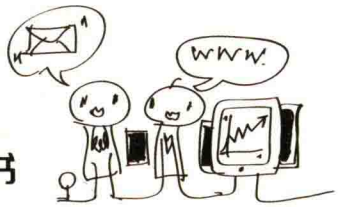

网络工程师教育丛书

Networking Security and Management

网络安全与管理

◎ 刘化君　郭丽红　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

6

网络工程师教育丛书

网络安全与管理

Networking Security and Management

刘化君　郭丽红　编著

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

本书是《网络工程师教育丛书》第 6 册，内容涵盖网络安全理论、攻击与防护、安全应用与网络管理，从“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多个方面进行讨论。全书分为 8 章。其中，第 1 章为绪论；第 2 章至第 5 章分别介绍密码技术、网络安全协议、网络安全防护技术和网络安全应用，将网络安全理论与应用完美结合起来；第 6、7、8 章分别介绍网络管理，网络系统的运维与管理，网络协议分析和故障诊断等内容，旨在保障网络的安全有效运行。为帮助读者更好地掌握基础理论知识并应对认证考试，各章均附有小结、练习题及测验题，并对典型题例给出解答提示。

本书可作为网络工程师培训和认证考试教材，或作为本科及职业技术教育相关课程的教材或参考书，也可供网络技术人员、管理人员以及有志于自学成为网络工程师的读者阅读。

本书的相关资源可从华信教育资源网（www.hxedu.com.cn）免费下载，或通过与本书策划编辑（zhangls@phei.com.cn）联系获取。

图书在版编目（CIP）数据

网络安全与管理 / 刘化君，郭丽红编著. —北京：电子工业出版社，2019.3
（网络工程师教育丛书）
ISBN 978-7-121-35869-2

Ⅰ. ①网… Ⅱ. ①刘… ②郭… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 001268 号

责任编辑：张来盛（zhangls@phei.com.cn）
印　　刷：北京市师印务有限公司
装　　订：北京京师印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：19.5　字数：496 千字
版　　次：2019 年 3 月第 1 版
印　　次：2019 年 3 月第 1 次印刷
定　　价：59.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254467；zhangls@phei.com.cn。

出 版 说 明

人类已进入互联网时代，以物联网、云计算、移动互联网和大数据为代表的新一轮信息技术革命，正在深刻地影响和改变经济社会各领域。随着信息技术的发展，网络已经融入社会生活的方方面面，与人们的日常生活密不可分。我国已成为网络大国，网民数量位居世界第一；但我国要成为网络强国，推进网络强国建设，迫切需要大量的网络工程师人才。然而据估计，我国每年网络工程师缺口约 20 万人，现有网络人才远远无法满足建设网络强国的需求。

为适应网络工程技术人才教育、培养的需要，电子工业出版社组织本领域专家学者和工作在一线的网络专家、工程师，按照网络工程师所应具备的知识、能力要求，参考新的网络工程师考试大纲（2018 年审定通过），共同修订、编撰了这套《网络工程师教育丛书》。

本丛书全面规划了网络工程师应该掌握的技术，架构了一个比较完整的网络工程技术知识体系。丛书的编写立足于计算机网络技术的最新发展，以先进性、系统性和实用性为目标：

- 先进性——全面地展示近年来计算机网络技术领域的新成果，做到知识内容的先进性。例如，对软件定义网络（SDN）、三网融合、IPv6、多协议标签交换（MPLS）、云计算、云存储、大数据、物联网、移动互联网等进行介绍。
- 系统性——加强学科基础，拓宽知识面，各册内容之间密切联系、有机衔接、合理分配、重点突出，按照“网络基础→局域网→城域网与广域网→TCP/IP 基础→网络互连与互联网→网络安全与管理→大数据技术→网络设计与应用”的进阶式顺序分为 8 册，形成系统的知识结构体系。
- 实用性——注重工程能力的培养和知识的应用。遵循“理论知识够用，为工程技术服务”的原则，突出网络系统分析、设计、实现、管理、运行维护和安全方面的实用技术；书中配有大量网络工程案例、配置实例和实验示例，以提高读者的实践能力；每章还安排有针对性的练习和近年网络工程师考试题，并对典型试题和练习给出解答提示，以帮助读者提高应试能力。

