网络攻防技术

网络攻防技术

- 主要内容
  - 1 网络空间攻防技术概述
  - 2 网络空间安全的法律法规
  - 3 网络扫描与网络嗅探技术
  - 4 口令破解技术
  - 5 欺骗攻防技术
  - 6 拒绝服务攻防技术
  - 7 恶意代码攻防技术
  - 8 Web应用攻防技术

网络攻防技术

- **考核方式**
  - **平时成绩（出勤+课堂表现+作业）40%+期末考试60%。**
  - **三次无故缺勤取消期末考试资格！**

1 网络空间攻防技术概述

1 网络空间攻防技术概括

- 主要内容
  - 1.1 网络空间安全基础知识
  - 1.2 网络空间安全的主要威胁
  - 1.3 网络空间攻击过程
  - 1.4 物理攻击
  - 1.5 社会工程学
  - 1.6 黑客

1.1 网络空间安全基础知识

1.1 网络空间安全基础知识

- 主要内容
  - 网络空间的概念
  - 网络空间安全的概念
  - 网络空间安全的重要性

1.1 网络空间安全基础知识

- 主要内容
  - 网络空间的概念
  - 网络空间安全的概念
  - 网络空间安全的重要性

网络空间的概念

- 人类社会在经历了机械化、电气化之后，进入了一个崭新的信息时代。在信息时代，信息产业成为第一大产业。信息就像水、电、石油一样，与所有行业和所有人都相关，成为一种基础资源。信息和信息技术改变着人们的生活和工作方式。离开计算机、网络设备、电视机和手机等电子信息设备，人们将无法正常生活和工作。可以说在信息时代，人们生存在物理世界、人类社会和信息空间组成的三维世界中。
- 20世纪80年代初，作家威廉·吉布森创造了“网络空间”这个术语，用它来描述包含大量可带来财富和权力信息的计算机网络。所谓的网络空间，是指将客观世界和数字世界交融在一起，让使用它的人感知一个由计算机产生的、现实中并不存在的虚拟世界，并且，这个充满情感的虚拟数字世界也影响着人类现实物质世界。

网络空间的概念

- 网络是一个用户无法触摸到的、抽象的东西，空间又是一个抽象的概念，所以网络空间的概念更是抽象的。仁者见仁，智者见智，对于网络空间的概念有多种，但根据联合国国际电信联盟（ITU）的定义，网络空间是指由以下所有或部分要素创建或组成的物理或非物理的领域，这些要素包括计算机、计算机系统、网络及其软件支持、计算机数据、内容数据、流量数据及用户。英国、美国和德国等对网络空间概念的定义都不尽相同，但本质都是一样的，都着重强调提供网络应用的整个系统。

1.1 网络空间安全基础知识

- 主要内容
  - 网络空间的概念
  - 网络空间安全的概念
  - 网络空间安全的重要性

网络空间安全的概念

- 基于对全球五大空间的新认知，网络领域与现实空间中的陆域、海域、空域、太空一起，共同形成了人类自然与社会及国家的公共领域空间，使网络空间安全具有全球空间的性质。有学者提出“网络空间安全”是指能够容纳信息处理的网络空间构建与管理的安全，是远比“信息安全”更为重要和根本的安全。网络空间安全保护是否得当不仅会影响用户的上网体验，还会对国家的安全和利益造成威胁。

网络空间安全的概念

- 从用户（个人、企业等）的角度来说，涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人利用窃听、冒充、篡改和抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。
- 从网络运行和管理者的角度来说，对本地网络信息的访问、读/写等操作应受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源造成的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。

网络空间安全的概念

- 对安全保密部门来说，应对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络被泄露，避免由于这类信息的泄露对社会产生危害，对国家造成巨大的经济损失，甚至威胁到国家安全。
- 从社会教育和意识形态角度来说，网络上不健康的内容会对社会的稳定和发展造成阻碍，必须对其进行控制。

网络空间安全的概念

- 因此，网络安全在不同的环境和应用中会得到不同的解释。
  - 网络运行系统的安全，即保证信息处理和传输系统的安全，包括计算机系统机房环境的保护、计算机结构设计上的安全性考虑、硬件系统的可靠安全运行、计算机操作系统和应用软件的安全、数据库系统的安全、电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁信息泄露而产生信息泄露，干扰他人（或受他人干扰）。本质上，网络运行系统的安全就是保护系统的合法操作和正常运行。

网络空间安全的概念

- 网络系统信息的安全，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、安全问题跟踪、计算机病毒防治和数据加密等。
- 网络信息传播的安全，即信息传播后的安全，包括信息过滤等。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、冒充和诈骗等有损合法用户利益的行为，其本质是保护用户的利益和隐私。

◆ 显而易见，网络安全与其所保护的信息对象有关。网络安全的本质是在信息的安全期内，保证信息在网络流动或静态存放时不被非授权用户非法访问，但授权用户是可以访问的。网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。

1.1 网络空间安全基础知识

- 主要内容
  - 网络空间的概念
  - 网络空间安全的概念
  - 网络空间安全的重要性

网络空间安全的重要性

- 在现代化社会中，网络以其开放、便捷等特性对社会发展起到了巨大的促进作用。网络空间涉及国家的军事、政治等多个领域信息，在其中存储、转发的信息多为涉及政府重要文件、金融商业信息、科研数据等重要信息，而且大都为敏感信息，多为国家机密。因此，这些信息往往会成为各种网络攻击的目标。

网络空间安全的重要性

- 虽然网络空间安全已经得到普遍重视，但近年来一些新的焦点问题相继显露。例如，“伪基站”导致的诈骗事件频频发生，暴露了通信领域对物理接入安全的忽视；云计算、大数据相关新概念、新应用的不断出现，使个人数据隐私泄露问题日益凸显；计算和存储能力日益强大的移动智能终端承载了大量与人们工作、生活相关的应用和数据，急需切实可用的安全防护机制，而互联网上匿名通信技术的滥用更是对网络监管、网络犯罪取证提出了严峻的挑战。

