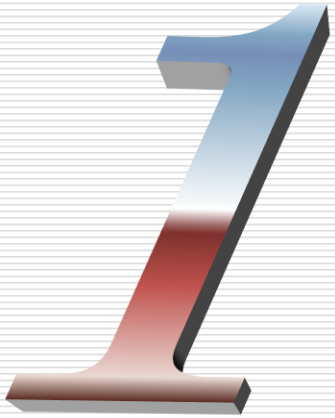
第一章 安全概述

国家计算机网络入侵防范中心

张玉清



内容安排

- **1.1** 网络安全基础知识
- **1.2** 网络安全的重要性
- **1.3** 网络安全主要威胁因素
- **1.4** 网络攻击过程
- **1.5** 网络安全策略及原则
- **1.6** 网络安全体系设计
- **1.7** 常用的防护措施
- **1.8** 小结

1.1 网络安全基础知识

- “安全”的含义（Security or Safety?）

  - 平安，无危险；远离危险的状态或特性。

  - 客观上不存在威胁，主观上不存在恐惧。即客体不担心其正常状态受到影响。

计算机安全定义

- 国际标准化委员会的定义：

  为数据处理系统而采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、泄露。

- 中国公安部计算机管理监察司的定义：

  计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。

安全的概念（重点）

“如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是安全，而是隐藏；相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全…”

-Bruce Schneier

网络安全定义

- 网络安全的一个通用定义指网络信息系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的破坏、更改、泄露，系统能连续、可靠、正常地运行，服务不中断。
- 网络安全简单的说是在网络环境下能够识别和消除不安全因素的能力 。

网络安全定义

- 狭义解释：针对网络中的一个运行系统而言，网络安全就是指信息处理和传输的安全。它包括硬件系统的安全、可靠运行，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。狭义的网络安全，侧重于网络传输的安全。
- 广义解释：广义的网络安全是指网络系统的硬件、软件及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露。

网络安全类型

- 网络安全在不同的环境和应用中有不同的解释，主要有以下几类：
- 系统安全
- 网络安全
- 信息传播安全
- 信息内容安全

网络安全类型

- 系统安全

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。避免因为系统的崩演和损坏而对系统存储、处理和传输的消息造成破坏和损失。避免由于电磁泄翻，产生信息泄露，干扰他人或受他人干扰。

- 网络安全

网络上信息系统的安全。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、跟踪，计算机病毒防治，数据加密等。

网络安全类型

- 信息传播安全

  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。

- 信息内容安全

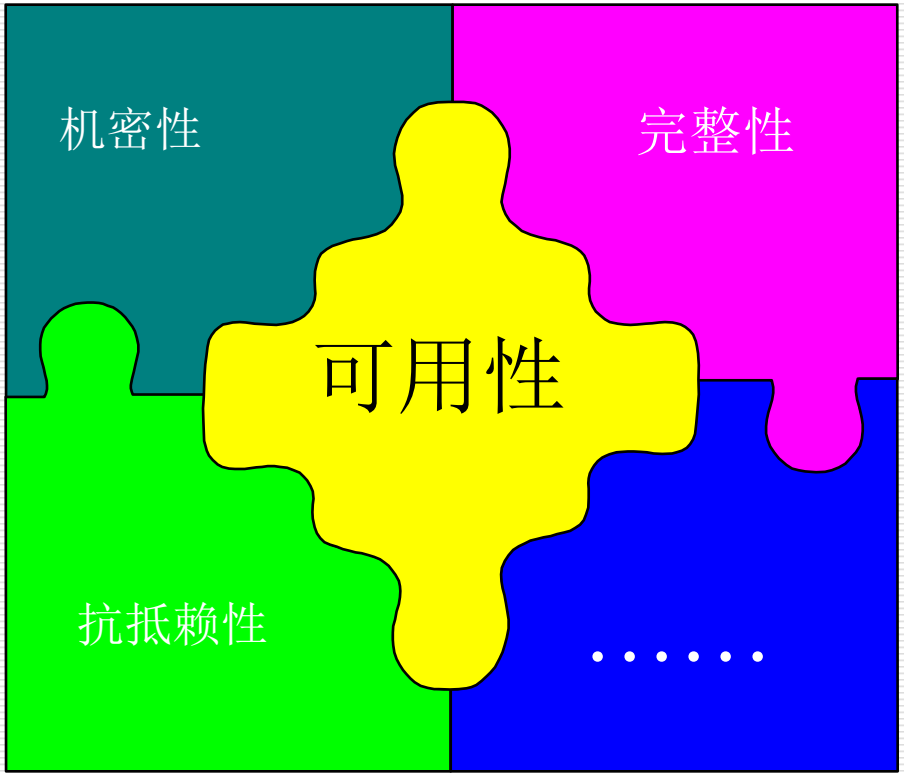
  网络上信息内容的安全。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈编等有损于合法用户的行为。其本质是保护用户的利益和隐私。

网络安全主体

- 网络安全的主体是保护网络上的数据和通信的安全。
- 数据安全性是指软硬件保护措施，用来阻止对数据进行非授权的泄漏、转移、修改和破坏等。
- 通信安全性是通信保护措施，要求在通信中采用保密安全性、传输安全性、辐射安全性等措施。

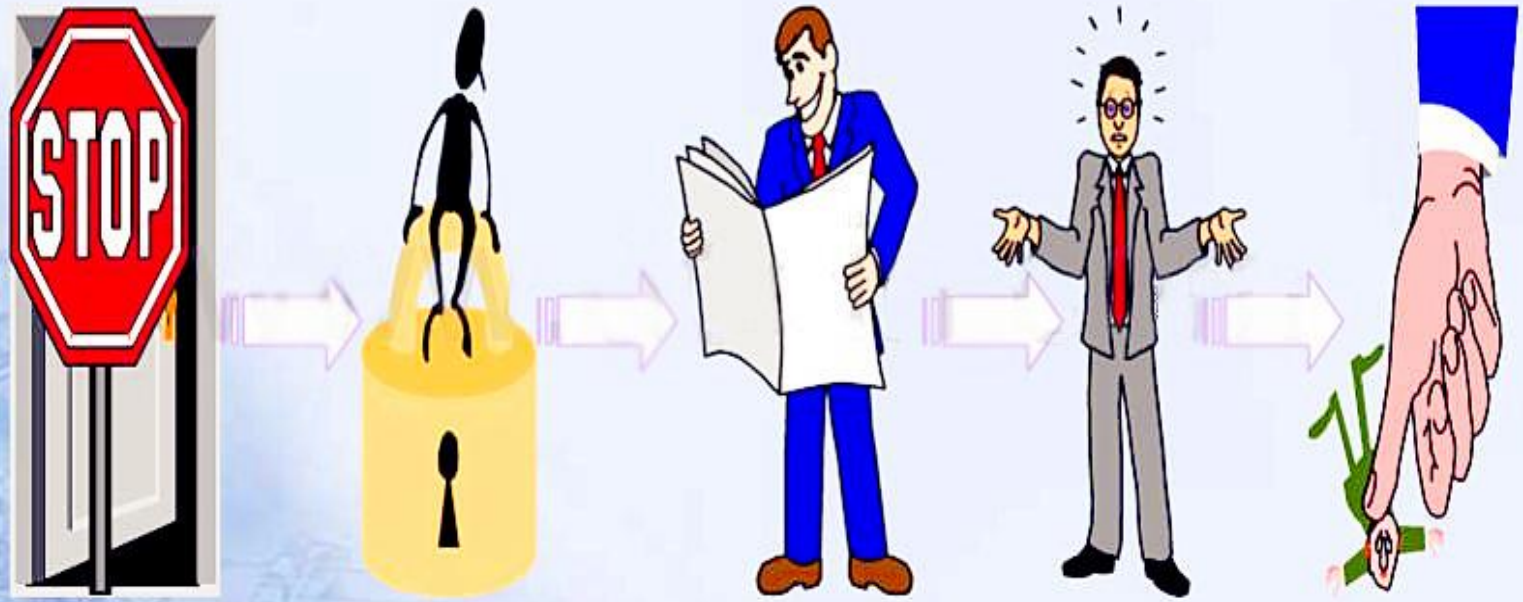
网络安全的基本需求

- 可靠性
- 可用性
- 保密性
- 完整性
- 不可抵赖性
- 可控性
- 可审查性
- 真实性



信息与网络安全的目标

进不来　　拿不走　　看不懂　　改不了　　跑不了



1.2 网络安全的重要性

- **随着网络的快速普及，网络以其开放、共享的特性对社会的影响也越来越大。**
  - 网络上各种新业务兴起，比如电子商务、电子政务、电子货币、网络银行等，使得各种机密信息的安全问题越来越重要 。
  - 计算机犯罪事件逐年攀升，已成为普遍的国际性问题。随着国际信息化加快，形成一个“地球村”，利用计算机及网络发起的网络安全事件频繁出现。不但影响到普通用户，也影响到国与国的关系。

国 际 背 景—中美黑客大战

2001年4月1日，美国一架侦察机在中国南海上空活动，中国派出两架军用飞机机对其进行监视。不料美机突然转向，向中方飞机直冲过来，导致其机头和左翼与中方一架飞机相撞坠毁。而当时驾驶这架飞机的飞行员王伟，当场机毁人亡。

国 际 背 景—中美黑客大战

事件经过

- 4月1号撞机事件为导火线。
- 4月初，以PoizonBox、Prophet为代表的美国黑客组织对中国国内站点进行攻击，约300个左右的网站页面被攻击修改。
- 4月下旬，国内红（黑）组织或个人开始对美国网站进行小规模攻击。26日有人发表了“五一卫国网站”的战前声明，宣布将在5月1日至8日，对美国网站进行大规模攻击。
- 美国当地时间5月4日上午9时到上午11时15分，美国白宫网站在数万人的攻击之下，被迫关闭了两个多小时。
- 随着各大媒体纷纷报到，评论，5月中旬结束大战。

被美国黑客更改的网页

国内某大型商业网站

国内某政府网站

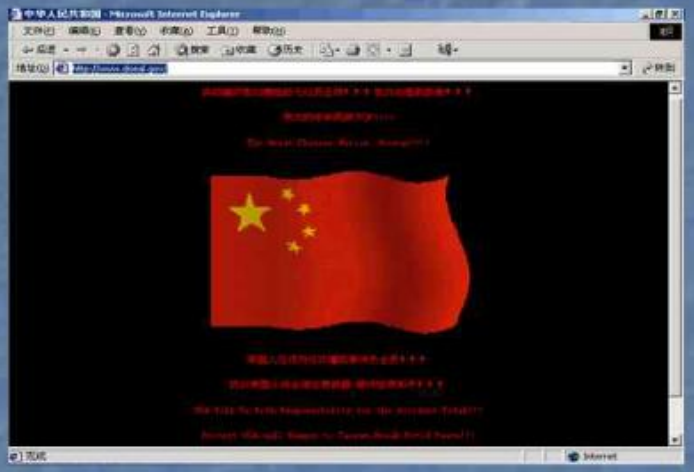
中国科学院心理研究所

中经网数据有限公司

国内黑客组织更改的美国网站

美国某大型商业网站

美国某政府网站



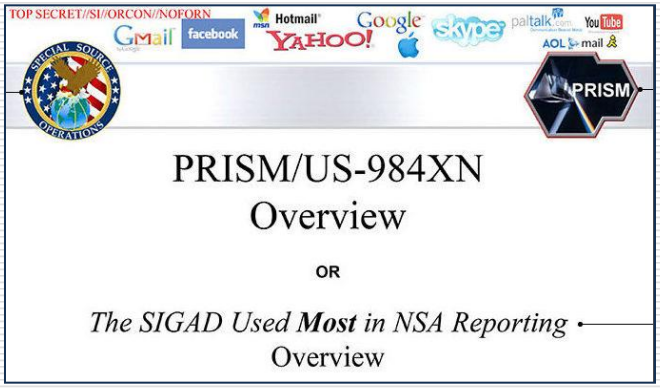
美国劳工部网站

美国某节点网站

国 际 背 景

美国一直大范围攻击中国网络

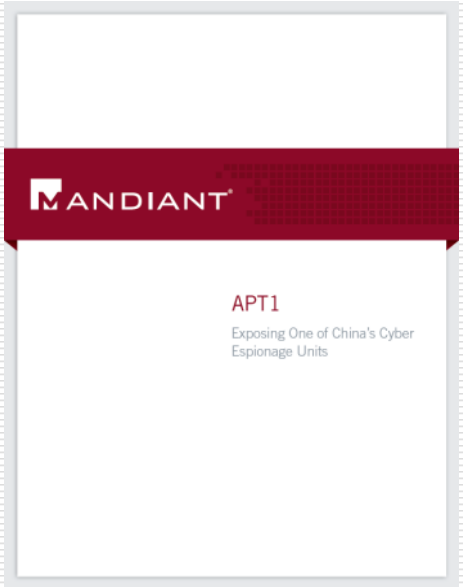
- 2013年，“斯诺登事件”彻底曝光了美国以“棱镜”为代号的全球网络监控项目，中国就是最大的受害国。
- 长期以来，美国对中国政府部门、机构、企业、大学、电信主干网络进行大规模监控。



国 际 背 景

美国一直就网络攻击问题施压中国

2013年2月19日，美国网络安全公司Mandiant称141家企业遭到总部位于上海浦东一栋12层白色建筑内的黑客攻击，隶属于中国人民解放军61398部队。



61398部队

国 际 背 景

美国一直就网络攻击问题施压中国

2014年5月19日，美国司法部对5名中国人民解放军军官提起网络间谍罪的刑事指控，声称他们涉嫌利用安全漏洞侵入美国能源、金属和太阳能企业的电脑窃取商业机密。被指控的五人都为61398部队工作。

国 际 背 景

出台《个人信息保护法》

2021年8月20日，第十三届全国人民代表大会常务委员会第三十次会议通过《中华人民共和国个人信息保护法》（以下简称“个保法”），该法案将在2021年11月1日起实施。

作为个人信息保护方面的专门立法，个保法包含了个人信息保护的基本原则、要求及相关制度。在前序文章中，我们分享了个保法原文（批准稿）以及与二审稿比较的异同，本次我们将与大家补充剖析个保法中亮点制度的立法本意及相关影响，包括数据保护立法体系内的冲突及兼容，与其他数据保护立法（如GDPR）之间的差异、立法原意及保留条款，并最终给出这些制度对企业隐私保护治理的影响及建议。

