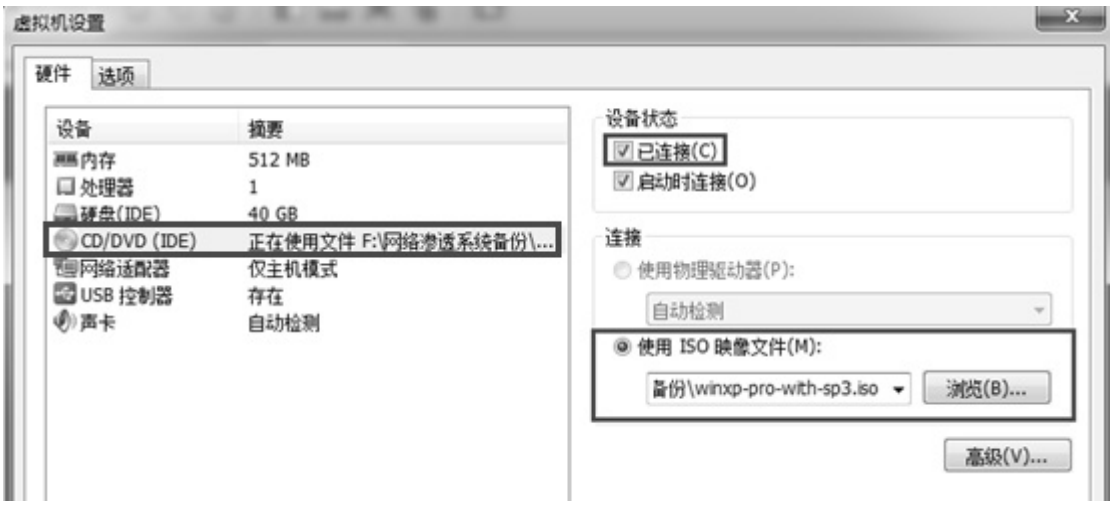

图 1-10　在虚拟机中使用 ISO 镜像文件

图 1-11　更新 VMware Tools

1.4　本章小结

本章简要叙述了网络安全的概念、网络不安全因素存在的原因，列举了一些知名的网络安全事件，并介绍了黑客和白帽子之间的区别，详细描述了黑客攻击系统的一般方法。