网络空间安全的重要性

- 在国家层面，危害网络空间安全的国际重大事件也是屡屡发生。例如，2010年伊朗核电站的工业控制计算机系统受到震网病毒（Stunxnet）攻击，导致核电站推迟发电；2013年美国棱镜计划被曝光，表明自2007年起美国国家安全局（NSA）即开始实施绝密的电子监听计划，通过直接进入美国网际网络公司的中心服务器挖掘数据、收集情报，涉及海量的个人聊天日志，存储的数据，语音通信、文件传输、个人社交网络数据。

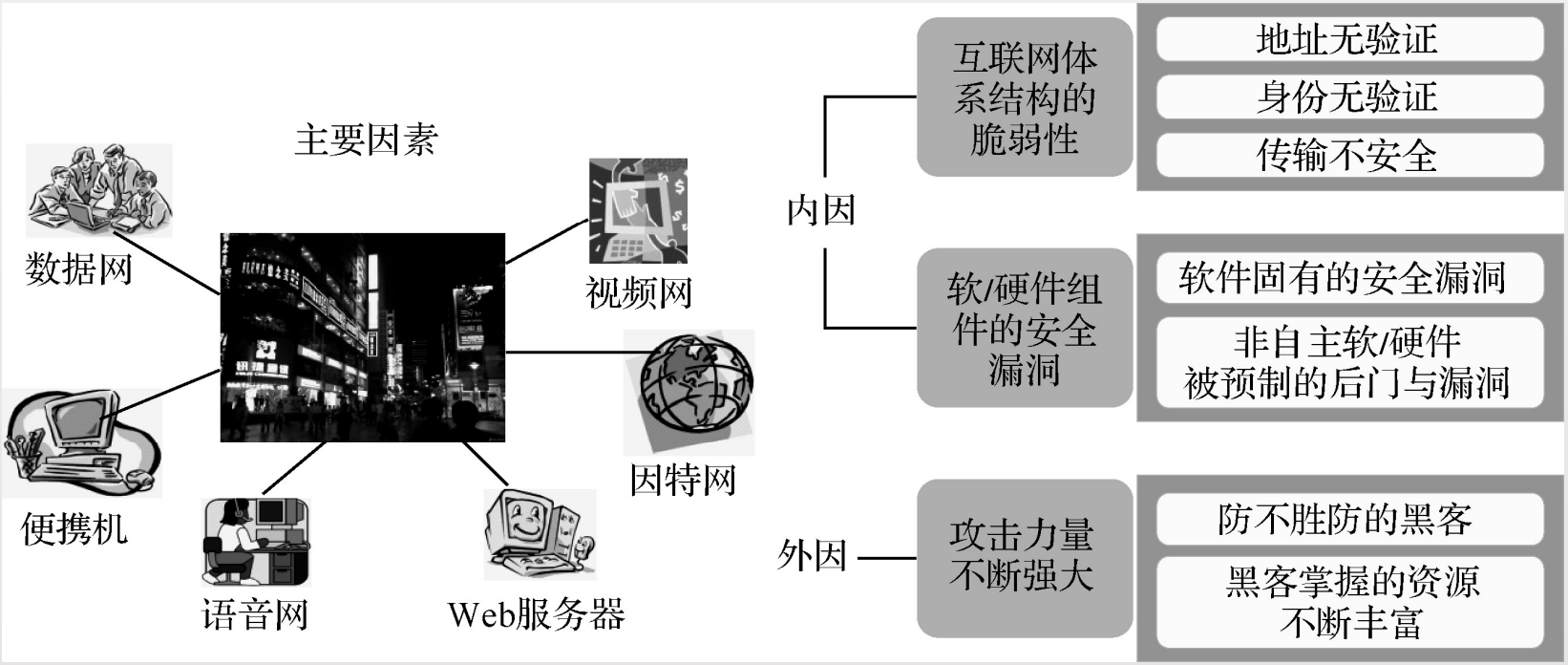
网络空间安全的重要性

- 上述种种安全事件的发生，凸显了网络空间仍然面临着从物理安全、系统安全、网络安全到数据安全等各个层面的挑战，迫切要进行全面而系统的安全基础理论和技术研究。安全是发展的前提，发展是安全的保障。当前，我国正在加速从网络大国向网络强国迈进，因此网络空间安全技术的研究起着越来越重要的支撑作用。

1.2 网络空间安全的主要威胁

1.2 网络空间安全的主要威胁

- **随着计算机网络的不断发展，出现了各式各样网络空间安全的威胁因素。这些网络安全的威胁因素可能来自内部，也可能来自外部。**



1.2 网络空间安全的主要威胁

- 主要内容
  - 安全漏洞
  - 恶意软件
  - 网络攻击
  - 网络犯罪

1.2 网络空间安全的主要威胁

- 主要内容
  - 安全漏洞
  - 恶意软件
  - 网络攻击
  - 网络犯罪

安全漏洞-软件编写bug

- 无论是服务器程序、客户端软件，还是操作系统，只要是用代码编写的，都会存在不同程度的bug，攻击者可以利用bug进行攻击。
  - （1）缓冲区溢出：攻击者只要发送超出缓冲区所能处理长度的指令，系统便进入不稳定状态。攻击者特别设置一串准备用作攻击的字符时，甚至能访问根目录，从而拥有对整个网络的绝对控制权。
  - （2）联合使用问题：一个程序经常由功能不同的多层代码组成，甚至会涉及最底层的操作系统。入侵者通常会利用这个特点为不同代码层输入不同的内容，以达到窃取信息的目的。
  - （3）资源竞争：若不能妥善处理多任务多线程的资源竞争问题，入侵者就可能利用这个处理顺序上的漏洞改写某些重要文件，从而达到闯入系统的目的。

安全漏洞-系统配置不当

- 系统配置通常由管理员进行，若管理员配置时不规范，则为攻击者提供了极大的便利。
  - （1）使用默认配置：许多系统安装后都有默认的安全配置信息，通常被称为easy to use，也就意味着easy to break in。
  - （2）空口令：系统安装后保持管理员口令的空值，不进行修改。入侵者第一步做的事情就是搜索网络上是否有这样的管理员口令为空的机器。
  - （3）临时端口：有时候为了测试，管理员会在机器上打开一个临时端口，但测试完成后却忘记了禁止它，这样就会给入侵者有漏可寻、有洞可钻。