国 际 背 景

出台《个人信息保护法》

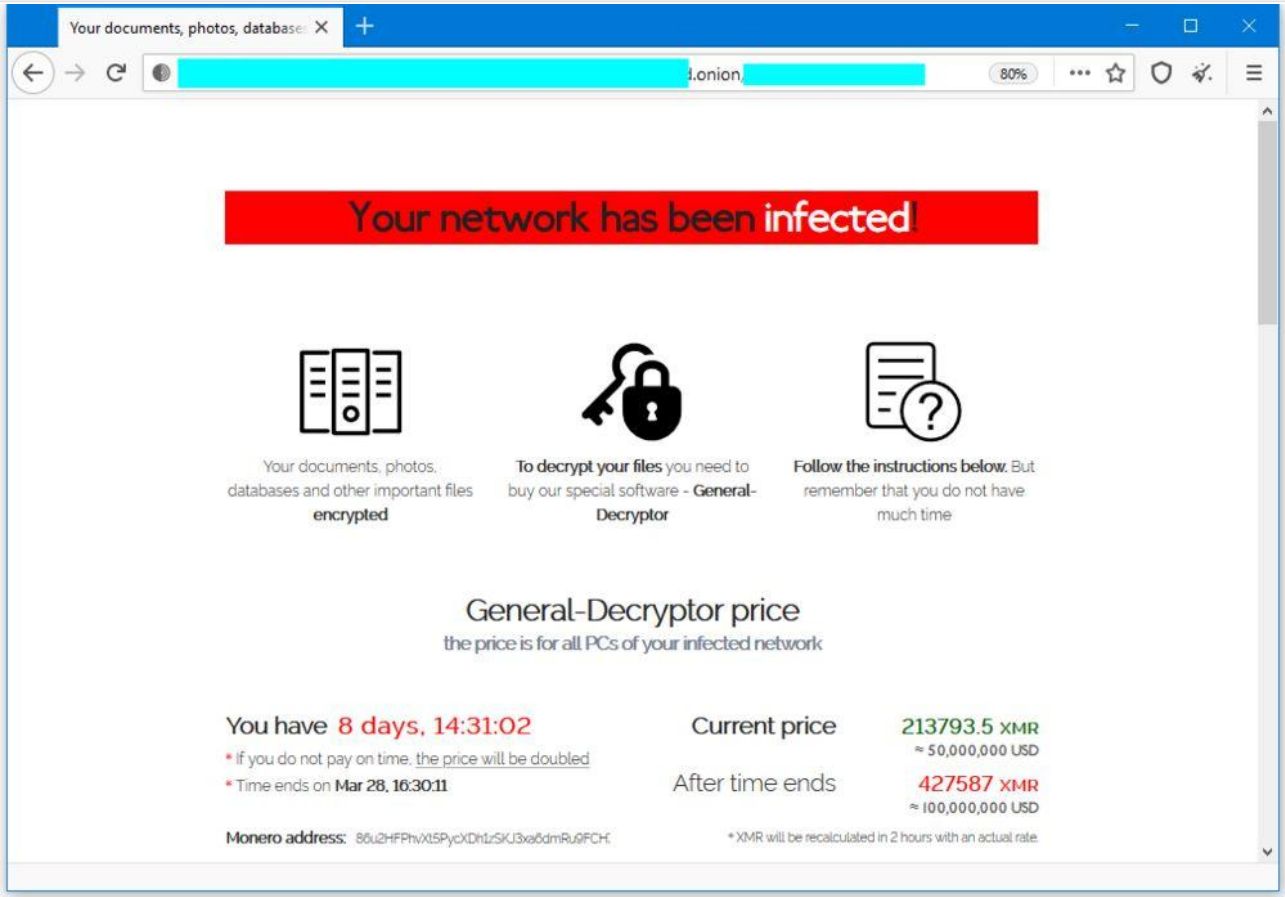
2021年网络攻击案例 Accellion攻击

2021年2月，美国、加拿大、新加坡、荷兰和其他国家/地区的多个组织遭遇了严重的数据泄露，这是由于Accellion 的文件传输服务存在漏洞。零售巨头克罗格是最大的受害者之一，其药房和诊所服务的员工和数百万客户的数据被暴露。这次攻击归因于与 Cl0p 勒索软件家族和 FIN11（一个出于经济动机的 APT 组织）有联系的威胁行为者，展示了勒索软件供应链攻击的危险性

2021年网络攻击案例 宏碁遭勒索软件攻击

2021年3月，总部位于台湾的跨国电脑制造商宏碁遭到赎金攻击，攻击者REvil组织公布了入侵宏碁系统的截图，并索要5,000万美元，是当时为止已知的最大的网络犯罪赎金，当宏碁拒绝支付赎金的时候，REvil 便在暗网上公布了窃取而来的资料，包含宏碁财务的表格、银行结余、银行通讯文档等机密材料。

2021年网络攻击案例 宏碁遭勒索软件攻击



2021年网络攻击案例

ColonialPipeline感染勒索软件

5 月份，美国最大的燃料管道公司Colonial Pipeline遭到勒索软件攻击，5500英里输油管停运，引发了美国东海岸大部分地区的暂时天然气短缺。此次勒索攻击事件与总部位于俄罗斯的 DarkSide 的组织有关。DarkSide 使用被盗的旧 VPN 凭据获得了对 Colonial Pipeline 网络的访问权限。这次攻击行为的影响将勒索软件提升为国家安全级别的担忧，并引发了白宫的反应。事件发生几天后，拜登总统发布了一项行政命令，要求联邦机构实施新的控制措施以加强网络安全。

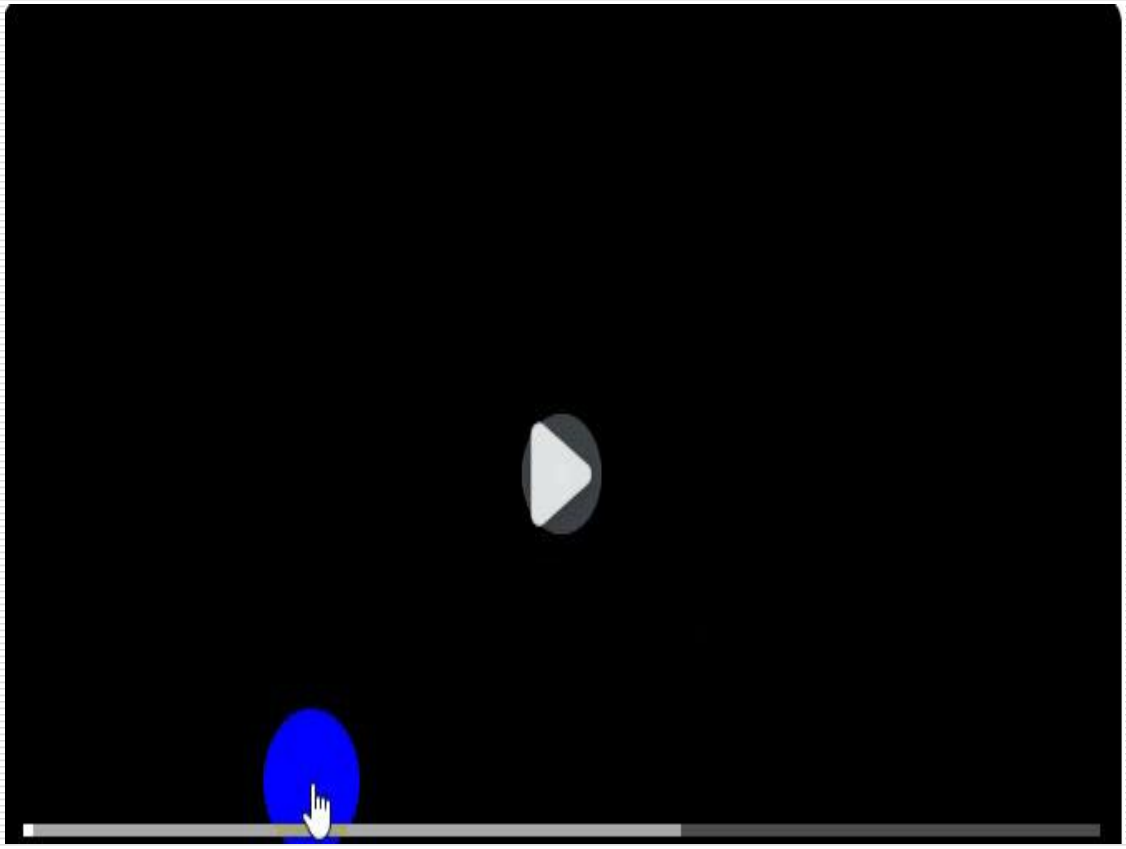
2021年网络攻击案例

Kaseya公司感染勒索软件

7 月初，IT 管理软件供应商 Kaseya 的系统被黑客入侵。黑客通过使用该公司的VSA产品来感染用户，然后再通过勒索软件来攻击这些用户。受害者中有瑞典杂货连锁店Coop，这是Kaseya客户之一，该事件目前已经导致Coop的500家商店店面关闭。信息安全公司Huntress称，至少有200家企业受到影响。该事件后来归因于 REvil/Sodinokibi 勒索软件组织的一个附属机构，其中涉及威胁行为者利用 Kaseya 的虚拟系统管理员 (VSA) 技术中的一组三个漏洞，许多托管服务提供商 (MSP) 使用这些漏洞来管理其客户的网络。攻击者利用这些漏洞利用 Kaseya VSA 在属于 MSP 下游客户的数千个系统上分发勒索软件。

2021年网络攻击案例

Kaseya公司感染勒索软件



2021年网络攻击案例 Log4j漏洞

2021年12月9日，Log4j2 日志记录框架中的一个严重的远程代码执行漏洞震撼了整个行业。Log4j2工具在企业、运营技术 (OT)、软件即服务 (SaaS) 和云服务提供商 (CSP) 环境中普遍使用，而且相对容易利用。该漏洞为攻击者提供了一种远程控制服务器、PC 和任何其他设备的方法，包括存在日志工具的关键 OT 和工业控制系统 (ICS) 环境中的设备。该漏洞（CVE-2021-44228）存在于 Log4j 2.0到 Log4j 2.15.0-RC1 版本中，可以通过多种方式利用。媒体报道称，比利时国防部网络最近受到不明攻击者的成功攻击，攻击者利用Apache log4j2的巨大漏洞实施攻击。

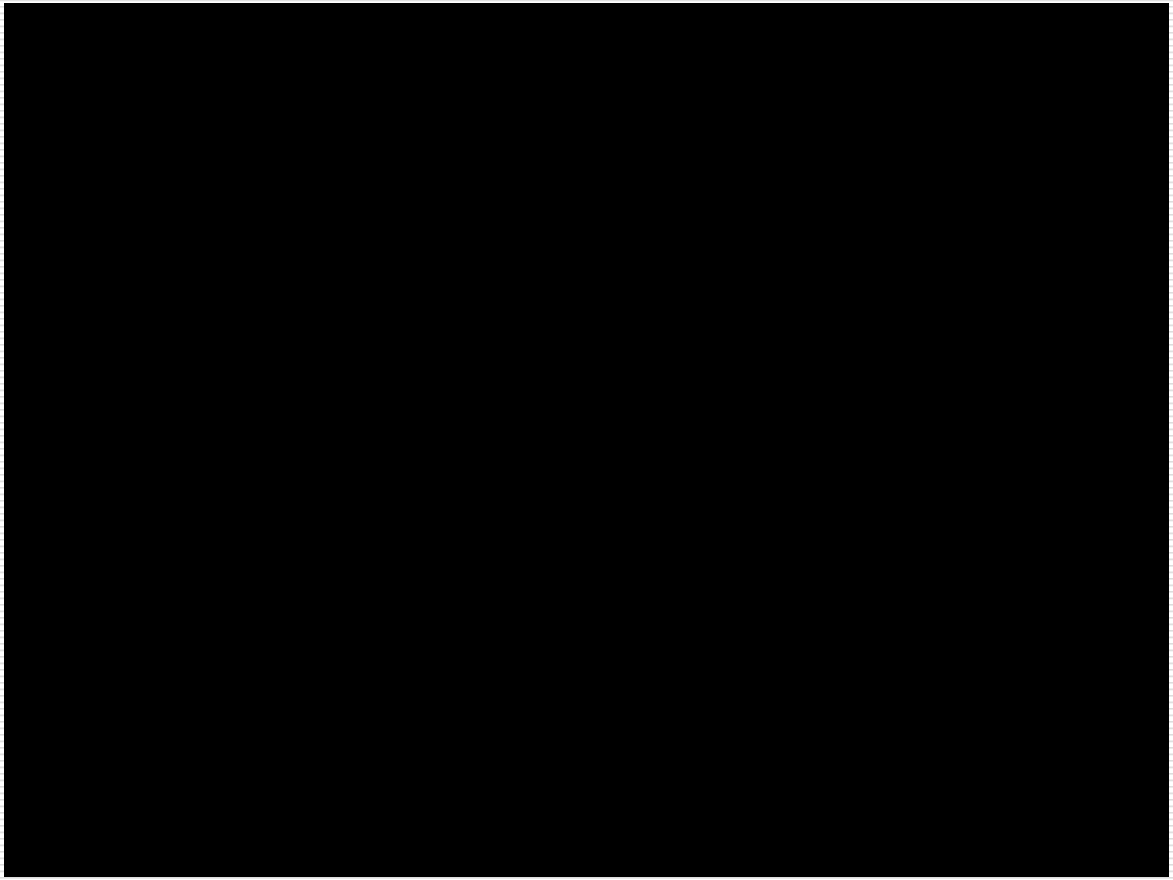
2021年网络攻击案例 Log4j漏洞

2021年网络攻击案例

Log4j漏洞

2021年网络攻击案例

Log4j漏洞



2021年网络攻击案例

Log4j漏洞

Apache log4j2是一款Apache软件基金会的开源基础框架,用于 Java 日志记录的工具,主要用来监视代码中变量的变化情况，周期性地记录到文件中供其他应用进行统计分析工作；跟踪代码运行时轨迹，作为日后审计的依据；担当集成开发环境中的调试器的作用，向文件或控制台打印代码的调试信息。其在JAVA生态环境中应用极其广泛,影响巨大。该漏洞的触发点在于利用org.apache.logging.log4j.Logger进行log或error等记录操作时未对日志message信息进行有效检查,从而导致漏洞发生。

2021年网络攻击案例

Log4j漏洞后续

据 21 世纪经济报道，近期，工业和信息化部网络安全管理局通报称，阿里云计算有限公司（简称“阿里云”）是工信部网络安全威胁信息共享平台合作单位。近日，阿里云公司发现阿帕奇（Apache）Log4j2 组件严重安全漏洞隐患后，未及时向电信主管部门报告，未有效支撑工信部开展网络安全威胁和漏洞管理。经研究，现暂停阿里云公司作为上述合作单位 6 个月。暂停期满后，根据阿里云公司整改情况，研究恢复其上述合作单位。

2021年网络攻击案例

国内外漏洞上报比较

国内外漏洞上报差异:

- 国内：网络产品提供者须在2日内向工信部报送相关漏洞信息；向社会发布安全漏洞信息的组织或个人不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供等等。
- 美国：与联邦机构签订合同的信息和通信技术 **(ICT)** 服务提供商在发现涉及向其提供的软件产品或服务（涉及到联邦机构信息系统）的网络事件时，必须立即向此类机构报告。另外，**ICT**服务提供商在向联邦民事行政部门 **(FCEB)** 机构报告时也必须直接向网络安全和基础设施安全局（**CISA**）报告，并且 **CISA**必须集中收集和管理此类信息等待。
- 英国：英国国家网络安全中心（**NCSC**）建议企业应避免强迫漏洞披露者签署保密协议，因为个人只是想确保漏洞已得到修复。另外，让研究人员了解漏洞的处理进展也很重要，这表明对漏洞披露的透明及赞赏。

2021年网络攻击案例

国内外漏洞上报比较

国内外漏洞上报差异:

