第7章

信息安全基础

任务1 了解信息安全常识

主 编 | 傅连仲 等

目 录

Contents

了解信息安全常识

从社会学的角度看，信息安全是关系国家安全、社会稳定、民族文化传承的重要方面。从技术的角度看，它又是一门涉及计算机科学、计算机网络、通信工程、密码技术、应用数学等多种学科的综合性学科，内容广泛且技术复杂，因此也造成了信息安全保障的复杂性。

任务情景

一天中午，小华的父母非常着急地来到学校找班主任老师。

下午上课前，老师来到班里，专门给同学们讲述了小华父母的遭遇。小华母亲在当天11点多的时候，突然接到一个语气焦急、自称是校医的电话，告知小华突发急病被送医需住院治疗，因事发突然，带钱不够，请小华母亲速转1万元至提供的账号。小华母亲被惊得六神无主，立刻使用手机转账，且赶紧联系小华父亲。因事出紧急，小华母亲忘记询问医院地址，回拨电话时无人接听，只好急忙赶来学校。

看到小华在学校安然无恙，小华父母才明白，是遭遇了电信诈骗，他们立刻报了警。

老师告诉同学们，并要求转告家长，谨防各种诈骗，遇到问题不要乱了方寸，第一时间要进行事件的真伪求证。

小华听后非常气愤，也感到不解，骗子怎么会知道小华上学的学校？怎么知道小华的母亲和他母亲的电话号码的？这些骗子被抓到后会得到怎么样的惩罚呢？

任务分析

老师看到许多学生都有和小华一样的疑问，于是细心解释：小华和他母亲的信息被泄露了，骗子利用获取的信息和人们面对突发情况时的紧张心理进行犯罪活动。信息泄露会产生严重的后果，小到个人遭受损失，大到国家受到严重威胁。

信息安全是一项长期且复杂的社会系统工程，既需要管理者充分运用先进的管理手段和技术进行专项治理，也需要信息应用者提高安全防护意识和安全应用技术，以有效保护信息在应用环节中的安全。作为信息专业的学生应该了解信息安全问题，有保护信息安全的意识、责任和技能。

小华感到责任重大，决心从案例入手，了解信息安全现状，掌握信息安全基本要求，了解信息安全法律、法规，全面、重新地认识信息安全。

了解信息安全常识，是深入学习信息安全防护技术的基础，更是安全使用计算机网络的需要。

7.1.1 研讨危害信息安全的案例

案例1：李某倒卖股票案

李某是证券管理专业的硕士研究生，当看到昔日的同学学有所成时，李某内心极度失衡，于是利用在证券公司实习的机会，了解了股票全国联网的计算机程序，开始盘算破解程序。经过几十天的“苦心钻研”，李某成功进入股民信息系统，盗取了众多股民的股票密码、投资金额、交易情况等核心机密。李某低价抛售他人股票自己抢购的违法行为，造成了股民钟某损失17万元、郭某损失38万元、林某损失100多万元的直接恶劣后果。最终李某投案自首，等待他的是法律的制裁。

案例2：网络谣言—“引力波”引发宇宙射线，靠近手机可能造成伤亡

2016年2月，一则“宇宙射线将贴近地球通过，可能对身体有害”的传言在微信朋友圈疯传。传言称：“当晚12时30分到凌晨3时30分，请务必关机，危险的、高辐射的宇宙射线将贴近地球通过。不要让手机靠近身体，可能造成手机损坏或人员伤亡。”此时适逢科研人员宣布“探测到引力波的存在”，许多人将二者混为一谈，一时人心惶惶。

真相：引力波天文学专家介绍，该传言完全是无稽之谈。宇宙射线指的是来自宇宙中一种具有相当大能量的带电粒子流，与“引力波”是两码事。而“引力波”是指两个黑洞在约13亿年前碰撞所传送出的扰动，于2015年9月14日抵达地球并被侦测到。中国电信客服人员表示，这类耸人听闻的传言被不法分子用于诈骗，此前曾发生多起因手机被骗关机，导致亲友被诈骗钱财的案例。

2．信息安全名词术语

（1）信息安全。

信息安全是指信息不会被故意或偶然地非法泄露、更改、破坏，不会被非法辨识、控制，人们能有益、有序地使用信息。

（2）网络安全。

网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏、非法使用，和意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（3）计算机病毒。

计算机病毒是指编制或在计算机程序中插入的破坏计算机功能或数据，影响计算机使用并且能够自我复制的一组计算机指令或程序代码。

（4）权利和义务。

权利是指依据法律规范规定，法律规范关系的参与者所具有的权能和利益。权能是指权利能够得以实现的可能性，它并不要求权利的绝对实现，只是表明权利具有实现的现实可能；利益则是权利的另一主要表现形式，是权能现实化的结果。