安全漏洞-设计缺陷

- 网络层、传输层、应用层的协议在设计上都存在一定的缺陷，可被攻击者利用。
  - （1）IP：IP非常容易“轻信”，使入侵者可以随意地伪造及修改IP数据包而不被发现。
  - （2）TCP/IP：TCP序列号预计是网络安全领域中最有名的缺陷之一，即受害主机不能接到信任主机应答确认时，入侵者通过预计序列号来建立连接，从而可以伪装成信任主机与目的主机通话。
  - （3）FTP：FTP用户的口令一般与系统登录口令相同，而且采用明文传输，这就增加了系统被攻破的危险。只要在局域网内或路由器上进行监听，就可以获得大量的口令，利用这些口令就可以尝试登录系统。

1.2 网络空间安全的主要威胁

- 主要内容
  - 安全漏洞
  - 恶意软件
  - 网络攻击
  - 网络犯罪

恶意软件

- 针对流氓软件在网络上泛滥成灾的现象，中国互联网协会联合国内30多家厂商对恶意软件的官方定义如下。
- （1）强制安装：是指未明确提示用户或未经用户许可，在用户计算机或其他终端上安装软件的行为。
  - ①在安装过程中未提示用户。
  - ②在安装过程中未提供明确的选项供用户选择。
  - ③在安装过程中未给用户提供退出安装的功能。
  - ④在安装过程中提示用户不充分、不明确（明确充分的提示信息，包括但不限于软件作者、软件名称、软件版本、软件功能等）。

恶意软件

- （2）难以卸载：是指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。
  - ① 未提供明确的、通用的卸载接口（如Windows系统下的“程序组”中“控制面板”的“添加或删除程序”）。
  - ② 软件卸载时附有额外的强制条件，如卸载时要联网、输入验证码、回答问题等。
  - ③ 在不受其他软件影响或人为破坏的情况下，不能完全卸载，仍有子程序或模块在运行（如以进程方式）。

恶意软件

- （3）浏览器劫持：是指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。
  - ① 限制用户对浏览器设置的修改。
  - ② 对用户所访问网站的内容擅自进行添加、删除、修改。
  - ③ 迫使用户访问特定网站或不能正常上网。
  - ④ 修改用户浏览器或操作系统的相关设置导致以上3种现象的行为。

恶意软件

- （4）广告弹出：是指未明确提示用户或未经用户许可，利用安装在用户计算机或其他终端上的软件弹出广告的行为。
  - ① 安装时未告知用户该软件的弹出广告行为。
  - ② 弹出的广告无法关闭。
  - ③ 广告弹出时未告知用户该弹出广告的软件信息。
- （5）恶意收集用户信息：是指未明确提示用户或未经用户许可，恶意收集用户信息的行为。
  - ① 收集用户信息时，未提示用户有收集信息的行为。
  - ② 未提供用户选择是否允许收集信息的选项。
  - ③ 用户无法查看自己被收集的信息。

恶意软件

- （6）恶意卸载：是指未明确提示用户、未经用户许可，或误导、欺骗用户卸载其他软件的行为。
  - ①对其他软件进行虚假说明。
  - ②对其他软件进行错误提示。
  - ③对其他软件进行直接删除。
- （7）恶意捆绑：是指在软件中捆绑已被认定为恶意软件的行为。
  - ①安装时，附带安装已被认定的恶意软件。
  - ②安装后，通过各种方式运行其他已被认定的恶意软件。
- （8）其他侵犯用户知情权、选择权的恶意行为。

1.2 网络空间安全的主要威胁

- 主要内容
  - 安全漏洞
  - 恶意软件
  - 网络攻击
  - 网络犯罪

网络攻击

- 网络攻击可分为主动攻击和被动攻击。主动攻击会导致某些数据流的篡改和虚假数据流的产生。这类攻击可分为篡改、伪造消息数据和终端（拒绝服务）。被动攻击中的攻击者不对数据信息做任何修改，截取/窃听是指在未经用户同意和认可的情况下，攻击者获得了信息或相关数据，通常包括窃听、流量分析、破解弱加密的数据流等攻击方式。
- 主要内容
  - 篡改
  - 伪造消息数据
  - 拒绝服务
  - 流量分析
  - 窃听

网络攻击

- 篡改是指一个合法消息的某些部分被改变、删除，消息被延迟或改变顺序，通常用以产生一个未授权的效果。例如，修改传输消息中的数据，将“允许甲执行操作”改为“允许乙执行操作”。
- 伪造指的是某个实体（人或系统）发出含有其他实体身份信息的数据信息，假扮成其他实体，从而以欺骗方式获取一些合法用户的权利。
- 拒绝服务攻击会导致通信设备的正常使用或管理被无条件地中断。拒绝服务攻击通常是对整个网络实施破坏。这种攻击也可能有一个特定的目标，如到达某特定目的地（如安全审计服务）的所有数据包都被阻止。