本丛书从一开始就搭建了一个真实的、接近网络工程实际的网络，丛书各册均基于这个实例网络的拓扑和 IP 地址进行介绍，逐步完成对路由器、交换机、客户端和服务器的配置、应用设计等，灵活、生动地展现各种网络技术。

本丛书在编写时力求文字简洁，通俗易懂，图文并茂；在内容编排上既系统全面，又切合实际；在知识设计上层次分明、由浅入深，读者可根据自己的需要选择相应的图书进行学习，然后逐步进阶。

鉴于网络技术仍在不断地飞速发展，本丛书将根据需要和读者要求适时更新、完善。热忱欢迎广大读者多提宝贵意见和建议。联系方式：zhangls@phei.com.cn。

电子工业出版社

前　言

为了保障网络安全，促进经济社会信息化健康发展，网络安全问题已经提升到国家安全的战略高度，网络安全也因此成为信息技术领域的重要研究课题。为适应网络安全技术发展以及网络工程师教育培训、认证考试和相关院校教学的需要，我们编写了《网络安全与管理》一书，作为《网络工程师教育丛书》的第 6 册。

考虑到网络安全技术的发展应用，本书内容涵盖网络安全理论、攻击与防护、安全应用与网络管理，从“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多个方面进行讨论和介绍，突出理论与实际紧密结合的工程应用性。主要特色如下：

- 贯彻落实国家有关“建设网络强国和安全网络”的战略部署，以培养网络工程师为目标追寻网络技术发展，搭建了一个网络安全与管理知识体系；
- 内容丰富，科学合理，各章内容既相互依赖又相对独立，形成了一条完整知识链；
- 理论与实践密切结合，注重网络安全实际能力的培养，将大量网络安全实例融合到理论阐释之中，以实现理论指导下的实践和实践基础上的理论提升；
- 言简意赅，清楚易懂，理论阐述严谨、透彻，技术讨论翔实、细致，并通过大量图表，形象直观地讲解网络安全知识；
- 许多典型问题解析、练习题及测验题，直接选自近几年的网络工程师考试真题。

全书内容分为 8 章：第 1 章为绪论；第 2 章至第 5 章分别介绍密码技术、网络安全协议、网络安全防护技术和网络安全应用，将网络安全理论与应用有机结合起来，以实用和最新的网络安全技术展示给读者；第 6、7、8 章分别介绍网络管理、网络系统的运维与管理、网络协议分析和故障诊断等内容，旨在保障网络的安全有效运行。为帮助读者更好地掌握基础理论知识并应对认证考试，各章均附有小结、练习题及测验题，并对典型题例给出解答提示。

本书内容适合计算机网络和通信领域的教学、科研和工程设计参考，适用范围较广，既可以用作网络工程师教育培训教材，以及本科和高职院校相关课程的教材或参考书，也可供网络技术人员、管理人员以及有志于自学成为网络工程师的读者阅读。

本书由刘化君、郭丽红编著。在编写过程中，得到了许多同志的支持和帮助，在此一并表示衷心感谢！

网络安全与管理是一个内容广博、不断发展的技术领域。在本书的编写过程中，尽管力求精益求精，及时吸纳最新的网络安全与管理研究成果与技术，但囿于编著者理论水平和实践经验，书中仍可能存在不妥之处，恳请广大读者不吝赐教，以便再版时予以订正。

编著者

2019 年 1 月 8 日

目　录

第一章 绪 论

概 述

互联网技术的普及应用，使得信息突破了时间和空间上的障碍，信息的价值在不断提高。然而，计算机、网络等信息技术与其他技术一样，是一把“双刃剑”：一方面，它们在计算机用户之间架起了通信的通道；另一方面，也为某些窃取机密数据的非法之徒打开了方便之门。就在大部分人使用信息网络技术提高工作效率，为社会创造更多财富的同时，也有一些人在利用信息技术做着相反的事情，非法侵入网络系统窃取机密信息，篡改和破坏数据，给社会造成难以估量的巨大损失。网络安全越来越成为关系国计民生的大事，已经引起了全社会的高度重视。