- 日本：新设以内阁官房长官为首的“网络安全战略本部”，协调各政府部门的网络安全对策，与日本国家安全保障会议、IT综合战略本部等其他相关机构加强合作。且电力、金融等重要社会基础设施运营商、网络相关企业、地方自治体等有义务配合网络安全相关举措或提供相关情报
- 欧盟：成员国应确保核心服务运营商采取合理及适度的技术和组织措施，以应对其运营所使用的网络与信息系统安全中存在的风险，应要求各公司上报具有“重大破坏性影响”的事故，报告中须包括所有与事故相关的信息，以使得主管部门或CSIRT确定该事故的跨境影响。非提供核心服务的公司可以自愿报告对其所提供的服务持续性具有重大影响的事故。另外，像谷歌和亚马逊这样的网络公司巨头在发生黑客袭击事件后，必须向有关部门报备。

2021年网络攻击案例

Log4j漏洞后续

思考：

- 国内公司发现了产品漏洞是应该先采取防御措施还是应该先报告给工信部？

- 对于中国公民开在国外的公司，一旦发现了漏洞是遵循中国的上报措施还是遵循当地国家的上报措施？

信息化与国家安全——信息战

- “谁掌握了信息，控制了网络，谁将拥有整个世界。”

——美国著名未来学家阿尔温.托尔勒

- “今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

——美国总统克林顿

- “信息时代的出现，将从根本上改变战争的进行方式。”

——美国前陆军参谋长沙利文上将

美国网络安全规划

- 联邦政府第一个大规模网络防御计划
- 保护联邦政府网络基础设施
- 分三期建设，历时五年，耗资数十亿美金
- 第三期合入美国国家网络安全计划（CNCI）

美国网络安全规划

- 美国国家网络安全综合计划：CNCI（300 ~ 400亿美金）
- 美国网络安全最高指挥协调机构：网络沙皇
- 美国网络打击力量：网络司令部 & 网络部队

2008年1月：布什签发了第54号国家安全总统令/第24号国土安全总统令，即：CNCI

美国网络战打击力量一览

美国网络战的尖刀：第24航空队，2010年1月25日成立，人数超过10000人

美国网络部队：27支防御部队 + 13支攻击部队，总人数超10万，其中司令部人员4900人，由电脑专家、职业黑客组成，大多数成员智商140以上，被外界称为“140”部队

位于美国马里兰州米德基地的美国网战部队总部

美国对网络空间的主导思想

- 将网络空间列为与陆、海、空、太空同等重要的第五空间

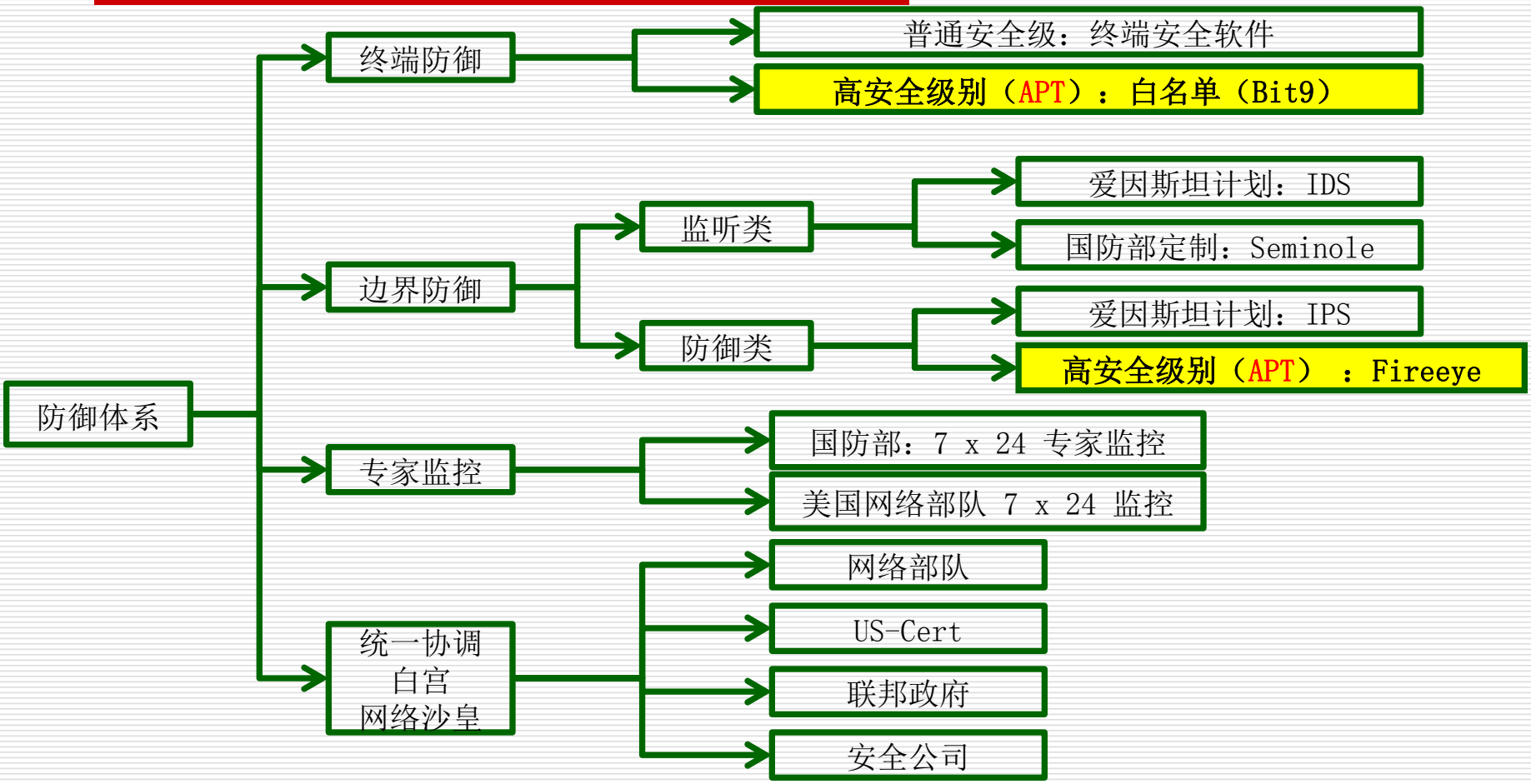
2005年3月，美国国防部，《国防战略报告》：将网络空间和陆、海、空、太空定义为同等重要、需要美国维持决定性优势的五大空间

- 网络安全项目优先

奥巴马：把保护美国**最重要**的计算机网络的安全作为美国国家和经济安全**最优先**项目

- 主动进攻，先发制人
  - 五角大楼最近的一份报告在一条条款建议，当美国遭受网络攻击时，有一种应对选择是发射核武器
  - 奥巴马2012年签署一份密令，要求在美国面临可能导致死亡或者损害国家安全的"迫在眉睫"时，就采取军事网络行动阻止

美国网络防御体系


防御体系
终端防御
普通安全级：终端安全软件
高安全级别（APT）：白名单（Bit9）
边界防御
监听类
爱因斯坦计划：IDS
国防部定制：Seminole
防御类
爱因斯坦计划：IPS
高安全级别（APT）：Fireeye
专家监控
国防部：7 x 24 专家监控
美国网络部队 7 x 24 监控
统一协调
白宫
网络沙皇
网络部队
US-Cert
联邦政府
安全公司

中国网络安全规划

- **2014年2月27日，中央网络安全和信息化领导小组召开第一次会议，组长习近平，副组长李克强、刘云山。**

没有网络安全，

就没有国家安全

中国网络安全法

- 《中华人民共和国网络安全法》是为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定的法律。
- 由全国人民代表大会常务委员会于**2016**年**11**月**7**日发布，自**2017**年**6**月**1**日起施行。中华人民共和国主席令（第五十三号）公布。

中国网络安全规划

- **2018年3月，根据中共中央印发了《深化党和国家机构改革方案》，将中央网络安全和信息化领导小组改为中国共产党中央网络安全和信息化委员会。**
- **2019年3月12日，教育部办公厅印发的《2019年教育信息化和网络安全工作要点》（下称"工作要点"）中表示，将加快推进网络安全领域新工科建设，推进产学合作协同育人，引导鼓励有条件的职业院校开设网络安全类专业。**

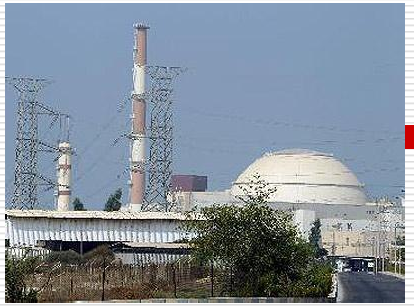
我国互联网网络安全形势1

- 网络基础设施运行总体平稳，但依然面临严峻挑战。
- 网站被植入后门等隐蔽性攻击事件呈增长态势，网站用户信息成为黑客窃取的重点。
- 网络钓鱼日渐猖獗，严重影响在线金融服务和电子商务的发展，危害公众利益。
- 移动互联网恶意程序数量急剧增，**Android**平台成为安全重灾区。

我国互联网网络安全形势2

- 拒绝服务攻击仍然是影响互联网运行安全最主要的威胁之一。
- 实施**APT**攻击(**Advanced Persistent Threat**，高级持续性攻击)的恶意程序频被披露，国家和企业的数据安全面临严重威胁。
- 安全漏洞旧洞未补新漏洞迭出，留下安全隐患。
- 我国面临的境外攻击威胁依然严重。

APT 攻击



2004 – 2011 年之间，美国、以色列针对伊朗核设施的“震网攻击”

2012年，伊朗利用GPS漏洞俘获美国无人机

2013年5月，韩国多家银行和电视台遭遇黑客攻击，网络大面积瘫痪

- 2012年，我国涉密单位发现一个已经潜伏了长达7年之久的恶意代码
- 2013年斯诺登爆料：美国曾入侵中国移动网络获取大量短信信息，同时斯诺登也证明，美国用类似的方式入侵了清华大学的教育网节点
- 在2010 – 2013年期间，奇虎360内网遭遇过至少2次APT攻击渗透
- ……

漏洞概念

背景

- 随着黑客攻击事件数量的不断上升，各种计算机病毒和其他恶意程序在网络上大肆泛滥，信息安全面临诸多挑战，逐渐成为人们眼中的焦点。
- 信息安全的一个核心问题就是存在于计算机系统和网络系统中的安全漏洞。恶意的攻击者可以利用这些安全漏洞访问未授权资源，破坏敏感数据，进而威胁信息系统的安全。安全漏洞作为安全问题的焦点越来越受到人们的重视。

漏洞的概念

- 安全漏洞：是指信息系统在设计、实现或者运行管理过程中存在的缺陷或不足，从而使攻击者能够在未授权的情况下利用这些缺陷破坏系统的安全策略。
- 存在于信息系统的需求、设计、实现、配置、运行等环境
- 能够被恶意主体所利用，影响信息系统及其服务的正常运行
- 网络攻防的核心：
  - 攻击----漏洞利用
  - 防御----漏洞修复

Note：
*这里对于攻防的理解是比较简单和直接，当然攻防还包括除漏洞以外的技术和手段。


国家计算机网络入侵防范中心
NATIONAL COMPUTER NETWORK INTRUSION PROTECTION CENTER
网站首页
中心简介
新闻中心
安全漏洞
联系我们
您当前的位置是：安全漏洞 | 漏洞库
搜索
首页
网站首页
中心简介
中心概况
组织结构
新闻中心
新闻动态
安全公告
安全漏洞
漏洞库
漏洞检索
漏洞周报
漏洞月报
其他
联系我们
漏洞库结果显示列表
严重级别：
紧急
高
中
第一页 ------ ------ 最后一页
1
总共有 7 条匹配结果，共有 1 页，现为第
NIPC-2011-2075 Android Picasa访问权限获取漏洞
NIPC-2009-2829 Open Handset Alliance Android SMS
(2009-08-03)
NIPC-2009-2693 Android手机平台权限验证多个绕过安
17)
NIPC-2009-2098 Android ' PackageManagerService类
05-26)
NIPC-2009-0688 Open Handset Alliance Android M多
17)
NIPC-2008-0618 Android软件开发工具包BMP文件处理
05)
NIPC-2008-0617 Android Web浏览器GIF文件堆溢出漏


总共有 26 条匹配结果，共有 2 页，现为第 1页
NIPC-2010-4265 Apple iOS 堆缓冲区溢出漏洞 (2010-11-26)
NIPC-2010-4264 Apple iOS 不安全通信漏洞 (2010-11-26)
NIPC-2010-4263 Apple iOS权限提升漏洞 (2010-11-26)
NIPC-2010-4262 Apple iOS 未指明漏洞 (2010-11-26)
NIPC-2010-4261 Apple iOS 未指明漏洞 (2010-11-26)
NIPC-2010-4260 Apple iOS 验证不充分漏洞 (2010-11-26)
NIPC-2010-3354 Apple iOS ImageIO缓冲区溢出漏洞 (2010-09-09)
NIPC-2010-3353 Apple iOS WebKit对象释放后再利用漏洞 (2010-09-09)
NIPC-2010-3352 Apple iOS WebKit远程代码执行漏洞 (2010-09-09)
NIPC-2010-3351 Apple iOS WebKit远程代码执行漏洞 (2010-09-09)
NIPC-2010-3350 Apple iOS WebKit对象释放后再利用漏洞 (2010-09-09)
NIPC-2010-3349 Apple iOS ImageIO远程代码执行漏洞 (2010-09-09)
NIPC-2010-3347 Apple iOS Accessibility组件未指明漏洞 (2010-09-09)
NIPC-2010-3346 Apple iOS WebKit重复释放漏洞 (2010-09-09)

国家计算机网络入侵防范中心

NATIONAL COMPUTER NETWORK INTRUSION PROTECTION CENTER

网站首页 中心简介 新闻中心 安全漏洞

您当前的位置是：安全漏洞 | 漏洞库

首页
网站首页
中心简介
中心概况
组织结构
新闻中心
新闻动态
安全公告
安全漏洞
漏洞库
漏洞检索
漏洞周报
漏洞月报
其他
联系我们

漏洞库

严重级别: 紧急

第一页 ----

总共有 7 条匹配结

NIPC-2011-2075 Android Pi

NIPC-2009-2829 Open Hands (2009-08-03)

NIPC-2009-2693 Android手 17)

NIPC-2009-2098 Android ' 05-26)

NIPC-2009-0688 Open Hands 17)

NIPC-2008-0618 Android软 05)

NIPC-2008-0617 Android We

Microsoft Internet Explorer 安全漏洞(MS15-124) (MS15-125)

漏洞编号： NIPC-2015-5562

CVE编号： CVE-2015-6142

漏洞类别： 许可，权限和访问控制错误

发布日期： 2015-12-09

更新日期： 2015-12-09

CVSS值： 9.3

严重级别： 紧急

利用范围： 网络

攻击复杂度： 中

认证级别： 没有

机密性影响： 整体

完整性影响： 整体

可用性影响： 整体

漏洞描述：

Microsoft Internet Explorer 中存在安全漏洞，受影响的产品，11 和 Microsoft Edge，由于对内存缓冲区的创建、修改、管理或删除有误，允许远程攻击者，通过精心构造的 web 站点执行任意代码或者引起拒绝服务攻击（内存破坏）.

