

信息安全专业系列教材

信息安全专业 科技英语

English for
Information Security

李 剑 编著



北京邮电大学出版社
www.buptpress.com

信息安全专业系列教材

信息安全专业科技英语

English for Information Security

李 剑 主编

北京邮电大学出版社

· 北 京 ·

内 容 简 介

本书采用英文方式介绍了信息安全领域最常用的知识。从技术方面来讲主要有黑客攻击技术、密码学、防火墙技术、入侵检测技术、网络安全协议、虚拟专用网技术、计算机病毒、公钥基础设施等。除此之外还介绍了当前信息安全管理方面的一些知识。

本书适合于信息安全专业的研究生或本科生。本书一方面可以作为“信息安全专业科技英语”课的教材,另一方面也可以作为信息安全专业“信息安全概论”课的英文版教材。

图书在版编目(CIP)数据

信息安全专业科技英语/李剑主编. —北京:北京邮电大学出版社,2007(2007.7 重印)
ISBN 978-7-5635-1388-8

I. 信… II. 李… III. 信息系统—安全技术—英语—高等学校—教材 IV. H31

中国版本图书馆 CIP 数据核字(2007)第 001486 号

书 名: 信息安全专业科技英语

作 者: 李 剑

责任编辑: 李欣一

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路 10 号(邮编:100876)

北方营销中心:电话:010—62282185 传真:010—62283578

南方营销中心:电话:010—62282902 传真:010—62282735

E-mail:publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京市梦宇印务有限公司

开 本: 787 mm×960 mm 1/16

印 张: 18.75

字 数: 408 千字

印 数: 3 001—6 000 册

版 次: 2007 年 2 月第 1 版 2007 年 7 月第 2 次印刷

ISBN 978-7-5635-1388-8/TN·475

定 价:28.00 元

· 如有印装质量问题,请与北京邮电大学出版社营销中心联系 ·

前 言

目前信息安全专业已经在全国如火如荼地开展起来,但是一直没有这门专业的专业英语教材。这对于培养全面发展的信息安全专业人员是不利的。主要有以下原因:

(1) 目前在信息安全领域,国内和国外的产品在很多方面还有很大差距,所以需要学习国外技术,这就需要有高的信息安全专业英语水平;

(2) 学生在研究时,需要看国外信息安全方面的专业英文资料;

(3) 学生在学习中文专业词语的时候,不明白相应的英语应该怎么写,特别是在写科技论文的时候,如“漏洞”一词应该是“Vulnerability”,许多同学就不会。

本教材就是为满足这些需求而编写的。

全书分为9章。第1章“Hacker Attack Technology”主要介绍黑客和攻击的概念以及目前常见的黑客攻击手法。第2章“Cryptography”,主要介绍当前各种密码学技术。第3章“Firewall”主要介绍防火墙技术及防火墙的结构。第4章“Intrusion Detection System”主要介绍入侵检测系统、入侵防御系统以及异常防御系统等。第5章“Network Security Protocol”主要介绍当前流行的一些网络安全协议,包括 Kerberos 协议、SSL 协议、SET 协议和 IPSec 协议。第6章“Virtual Private Network”主要介绍虚拟专用网技术。第7章“Computer Virus”主要介绍计算机病毒。第8章“Public Key Infrastructure”主要介绍公钥基础设施及 CA 证书。第9章“Information Security Management”简要介绍了当前信息安全管理方面的一些知识。

本教材包含了目前信息安全领域常用的攻击技术和防护技术,以及信息安全管理知识。在讲解时,可以根据学生对象来选择要教的内容以及内容的深度。

本教材可以作为信息安全专业学生的“信息安全专业英语”,也可以当做“信息安全概论”的英文版本。

感谢杨义先教授、罗群副教授,他们对本书的出版提出了宝贵的意见和建议。其他参与本书审阅编写等工作的还有景博、王智贤、许亮等,这里一并谢过!