从本质上说，网络安全就是网络上的信息安全。信息安全是对信息的保密性、完整性和可用性等特性的保护，包括物理安全、网络系统安全、数据安全、信息内容安全和信息基础设施安全等多个方面。

网络安全是一个非常复杂的综合性问题，涉及技术、产品和管理等诸多因素。网络安全所研究的，主要是信息网络的安全理论、安全应用和安全管理技术，以确保网络免受各种威胁和攻击，使之能够正常工作。本章主要讨论与网络安全相关的一些基本概念、安全策略与关键技术，以及信息网络安全标准。

第一节 网络安全的概念

信息与网络系统安全现在已经成为一门新兴的学科，而且是一门边缘交叉性学科。它涉及通信技术、计算机科学与技术、网络工程、信息论、数论、密码学、人工智能及社会工程学，既有安全理论、安全应用技术，也包括安全管理，还有社会、教育、法律等问题。因此，只有多个方面相互补充，才能有效地保障网络系统的安全。

学习目标

- ▶ 了解网络安全的基本概念；
- ▶ 掌握网络安全的目标和技术体系。

关键知识点

- ▶ 利用网络通信安全服务可以免受各种安全威胁和攻击。

网络安全的定义

“安全”一词通常被理解为“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、

犯罪、攻击或逃跑而采取的措施”。这是在广泛意义上对安全的表述。

就信息技术而言，依其发展与广泛应用，信息安全涵盖的内容很丰富，包括操作系统安全、网络安全、病毒查杀、访问控制、加密与认证以及数据库安全等多个方面。国际标准化组织（ISO）将计算机系统信息安全（Computer System Security）定义为“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然和恶意的原因而遭到破坏、更改和泄露”，这一定义偏重于静态信息保护。因此，可将计算机系统信息安全进一步定义为“计算机的硬件、软件和数据得到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，保障系统连续正常运行”，这一定义侧重了动态意义的描述。显然，“安全”一词是指将服务与资源的脆弱性降到最低限度，其中脆弱性是指计算机信息系统的任何弱点。

《中华人民共和国网络安全法》对网络安全的定义是：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、破坏和非法使用以及意外事故，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。

网络安全是研究与计算机网络相关的安全问题的。具体地说，网络安全主要研究安全地存储、处理或传输信息资源的技术、体制和服务。假设 A 和 B 要应用网络进行通信，并希望该网络及其通信过程是“安全”的。在这里，A 和 B 可以是两台需要安全交换路由表的路由器，也可以是希望建立一个安全传输连接的客户机和服务器，或者是交换安全电子邮件的应用程序，因此可以把 A 和 B 看作两个网络通信实体，即应用进程。A 和 B 要进行网络通信并希望做到“安全”，那么此处的安全意味着什么呢？显然，这个“安全”的内涵是丰富多彩的，涉及多个方面。例如，A 和 B 希望存储在客户机或服务器中的数据不被破坏、篡改、泄露；它们之间的通信内容对于窃听者是保密的，而且的确是在与真实的对方进行通信；它们还希望所传输的内容即使被窃听者窃取了，也不能理解其报文的含义；还要确保它们的通信内容在传输过程中没有被篡改，或者即使被篡改了，也能够检测出该信息已经被篡改、破坏。由此归纳起来，对网络安全的定义可以表述如下：

所谓网络安全，就是在分布式网络环境中对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容遭到破坏、更改、泄露，或者网络服务被中断、拒绝或被非授权使用和篡改。网络安全具有信息安全的基本属性。从广义上说，凡是涉及网络上信息的机密性、完整性、认证、可用性、可靠性和不可否认性的相关理论和技术，都属于网络安全所要研究的范畴。网络的安全性包括网络安全目标、资产风险评估、安全策略和用户安全意识等多个方面。