义务是指依据法律规范规定，法律规范关系的参与者应当承担的责任。

（1）沉浸性。

沉浸性是指用户可以沉浸于计算机生成的虚拟环境中或投入计算机生成的虚拟场景中的能力。理想的虚拟环境是用户借助VR设备，能够摆脱时间、空间的限制，完全沉浸在虚拟世界中并与之对话，达到用户难以分辨真假的程度。沉浸感来源于对虚拟世界的多感知性，除了常见的视觉感知外，还有听觉感知、力觉感知、触觉感知、运动感知、味觉感知、嗅觉感知等。

（2）交互性。

交互性是指用户可以通过佩戴VR眼镜，借助压力传感器和位置信息的追踪，实现与虚拟创设的环境实时互动，拉近与目标对象之间的距离，获取更逼真的感知效果。虚拟现实系统中的交互系统强调人与虚拟世界之间的自然交互。与传统的多媒体技术不同，人机之间交互不再使用键盘、鼠标，人们甚至感觉不到计算机的存在。

（3）想象性。

想象性是指以再现场景方式被动接收信息的同时，引导用户主动探索新的知识，产生新的感受和构想。虚拟环境为不同个体提供了个性化的想象空间。

说一说

为什么会发生危害信息安全的事件？危害信息安全的不法行为可能带来什么危害？

7.1.2 了解信息安全的现状

1. 了解危及信息安全的主要问题

从已发生的互联网信息安全事件看，虽然近两年没有发生较大规模的病毒威胁，也没有发生影响恶劣、损失严重的网络攻击事件，但信息安全所面临的形势依然严峻。

（1）网页仿冒问题依然棘手。

2020上半年针对境内的仿冒网页高达1.9万个，仿冒者充分利用技巧和自动操作技术，借助热点、敏感问题强化仿冒网页的可信度，使网页仿冒问题依然棘手。2021年3月8日至14日，这一周内国家互联网应急中心处理了246起网页仿冒事件，其中仿冒银行网页的高达230起。

（2）垃圾邮件猖獗。

国外曾有黑客组织发送包含恶意JavaScript脚本的垃圾邮件给数百万用户，收到邮件的用户通过Hotmail浏览垃圾邮件时在不知不觉中泄露了账号。随着反垃圾邮件过滤技术的提高，全球垃圾邮件的比例显著下降，但电子邮箱的使用者还是会收到骚扰用户的垃圾邮件。

（3）数据泄露十分严重。

影响较大的数据泄露事件有某邮件网站10亿个邮箱账户泄露、某招聘网站简历信息泄露等。数据泄露事件持续增长是由各种因素造成的，由此凸显数据防丢失对于数据拥有者的重要性和强化技术防护、管理防护的必要性。

（4）系统漏洞不容忽视。

2017年互联网出现针对Windows操作系统的勒索软件攻击，就是利用Windows SMB服务漏洞进行的，受害对象有国内高校、能源的重要信息系统。新发现的漏洞数量不断增加，危害程度也相当高，由此对网络应用安全构成了重大威胁。2020年上半年，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞11073个，其中高危漏洞4280个，占比38.7%。

（5）网站被篡改事件屡禁不止。

2020年上半年，我国境内被篡改网站数量为7.4万个。

2．了解网络恶意代码的整体形势

病毒制造者和病毒传播者在巨大利益的驱使下，利用病毒、木马技术进行各种网络盗窃、诈骗、勒索活动，严重干扰计算机网络的正常应用，大家应予以高度关注。

（1）恶意代码的主流是木马。

木马在恶意代码数量中占绝大多数。在流行病毒中，主要以木马、后门为主。木马制造者通过盗取互联网上有价值的信息资料并转卖获利，其牟利目的十分明确。

（2）“挂马”成为恶意代码传播的主要手段。

“挂马”就是黑客通过各种手段获取管理员账号，修改网页加入恶意转向代码，使访问者进入网站后，自动进入转向地址或下载恶意代码。网站挂马成为恶意代码传播的主要手段，无论是主动或被动的挂马都为恶意代码的滋生和传播提供了优越的环境，当前相当数量的恶意代码变种来自这类网站。被挂马的网站覆盖新闻、软件下载、娱乐等各种网站，当用户使用有安全漏洞的浏览器访问这些网站时，恶意代码利用脚本下载并激活木马程序。