受影响系统或软件：

Denotes Vulnerable Software Changes related to vulnerability configurations

解决方案：

商已修复该漏洞

参考资源：

ttp://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-0151201-wmc

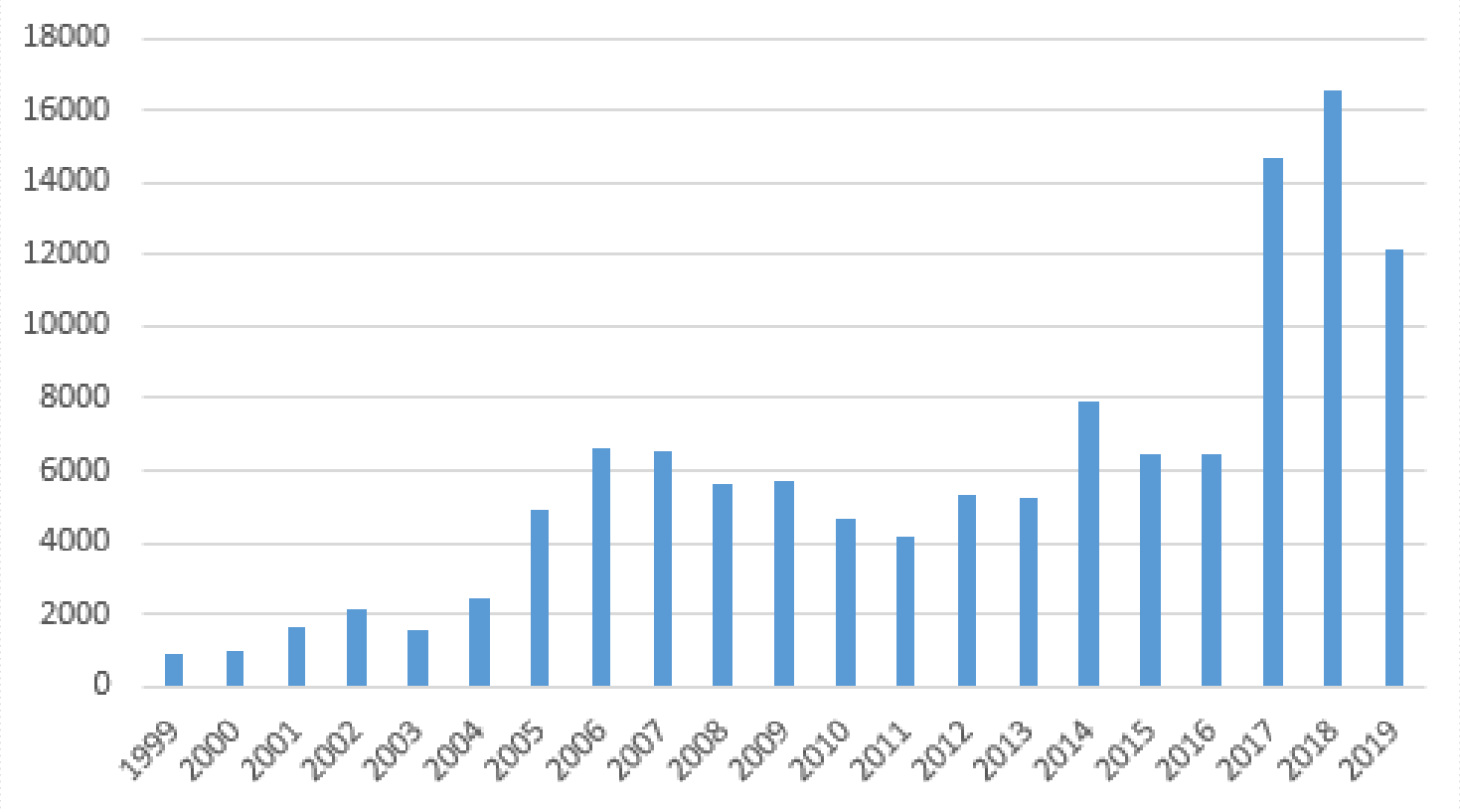
0 day漏洞

- 0 day漏洞，又称零日漏洞，指在安全补丁发布前被了解和掌握的漏洞信息。利用0 day漏洞的攻击称为0 day攻击。
  - 2006年9月27日，微软提前发布MS06-055漏洞补丁，修补了一个严重等级的IE图像处理漏洞。事实上，这个漏洞在当时属于零日漏洞，因为在微软公布补丁之前一个星期就已经出现了利用这个漏洞的网马。
- 谁在使用0 day漏洞：
  - 安全部门、渗透测试人员、黑客、甚至是蠕虫...

安全漏洞急剧增长

- 漏洞数量急剧增长
  - 美国国家漏洞数据库NVD披露的历年漏洞记录数量，2017年的漏洞记录数超过了2016年全年的漏洞记录数的2倍。
  - 根据Exploit-DB的统计数据，2017年共接收漏洞报告2127份，相比于2016年接收漏洞报告1548份，增幅37.4%。
  - 同时，多种原因导致漏洞修复的周期较长、进程缓慢，日益增多的存量漏洞和每日新增漏洞是基础信息网络和重要信息系统的主要安全隐患。

NVD漏洞详情



美国国家漏洞数据库NVD披露的历年漏洞记录数量

安全漏洞（以微软为例）

- 系统安全漏洞
  - 微软每周都有数个修正档需要更新
  - 案例：在2013年7月的"补丁星期二"(Patch Tuesday)那天，微软总共发布了7个安全公告，而其中有6个都属于"关键"(Critical)级别。
  - 微软MS08-067漏洞引发“扫荡波”
- 难题
  - 无法知道哪些机器没有安装漏洞补丁
  - 知道哪些机器但是找不到机器在哪里
  - 机器太多不知如何做起

网络安全现状（续）

- **安全漏洞数量增长较快，0 day攻击频繁**
  - 常用系统的安全漏洞保持递增趋势。
  - 路由器、交换机等网络硬件设备的严重级别漏洞增多。
  - 针对漏洞的攻击程序呈现出目的性强、时效性高的趋势，0 day攻击现象严重。
  - 各类应用软件的安全漏洞尚未引起足够重视。

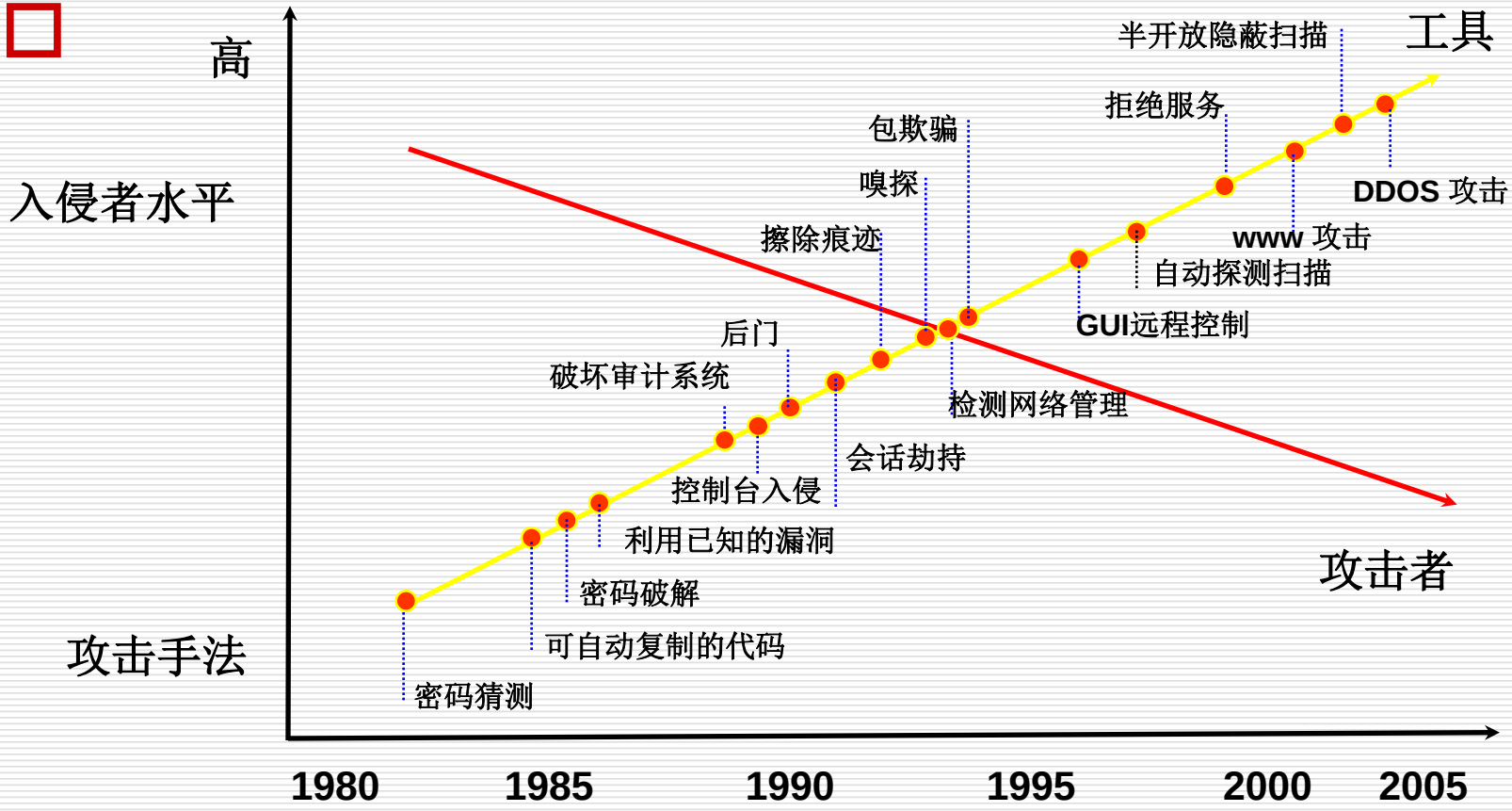
网络安全现状（续）

- 攻击者需要的技术水平逐渐降低，手段更加灵活，联合攻击急剧增多
  - 攻击工具易于从网络下载
  - 网络蠕虫具有隐蔽性、传染性、破坏性、自主攻击能力
  - 新一代网络蠕虫和黑客攻击、计算机病毒之间的界限越来越模糊

网络安全现状（续）

- **网络攻击趋利性增强、顽固性增加**
  - 木马类病毒的利益威胁最为严重；
  - 病毒传播的趋利性日益突出；
  - 病毒的反杀能力不断增强；
  - 网络攻击的组织性、趋利性、专业性和定向性继续加强，地下产业链逐步形成。

常见的黑客攻击及入侵技术的发展



1.3 网络安全的主要威胁因素

- 信息系统自身安全的脆弱性
- 操作系统与应用程序漏洞
- 安全管理问题
- 黑客攻击
- 感染病毒
- 网络犯罪

信息系统自身的安全脆弱性

- 信息系统脆弱性，指信息系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因而可能导致系统受到破坏、更改、泄露和功能失效，从而使系统处于异常状态，甚至崩溃瘫痪等的根源和起因。
- 这里我们从以下三个层面分别进行分析：
  - 操作系统
  - 计算机系统
  - 网络通信协议

操作系统的脆弱性

- 操作系统支持的程序动态连接与数据动态交换是现在系统集成和系统扩展的必备功能，而动态连接、I/O程序与系统服务、打补丁升级可被攻击者利用，滋生病毒。
- 操作系统可以创建进程，及时在网络的节点上同样也可以进行远程的创建于激活，且该进程有继续创建集成的权力，加上操作系统支持在网络上传输文件，在网络上能加载程序二者结合起来就可以在远端服务器上安装“间谍”软件，常以打补丁的方式躲避监测。
- 守护进程具有操作系统核心层软件的同等权力，会被黑客利用。
- 网络操作系统提供的远程过程调用服务以及它所安排的无口令入口也是攻击者的通道。

计算机系统的脆弱性

- 计算机系统存在超级用户，一旦口令泄露，整个系统将受控于入侵者。
- 计算机可能因硬件或软件故障停止运转，或被入侵者利用造成损失。硬盘故障、电源故障和芯片故障都是人们应考虑的硬件故障问题。软件故障可出现在操作系统中，也可能出现在应用软件中，主要是由于软件设计中的疏忽，功能冗余、逻辑混乱等。

网络和通信协议的安全隐患

- 协议：指计算机通信的共同语言，是通信双方约定好的彼此遵循的一定规则。
- **TCP/IP**协议簇是目前使用最广泛的协议，但其已经暴露出许多安全问题。
  - IP欺骗
  - TCP序列猜测
  - 路由选择信息协议攻击
  - TCP/IP协议数据采用明文传输
  - 其它应用层协议问题

TCP/IP协议簇脆弱性原因

- 支持Internet运行的TCP/IP协议栈最初设计的应用环境是相互信任的，其设计原则是简单、可扩展、尽力而为，只考虑互联互通和资源共享问题，并未考虑也无法兼顾解决网络中的安全问题。
- 基于TCP/IP的Internet是在可信任网络环境中开发出来的成果，体现在TCP/IP协议上的总体构想和设计本身，基本未考虑安全问题，并不提供人们所需的安全性和保密性。

操作系统与应用程序漏洞

- 漏洞是计算机系统在硬件、软件、协议等具体实现或系统安全策略上存在的缺陷和不足。
- 这些缺陷以不同形式存在于信息系统的各个层次和环节之中，一旦被恶意主体所利用和进行攻击，就会对信息系统的安全造成损害，从而影响构建于信息系统之上正常服务的运行，危害信息系统及信息的安全，窃取用户隐私信息，进而对用户、社会以及国家等造成重大损失。

操作系统与应用程序漏洞

- 操作系统是用户和硬件设备的中间层，操作系统一般都自带一些应用程序或者安装一些其它厂商的软件工具。
- 应用软件在程序实现时的错误，往往就会给系统带来漏洞。漏洞也叫脆弱性**(Vulnerability)**，是计算机系统在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷和不足。
- 漏洞一旦被发现，就可以被攻击者用来在未授权的情况下访问或破坏系统，从而导致危害计算机系统安全的行为。

信息系统面临的安全威胁

- 基本威胁
- 威胁信息系统的主要方法
- 威胁和攻击的来源

基本威胁

- 安全的基本目标是实现信息的机密性、完整性、可用性。对信息系统这3个基本目标的威胁即是基本威胁。
  - 信息泄漏
  - 完整性破坏
  - 拒绝服务
  - 未授权访问

基本威胁1—信息泄漏

- 信息泄漏指敏感数据在有意或无意中被泄漏、丢失或透露给某个未授权的实体。
- 信息泄漏包括：信息在传输中被丢失或泄漏；通过信息流向、流量、通信频度和长度等参数等分析，推测出有用信息。

基本威胁2—完整性破坏

- 以非法手段取得对信息的管理权，通过未授权的创建、修改、删除和重放等操作而使数据的完整性受到破坏。

基本威胁3—拒绝服务

- 信息或信息系统资源等被利用价值或服务能力下降或丧失。
- 产生服务拒绝的原因：
  - 受到攻击所致。攻击者通过对系统进行非法的、根本无法成功的访问尝试而产生过量的系统负载，从而导致系统的资源对合法用户的服务能力下降或丧失。
  - 信息系统或组件在物理上或逻辑上受到破坏而中断服务。