网络攻击

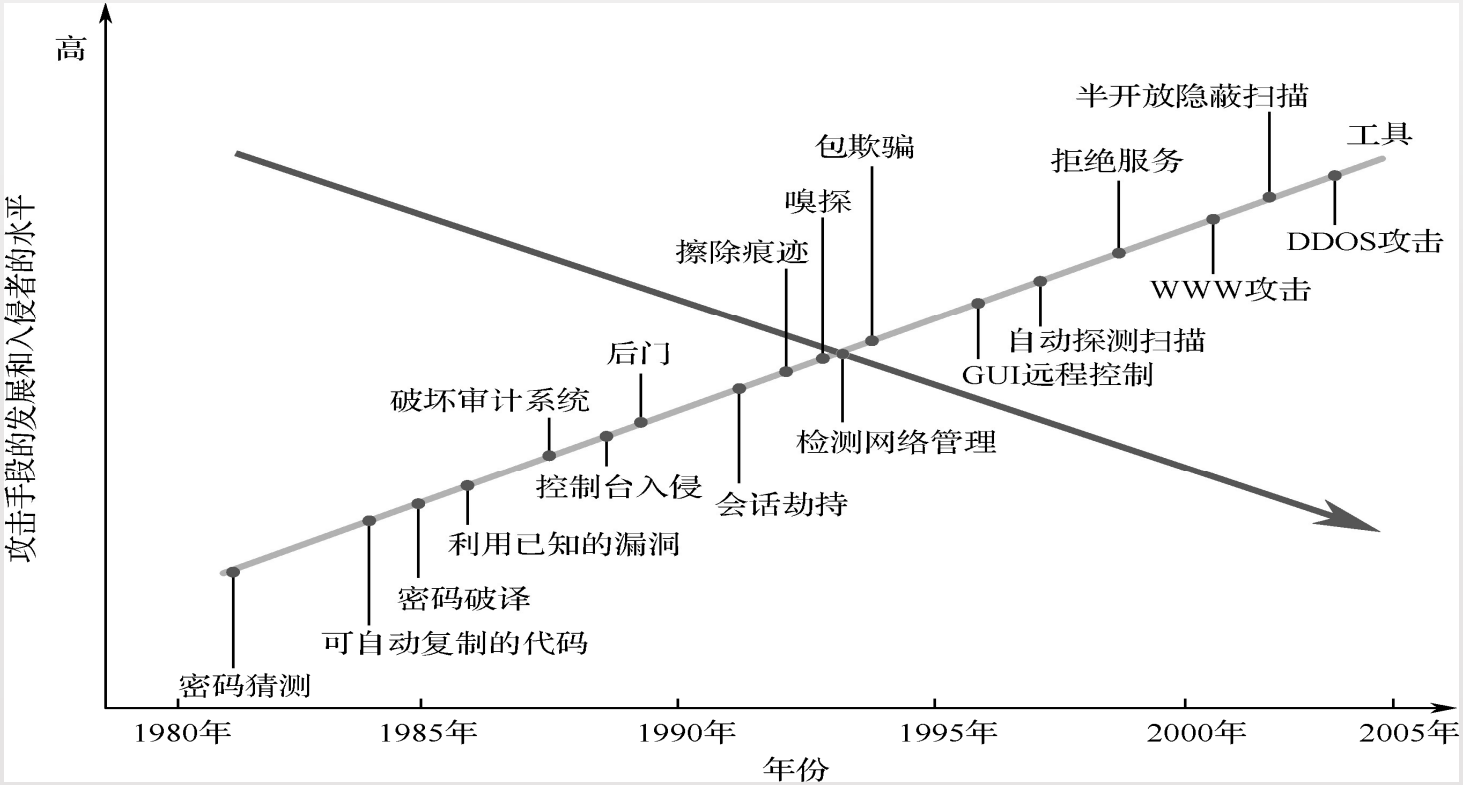
- 流量分析攻击方式适用于一些特殊场合。例如，敏感信息都是保密的，攻击者虽然从截获的消息中无法得到消息的真实内容，但攻击者还能通过观察这些数据报的模式，分析确定通信双方的位置、通信的次数及消息的长度，获知相关的敏感信息。

网络攻击

- 窃听是最常用的手段。目前应用最广泛的局域网上的数据传送是基于广播方式进行的，这就使一台主机有可能收到本子网上传送的所有信息。而计算机的网卡工作在混杂模式时，就可以将网络上传送的所有信息传送到上层，以供进一步分析。如果没有采取加密措施，通过协议分析，可以完全掌握通信的全部内容。窃听还可以用无线截获方式得到信息，通过高灵敏接收装置接收网络站点辐射的电磁波或网络连接设备辐射的电磁波，通过对电磁信号的分析恢复原数据信号从而获得网络信息。尽管有时数据信息不能通过电磁信号全部恢复，但可能得到极有价值的情报。