（3）恶意代码的自我保护能力增强。

一些新技术，如主动防御技术、磁盘过滤驱动技术、影像劫持技术、穿透还原卡或还原软件技术被应用到恶意代码的编写中，使恶意代码从通过修改样本特征值以躲避查杀，逐渐过渡到直接与安全软件对抗。

（4）下载者病毒加剧了恶意代码传播。

下载者病毒具备从指定地址下载大量恶意代码的功能，使其成为恶意代码的快速输送者。网络用户的计算机一旦受到下载者病毒入侵，系统将会陆续下载安装几种甚至几十种病毒、木马等，种类几乎涉及所有流行的在线游戏盗号木马，危害十分严重。

（5）应用软件漏洞扩大了恶意代码传播途径。

随着操作系统安全性的逐渐提高，恶意代码利用系统漏洞“施法”的空间越来越小，恶意代码制造者开始关注应用软件的漏洞。近年来，恶意代码除了利用Windows系统漏洞传播外，开始综合利用各类应用软件的漏洞以扩大恶意代码传播途径，多数恶意代码利用两个及两个以上的漏洞传播。

（6）恶意代码黑色产业链逐步形成。

制造木马、传播木马、盗窃账户信息、第三方平台销赃、洗钱一整套完整恶意代码黑色产业链已经形成，且正朝着销赃洗钱方式多元化的方向发展。

（7）利用社会工程学传播恶意代码。

恶意代码制造者利用人们关注热点事件的心理或好友信任的关系设套，加速恶意代码传播，偶有出现的热点事件或将成为恶意代码的传播“帮凶”。将恶意代码伪装成热门电影、网络视频、照片等，借助高点击率来诱骗用户点击下载，进而扩大传播范围。

说一说

目前的信息安全形势如何？演变趋势如何?

7.1.3 掌握信息安全的基本要求

信息安全不仅涉及技术问题、管理问题，还涉及法学、犯罪学、心理学等问题，是一门由多学科综合形成的新学科。只有了解信息安全的基本要求，才能为构建安全、可靠的应用环境做好准备。

1. 了解信息安全涉及的内容

信息系统是由设备实体、信息、人组成的人机系统，安全问题也应包括实体安全、信息安全、运行安全和安全管理等方面。内容涉及安全技术、安全管理、安全评价、安全产品、安全法律、安全监察等。

信息安全主要涉及信息存储安全、信息传输安全、信息应用安全3个方面，包括操作系统安全、数据库安全、访问控制、病毒防护、加密、鉴别等多类技术问题，可以通过保密性、完整性、真实性、可用性、可控性5种特性进行表述。

保密性，是信息不会泄露给非授权对象的特性。

完整性，是信息本身完整，且不会在未授权时发生变化的特性。

真实性，是保证处理过程真实可靠的特性。

可用性，是合法对象能有效使用信息资源的特性。

可控性，是对信息资源能进行有效控制的特性。

2．了解信息安全控制层面

信息安全控制是复杂的系统工程，需要安全技术、科学管理和法律规范等多方面协调，并构成层次合理的保护体系，只有这样才能达到保障信息安全的目的。安全防护技术是保障实体、软件、数据安全的基础，安全管理是保障安全技术发挥作用的前提，法律规范是制约和打击危害信息安全行为的武器，所以，信息安全控制分为4个层面：实体安全防护、软件安全防护、安全管理和法律规范。

实体安全防护：对信息设备实体进行安全防护是保证信息安全的重要环节，是保证信息安全的基础。

软件安全防护：软件系统故障同样会导致信息安全问题，所以，软件运行安全也是保证信息安全的基础。

安全管理：统计结果表明，70%以上的安全问题是管理不善造成的，真正由于技术原因出现的安全问题很少，由此可见，安全管理在保证信息安全中的作用极其重要。

法律规范：在发生安全问题前，安全法律有规范信息应用行为、威慑破坏行为的作用，是信息安全的法律保障。在发生安全问题后，安全法律是处理安全问题的法律依据。

说一说

信息安全问题为什么会涉及众多学科或领域?