由于本书作者水平有限,书中疏漏与错误之处在所难免,恳请广大同行和读者指正,我将在下一版中改正。我的电子邮箱是 securitydoctor@163.com。

李 剑

2006 年 11 月 30 日

北京邮电大学信息安全中心

目 录

Catalogue

Chapter 1 Hacker Attack Technology

1.1	Definition and Classification of Attack	1
1.1.1	Definition of Hacker	1
1.1.2	Definition of Attack	2
1.1.3	Classification of Attack	2
1.2	The Process or Methodology Hackers Use to Attack	3
1.2.1	Performing Reconnaissance	3
1.2.2	Scanning and Enumeration	4
1.2.3	Gaining Access	5
1.2.4	Escalation of Privilege	5
1.2.5	Maintaining Access	6
1.2.6	Covering Tracks and Placing Backdoors	6
1.3	The Methods and Ways of Attack	7
1.3.1	Network Scanning	7
1.3.2	Password Cracking Attack	12
1.3.3	IP Spoofing Attack	18
1.3.4	The Buffer Overflow Attack	20
1.3.5	DoS Attack	24
1.3.6	SQL Injection Attack	30
1.3.7	Trojan Horse Attack	32
1.3.8	Social Engineering	34

Chapter 2 Cryptography

2.1	Cryptography Introduction	41
-----	---------------------------------	----

2.1.1	Terminology	41
2.1.2	History of Cryptography and Cryptanalysis	43
2.1.3	Modern Cryptography	47
2.1.4	Legal Issues Involving Cryptography	54
2.2	Substitution Cryptography	56
2.2.1	Simple Substitution	57
2.2.2	Homophonic Substitution	59
2.2.3	Polyalphabetic Substitution	60
2.2.4	Polygraphic Substitution	61
2.2.5	Mechanical Substitution Ciphers	63
2.2.6	The One-time Pad	63
2.2.7	Substitution in Modern Cryptography	64
2.3	Symmetric-key Cryptography	64
2.3.1	Types of Symmetric-key Algorithms	65
2.3.2	Speed	65
2.3.3	Limitations	65
2.3.4	Reversibility	66
2.3.5	Attacks on Symmetric Ciphers	66
2.3.6	Examples	67
2.4	Public-key Cryptography	67
2.4.1	History	68
2.4.2	Security	69
2.4.3	Applications	70
2.4.4	Practical Considerations	70
2.4.5	Examples	76
2.5	Cryptographic Hash Function	79
2.5.1	Overview	79
2.5.2	Related Algorithms	80
2.5.3	Cryptographic Properties	80
2.5.4	Applications of Hash Functions	81
2.5.5	Merkle-Damgård Hash Functions	82
2.5.6	Hash Functions Based on Block Ciphers	83
2.5.7	Hash Functions to Build other Cryptographic Primitives	83
2.5.8	List of Cryptographic Hash Functions	83

Chapter 3 Firewall

3.1	Introduction	88
3.2	Firewall Technologies	94
3.2.1	Packet Filtering Firewall	94
3.2.2	Circuit Level Gateway Firewall	95
3.2.3	Application Level Gateway Firewall	95
3.2.4	Stateful Multilayer Inspection Firewall	96
3.3	Firewall Architectures	97
3.3.1	Single-Box Architectures	97
3.3.2	Screened Host Architectures	101
3.3.3	Screened Subnet Architectures	103
3.4	Windows Firewall	108
3.4.1	Introduction	108
3.4.2	Using the Exceptions Tab	110
3.5	Problems and Benefits of Firewall	112
3.5.1	Firewall Related Problems	112
3.5.2	Benefits of a Firewall	113

Chapter 4 Intrusion Detection System

4.1	Introduction	116
4.1.1	Types of Intrusion Detection Systems	116
4.1.2	Passive System vs. Reactive System	117
4.2	State of the Art	118
4.2.1	From Intrusion Detection to Anomaly Prevention	118
4.2.2	Focus on Anomaly Prevention Systems	119
4.2.3	Generic Functional Architecture	120
4.3	Data Collection	123
4.3.1	Short Definition	123
4.3.2	NIDS	124
4.3.3	HIDS	125
4.3.4	NNIDS	125
4.3.5	Honeypot as a Sensor	125
4.3.6	IPS	126

4.3.7	DIDS	126
4.3.8	Multi-layered Integration	127
4.3.9	Correlation	127
4.4	Data Processing for Detection	128
4.4.1	Short Definition	128
4.4.2	Misuse Detection (or Scenario Based Analysis)	128
4.4.3	Anomaly Detection (or Behavior Analysis)	129
4.4.4	Emerging Algorithms	131
4.5	Alarms, Logs and Actions	133
4.5.1	Passive Actions	133
4.5.2	Active Actions	133
4.6	Example: Data Mining Approaches for IDS	134
4.6.1	Introduction	135
4.6.2	The Architecture	137
4.6.3	Mining Audit Data	141
4.6.4	Feature Construction	146
4.6.5	Experiments	149
4.7	Known Problems with IDS	149
4.7.1	Lack of Adaptivity	149
4.7.2	False Positive & False Negative	151
4.7.3	Field of Vision	151
4.7.4	Performance	152
4.7.5	Increasing Cost	153
4.7.6	Complex Management Issues	154
4.7.7	Evasion Techniques	155