网络攻击

- 从最早的密码猜测到嗅探、拒绝服务等，随着攻击手段的不断发展，入侵者的水平却变得越来越低。



单选题 1分

设置

下列选项属于被动攻击的是：

A 篡改

B 伪造

C 拒绝服务

D 窃听

提交

1.2 网络空间安全的主要威胁

- 主要内容
  - 安全漏洞
  - 恶意软件
  - 网络攻击
  - 网络犯罪

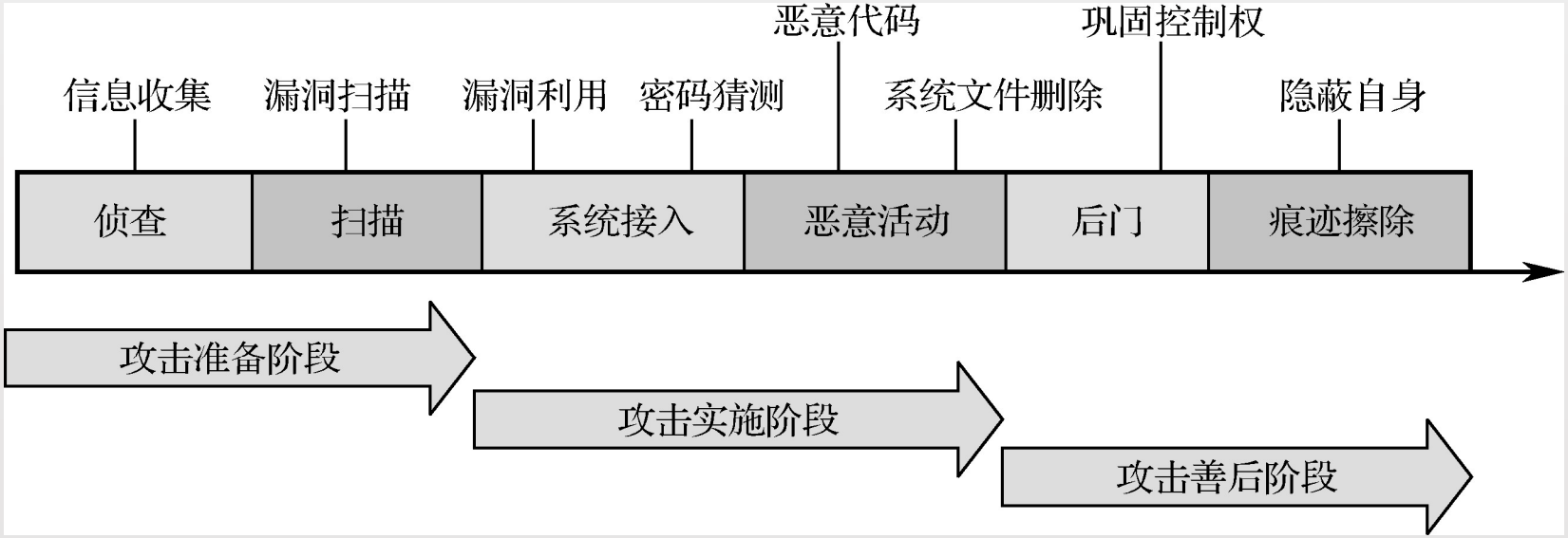
网络犯罪

- 主要内容
  - 网络色情和性骚扰
  - 贩卖盗版光盘
  - 欺诈
  - 妨害名誉
  - 侵入他人网站、电子信箱、系统
  - 制造、传播计算机病毒
  - 网络赌博
  - 教唆、煽动各种犯罪，传授各种犯罪方法

1.3 网络空间攻击过程

1.3 网络空间攻击过程

- 为了保护网络空间安全，首先需要掌握攻击者常用的攻击手段，根据攻击过程采用针对性的措施以防御网络攻击。本节主要讨论网络空间攻击的主要过程。
- 网络攻击一般有3个阶段：**攻击准备阶段、攻击实施阶段、攻击善后阶段**。



网络空间攻击过程-攻击准备阶段

- 1）侦查：攻击前最主要的准备工作就是收集尽量多的关于攻击目标的信息。这些信息主要包括目标的操作系统类型及版本、相关软件的类型和版本、端口开放情况、提供的服务及相关的社会信息等。

网络空间攻击过程-攻击准备阶段

- 黑客用来收集目标系统相关信息的协议和工具如下：
  - ping程序：可以用来确定一个指定的主机位置。
  - SNMP：用来查阅路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。
  - TraceRoute程序：用该程序获得到达目标主机所要经过的网络结点数和路由器数。
  - Whois协议：该协议的服务信息能提供所有DNS域和相关的管理参数。
  - 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。

网络空间攻击过程-攻击准备阶段

- 2）扫描
  - 除了了解目标的基本信息，还需要找到目标系统的漏洞以便入侵系统。发现系统漏洞的方法可以分为手动分析和自动分析两种。
  - 手动分析的过程比较复杂、技术含量较高，但是效率低下，一般用于分析简单的漏洞或者还没有检测软件的漏洞。
  - 自动分析则采用软件对目标系统进行自动分析，需要的人为干预过程少，效率高，即使对漏洞不了解的人也可以判断目标是否存在漏洞。自动检测漏洞的工具分为两大类，其中一类是综合型漏洞检测工具，如Nessus和X-Scan，它们可以检测出多种漏洞；另一类是专用型漏洞检测工具，如用于检测振荡波蠕虫漏洞的工具RetinaSasser，只检测某种特定的漏洞。

网络空间攻击过程-攻击实施阶段

- 当收集到足够的信息之后，攻击者就要开始实施攻击行动了。作为破坏性攻击，只需要利用工具发动攻击即可；而作为入侵性攻击，需要利用准备阶段收集到的信息与目标的系统漏洞，然后利用漏洞获取一定的权限，一般攻击者会试图获取尽可能高的权限，以执行更多可能的操作。
- 1）系统接入
  - 攻击的第一步是要进入系统。攻击者可以设法盗窃账户文件，进行破解，从中获取某用户的账号和口令，或者根据用户的默写习惯进行账号和密码的猜测，再寻觅合适时机以用户身份登录主机。当然，利用某些工具或系统的远程漏洞登录主机也是攻击者常用的一种技法。

网络空间攻击过程-攻击实施阶段

- 2）恶意活动
  - 利用远程漏洞登录之后获取的不一定是最高权限，很多时候只是一个普通用户的权限，常常没有办法做黑客们想要做的事。这时就需要配合本地漏洞来把获得的权限进行提升，常常是提升到系统的管理员权限。
  - 获得了最高管理员权限之后，可以在系统中进行恶意操作，如执行恶意代码、进行系统文件的删除、下载敏感信息等。

网络空间攻击过程-攻击善后阶段

- 攻击者利用种种手段进入目标主机系统并获得控制权之后，为了能长时间保留和巩固对系统的控制权，而不被管理员发现，常常会做两件事：留下后门和擦除痕迹。
- 1）留下后门
  - 从前面的叙述中可以看出，攻破一个系统是一件费时费力的事情，非常不容易，为了下次再进入系统时方便，攻击者一般都会留下一个后门。例如，攻击者在目标主机上增加一个用户名和密码都是hack的用户，并把该用户添加到Administrator组。通过增加具有管理员权限的用户，就可以在远程实现启动服务、登录系统等操作，这样就在目标主机上留下了一个后门，巩固了攻击者对这台主机的控制权。

网络空间攻击过程-攻击善后阶段

- 2）擦除痕迹
  - 众所周知，所有的网络操作系统一般都提供日志记录功能，该功能是指将系统中发生的动作记录下来。因此，为了自身的隐蔽性，攻击者都会抹掉自己在日志中留下的痕迹。
  - 最简单的方法是直接删除日志文件，但这样做虽然避免了真正的系统管理员根据IP追踪到自己，却也明确无误地告诉了管理员，系统已经被入侵了。所以，更常用的办法是只对日志文件中有关自己的部分进行修改，关于修改方法的细节会根据不同的操作系统有所区别。网络上有许多辅助修改日志的程序，如Zap、Wipe等，其主要做法就是清除Utmp、Wtmp、Lastlog和Pacct等日志文件中某用户的信息，使得当使用who、last等命令查看日志文件时，隐藏此用户的信息。