7.1.4 了解信息安全相关法律、法规

随着信息、信息系统在国家安全、社会稳定、经济建设中的作用和地位不断提高，社会迫切需要调整、规范信息关系，为此保护信息安全的法律、规范应运而生，并逐渐形成完整的法律、规范体系，以适应信息化社会有序发展的要求。

1．了解信息安全保护的法律法规

自1994年我国开始计算机信息系统立法活动，到目前为止，已基本形成了较为完整的法律体系。关于信息安全保护的刑事立法可以归纳为以刑法典为中心，辅之以单行刑法、行政法规、司法解释、行政规章及其他规范性文件的框架体系。目前我国惩治危害信息安全犯罪的现行主要规范性文件如表所示。

类 别	文 件 名	年 份	颁 布 单 位
法律类	《中华人民共和国刑法》（2020年修正）	2021年	全国人民代表大会常务委员会
	《全国人民代表大会常务委员会关于维护互联网安全的决定》	2000年	全国人民代表大会常务委员会
	《中华人民共和国网络安全法》	2017年	全国人民代表大会常务委员会
行政法规类	《中华人民共和国计算机信息系统安全保护条例》	1994年	国务院
	《中华人民共和国计算机信息网络国际联网管理暂行规定》	1996年	国务院
	《中华人民共和国电信条例》	2000年	国务院
	《互联网信息服务管理办法》	2000年	国务院
司法解释类	《最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》	2000年	最高人民法院
	《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	2017年	最高人民法院、最高人民检察院
	《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》	2019年	最高人民法院、最高人民检察院
行政规章类	《计算机信息网络国际联网出入口信道管理办法》	1996年	邮电部

类 别	文 件 名	年 份	颁 布 单 位
行政规章类	《计算机信息网络国际联网安全保护管理办法》	1997年	公安部
	《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》	1998年	国务院信息化工作领导小组
	《计算机信息系统国际联网保密管理规定》	2000年	国家保密局
	《计算机病毒防治管理办法》	2000年	公安部
	《互联网站从事登载新闻业务管理暂行规定》	2000年	国务院新闻办公室、信息产业部
	《信息安全等级保护管理办法》	2007年	公安部、国家保密局、国家密码管理局、国务院信息化工作办公室
网络安全等级保护2.0主要标准	《信息安全技术 网络安全等级保护定级指南》（GB/T 22240—2020）	2020年	国家市场监督管理总局和国家标准化管理委员会
	《信息安全技术 网络安全等级保护基本要求》（GB/T 22239—2019）	2019年	国家市场监督管理总局和国家标准化管理委员会
	《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）	2019年	国家市场监督管理总局和国家标准化管理委员会
	《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449—2018）	2018年	国家市场监督管理总局和国家标准化管理委员会
	《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070—2019）	2019年	国家市场监督管理总局和国家标准化管理委员会
	《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》（GB/T 36959—2018）	2018年	国家市场监督管理总局和国家标准化管理委员会

2．了解信息安全保护的法律责任

法律规范对主体行为实施制约的强制性，具体表现为当主体行为违反了法律规范的规定后，一定要追究法律规范主体应当承担的相关责任。根据所触犯的法律规范类型和情节轻重，应当承担的责任大体分为刑事责任、行政责任和民事责任。

（1）网络应用中的刑事法律责任。

利用信息系统或信息知识作为手段，或者针对信息系统，对国家、团体或个人造成危害，依据法律规定，应当予以刑罚处罚的行为。

《中华人民共和国刑法》和《全国人民代表大会常务委员会关于维护互联网安全的决定》中关于计算机网络犯罪的直接或间接条款警示我们，在计算机网络活动中实施危害行为可能承担刑事责任，必须引起高度重视。

案例：徐某利用QQ尾巴等程序在互联网上传播其编写的ipxsrv.exe程序，先后植入40000余台计算机，形成Botnet僵尸网络。徐某操纵僵尸网络对某音乐网站发动多次DDoS攻击，致使该公司遭受重大经济损失，造成恶劣的社会影响。经法院审理认为：徐某的行为已构成破坏计算机信息系统罪。依照《中华人民共和国刑法》判处徐某有期徒刑一年零六个月；依法没收作案笔记本电脑、服务器、U盘。

（2）网络应用中的行政法律责任。

违反计算机网络系统安全保护行政法规规定，主要是指违反有关计算机网络系统安全保护的法律、行政法规，以及地方性行政法规所规定的应负法律责任的内容。在相关的法规中有许多法律责任的条目，旨在提醒计算机网络用户遵纪守法，否则，将会承担相应的法律责任。

案例：2019年5月22日，某地网警在工作中发现，某地某科技有限公司开发的查看视频监控“NXXIP”移动应用，在未明示收集、使用信息的目的、方式和范围的情况下，获取该应用的用户通信录信息，存在超范围收集公民个人信息的行为，涉嫌违反《中华人民共和国网络安全法》第二十二条第三款、第四十一条至第四十三条、第六十四条的规定。依法给予该公司责令改正并处警告的行政处罚。

（3）网络应用中的民事责任。

“应当依法承担民事责任”是相关民事法律责任的原则性规定，也是对各种违反民事义务行为的概括性规定，满足民事法律责任构成要件的民事行为的行为人都要承担民事责任。一些具体的限制行为，在相关的法律法规中也有明确规定。