基本威胁4—未授权访问

- 未授权实体非法访问信息系统资源，或授权实体超越权限访问信息系统资源。
- 非法访问主要有：假冒和盗用合法用户身份攻击、非法进入网络系统进行违法操作，合法用户以未授权的方式进行操作等形式。

威胁信息系统的主要方法

- 冒充
- 旁路控制
- 破坏信息的完整性
- 破坏系统的可用性
- 重放
- 截收和辐射侦测
- 陷门
- 特洛伊木马
- 抵赖

威胁方法1—冒充

- 某个未授权的实体假装成另一个不同的实体，进而非法获取系统的访问权利或得到额外特权。
- 攻击者可以进行下列假冒：
  - 假冒管理者发布命令和调阅密件；
  - 假冒主机欺骗合法主机及合法用户；
  - 假冒网络控制程序套取或修改使用权限、口令、密钥等信息，越权使用网络设备和资源；
  - 接管合法用户欺骗系统，占用合法用户资源。

威胁方法2—旁路控制

- 攻击者为信息系统等鉴别或者访问控制机制设置旁路。
- 为了获取未授权的权利，攻击者会发掘系统的缺陷或安全上的某些脆弱点，并加以利用，以绕过系统访问控制而渗入到系统内部。

威胁方法3—破坏信息完整性

- 攻击者可从三个方面破坏信息到完整性：
  - 篡改：改变信息流的次序、时序、流向、内容和形式。
  - 删除：删除消息全部和一部分。
  - 插入：在消息中插入一些无意义或有害信息。

威胁方法4-破坏系统可用性

- 攻击者可以从以下三个方面破坏系统可用性：
  - 使合法用户不能正常访问网络资源；
  - 使有严格时间要求的服务不能即时得到响应；
  - 摧毁系统。如，物理破坏网络系统和设备组件使网络不可用，或破坏网络结构。

威胁方法5－重放

- 攻击者截收有效信息甚至是密文，在后续攻击时重放所截收的消息。

威胁方法6—截收与辐射侦测

- 攻击者通过搭线窃听和对电磁辐射探测等方法截获机密信息，或者从流量、流向、通信总量和长度等参数分析出有用信息。

威胁方法7—陷门

- 在某个（硬件、软件）系统和某个文件中设计的“机关”，使得当提供特定的输入条件时，允许违反安全策略而产生非授权的影响。
- 陷门通常是设计时插入的一小段程序，用来测试模块或者为程序员提供一些便利。开发后期会去掉这些陷门，可能会基于某种目的得到保留。
- 陷门被利用，会带来严重后果。

威胁方法8—特洛伊木马

- 指一类恶意的妨害安全的计算机程序或者攻击手段。
- 形象的来说，是指：一个应用程序表面上在执行一个任务，实际上却在执行另一个任务。以达到泄漏机密信息甚至破坏系统的目的。

威胁方法9—抵赖

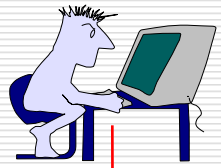
- 通信的某一方出于某种目的而出现下列抵赖行为：
  - 发信者事后否认曾经发送过某些消息；
  - 发信者事后否认曾经发送过的某些消息的内容；
  - 收信者事后否认曾经接受过某些消息；
  - 收信者事后否认曾经接受过某些消息的内容。

威胁和攻击来源

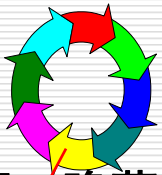
- 内部操作不当
  - 信息系统内部工作人员越权操作、违规操作或其他不当操作，可能造成重大安全事故。
- 内部管理不严造成信息系统安全管理失控
  - 信息体系内部缺乏健全管理制度或制度执行不力，给内部工作人员违规和犯罪留下缝隙。
- 来自外部的威胁与犯罪
  - 从外部对信息系统进行威胁和攻击的实体主要有黑客、信息间谍、计算机犯罪人员三种。

网络安全主要威胁来源

特洛伊木马

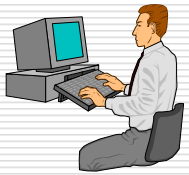


黑客攻击



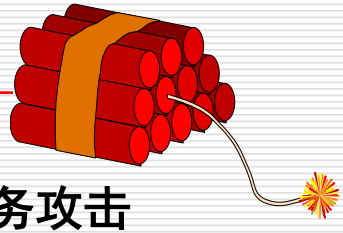
后门、隐蔽通道

计算机病毒

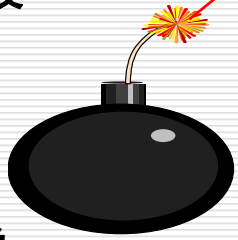


信息丢失、篡改、销毁

网络

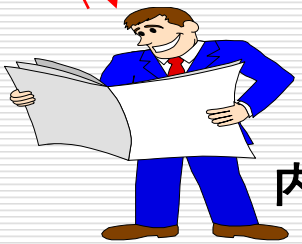


拒绝服务攻击



逻辑炸弹

蠕虫



内部、外部泄密

安全管理问题

- 管理策略不够完善，管理人员素质低下，用户安全意识淡薄，有关的法律规定不够健全。管理上权责不分，缺乏培训意识，管理不够严格。缺乏保密意识，系统密码随意传播，出现问题时相互推卸责任。
- 安全配置不当，例如，防火墙软件配置不正确，那么它根本不会起作用。许多站点在防火墙配置上无意识的扩大了访问权限，忽视了这些权限可能会被其他人利用。除非用户禁止该网络程序或对其进行正确配置，否则，安全隐患始终存在。
- 三分技术，七分管理

黑客攻击

- 黑客（**hacker**），源于英语动词**hack**，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧。
- 他们通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统。

黑客起源

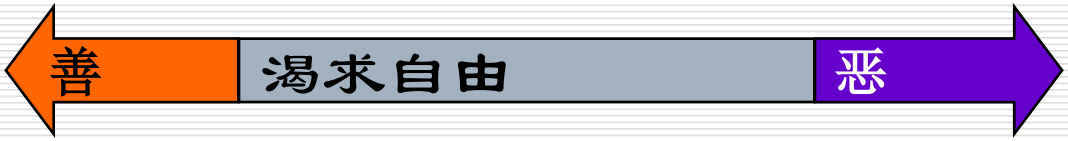
- **起源地：**
  - 美国
- **精神支柱：**
  - 对技术的渴求
  - 对自由的渴求
- **历史背景：**
  - 越战与反战活动
  - 马丁·路德金与自由
  - 嬉皮士与非主流文化
  - 电话飞客与计算机革命

- 中国黑客发展历史
  - 1998年印尼事件
  - 1999年南联盟事件
  - 绿色兵团南北分拆事件
  - 中美五一黑客大战事件
  - ……

黑客攻击

- 黑客基本涵义是指一个拥有熟练电脑技术的人，但大部分的媒体习惯将“黑客”指作电脑侵入者。
- 白帽黑客有能力破坏电脑安全，但不具恶意目的的黑客。白帽子一般有清楚的定义道德规范，并常常试图同企业合作去改善被发现的安全弱点。
- 灰帽黑客对于伦理和法律暧昧不清的黑客。
- 黑帽黑客骇客（“Cracker”的音译，“破解者”意思）：经常使用于区分黑帽子黑客和一般（正面的）有理性的黑客，这个词自1983年开始流行。
- 在中国，人们经常把黑客跟骇客搞混，实际区别很大。

黑客分类



白帽子创新者
- 设计新系统
- 打破常规
- 精研技术
- 勇于创新

没有最好，
只有更好

MS -Bill Gates
GNU -R.Stallman
Linux -Linus

灰帽子破解者
- 破解已有系统
- 发现问题/漏洞
- 突破极限/禁制
- 展现自我

计算机
为人民服务

漏洞发现 - Flashsky
软件破解 - 0 Day
工具提供 - Glacier

黑帽子破坏者
- 随意使用资源
- 恶意破坏
- 散播蠕虫病毒
- 商业间谍

人不为己，
天诛地灭

入侵者 -K.米特尼克
CIH -陈盈豪
攻击Yahoo -匿名

著名黑客 凯文·米特尼克

- Kevin Mitnick：凯文·米特尼克，1964年美国洛杉矶出生，被称为世界上“头号电脑骇客”。
- Robert Tappan Morrisgeek：美国历史上五大最著名的黑客之一。Morris的父亲是前美国国家安全局的一名科学家，叫做Robert Morris。Robert是Morris蠕虫病毒的创造者，也是首个通过互联网传播的蠕虫病毒。因此，他成为了首个被以1986年电脑欺骗和滥用法案起诉的人。

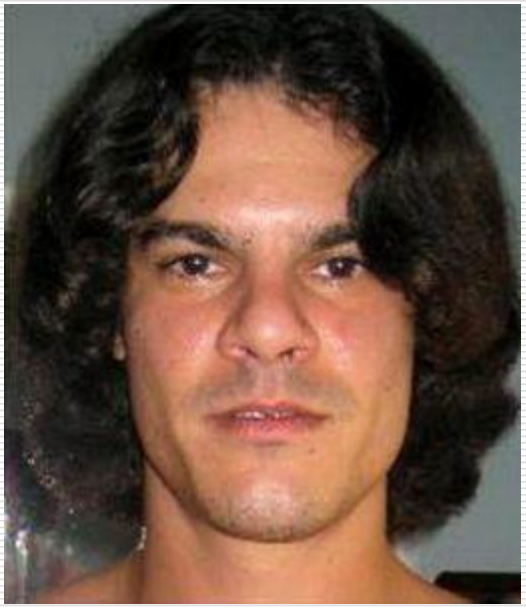
Robert Tappan Morrisgeek.

著名黑客 迈克尔·卡尔斯

迈克尔·卡尔斯现在是计算机安全方面的专家，2000年2月7日，这名当时15岁的加拿大人针对亚马逊、亿贝、国际足联、美国有线电视新闻网和雅虎等公司和机构的网站实施了一系列拒绝服务攻击。

著名黑客 阿尔伯特·冈萨雷斯

阿尔伯特·冈萨雷斯和其同伙在2005年至2007年之间从大约1.8亿个信用卡账户中窃取了数据。2003年，他被指控为黑客组织ShadowCrew的成员，该组织窃取并贩卖了150万个信用卡账户的信息。但他以向当局提供证据和信息免于坐牢。2010年3月，他因黑客行为和窃取多家公司的信息而被判处20年监禁。



中国黑客——龚蔚

- 龚蔚（Goodwell）中国黑客教父，绿色兵团创始人，COG发起人。1999年，龚蔚率领黑客组织“绿色兵团”成立上海绿盟信息技术公司。

- 计算机信息管理专业本科，注册审计师、CISP 认证讲师、ISO27001 审核员、CCIE 安全、CCNP。

中国黑客——袁仁广

- 大兔子(datuzi)，中国国家信息安全漏洞库特聘专家，北京奥运会特聘信息安全专家，现任腾讯湛泸实验室负责人。
- 1999年就曾提出过windows的共享漏洞。

中国黑客——林正隆

- CoolFire，Fetag，中国台湾著名黑客，中国黑客界元老人物，2011年获得COG信息安全终身成就奖。

中国黑客——郭盛华

- 郭盛华，被誉为“黑客教父”。
- 16岁时，郭盛华和他的朋友们组织了一个黑客组织，叫做东方联盟。
- 2013年，日本黑客入侵中国互联网。郭盛华带领他的团队与号称“日本第一”的黑客组织展开了战斗。日本所谓的头号黑客是无能为力的，最后没办法只好认输，真是一大乐事。也许是因为郭盛华太厉害了，后来他被列入了禁止去日本的国家名单。

中国黑客——林勇

- Lion，中文名叫林勇，中国红客联盟（HUC）创始人，将正义的黑客聚集在一起，为祖国的尊严而“黑”。
- 在2001年4月1日，南海撞机事件发生后，中国飞行员王伟英勇就义，而林勇得知此事后，便率领红客联盟的8万成员，对白宫网站发起了进攻，并成功将五星红旗插到了国外，以独特的方式，维护了祖国的尊严。

黑客守则

- 不要恶意破坏任何的系统，这样做只会给你带来麻烦。
- 不要破坏别人的软件和资料。
- 不要修改任何系统文件，如果是因为进入系统的而修改了系统文件，请在目的到达后将之改回原状。
- 不要轻易的将你要黑的或者黑锅的站点告诉不信任的人。
- 在发表黑客文章使不要用你的真实 。
- 正在入侵的时候，不要随意离开你的电脑。
- 不要入侵或破坏政府机关的主机。
- 将你的笔记放在安全的地方。
- 已入侵的电脑中的账号不得清除或修改。
- 可以为隐藏自己的侵入而做一些修改，弹药尽量保持原系统的安全性，不能因为得到系统的控制权而将门户大开。

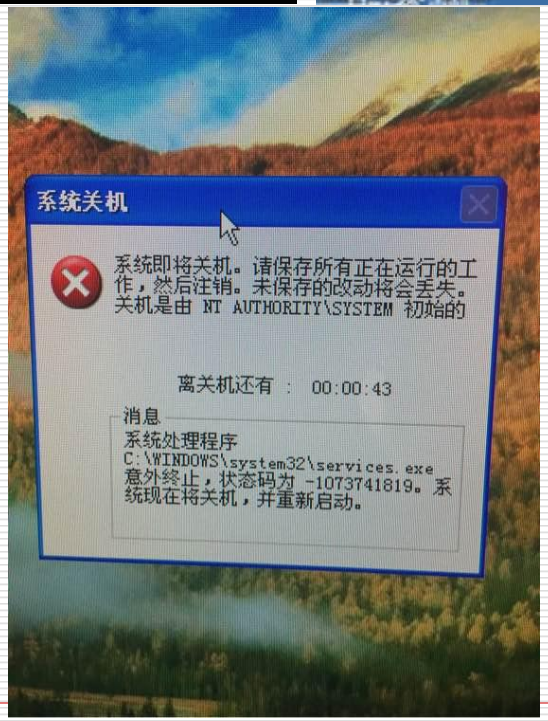
病毒感染

- 病毒是编制者在计算机程序中插入的破坏计算机功能或数据，影响硬件的正常运行并且能够自我复制的一组计算机指令或程序代码。
- 产生原因：
  - 编制人员处于一种炫耀和显示自己能力的目的；
  - 某些软件作者处于版权保护目的而编制；
  - 处于某种报复目的或恶作剧而编写病毒；
  - 处于商业利益；
  - 处于政治、战争的需要。

CIH病毒

“熊猫烧香”病毒

“冲击波”病毒



网络犯罪

- 网络数量大规模增长，网民素质参差不齐，而这一领域的各种法律规范未能及时跟进，网络成为一种新型的犯罪工具、犯罪场所和犯罪对象。
- 网络犯罪中最为突出的问题有：网络色情泛滥成灾，严重危害未成年人的身心健康；软件、影视唱片的著作权受到盗版行为的严重侵犯；电子商务备受诈欺困扰；信用卡被盗刷；购买的商品石沉大海，发出商品却收不回货款；更有甚者，侵入他人网站、系统后进行敲诈，制造、贩卖计算机病毒、木马或其它恶意软件，已经挑战计算机和网络几十年之久的黑客仍然是网络的潜在危险。