在实际中，对网络安全内涵的理解会随着“角色”的变化而有所不同，而且还在不断地延伸和丰富。例如：从用户（个人、企业等）的角度来看，他们希望涉及其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，避免他人利用窃听、假冒、篡改、抵赖等手段侵犯其利益。

从网络运营者的角度来看，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现陷门、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

从安全保密部门的角度来看，他们希望对非法、有害的或者涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。

从社会教育和意识形态的角度来看，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

可见，网络安全的内涵与其保护的信息对象有关，但本质上都是在信息的安全期内保证在网络上传输或静态存放时允许授权用户访问，而不被未授权用户非法访问。网络安全涉及网络的可用性、机密性、完整性、可靠性、访问控制、不可否认性及匿名性。网络安全除了以上这些技术问题之外，还涉及组织和法律方面的问题。显然，网络安全涵盖的内容很多，并不像初次接触网络安全技术的人想象得那么简单。

网络安全目标

网络安全与信息安全的研究领域相互交错与关联，网络安全具有信息安全的基本属性。从本质上来说，网络安全就是要保证网络上信息存储和传输的安全性。根据网络安全的定义，网络安全的主要目标是保护网络信息系统，使其远离安全危险、不受安全威胁、不出安全事故。从网络安全技术的角度来看，网络安全目标主要包含以下几个方面：

1. 机密性

机密性也称保密性，是指网络通信中的信息不被非授权者所获取与使用，只允许授权用户访问的特性。机密性是一种面向信息的安全性，它建立在可靠性和可用性的基础之上，是保障网络信息系统安全的基本要求。在网络系统的不同层次上有着不同的机密性及相应的防范措施。在物理层上，主要采取电磁屏蔽技术、干扰及跳频技术来防止电磁辐射所造成的信息外泄；在网络层、传输层和应用层则主要采取加密、访问控制、审计等方法来保障信息的机密性。

2. 完整性

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。只有得到允许的用户才能修改实体或进程，并且能够判别实体或进程是否已被篡改。也就是说，信息的内容不能被未授权的第三方修改；数据在存储或传输的过程中不被修改、破坏，不出现数据包的丢失、乱序等。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。

3. 可用性

网络可用性指网络信息系统可被授权实体访问并按要求可使用的特性，用来衡量计算机网络系统提供持续服务的能力，与其相关的参数包括链路长度（km）、双向全程故障（次/年）、无故障工作时间 MTBF（h）、失效率 F（%）、可用性。可用性常用网络可用率 A（%）来描述，即一个网络系统或设备在一个给定的时间间隔内可操作的总时间与时间间隔的比，计算公式是：

$$A（\%）=（网络总运行时间–网络无效时间）/网络总运行时间$$

实际上，可用率就是“网络有效时间/网络总运行时间”，也等于“1–（网络无效时间/网络总运行时间）”。例如，PSTN 交换系统要求有 99.999%的可用性，就是每年大多只能有 5 分钟的停工时间。

4. 可靠性

网络的可靠性，是指网络系统能够在规定的条件下和规定的时间内完成预定功能的能力，它包括网络结构的安全性、适用性和耐久性；当以概率来度量时，称之为可靠度。可靠性包括网络硬件的可靠性、软件的可靠性、通信系统的可靠性、人员可靠性和环境可靠性等方面，其

主要参数为无故障运行时间、环境条件和规定的功能。人为攻击或自然破坏所造成的网络不稳定性属于网络安全问题。可靠度可用关于时间 t 的函数表示：

$$R(t) = P(T > t)$$

其中，t 为规定的时间，T 表示网络系统或者设备的寿命。

由可靠度的定义可知，$R(t)$描述了网络系统或者设备在$(0, t)$时间内完好的概率，且 $R(0)=1$，$R(+\infty)=0$。

5. 真实性

真实性是指网络信息系统的访问者与其声称的身份是一致的。一般通过认证来验证其真实性，以保证信息的发送者和接收者都能证实网络通信过程中所涉及的另一方，确信通信的另一方确实具有其所声称的身份。人类面对面通信可以通过视觉很轻松地解决这个问题，但当通信实体在不能看到对方的媒体上交换信息时，认证就比较复杂了。例如，你如果收到一封电子邮件，其中所包含的信息称这是你的朋友发送的邮件或者你的上级领导发来的通知或函件。那么，你如何才能确信该邮件的真实性呢？这时就需要认证技术来帮助解决。认证是网络通信系统安全的基础。