案例：2003年，某晨报发表“持伪证、民告官、骗局被揭穿”一文；同日，某信息服务公司在其经营的网站中转载了上述文章，并长达8年之久。另案生效判决认定某晨报社侵犯了徐某某的名誉权并赔偿精神抚慰金人民币2万元。2006年6月9日该晨报社在当日报刊尾版夹缝中刊登了对徐某某的致歉声明，但是字数、篇幅过小不是很显著。因转载此文的网络平台并未删除该文，徐某某以未及时更正为由请求经营该网络平台的公司承担侵权责任。

法院审理认为：某公司在其网站上转载某晨报的侵权文章并无不妥，但在法院于2004年年底认定某晨报的行为构成侵害原告名誉权且其在报纸刊载致歉声明后，某公司仍未更正或删除该信息。因某晨报的致歉声明篇幅过小且位置不显著，因此某公司虽不具有主观恶意但却具有过失，应当承担相应的民事责任。法院判定某公司赔偿原告经济损失人民币8万元及精神损害抚慰金人民币2万元。

做一做

在网上发布不负责任的言论需要承担什么法律责任?

第7章

信息安全基础

任务2 防范信息系统恶意攻击

主 编 | 傅连仲 等

目 录

Contents

防范信息系统恶意攻击

近年来，攻击信息系统事件接连不断，黑客入侵的触角几乎无处不在，其社会危害性十分严重。由于黑客网站不断增加，使学习黑客技术、获得黑客攻击工具变得轻而易举。据报道，黑客每年给全世界带来的经济损失估计高达100亿美元，而攻击一个国家的政治、军事系统所造成的损失更是难以用金钱来衡量。

任务情景

小华经常参与学校计算机中心信息系统的管理和维护工作，协助老师进行软件升级、安装，自己的计算机操作水平也在不断提升。

一天，有老师反映，自己存储在学校服务器中的一些教学资料丢失了许多，不知道是什么原因造成的，丢失的资料能否找回来?

老师让小华协助查找原因。小华认真检查了计算机信息系统，发现计算机中莫名其妙地增加了一些文件。他请教老师，老师复查小华发现的那些文件后告诉小华，学校的计算机系统受到了黑客的恶意攻击。

对“黑客”一词小华并不陌生，对于黑客他甚至还有些“崇拜”。老师发现小华对黑客的认识存在问题，认真引导说：你只看到了黑客令人羡慕的高技术手段，没有深入想想黑客行为可能造成的后果。对学校老师来说，教学资料丢失会影响他的教学，如果是国家重要信息资料丢失呢?

任务分析

小华认真反思了老师的那些话，觉得自己对黑客的认识仅仅停留在肤浅的表面，既不知道黑客到底采用什么手段侵入系统，也不知道黑客行为会造成什么危害，对黑客是一种盲目崇拜。

因此，他决定从了解最基本的黑客行为开始，逐步深入，全面了解黑客恶意攻击手段，学习防范攻击的基本技能，学会安全管理方法，全力保障网络设施的安全运行。

7.2.1 了解黑客行为的危害性、违法性

“黑客”一词来自英文Hacker的音译，在不同的人群和环境中，也出现了不同的解释。媒体经常提及的黑客是指专门入侵他人系统进行不法行为的人。

1．了解黑客行为的危害性

黑客行为的表现形式多样，结果多呈现破坏性，有商业机密、国家和军事情报窃取，有巨额资金盗窃，也有严重破坏经济秩序、干扰经济建设、危及国家安全的入侵破坏行为。黑客危害的主要表现形式有五种。

（1）非法入侵机密信息系统或金融、商业系统，盗取机密信息或商业信息，由此可能危害国家安全或造成重大经济损失。

（2）充当政治工具。攻击政府网络，在网上进行反政府、反社会活动，如在微博、朋友圈散布不当言论等。

（3）利用黑客手段在网络中肆意传播有害信息。如宣扬封建迷信、传播邪教言论、传播色情信息、教唆犯罪及传播其他一些危害国家安全、破坏社会安定的有害信息。

（4）获取别人隐私，破坏他人电子邮箱，攻击信息系统等。

（5）充当战争工具。在战争中利用黑客手段侵入对方信息系统，获取军事信息，发布假信息，扩散计算机病毒，扰乱对方系统等。

2．认识黑客行为的违法性

尽管许多黑客声称，侵入网络系统并不是要进行破坏活动，只是想探测网络系统中的漏洞，帮助完善系统。也有人称黑客行为多是恶作剧，甚至还有人把黑客行为分为“善意”探测和恶意入侵两种。然而现实情况绝非如此，许多黑客及黑客行为，已经不再是个人编程能力的“炫耀”，或小小的“恶作剧”，许多黑客行为毫无善意可言，而是一种极不道德的、违法犯罪的行为。在网络这个虚拟世界中，非法入侵就如同现实世界中私闯民宅，对此行为法律会予以严厉惩治。