Chapter 5 Network Security Protocol

5.1	Introduction	159
5.2	Kerberos Protocol	160
5.2.1	History and Development	160
5.2.2	Description	161
5.2.3	Use	162
5.2.4	The Protocol	162
5.2.5	Kerberos Operation	163

5.2.6	Kerberos Drawbacks	165
5.3	SSL Protocol	165
5.3.1	Description	165
5.3.2	Ciphers Used with SSL	167
5.3.3	The SSL Handshake	169
5.3.4	Server Authentication	171
5.3.5	Client Authentication	172
5.3.6	Applications	175
5.4	SET Protocol	176
5.4.1	Introduction	176
5.4.2	Overview of SET Protocol	177
5.4.3	SET Cryptography	179
5.4.4	SET Process	180
5.4.5	Certificates Insurance	181
5.4.6	Security of SET	181
5.4.7	Future of SET	182
5.5	IPSec Protocol	182
5.5.1	Current Status as a Standard	183
5.5.2	Design Intent	184
5.5.3	Technical Details	184
5.5.4	IPSec Protocol Types	186
5.5.5	Implementations	191

Chapter 6 Virtual Private Network

6.1	Authentication Mechanism	195
6.2	Types of VPN	196
6.3	Characteristics in Application	197
6.4	Tunneling	198
6.4.1	Two Types of VPN Tunneling	199
6.4.2	Point-to-Point Tunneling Protocol	199
6.4.3	Layer 2 Tunneling Protocol	201
6.4.4	SSL VPN	207
6.4.5	MPLS VPN	208
6.5	Various Topology Scenarios	211

6.5.1	Topology 1	212
6.5.2	Topology 2	212
6.5.3	Topology 3	213
6.5.4	Topology 4	213
6.5.5	Topology 5	214
6.5.6	Topology 6	214
6.6	VPN Security Dialogs	215

Chapter 7 Computer Virus

7.1	Introduction	218
7.1.1	Comparison with Biological Viruses	218
7.1.2	Distinction between Malware and Computer Viruses	219
7.1.3	Effects of Computer Viruses	219
7.1.4	Use of the Word “Virus”	219
7.1.5	History	219
7.2	Virus Classification	221
7.2.1	Boot Sector Virus	221
7.2.2	Companion Virus	224
7.2.3	E-mail Virus	224
7.2.4	Logic Bomb	227
7.2.5	Macro Virus	228
7.2.6	Cross-site Scripting Virus	235
7.2.7	Trojan Horse	241
7.2.8	Computer Worm	241
7.3	Why People Create Computer Viruses	245
7.4	Replication Strategies	245
7.4.1	Nonresident Viruses	246
7.4.2	Resident Viruses	246
7.4.3	Host Types	247
7.5	Methods to Avoid Detection	247
7.5.1	Avoiding Bait Files and Other Undesirable Hosts	248
7.5.2	Stealth	249
7.5.3	Self-modification	249
7.5.4	Simple Self-modifications	249

7.5.5	Encryption with a Variable Key	250
7.5.6	Polymorphic Code	250
7.5.7	Metamorphic Code	251
7.6	Vulnerability and Countermeasures	251
7.6.1	The Vulnerability of Operating Systems to Viruses	251
7.6.2	The Role of Software Development	252
7.6.3	Anti-virus Software and Other Countermeasures	253

Chapter 8 Public-Key Infrastructure

8.1	PKI Introduction	256
8.1.1	Purpose	256
8.1.2	Functions	257
8.1.3	How Public and Private-key Cryptography Works	258
8.1.4	Who Provides the Infrastructure	259
8.1.5	PKI Typical Use	260
8.1.6	Alternatives	261
8.1.7	PKI History	262
8.1.8	Usage Examples	263
8.2	Certificate Authority	263
8.2.1	Issuing a Certificate	264
8.2.2	Security	264
8.2.3	Public-Key Certificate	265
8.3	X.509	267
8.3.1	History and Usage	267
8.3.2	Certificates	268
8.3.3	Sample X.509 Certificates	269
8.3.4	Security	272
8.3.5	Public-Key Infrastructure Working Group	272
8.3.6	Protocols and Standards Supporting X.509 Certificates	273
8.4	Trusted Third Party	273
8.4.1	An Example	274
8.4.2	Actual Practice	274
8.4.3	Parallels Outside Cryptography	274
8.5	Certificate Revocation List	275