网络空间攻击过程-攻击善后阶段

- 然而，只修改日志是不够的，由于安装了后门程序，运行后很有可能被管理员发现。所以，一些黑客高手可以通过替换系统程序的方法来进一步隐藏踪迹。这类用来替换正常系统程序的黑客程序是Rootkit，比较常见的有Linux-Rootkit，它可以替换ls、ps、netstat、inetd等一系列重要的系统程序。例如，替换了ls后就可以隐藏特定的文件，使管理员在使用ls命令时无法看到这些文件，从而达到隐藏自己的目的。

单选题 1分

设置

下列选项属于攻击实施阶段的是：

A 漏洞扫描

B 执行恶意代码

C 留下后门

D 擦除痕迹

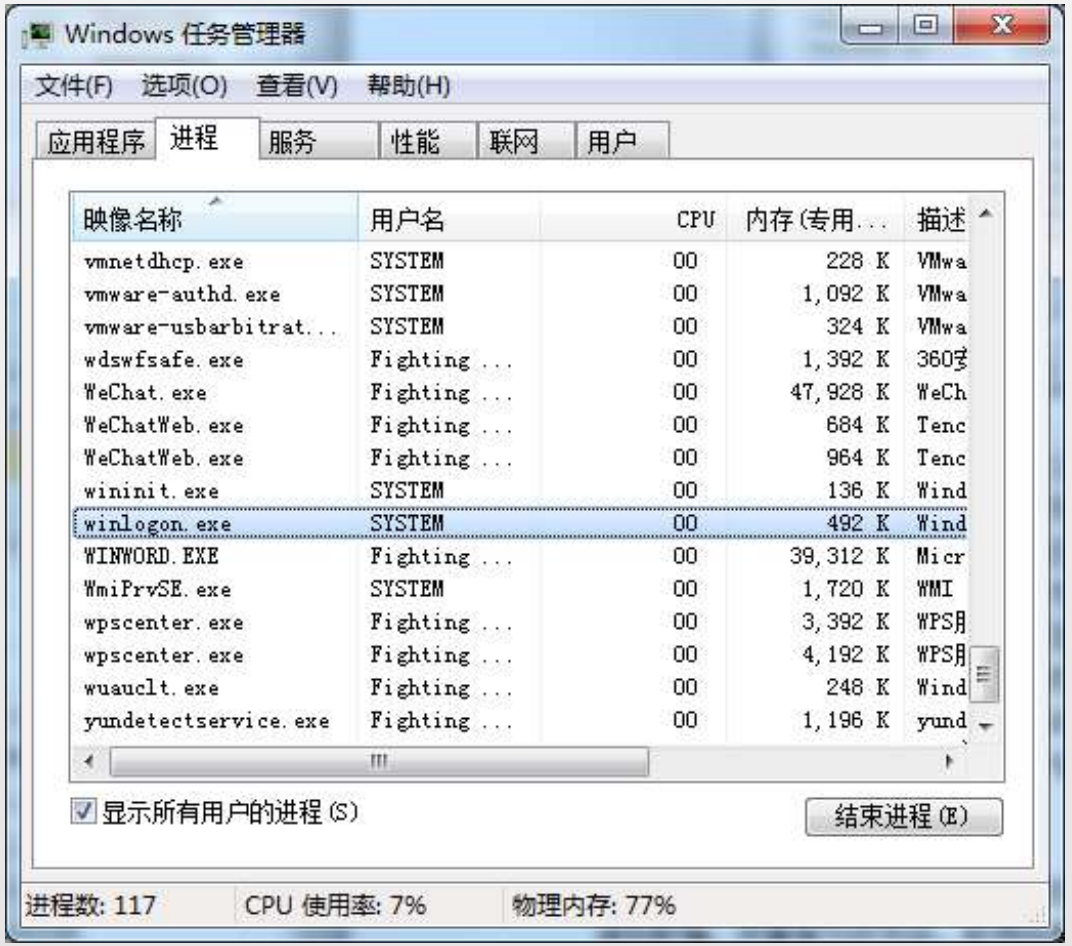
提交

物理攻击

- 物理攻击是指通过各种技术手段绕开物理安全防护体系，从而进入受保护的设施场所或设备资源内，获取或者破坏系统中受保护信息的攻击方式。物理安全主要是保证某些特别重要的设备不被接触从而免受破坏攻击。
- 典型的物理攻击手段，如计算机被盗走或物理破坏，从而导致计算机内数据信息的丢失或毁坏；或被攻击者接触个人计算机，导致管理员账号被获取从而登录计算机导致信息的丢失。