中国的计算机信息系统安全保护法律、法规对黑客行为有严格限制。

（1）根据公安部颁布的《计算机信息网络国际联网安全保护管理办法》第六条的规定，任何单位和个人不得从事下列危害计算机安全的活动，其中第六条第一款所列就是“未经允许，进入计算机信息网络或者使用计算机信息网络资源的；”显然，触犯此条规定就是违法。

（2）根据《中华人民共和国刑法》第二百八十五、第二百八十六条的规定，对违反国家规定，侵入国家事务、国防建设、尖端科学技术领域计算机信息系统的，要受到刑罚；即使侵入的是一般信息系统，如果造成严重后果，同样也要受到刑罚，显然，黑客行为达到一定程度就是犯罪。

（3）《中华人民共和国网络安全法》第七十五条规定，境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任。

3．系统攻击中的名词术语

（1）安全漏洞。

安全漏洞是指信息系统中存在的不足或缺陷，有硬件、软件、协议实现疏漏导致的缺陷，也有安全管理策略不当造成的问题。

（2）网络攻击。

网络攻击是指利用信息系统自身存在的安全漏洞，非法进入网络系统或破坏系统，扰乱信息系统的正常运行，致使计算机网络系统崩溃、失效或错误工作。

（3）渗透测试。

渗透测试是测试人员通过模拟恶意攻击者的技术和方法，来评估计算机网络系统安全的一种评估方法。整个过程包括对系统任何弱点、技术缺陷或漏洞的主动分析及利用。

说一说

为什么说黑客的行为是违法的?

7.2.2 防范恶意攻击

防范恶意攻击的前提是了解攻击，了解网络攻击方法、攻击原理、攻击过程才能有针对性地采取应对措施，更有效防止发生各种攻击事件。根据入侵的对象不同，入侵方式会有差异，相应的应对方法当然存在差别，但就入侵行为来看依然存在许多共性，防范网络恶意攻击也有章可循。

1．发现入侵事件

发现入侵是响应入侵的前提，发现得越早，响应得越及时，损失就越小。非法入侵的特性决定了入侵的隐秘性，所以发现入侵较为困难。一般情况下，可以考虑从以下几个方面入手，争取尽早发现入侵的迹象。

（1）安装入侵检测设备。

（2）对Web站点的出入情况进行监视控制。

（3）经常查看系统进程和日志。

（4）使用专用工具检查文件修改情况。

2．响应入侵事件

应急响应是针对不同的入侵事件做出的不同应对措施，以减少损失为目的，不同入侵事件的响应策略大同小异，一般包括以下内容。

（1）快速估计入侵、破坏程度。

尽快估计入侵造成的破坏程度是减少损失的前提，也是采取正确应急方法的基础，对于不同的入侵、破坏程度，可以使用不同的阻止方式遏制势态发展。为了便于快速得出正确结论，应事先根据网络应用情况和具体管理策略，制作出问答形式的入侵情况判断表，其中包括必须采取的应急策略。

（2）决定是否需要关闭电源、切断系统连接。

如果明显存在入侵证据被删除或丢失的危险，可以考虑切断电源供给，但是，严禁随意干预电力供应，避免出现因电源改变系统运行环境的现象。

迅速判断系统保持连接或断开系统连接可能造成的后果，如果断开系统连接不会对正常工作和入侵证据产生影响，应立即断开系统连接，以保持系统的独立性。

（3）实施应急补救措施。

在系统投入运行之前，应针对各种可能出现的危害，制定出快速、可行的应急预案。危害事件发生后，应尽快实施应急补救措施，以减少危害带来的损失。

3．追踪入侵行为

追踪入侵行为不但是将危害行为制造者绳之以法的前奏，也是深入分析入侵行为造成危害的基础，由于黑客会想尽办法隐匿行踪，追踪入侵行为较为困难。

（1）获取可疑IP地址。

基于TCP/IP协议的网络设备在网络连接时，必须有独一无二的IP地址，这样才能保证数据的准确传输。IP地址与计算机的物理地址可以无关，但它能反映连接到网络的计算机的某些信息，所以获取可疑IP地址是追踪入侵行为的重要一步。