网络犯罪（续）

- 网络犯罪的类型
  - 网络文化污染
  - 盗版交易
  - 网络欺诈
  - 妨害名誉
  - 侵入他人主页、网站、邮箱
  - 制造、传播计算机病毒
  - 网络赌博
  - 教唆、煽动各种犯罪，传授犯罪方法

网络犯罪（续）

- 打击网络犯罪面临的问题
  - ✓ 互联网本身缺陷
  - ✓ 黑客软件泛滥
  - ✓ 互联网的跨地域、跨国界性
  - ✓ 网上商务存在的弊端
  - ✓ 互联网性质的不确定性
  - ✓ 司法标准不一

黑客攻击汽车视频演示

1.4 网络攻击过程

- 网络攻击（**Cyber Attacks**，也称赛博攻击）是指针对计算机信息系统、基础设施、计算机网络或个人计算机设备的，任何类型的进攻动作。对于计算机和计算机网络来说，破坏、揭露、修改、使软件或服务失去功能、在没有得到授权的情况下偷取或访问任何计算机的数据，都会被视为于计算机和计算机网络中的攻击。
- 攻击分类：

  按照攻击方式：主动攻击、被动攻击

  按照攻击位置：远程攻击、本地攻击、伪远程攻击

网络攻击过程—主动攻击

- 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：

  篡改消息、伪造消息、拒绝服务。

- 篡改消息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。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”。

网络攻击过程—主动攻击

- 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和特权。
- 拒绝服务即常说的**DoS（Deny of Service）**，会导致对通讯设备正常使用或管理被无条件地中断。通常是对整个网络实施破坏，以达到降低性能、终端服务的目的。这种攻击也可能有一个特定的目标，如到某一特定目的地（如安全审计服务）的所有数据包都被阻止。

网络攻击过程—被动攻击

- 被动攻击中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。
- 由于被动攻击不会对被攻击的信息做任何修改，留下痕迹很好，或者根本不留下痕迹，因而非常难以检测，所以抗击这类攻击的重点在于预防。具体措施包括自动审计、入侵检测和完整性恢复等。

网络攻击过程—本地攻击和伪远程攻击

- 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。

- 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，攻击过程从外部远程发起，造成外部入侵的现象。

  这里主要介绍远程攻击的一般过程。

网络攻击过程—攻击层次

- 简单拒绝服务
- 本地用户获得非授权读权限
- 本地用户获得非授权写权限
- 远程用户获得非授权账号信息
- 远程用户获得特权文件的读权限
- 远程用户获得特权文件的写权限
- 远程用户拥有了系统管理员权限

由上到下，破坏程度依次增强。

网络攻击过程—远程攻击

- **远程攻击的一般步骤：**
  - 远程攻击的准备阶段
  - 远程攻击的实施阶段
  - 远程攻击的善后阶段
- **基本过程：**

  攻击源隐藏→目标信息收集→弱点挖掘→掌握控制权→攻击行为隐藏→实施目标攻击→开辟后门→攻击痕迹清除

远程攻击的准备阶段

- 确定攻击目标
- 信息收集
- 服务分析
- 系统分析
- 漏洞分析

攻击准备1—确定攻击目标

- 攻击者在进行一次完整的攻击之前，首先要确定攻击要达到什么样的目的，即给受侵者造成什么样的后果。
- 常见的攻击目的有破坏型和入侵型两种。
  - 破坏型攻击——是指只破坏攻击目标，使之不能正常工作，而不能随意控制目标上的系统运行。
  - 入侵型攻击——这种攻击要获得一定的权限才能达到控制攻击目标的目的。应该说这种攻击比破坏型攻击更为普遍，威胁性也更大。因为攻击者一旦掌握了一定的权限、甚至是管理员权限就可以对目标做任何动作，包括破坏性质的攻击。

攻击准备2—信息收集

- 包括目标的操作系统类型及版本、相关软件的类型、版本及相关的社会信息。
- 收集目标系统相关信息的协议和工具：
  - Ping实用程序
  - TraceRoute、Tracert、X-firewalk程序
  - Whois协议
  - Finger协议
  - SNMP协议

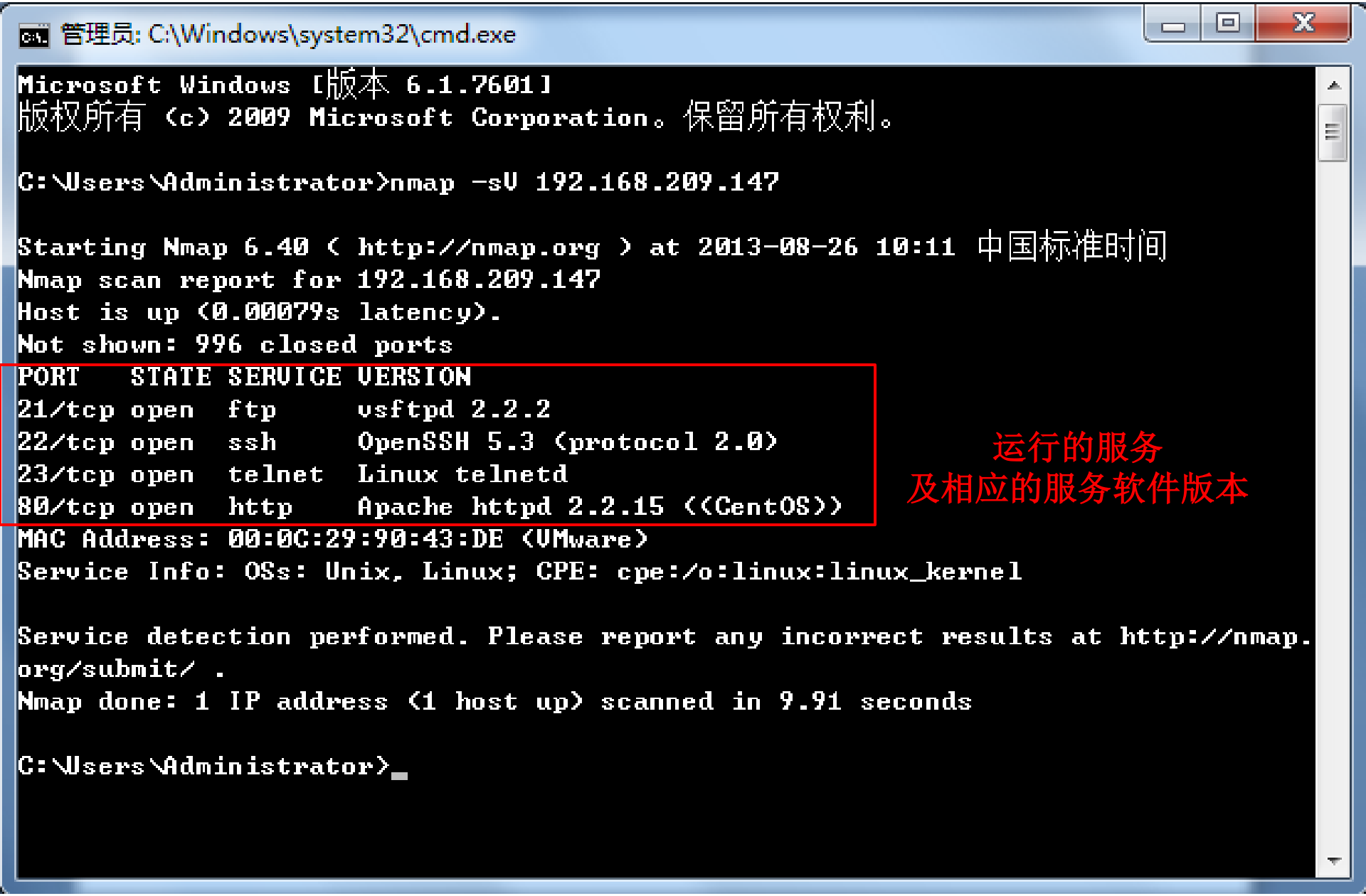
攻击准备2—信息收集

- 在网络中主机一般以**IP**地址进行标识。
- 例如选定**192.168.0.111**这台主机为攻击目标，使用**ping**命令可以探测目标主机是否连接在**Internet**中。
- 在**Windows**下使用**ping**命令测试：
  - **ping 192.168.0.111**
  - 测试结果如下页图所示。

能收到来自目标主机的回复，说明目标主机处于活动状态

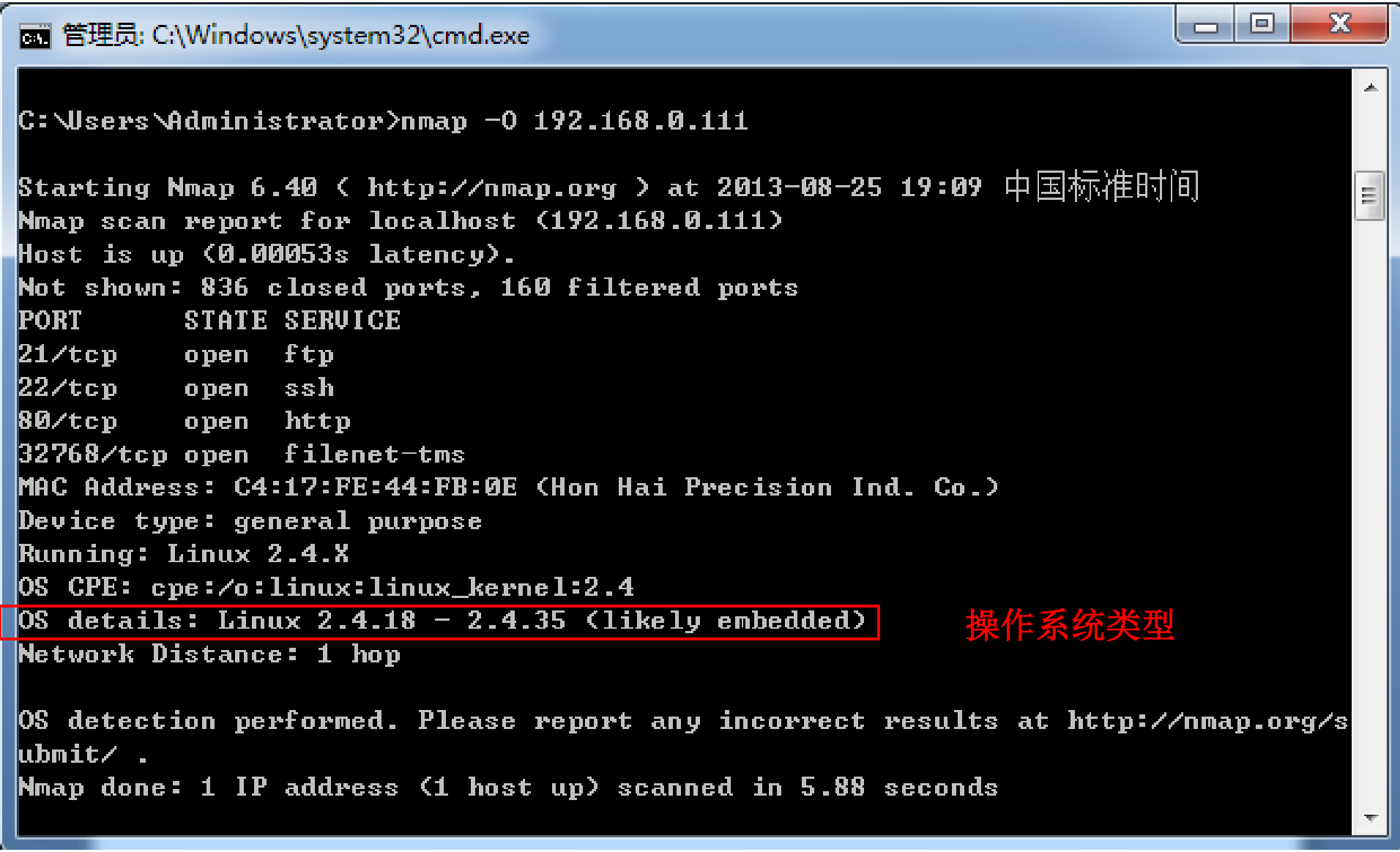
攻击准备3—服务分析

- 探测目标主机所提供的服务、相应端口是否开放、各服务所使用的软件版本类型：如利用**Telnet**、**haktek**等工具，或借助**SuperScan**、**Nmap**等这类工具的端口扫描或服务扫描功能。
- 举例：
  - Windows下，开始—运行—cmd
  - 输入：**nmap –sV 192.168.209.147** ，然后回车
  - 结果如下页图所示，说明192.168.209.147这台主机上运行了ftp,telnet,http服务以及相应的服务软件版本类型


管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\Administrator>nmap -sV 192.168.209.147
Starting Nmap 6.40 (http://nmap.org) at 2013-08-26 10:11 中国标准时间
Nmap scan report for 192.168.209.147
Host is up (0.00079s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.2.2
22/tcp open ssh OpenSSH 5.3 (protocol 2.0)
23/tcp open telnet Linux telnetd
80/tcp open http Apache httpd 2.2.15 ((CentOS))
MAC Address: 00:0C:29:90:43:DE (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.91 seconds
C:\Users\Administrator>
运行的服务
及相应的服务软件版本