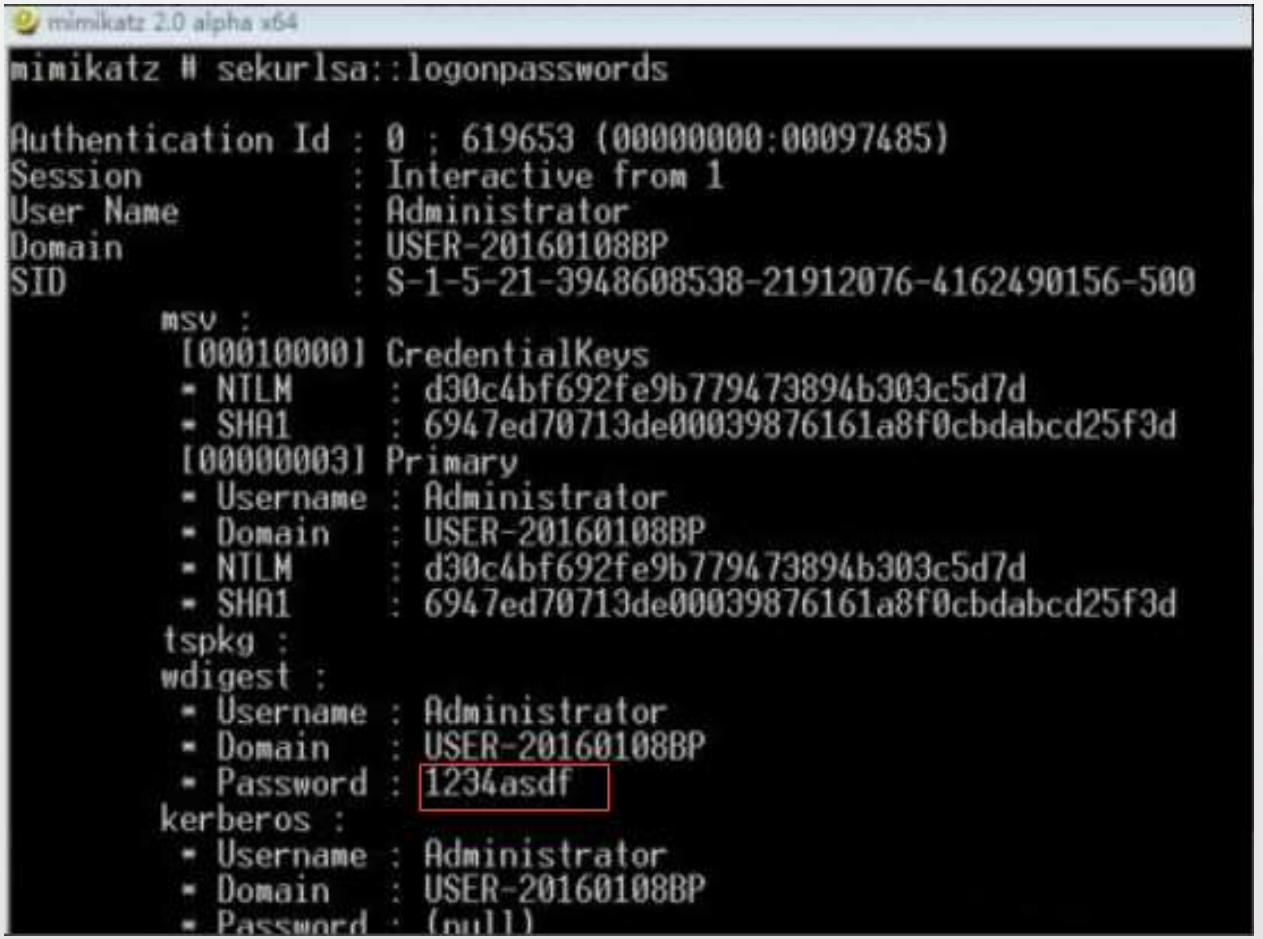
物理攻击-实例

- 一般来说，在使用自己的计算机时都会采用管理员登录，而管理员账号在登录后，所有的用户信息都存储在系统的一个进程中，这个进程是“winlogon.exe”，物理攻击者就可以利用程序将当前登录用户的密码解码。



物理攻击-实例

- 在此情况下，攻击者可以利用如FindPass.exe或者Mimikatz等工具，对该进程进行解码，然后直接将用户的密码显示出来。该过程就是一次完整物理攻击获取管理员密码的过程。



物理攻击-实例

- 针对这种情况，作为管理员，为保证账户安全可能会选择为其他用户建立一个普通账号。但事实上，攻击者用普通用户账号登录后，可以利用如GetAdmin.exe等工具将自己加到管理员组或者新建一个具有管理员权限的用户。甚至利用命令行的配置，通过普通用户的账号获得管理员权限或新建具有管理员权限的用户。

物理攻击-实例

- 另一个对于犯罪分子来说极具诱惑的场景就是入侵自动取款机（ATM）。其中，物理方式Skimmer（通过伪造ATM的一些部件，如读卡器或键盘，来欺骗取款者把读取到的密码或磁卡信息发送到犯罪者手中的设备）是攻击者最常用的手段。或者，犯罪分子通过USB端口或CD-ROM驱动器来物理访问目标ATM，然后利用恶意软件感染或绕过ATM的防护系统，从而对ATM进行操作。

物理攻击-实例

- 通过伪造ATM的键盘来窃取密码

社会工程学

- 社会工程学是指**利用人类的心理弱点/本能反应、好奇心、信任、贪婪等心理陷阱，采用诸如欺骗、伤害等手段取得自身利益的技术**。简而言之，通过蒙蔽、影响、劝导等手段实现从他人处获取信息的手法，称为社会工程学方法。

社会工程学-攻击形式

- 1）收集敏感信息
  - 社会工程师可以根据搜索引擎对目标信息收集及整理，从而根据已掌握信息对用户进行攻击。或者根据踩点或调查所得到的信息进行欺骗。此外，还可以通过网络钓鱼方式或直接通过目标信息管理缺陷等获得目标的敏感信息。
  - 例如，当一个社会工程师想得到一个教授的电子邮箱、生日等私人信息时，他可以通过百度搜索引擎进行检索搜集。
  - 攻击者还可以用非法手段在薄弱站点获得安全站点的人员信息，如通过论坛挖掘其用户的信息，通过公司间的合作进行渗透，截获相关信息等。甚至，社会工程师可以利用QQ等聊天工具诱导受害者，获得其敏感信息。

社会工程学-攻击形式

- 2）网络钓鱼式攻击
  - 钓鱼式攻击是针对大量受害者的诈骗攻击，攻击者利用模仿合法站点获取受害者的个人信息，例如，利用欺骗性的虚假电子邮件或者虚假网站诱导用户进入伪装后的站点，进行信息输入，以及利用IM程序（QQ、微信等）或移动通信工具假冒他人进行欺骗。如冒充重要人物，假装是部门的高级主管，要求工作人员提供所需信息；或者冒充求助职员，假装是需要帮助的职员，请求工作人员帮助解决网络问题，借以获得所需信息；冒充技术支持，假装是正在处理网络问题的技术支持人员，通过要求获得所需信息以解决问题，来获得用户的相关信息。

社会工程学-攻击形式

- 3）心理学攻击
  - 分析用户的一般心理，以获得用户的相关隐私信息，尤其常见于分析用户密码。如根据生日进行密码猜解，或者根据移动电话号码或身份证号码进行猜解，根据亲朋好友姓名或生日进行密码推算。甚至考虑到很多用户并不进行复杂的密码设置，就直接猜测系统自带的默认密码来得到受害者的密码信息。
  - 当然，除了密码的猜解，利用用户在安全上的心理盲区，也是社会工程学中常见的攻击手段。如利用用户常常容易忽视本地和内网安全、对安全技术（如防火墙、入侵检测系统、杀毒软件等）盲目信任等心理，进行薄弱环节的突破；利用人的同情心或者内疚感，通过心理压力进行“胁迫”来获得相关信息。