若能截获黑客侵入系统的通信信息，可从中解析IP地址，追踪使用该IP地址的用户。现在有许多IP地址查询工具可以从信息发送方发送的信息中，提取发送方的IP地址和端口号。有效使用防火墙的UDP数据包监测功能，也可以显示接收信息的IP地址和端口号。IP地址和联网设备有唯一的对应关系，且IP地址分配遵循一定的规律和规则，所以根据IP地址可以定位联网设备。

（2）验证IP地址的真实性。

使用各种方法获取的IP地址的真实性必须经过认真验证，真实的IP地址才具有追查价值。造成IP地址不准确的原因有很多，如从安全角度考虑隐藏IP地址造成的虚假、网络应用环境造成的IP虚假、人为伪造造成的IP虚假，不同情况应区别对待。

说一说

制定防范攻击应急预案的重要性。

7.2.3 使用“360安全卫士”清除木马

以病毒和木马为代表的恶意代码，是影响计算机和网络应用的顽疾，使用专用工具能够有效遏止恶意代码的破坏。常用病毒查杀工具有360安全卫士、金山、瑞星、卡巴斯基等，以下是使用360安全卫士清除计算机木马的具体操作。

（1）双击“360安全卫士”图标，启动360安全卫士，启动后的操作界面如图所示。

（2）单击“木马查杀”按钮，进入木马查杀操作界面，如图所示。

（3）单击“全盘查杀”按钮，即可开始对全部文件进行木马扫描，扫描进度显示如图所示。

360安全卫士提供4种木马查杀方式。

快速查杀：此方式仅扫描系统内存、启动对象等关键位置，由于扫描范围小，所以速度较快。

按位置查杀：由用户自己指定需要扫描的范围，此方式特别适用于扫描U盘等移动存储设备。

全盘查杀：此方式扫描系统内存、启动对象及全部磁盘，由于扫描范围广，速度较慢。由于木马可能会存在于系统的任何位置，用户在第一次使用360安全卫士或者已经确定系统中了木马的情况下，需要采取此种方式。

强力查杀：正常模式下难以查杀的顽固病毒及木马，可使用强力查杀模式。

（4）扫描完成，显示使用360查杀木马的结果，如图所示。如发现在计算机中存在木马，单击“一键处理”按钮，删除硬盘中的木马。

说一说

为什么提倡使用多种软件交叉杀毒?

7.2.4 了解网络安全管理的基本方法

对计算机网络实施安全管理，必须有一套切实可行的网络安全管理办法。实现计算机网络安全管理的重要前提是建立安全管理制度、进行明确的责任分工，并且认真、严格执行及不断完善安全管理制度。只有这样，才可能达到网络安全管理的最终目的。

1．了解基本的网络安全管理制度

建立网络安全机制，必须深刻理解网络涉及的全部内容，并根据网络环境和工作内容提出解决方案，因此，可行的安全管理策略是使用专门的安全防护技术、建立健全安全管理制度并严格执行。

建立网络安全管理制度是网络安全管理中的重要组成部分，使用网络的机构、企业和单位都应建立相应的网络安全管理制度。制定网络安全管理制度的基本依据是《互联网信息服务管理办法》《互联网站从事登载新闻业务管理暂行规定》和《中国互联网络域名注册暂行管理办法》等法律法规。一般认为对计算机网络实施安全管理应制定以下安全管理制度。

① 计算机网络系统信息发布、审核、登记制度；

② 计算机网络系统信息监视、保存、清除、备份制度；

③ 计算机网络病毒和漏洞检测管理制度；

④ 计算机网络违法案件报告和协助查处制度；

⑤ 计算机网络账号使用登记及操作权限管理制度；

⑥ 计算机网络系统升级、维护制度；

⑦ 计算机网络系统工作人员人事管理制度；

⑧ 计算机网络应急制度。

2．了解网络安全管理工作原则

实现计算机网络安全管理所依据的基本原则是多人负责原则、任期有限原则、职责分离原则。

多人负责原则，指从事每项与计算机网络有关的活动，都必须有两人或多人在场。

任期有限原则，指担任与计算机网络安全工作有关的职务，应有严格的时限。

职责分离原则，指在计算机网络使用、管理机构内，把各项可能危及计算机网络安全的工作拆分，并划归到不同工作人员的职责范围中。

3．了解网络安全审计

网络安全审计是指对网络安全活动进行识别、记录、存储和分析，以查证是否发生安全事件的一种安全技术。它能够为管理人员提供追踪安全事件和入侵行为的有效证据，以提高网络系统的安全管理能力。