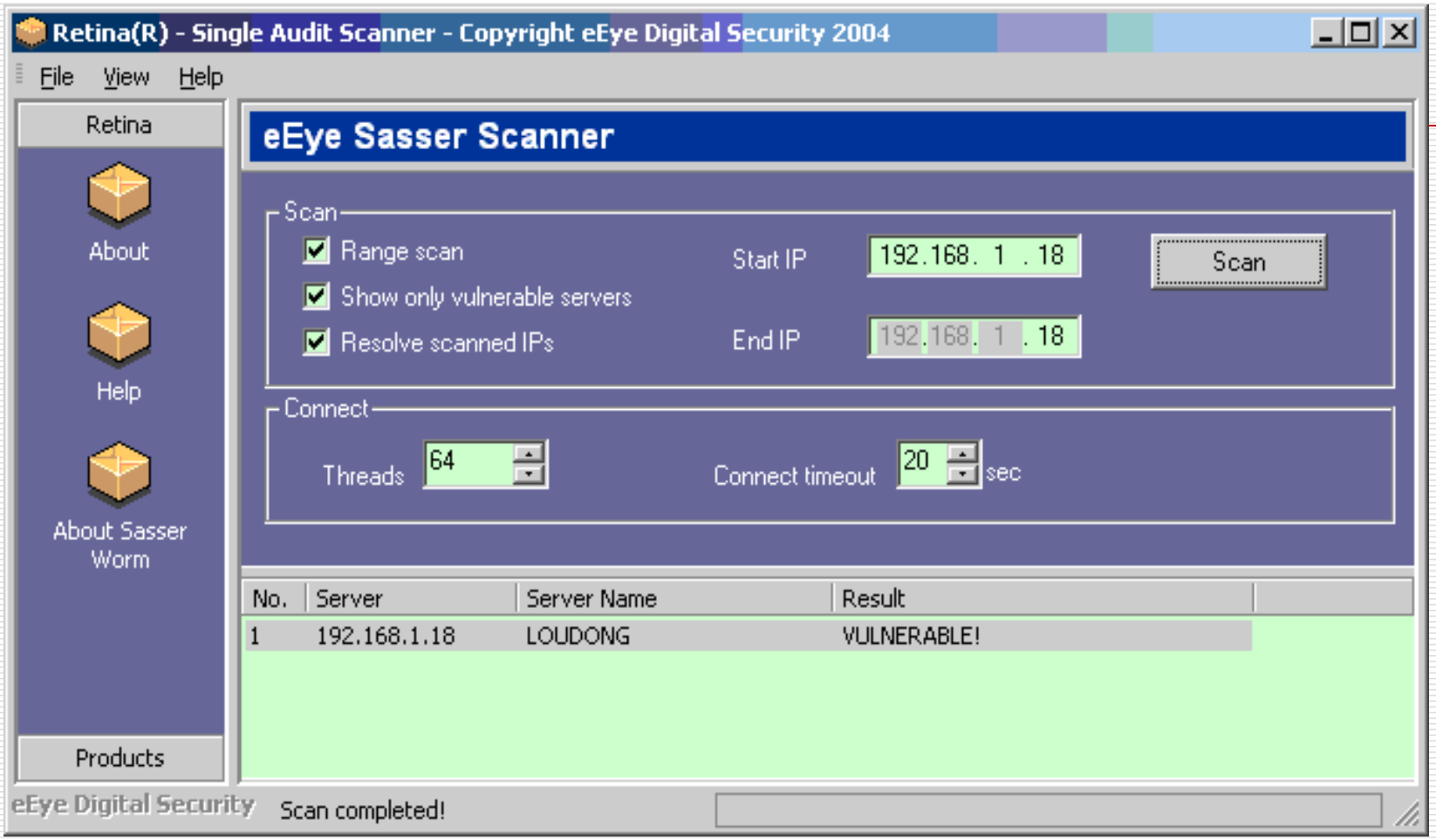
攻击准备4—系统分析

- 确定目标主机采用何种操作系统
- 例如
  - 在Windows下安装Nmap v6.40扫描工具，此工具含OS Detection的功能（使用-O选项）。
  - 打开cmd.exe，输入命令：**nmap –O 192.168.0.111**
  - 探测结果如下页图所示，说明操作系统是OS details: Linux 2.4.18 - 2.4.35 (likely embedded)


管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>nmap -O 192.168.0.111
Starting Nmap 6.40 (http://nmap.org) at 2013-08-25 19:09 中国标准时间
Nmap scan report for localhost (192.168.0.111)
Host is up (0.00053s latency).
Not shown: 836 closed ports, 160 filtered ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
32768/tcp open filenet-tms
MAC Address: C4:17:FE:44:FB:0E (Hon Hai Precision Ind. Co.)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.18 - 2.4.35 (likely embedded)
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.88 seconds
操作系统类型

攻击准备5—漏洞分析

- 分析确认目标主机中可以被利用的漏洞
- 手动分析：过程复杂、技术含量高、效率较低
- 借助软件自动分析：需要的人为干预过程少，效率高。如**Nessus**、**X-Scan**等综合型漏洞检测工具、**eEye**等专用型漏洞检测工具等。
- 例如
  - 在Windows下使用eEye SasserScanner对目标主机**192.168.1.18**进行系统漏洞分析。探测结果如下页图所示，说明目标主机存在震荡波漏洞。


Retina(R) - Single Audit Scanner - Copyright eEye Digital Security 2004
File
View
Help
Retina
About
Help
About Sasser Worm
Products
eEye Sasser Scanner
Scan
Range scan
Show only vulnerable servers
Resolve scanned IPs
Start IP
192.168. 1 . 18
End IP
192.168. 1 . 18
Scan
Connect
Threads
64
Connect timeout
20
sec
No.
Server
Server Name
Result
1
192.168.1.18
LOUDONG
VULNERABLE!
eEye Digital Security
Scan completed!

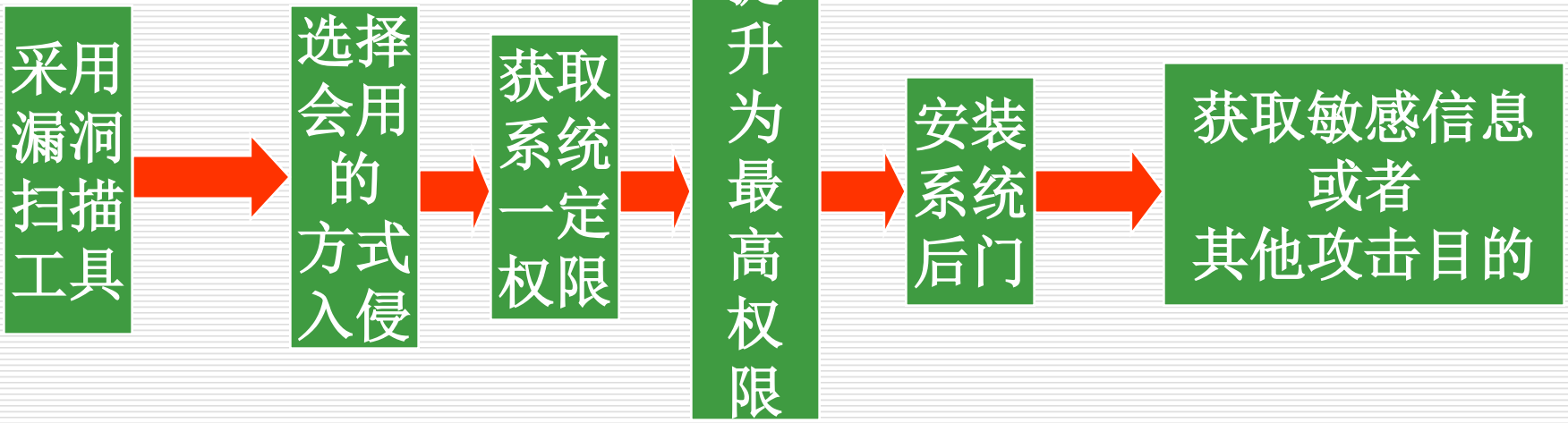
远程攻击的实施阶段

- 作为破坏性攻击，可以利用工具发动攻击即可。
- 作为入侵性攻击，往往需要利用收集到的信息，找到其系统漏洞，然后利用漏洞获取尽可能高的权限。
- 攻击的主要阶段包括：
  - 预攻击探测：为进一步入侵提供有用信息。一般过程：端口扫描、漏洞扫描、操作系统类型鉴别、网络拓扑分析。
  - 实施攻击：缓冲区溢出攻击、脚本程序漏洞攻击、口令攻击、错误及弱配置攻击、网络欺骗与劫持攻击。
  - 其他攻击：拒绝服务攻击、嗅探、恶意网页、社会工程等。

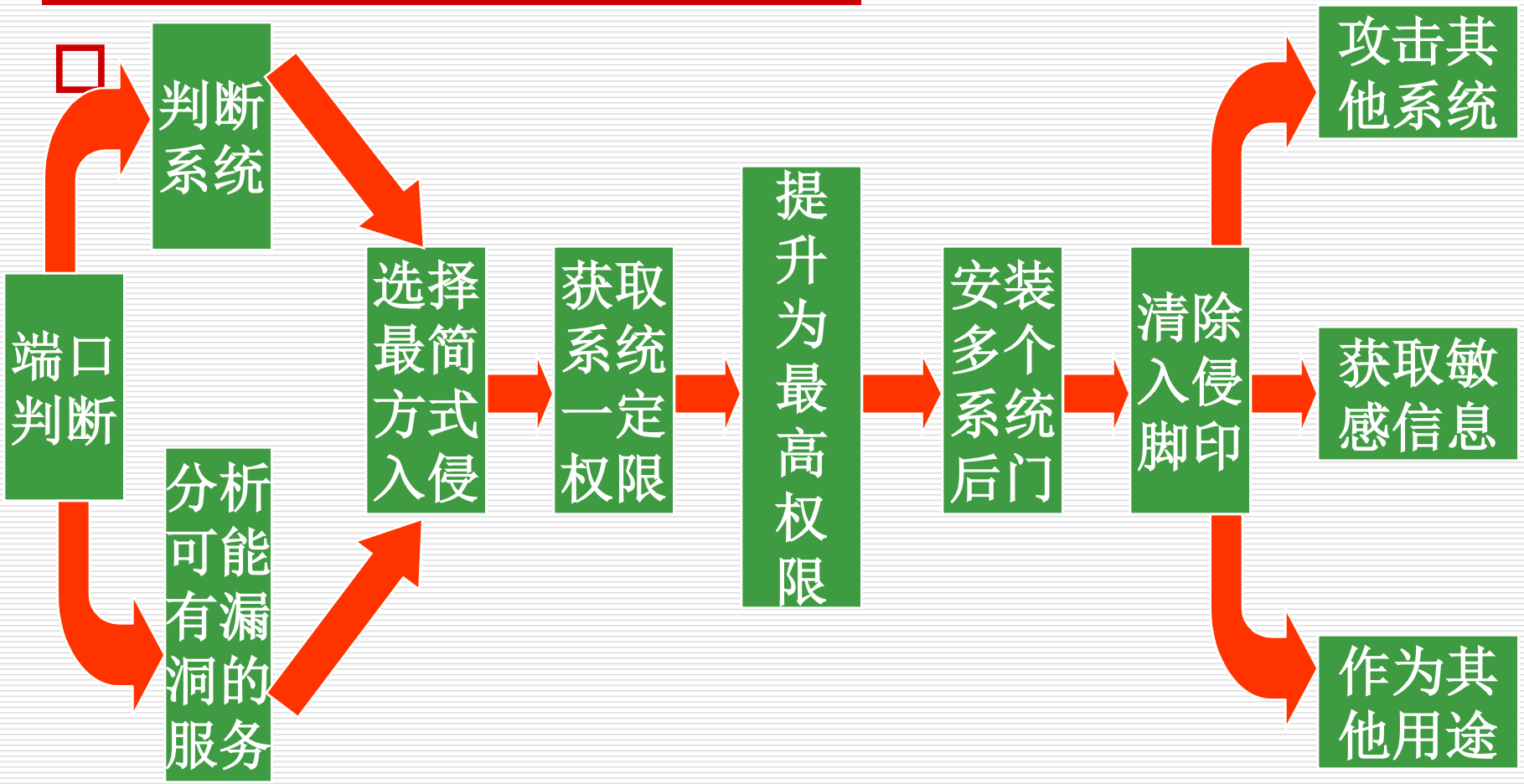
远程攻击的善后阶段

- 入侵成功后，攻击者为了能长时间地保留和巩固他对系统的控制权，一般会留下后门。
- 此外，攻击者为了自身的隐蔽性，须进行相应的善后工作——隐藏踪迹：
  - 攻击者在获得系统最高管理员权限之后就可以任意修改系统上的文件了，所以一般黑客如果想隐匿自己的踪迹，最简单的方法就是删除日志文件。
  - 但这也明确无误地告诉了管理员系统已经被入侵了。更常用的办法是只对日志文件中有关自己的那部分作修改，关于修改方法的细节根据不同的操作系统有所区别，网络上有许多此类功能的程序。

入侵系统的常用步骤


采用漏洞扫描工具
选择会用的方式入侵
获取系统一定权限
提升为最高权限
安装系统后门
获取敏感信息或者其他攻击目的

较高明的入侵步骤


端口判断
判断系统
分析可能有漏洞的服务
选择最简方式入侵
获取系统一定权限
提升为最高权限
安装多个系统后门
清除入侵脚印
攻击其他系统
获取敏感信息
作为其他用途

演示

- ✓ 一个完整的攻击视频

1.5 网络安全策略及制订原则

- 安全策略，是针对那些被允许进入某一组织、可以访问网络技术资源和信息资源的人所规定的、必须遵守的规则。
- 即：网络管理部门根据整个计算机网络所提供的服务内容、网络运行状况、网络安全状况、安全性需求、易用性、技术实现所付出的代价和风险、社会因素等许多方面因素，所制定的关于网络安全总体目标、网络安全操作、网络安全工具、人事管理等方面的规定。

制定安全策略的目的

- 保证网络安全保护工作的整体、计划性及规范性。
- 保证各项措施和管理手段的正确实施。
- 是网络系统信息数据的机密性、完整性及可用性受到全面、可靠的保护。

制定安全策略的目的

- 内容包括：
  - 进行安全需求分析。
  - 对网络系统资源进行评估。
  - 对可能存在的风险进行分析。
  - 确定内部信息对外开放的种类及发布方式和访问方式。
  - 明确网络系统管理人员的责任和义务。
  - 确定针对潜在风险采取的安全保护措施的主要构成方面，制定安全出去、访问规则。

安全策略的必要性

- 网络管理员在作安全策略时的依据在很大程度上取决于网络运行过程中的安全状况，网络所提供的功能以及网络的易用程度。
- 安全策略应以要实现目标为基础，而不能简单地规定要检验什么和施加什么限制。
- 在确定的安全目标下，应该制定如何有效地利用所有安全工具的策略。

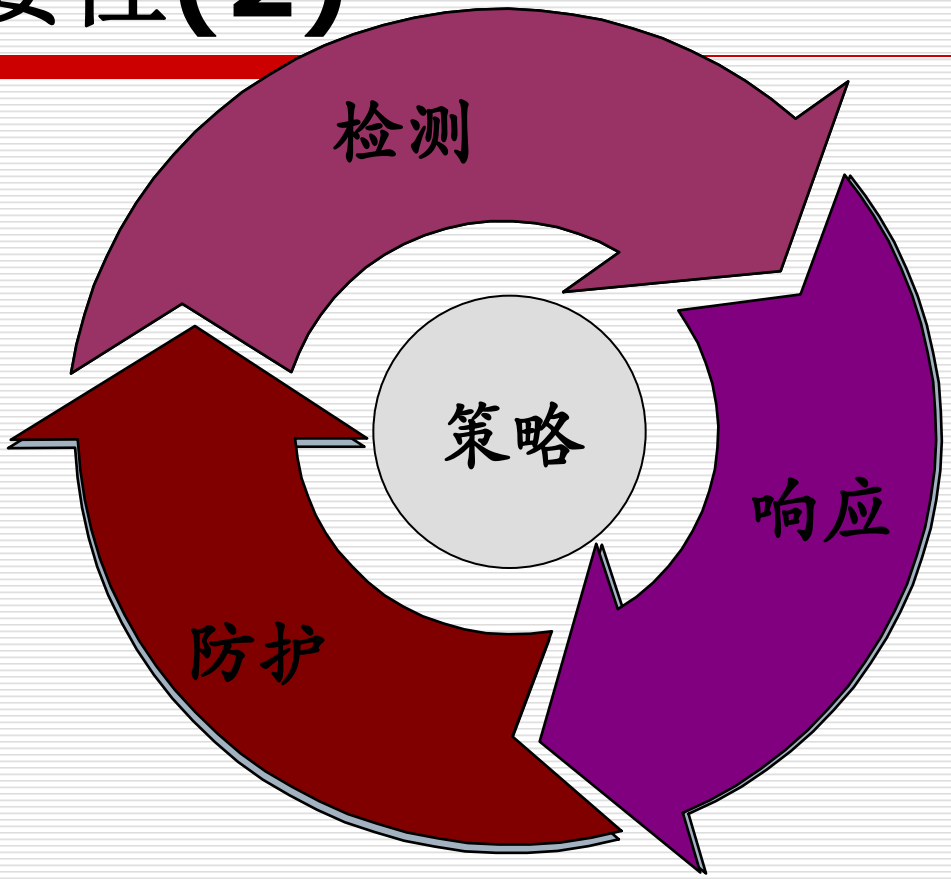
安全策略的必要性(2)