6. 不可否认性

不可否认性也称作不可抵赖性，即在网络信息系统的信息交互过程中所有参与者都不可能否认或抵赖曾经完成的操作。不可否认性是对面向通信双方（人、实体或进程）的信息真实统一的安全要求，它包括收、发双方均不可抵赖。不可否认性涉及两个方面：一是源节点发送证明，它是提供给信息接收者的证据，使发送者谎称未发送过这些信息或者否认其内容的企图不能得逞；二是交付证明，它是提供给信息发送者的证据，使接收者谎称未接收过这些信息或者否认其内容的企图不能得逞。

网络安全是一个系统

由上述对网络安全定义和安全目标的讨论可知，网络安全的内涵主要集中在对通信和网络资源的保护方面。实际上，网络安全不仅涉及安全防护，还包括入侵检测、应急响应以及数据灾难备份与恢复等内容。在许多情况下，作为对攻击的响应，网络管理员需要设置附加的保护机制和措施。同时，网络攻击技术也应包含在网络安全研究的范畴之中。只有对网络攻击技术有比较深刻的了解，才能做好网络安全工作。因此，ITU-T X.800 标准认为：网络安全包含了安全攻击（Security Attack）、安全服务（Security Service）和安全机制（Security Mechanism）等方面，并在逻辑上分别进行了定义。安全攻击是指损害机构所拥有信息安全的任何行为；安全服务是指采用一种或多种安全机制来抵御安全攻击，提高机构的数据处理系统的安全性和信息传输安全性的服务；安全机制是指用于检测、预防安全攻击或者恢复系统的机制。在这种意义上，网络安全是通过循环往复的保护、攻击、检测和响应而实现的。

由此看来，网络安全不仅研究安全防护技术，还要研究网络攻击技术以及用于防御这些攻击的对策。从网络系统安全的角度考虑，网络安全攻防技术包括网络防护和网络攻击两大类，如图 1.1 所示。

对于不同环境和应用中的网络安全，还可以将其划分为以下方面：

► 运行系统安全，即保证数据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、处理和传输的数据造成破坏和损失；避免由于电磁泄漏而产生信息泄露，同时干扰他人或受他人干扰。

- 网络系统信息的安全，包括用户口令认证、用户存取权限控制、数据存取权限、访问方式控制、安全审计、安全问题跟踪、计算机病毒防治和数据加密等。
- 网络信息的健康性，包括信息过滤等，主要指防止和控制非法、不健康的信息自由传输，抑制公用网络信息传输失控。
- 网络上信息内容的安全，主要侧重于保护信息的机密性、真实性（认证）和完整性。避免攻击者利用系统漏洞实施篡改、泄露、窃听、冒充、欺骗等破坏行为。