网络安全审计分为审计数据收集和审计分析两部分。审计数据收集有不同的方式，包括从网络上截取数据，获取与系统、网络等有关的日志统计数据，以及利用应用系统和安全系统的审计接口获取数据等，目的是为审计分析提供基础数据。审计分析首先对收集的数据进行过滤，然后按照审计策略和规则进行数据分析处理，从而判断系统是否存在安全风险。

说一说

实施网络安全管理的重要性。

7.2.5 了解信息系统安全等级保护

为了维护国家网络安全，有效控制网络安全风险，我国实行计算机信息系统安全等级保护制度。在《计算机信息系统安全保护等级划分准则》中，将计算机系统安全保护能力分成5个等级，随着安全保护等级的提高，计算机信息系统安全保护能力逐渐增强。

1．了解计算机信息系统安全保护等级划分

《计算机信息系统安全保护等级划分准则》规定了安全保护的5个等级，可解决不同系统的安全保护问题，具体内容如表所示。

等　级	名　称	要　求
第一级	用户自主保护级	隔离用户与数据，使用户具备自主安全保护的能力
第二级	系统审计保护级	实施粒度更细的自主访问控制，通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责
第三级	安全标记保护级	具有系统审计保护的所有功能，还提供有关策略模型、数据标记及主体对客体强制访问控制的非形式化描述
第四级	结构化保护级	要求将第三级中的强制访问控制扩展到所有主体和客体，并考虑隐蔽通道
第五级	访问验证保护级	访问监控器仲裁主体对客体的全部访问，访问控制器具有抗篡改性，且能分析测试

2．了解信息系统安全等级保护的管理要求

信息系统安全等级保护，是指对国家秘密信息及公民、法人和其他组织的专有信息等公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

从安全管理的角度，信息系统的安全等级保护也按照国家标准对应分为5级，具体内容如表7-3所示。

等级	名　称	适用对象	危害后果	保护单位
第一级	自主保护级	适用于一般的信息系统	该类系统受到破坏后，会对公民、法人和其他组织的合法权益产生损害，但不损害国家安全、社会秩序和公共利益	该类系统由运营、使用单位或者个人依据国家管理规范和技术标准进行保护
第二级	指导保护级	适用于一般的信息系统	该类系统受到破坏后，会对社会秩序和公共利益造成轻微损害，但不损害国家安全	该类系统由运营、使用单位依据国家管理规范和技术标准进行保护
第三级	监督保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统	该类系统受到破坏后，会对国家安全、社会秩序和公共利益造成损害	该类系统由运营、使用单位依据国家管理规范和技术标准进行保护，国家有关信息安全职能部门对其信息系统安全等级保护工作进行监督、检查
第四级	强制保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统	该类系统受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害	该类系统由运营、使用单位依据国家管理规范和技术标准进行保护，国家有关信息安全职能部门对其信息系统安全等级保护工作进行强制监督、检查
第五级	专控保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统的核心子系统	该类系统受到破坏后，会对国家安全、社会秩序和公共利益造成特别严重的损害	该类系统由运营、使用单位依据国家管理规范和技术标准进行保护，国家指定的专门部门或者专门机构对其信息系统安全等级保护工作进行专门监督、检查

公安机关负责信息系统安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律规范的规定进行管理。国务院信息化工作领导小组办公室及地方信息化领导小组办事机构负责等级保护工作部门间的协调。

3．了解网络安全等级保护制度和信息安全等级保护制度的关系

信息安全等级保护制度是国家网络安全保障的重要制度，其核心是分清系统边界，明确系统责任，确保重点目标的安全。信息安全等级保护制度在国家网络安全保障中发挥了重要作用，但是随着云计算、大数据、物联网、移动互联网等技术的发展，系统边界日益模糊，因此，《中华人民共和国网络安全法》提出“实行网络安全等级保护制度”，明确了网络安全等级保护制度的基本要求，这是根据网络安全形势、特点所做的转变，标志着信息安全保护制度从1.0时代进入2.0时代的新阶段。

等级保护1.0主要强调物理安全、主机安全、网络安全、应用安全、数据安全及备份恢复等通用要求，而等级保护2.0标准在对等级保护1.0标准基本要求进行优化的同时，针对云计算、物联网、移动互联网、工业控制、大数据新技术提出了新的安全扩展要求。

4．了解强制性国家网络安全标准

强制性标准是在一定范围内通过法律、行政法规等强制性手段加以实施的标准，具有法律属性，强制性标准可分为全文强制和条文强制两种形式。全国信息安全标准化技术委员会按照《中华人民共和国网络安全法》的要求和网络安全工作需要，从维护国家安全、用户利益出发，对网络产品、服务制定强制性国家网络安全标准。

说一说

为什么要实行网络安全等级保护制度?