社会工程学-攻击形式

- 4）反向社会工程
  - 反向社会工程是指迫使目标人员反过来向攻击者求助的技术手段。攻击者通过技术或非技术手段，给网络或者计算机应用制造“问题”，引诱受害者或者相关管理人员透露或者泄露攻击者需要的信息。该攻击手段比较隐蔽，往往较难发现，并且危害大，难以防范。

社会工程学-典型案例

- 1) “最大的计算机诈骗案”

  (1) 获得密码。

  - 1978年的某天，瑞夫金无意中进入了美国太平洋银行的电汇室，这里每天的转款额高达几十亿美元。瑞夫金当时工作的那家公司恰巧负责开发电汇室的数据备份系统，这给了他了解转账程序的机会，包括银行职员拨款的步骤。他了解到被授权进行电汇的交易员每天早晨都会收到一个严密保护的密码，用来进行电话转账交易。
  - 电汇室里的交易员图省事把密码记到一张纸片上，并把它贴到很容易看得见的地方。1978年11月的某天，瑞夫金有了一个特殊的理由出入电汇室。到达电汇室后，他做了一些操作过程的记录，借此机会偷看到纸片上的密码，并用脑子记了下来，几分钟后他走出电汇室。瑞夫金后来回忆道：“感觉就像中了大奖。”

社会工程学-典型案例

（2）转款入户。

- 瑞夫金约在下午3点离开电汇室，径直走到大厦前厅的付费电话旁，塞入一枚硬币，打给电汇室。此时，他改变身份，装扮成一名银行职员—工作于国际部的麦克·汉森（Mike Hansen），对话内容大概是这样的：
- “喂，我是国际部的麦克·汉森。”他对接听电话的小姐说，小姐按正常工作程序让他报上办公室电话。“286。”他已有所准备。小姐接着说：“好的，密码是多少？”“4789。”他尽量平静地说出密码。接着他让对方从纽约欧文信托公司（Irving Trust Company）贷1020万美元到瑞士苏黎士某银行，他已经建立好的账户上。对方说：“好的，我知道了，现在请告诉我转账号。”

社会工程学-典型案例

- 瑞夫金吓出一身冷汗，这个问题事先没有考虑到，他的骗钱方案出现了纰漏。但他尽量保持自己的角色，十分沉稳，并立刻回答对方：“我看一下，马上给你打过来。”这次，他装扮成电汇室的工作人员，打给银行的另一个部门，拿到账号后打回电话。对方收到后说：“谢谢。”

（3）成功结束。

- 几天后，瑞夫金乘飞机来到瑞士提取了现金，他拿出800万美元通过俄罗斯一家代理处购置了一些钻石，然后把钻石封在腰带里通过了海关，飞回美国。瑞夫金成功实施了历史上最大的银行劫案，他没有使用武器，甚至不需要计算机的协助。

社会工程学-典型案例

- 2）黑客反遭攻击
  - John是一名渗透测试人员，受雇为一家客户从事标准的网络渗透测试。他使用开源的安全漏洞检测工具Metasploit进行扫描，结果发现了一台敞开的VNC（虚拟网络计算）服务器，这台服务器允许控制网络上的其他机器。
  - 他在VNC会话开启的情况下记录了发现的结果，这时候鼠标在后台突然开始在屏幕上移动。John意识到这是个危险信号，因为在出现这个异常情况的时间段，谁也不会以正当的理由连接至网络。他怀疑有人入侵进入了网络。
  - John决定冒一下险，于是打开记事本，开始与入侵者聊天，冒充自己是化名为“n00b”的黑客，佯称自己是个新手，缺乏黑客技能。

社会工程学-典型案例

- John想：“我怎样才能从这个家伙身上收集到更多的信息，为我的客户提供更大的帮助呢？”John尽量装成自己是个菜鸟，向这个黑客问了几个问题，装作自己是刚入道的年轻人，想了解黑客行业的一些手法，想与这名黑客保持联系。等到聊天结束后，他已弄来了这个入侵者的电子邮箱和联系信息，甚至还弄来了对方的照片。他随后将这些信息汇报给了客户，系统容易被闯入的问题随之得到了解决。
- John通过与黑客进行一番聊天后还得知：对方只是四处寻找容易闯入的系统，没想到轻而易举地就发现了这个敞开的系统。

黑客

- 黑客源自英文Hacker，最初曾指热心于计算机技术、水平高超的计算机专家，并非像大部分的圈外或媒体习惯定义的那样—将“黑客”指为计算机侵入者。在黑客圈中，“Hacker”一词无疑是带有正面的意义，例如：system hacker—熟悉操作的设计与维护，password hacker—精于找出使用者的密码，computer hacker—通晓计算机并进入他人计算机操作系统的高手。真正的黑客们精通各种编程语言和各类操作系统，是一群纵横于网络上的技术人员。
- 但随着时代的发展，网络上出现了越来越多的骇客（Cracker），在Hacker眼中Cracker属于层次较低的计算机入侵者，他们只会入侵、使用扫描器到处乱扫、用IP炸弹炸，毫无目的地进行入侵和破坏。如果黑客是炸弹制造专家，那么骇客就是恐怖分子。

黑客

- 实际上黑客可以大致分为3个群体：白帽黑客（White Hat）、灰帽黑客（Grey Hat）、黑帽黑客（Black Hat）。
- 白帽黑客以“改善”为目标，破解某个程序并做出（往往是好的）修改，从而增强（或改变）该程序之用途，或者透过入侵去提醒该系统管理者计算机存在安全漏洞，有时甚至会主动予以修补。白帽黑客大多是计算机安全公司的雇员，或者响应招测单位的悬赏，在完全合法的情况下攻击某系统。
- 灰帽黑客以“昭告”为目标，透过破解、入侵去炫耀自己拥有高超的技术，或者宣扬某种理念。
- 黑帽黑客以“利欲”为目标，透过破解、入侵去获取不法利益，或者发泄负面情绪。黑帽黑客也就是前面所说的Cracker。