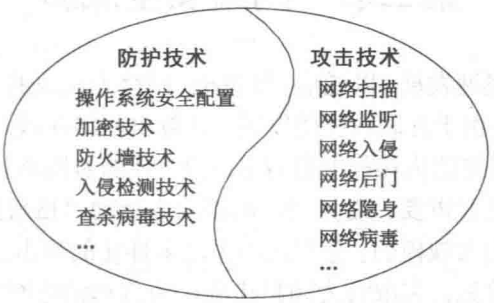

图 1.1 网络安全攻防技术

根据以上对网络安全定义的讨论可知，网络安全显然是一个系统。它不是防火墙、入侵检测和虚拟专用网，不是加密、认证、授权和审计，也不是网络设备公司及其任何合作伙伴或竞争对手能够给你提供的任何东西。尽管这些产品、技术在其中扮演着十分重要的角色，但网络安全的概念更为宽泛。网络安全起始于安全策略，还涵盖了必须遵守这些安全策略的人以及实施这些策略的人。那么，对于网络安全来说什么是系统呢？网络安全系统是指通过相互协作的方式为信息资产提供安全保障的全体网络产品、技术、策略以及最优做法的集合。因此，从狭义的角度看，网络安全是指防护网络系统以及信息资源不受自然和人为有害因素的威胁和危害。若从广义的角度看，凡是与网络上信息的机密性、完整性、认证、可用性、可控性、不可否认性等相关的理论、技术和产品，都属于网络安全的研究范畴；若从社会学的角度看，网络安全是一个系统，涵盖网络安全战略布局、安全文化、人才培养、产业发展等方面。

练习

1．简述计算机网络安全的定义和基本特性。

2．为什么要研究网络安全？

3．为什么说网络安全是一个系统？

4．在短时间内向网络中的某台服务器发送大量无效连接请求，导致合法用户暂时无法访问服务器的攻击行为，破坏了（ ）。

a．机密性 b．完整性 c．可用性 d．可控性

5．统计显示，80%的网络攻击源于内部网络，因此必须加强对内部网络的安全控制和防范。在下面的措施中，无助于提高局域网内安全性的措施是（ ）。

a．使用防病毒软件 b．使用日志审计系统

c．使用入侵检测系统 d．使用防火墙防止内部攻击

【参考答案】 5.c 6.d。

补充练习

1. 进一步深入研究、理解“网络安全”“网络运营者”“网络数据”“个人信息”等与网络安全法相关的专业术语。

2. 通过互联网，查找对网络安全的有关定义描述，研究网络安全所要实现的主要目标。

第二节 网络安全威胁

当今世界信息化建设飞速发展，以通信、计算机、网络为代表的互联网技术更是日新月异，令人眼花缭乱、目不暇接。由于互联网络的发展，计算机网络在政治、经济和生活的各个领域正在迅速普及，全社会对网络的依赖程度也越来越高。伴随着网络技术的发展和进步，网络信息安全问题已变得日益突出和重要。近年来，网络攻击活动“日新月异”，攻击行为已经从零碎的小规模的攻击发展成为大规模的、分布式和手段多样化的攻击。只有了解网络所面临的各种安全威胁，才能够有的放矢，采取有力防护措施，防范和消除网络安全隐患。

学习目标

- ▶ 了解网络安全的脆弱性；
- ▶ 了解网络所面临的安全威胁。

关键知识点

- ▶ 网络系统的脆弱性导致了网络安全问题。

网络安全的脆弱性

网络通信要求各方都要按照规定的协议或规则进行；若通信用户不按照规则或者利用协议缺陷进行通信，就可能导致网络系统通信出现混乱、系统出现漏洞或者信息被非法窃取。由于因特网在设计之初缺乏安全方面的总体构想与设计，致使互联网存在脆弱性。也就是说，互联网本身存在一些固有的脆弱性（脆弱点），非授权用户利用这些脆弱点可对网络系统进行非法访问。这种非法访问会使系统内数据的完整性受到威胁，也可能使信息遭到破坏而不能继续使用，更为严重的是有价值的信息被窃取而不留任何痕迹。

脆弱点也称为漏洞，是在网络安全领域无法忽略的概念。一个脆弱点可能是某个应用程序、系统、设备或者服务本身在编码或设计时所产生的错误或缺陷，它反映该程序、系统、设备或服务对特定威胁攻击或者危险事件的敏感性或者攻击起作用的可能性。在软件方面，脆弱点可能来自编码时产生的错误，也可能来自业务逻辑设计的缺陷或者交互的不合理性；在硬件方面，脆弱点则主要来自设计的不合理之处，例如硬件芯片的设计存在问题。这些安全缺陷、错误或者不合理之处如果被人利用，不管是有意还是无意，都会给整个网络系统带来不利影响。例如，网络系统管理权限被窃取，重要的数据或者资料被窃取、篡改甚至破坏等。