- 强调了策略的核心作用
- 强调了检测、响应、防护的动态性
- 检测、响应、防护必须遵循安全策略进行
- 安全策略(Policy)

  保　　护(Protection)

  检　　测(Detection)

  响　　应(Response)



PPDR模型

制订安全策略的基本原则

- 适用性原则
- 可行性原则
- 动态性原则
- 简单性原则
- 系统性原则
- 最小特权原则

适用性原则

- 安全策略是在一定条件下采取的安全措施，必须与网络的实际应用环境相结合。
- 网络的安全管理是一个系统化的工作，因此在制定安全策略时，应全面考虑网络上各类用户、设备等情况，有计划有准备地采取相应的策略，任何一点疏忽都会造成整个网络安全性的降低。

可行性原则

- 安全管理策略的制定还要考虑资金的投入量，因为安全产品的性能一般是与其价格成正比的，所以要适合划分系统中信息的安全级别，并作为选择安全产品的重要依据，使制定的安全管理策略达到成本和效益的平衡。

动态性原则

- 安全管理策略有一定的时限性，不能是一成不变的。
- 由于网络用户在不断地变化，网络规模在不断扩大，网络技术本身的发展变化也很快，而安全措施是防范性的，所以安全措施也必须随着网络发展和环境的变化而变化。

简单性原则

- 网络用户越多，网络管理人员越多，网络拓扑越复杂，采用网络设备种类和软件种类越多，网络提供的服务和捆绑越多，出现安全漏洞的可能性就越大。
- 因此制定的安全管理策略越简单越好，如简化授权用户的注册过程等。

系统性原则

- 网络的安全管理是一个系统化的工作，因此在制定安全管理策略时，应全面考虑网络上各类用户，各种设备，各种情况，有计划有准备地采取相应的策略，任何一点疏忽都会造成整个网络安全性的降低。

最小特权原则

- 每个用户并不需要使用所有的服务，不是所有用户都需要去修改系统的每一个文件，每一个用户并不需要都知道系统的根口令，每个系统管理者也没有必要都知道系统的跟口令。

安全策略的特点

- 所有有效的安全策略都至少具备以下特点：
  - 发布——必须通过系统正常管理程序，采用合适的标准出版物或其他适当的方式来发布。
  - 强制执行——在适当的情况下，必须能够通过安全工具来实现其强制实施，并在技术确定不能满足要求的情况下强迫执行。
  - 人员责任规定——必须明确规定用户、系统管理员和公司管理人员等各类人员的职责范围和权限。

安全策略分类

- 安全策略可分以下几类：
  - 物理安全策略
  - 访问控制策略
  - 网络安全管理策略
  - 信息加密策略

安全策略分类—物理安全策略

- 保护计算机系统、网络服务器及打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击。
- 验证用户的身份和使用权限、防止用户越权操作。
- 确保计算机系统有一个良好的电磁兼容工作坏境。
- 建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

安全策略分类—访问控制策略

- 访问控制是网络安全防范和保护的主要策略。它的主要任务是保证网络资源不被非法使用和非常访问。包括：
  - 入网访问控制
  - 网络的权限控制
  - 目录级安全控制
  - 属性安全控制
  - 网络服务器安全控制
  - 网络监测和锁定控制
  - 防火墙控制
  - 网络端口和节点的安全机制

安全策略分类—网络安全管理策略

- 网络安全管理策略
  - 确定安全管理等级和安全管理范围。
  - 制定有关网络操作使用规程和人员出入机房管理制度。
  - 制定网络系统的维护制度和应急措施。

安全策略分类—信息加密策略

- 目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。
- 网络加密常用的方法有链路加密、端点加密和节点加密三种。
  - 链路加密的目的是保护网络节点之间的链路信息安全；
  - 端点加密的目的是对源端用户到目的端用户的数据提供保护；
  - 节点加密的目的是对源节点到目的节点之间的传输链路提供保护。

1.6 网络安全体系设计

- 1.6.1 网络安全体系层次
- 1.6.2 网络安全体系设计准则

1.6.1 网络安全体系层次

- 作为全方位的、整体的网络安全防范体系也是分层次的，不同层次反映了不同的安全问题。
- 根据网络的应用现状情况和网络的结构，安全防范体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理。

物理层安全

- 物理环境的安全性。包括通信线路的安全，物理设备的安全，机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件、传输介质），软硬件设备安全性（替换设备、拆卸设备、增加设备），设备的备份，防灾害能力、防干扰能力，设备的运行环境（温度、湿度、烟尘），不间断电源保障，等等。

系统层安全

- 该层次的安全问题来自网络内使用的操作系统的安全，如**Win10**、**Linux**等。主要表现在三方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等。二是对操作系统的安全配置问题。三是病毒对操作系统的威胁。

网络层安全

- 该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等等。

应用层安全

- 该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性而产生，包括**Web**服务、电子邮件系统、**DNS**等。

管理层安全

- 安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其它层次的安全漏洞。

1.6.2 网络安全体系设计准则

- 木桶原则
- 整体性原则
- 安全性评价与平衡原则
- 标准化与一致性原则
- 技术与管理相结合原则
- 统筹规划分步实施原则
- 等级性原则
- 动态发展原则
- 易操作性原则

1.7 常用的防护措施

我们怎么办？

1.7 常用的防护措施—防病毒技术

- 计算机病毒种类繁多，新的变种不断出现，而且在开放的网络环境中，其传播速度更快，机会更多。对于用户而言，需要采用全方位的防病毒产品及多层次的安全工具，尽量保障网络中计算机的安全。电子邮件传输、文件下载等过程都有可能携带病毒。
- 用户务必要针对网络中病毒所有可能传播的方式、途径进行防范，设置相应的病毒防杀软件，进行全面的防病毒系统配置，并保证防病毒软件及病毒库的不断更新，保障计算机系统及网络的安全，防止病毒的攻击。

1.7 常用的防护措施—数据加密技术

- 数据加密技术代价小而作用明显，是互联网信息传输过程中经常使用的安全技术，是最基本也是最核心的信息安全技术。
- 加密技术以密码学为基础， 通过使用各种加密算法将要传输的数据转化成为密文，再进行传输，到达接收方再用解密算法进行解密，将密文转化为明文来读取。在此过程中只有合法用户才拥有密钥，才能解密，这样在传输过程中即使有非授权人员获取数据，也确保他人识别不了信息的真实内容，从而保证信息在传输过程中的安全。

1.7 常用的防护措施—防火墙技术

- 防火墙技术是目前使用最为广泛的一种保护计算机网络安全的技术性措施，介于内部网络和外部网络之间，用来保护内部网络不受到来自外部互联网的侵害。
- 防火墙安全控制策略是在两个网络通信时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入网络，同时将你“不同意”的人和数据拒之门外，最大限度的保护内网安全。它禁止一切未被允许的访问服务，同时允许一切未被禁止的访问服务。

1.7 常用的防护措施—入侵检测技术

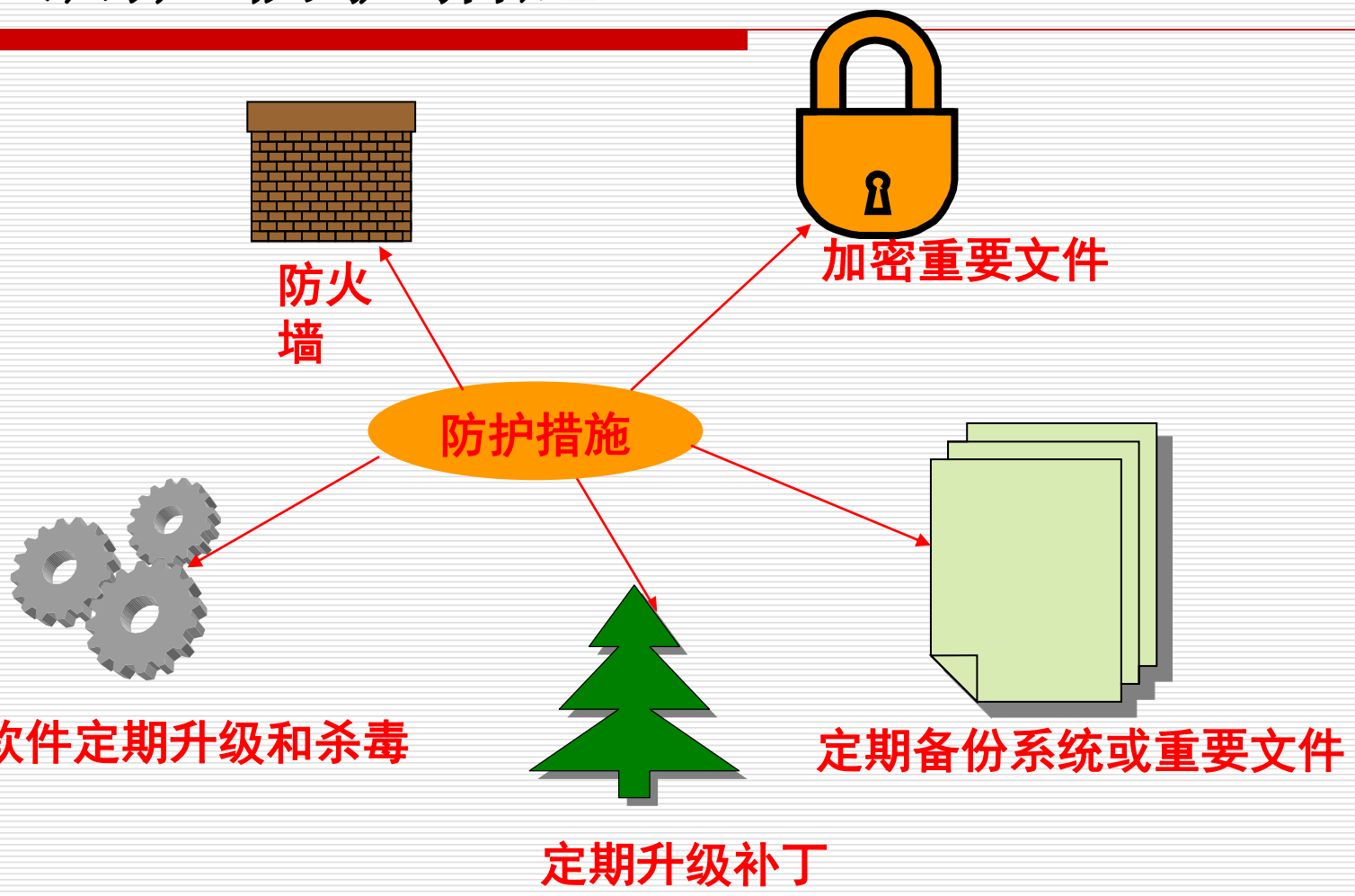
- 入侵检测技术，即实时检测技术，主要是为保证计算机安全而对系统中的入侵行为进行实时检测的技术。
- 它通过检测网络上的数据流，进而查看有无违反安全策略的行为。如果入侵检测系统识别出有任何异常的行为，则根据用户预先的设置做出响应。
- 利用此技术可以实现对计算机系统的实时监控，及时发现异常行为、危险因素，但是它往往需要和防火墙系统结合起来使用，以限制这些行为，保障计算机系统的安全。

1.7 常用的防护措施—身份认证技术

- 身份认证技术主要是通过对通信双方进行身份的鉴别，以确保通信的双方是合法授权用户，有权利进行信息的读取、修改、共享等操作，识别出非授权用户的虚假身份。
- 身份认证技术要求用户先向系统出示自己的身份证明，然后通过标识鉴别用户的身份，判断是否是合法授权用户，从而阻止假冒者或非授权用户的访问。
- 其他的一些防护措施？

  物理安全防护、配备网络安全设备或系统、服务器访问控制策略、安全的电子邮件系统、提高网络工作人员的素养等。

个人用户防护措施



防止黑客入侵

关闭不常用端口

关闭不常用程序和服务

及时升级系统和软件补丁

发现系统异常立刻检查

1.8 小结

- 当今社会，网络安全是最急需解决的重要问题之一：各种计算机安全和网络犯罪事件直线上升，病毒增长呈很高幅度，但是很多机构仍没有认识到这些潜在的威胁。
- 信息，信息资产以及信息产品对于我们的日常生活及整个社会的正常运转是至关重要的，加强网络安全的必要性和重要性已不言而喻。
- 保护网络中敏感信息免受各种攻击，正是现在迫切需要解决的问题。

布什提名国土安全部长 上诉院法官有望出任 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址(D) http://www.ynet.com/view.jsp?oid=4475458

布什提名国土安全部长 上诉院法官有望出任

◇字体：【大 中 小】 北京青年报 (01/13 03:41)

■1月11日，美国总统布什（右）与切尔托夫在白宫出席提名仪式

在经历了上次任命告吹的难堪后，美国总统布什11日正式提名上诉法院法官迈克尔·切尔托夫出任国土安全部部长。

■热情赞扬

在白宫举行的提名仪式上，布什总统高度赞扬了切尔托夫在历任岗位上的工作业绩。

“‘9·11’事件发生后，迈克（切尔托夫的昵称）帮助确定了实施袭击者就是‘基地’组织网络。他迅速意识到反恐战争的最高策略就是防患于未然，”布什说，“他的精力和智慧使他处于国土安全领域重大革新的中心地位，尤其是在加强同联邦调查局（FBI）和地方官员信息共享方面。”

布什总统还专门指出，切尔托夫因工作出色，曾3次受到参议院的肯定。言下之

组合检索

YNET 专题

- 情人节影讯
- 2005体坛焦点
- 牵振甫病逝
- 影说中国足球
- 红人大盘点
- 北京山友遇险
- 创意生活
- 2004大背景下的..
- 盘点焦点话题
- 2004世界体坛风..

独家报道

- 看舞台剧《半生缘..
- 《Hi 可爱》大..
- 2004年娱闻杂..
- 离婚分财产牵出企..
- 与野牦牛队员重温..
- 李霞不做“花瓶女..
- 陈坤：梦想中绽放..

新闻排行

- 机动车负全责有望获..
- 中国国青难破恐韩症
- 足协上交第二份处理..
- 哺乳易激发女性性冲..
- 姐弟合谋劫杀同窗案..
- 18岁女生荣当国际..
- 贪官毕玉玺六千万是..
- 香港立法会候选人嘌..
- 新版车贷规定有六大..
- 北航高招丑闻是冰山..

Internet

开始 漏洞报告 Google... 新建 Mic... Microsoft... 布什任... 布什提... ■1月11... CH 22:16

孙子兵法的启示

- 孙子曰
  - 昔之善战者，先为不可胜，以待敌之可胜。不可胜在己，可胜在敌。故善战者，能为不可胜，不能使敌必可胜。故曰：胜可知，而不可为。
  - 不可胜者，守也；可胜者，攻也。守则有余，攻则不足。善守者，藏于九地之下；善攻者，动于九天之上，故能自保而全胜也。


HTTP://WWW.DESKCITY.COM

谢谢各位！