8.5.1	CRL Introduction	275
8.5.2	Problems with All CRLs	276
8.6	An Example of a PKI in Action	277
Chapter 9 Information Security Management		
9.1	ISO/IEC 17799	282
9.2	ISO/IEC 27001	284
9.3	ISM3	284
参考文献		287

Chapter 1

Hacker Attack Technology

With the rapid growth of interest in the Internet and the Windows operating system, network security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has only increased that concern.

1.1 Definition and Classification of Attack

1.1.1 Definition of Hacker

A hacker is someone who creates and modifies computer software and computer hardware, including computer programming, administration, and security-related items. The term usually bears strong connotations, but may be either favorable or denigrating depending on cultural context. Common definitions include:

In computer programming, a hacker is a software designer and programmer who builds elegant, beautiful programs and systems. A hacker can also be a programmer who hacks or reaches a goal by employing a series of modifications to exploit or extend existing codes or resources. For some, “hacker” has a negative connotation and refers to a person who “hacks” or uses kludges to accomplish programming tasks that are ugly, inelegant, and inefficient. This negative form of the noun “hack” is even used among users of the positive sense of “hacker”.

In computer security, a hacker is a person who specializes in work with the security mechanisms for computer and network systems. While including those who endeavor to



strengthen such mechanisms, it more often is used, especially in the mass media, to refer to those who seek access despite them.

In other technical fields, hacker is extended to mean a person who makes things work beyond perceived limits through their own technical skill, such as a hardware hacker, or reality hacker.

In hacker culture, a hacker is a person who has attained a certain social status and is recognized among members of the culture for commitment to the culture's values and a certain amount of technical knowledge.

1.1.2 Definition of Attack

Attack is an assault against a computer system or network as a result of deliberate, intelligent action; for example, denial of service attacks, penetration and sabotage. Such as brute force attack, dictionary attack, denial of service attack, replay attack, piggybacking, penetration and sabotage.

1.1.3 Classification of Attack

According to the different classification standard, there can be different attack classification. Based on the service of network is changed or not, attacks can be divided into two categories: passive attack and active attack.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is transmitted.

Active attack involves modification of the data stream or the creation of the false stream. A typical active attack is one in which an intruder impersonates one end of the conversation, or acts as a man-in-the-middle. We can simply say that passive attack is trying to get the content of message and active attack try to do modification on the data and send the false message to the receiver. Passive attack can sub category to release of message contents and traffic analysis. Active attack has four categories: masquerade, replay, modification of messages and denial of service.

Another attack classification standard is based on the attacker is the system natural user or not. Attacks can be divided into two categories: exterior attack and interior attack.

Exterior attack is initiated by the user who is not the system's own user and enters the system through deviant way. Hacker attack belongs to the exterior attack.



Interior attack is initiated by the system natural user who has the system's account and authorization.

1.2 The Process or Methodology Hackers Use to Attack

Attackers follow a fixed methodology. To beat a hacker, you have to think like one, so it's important to understand the methodology. The steps a hacker follows can be broadly divided into six phases, which include pre-attack and attack phases:

- (1) Performing reconnaissance
- (2) Scanning and enumeration
- (3) Gaining access
- (4) Escalation of privilege
- (5) Maintaining access
- (6) Covering tracks and placing backdoors

NOTE: A denial of service (DoS) might be included in the preceding steps if the attacker has no success in gaining access to the targeted system or network.

Let's look at each of these phases in more detail so that you could understand the steps better.

1.2.1 Performing Reconnaissance

Reconnaissance is considered the first pre-attack phase and a systematic attempt to locate, gather, identify, and record information about the target. The hacker seeks to find out as much information as possible about the victim. This first step is considered a passive information gathering. As an example, many of you have probably seen a detective movie in which the policeman waits outside a suspect's house all night and then follows him from a distance when he leaves in the car. That's reconnaissance; it is passive in nature, and, if done correctly, the victim never even knows it is occurring.

Hackers can gather information in many different ways, and the information they obtained allows them to formulate a plan of attack. Some hackers might dumpster dive to find out more about the victim. Dumpster diving is the act of going through the victim's trash. If the organization does not have good media control policies, many types of sensitive information will probably go directly in the trash. Organizations should inform employees to shred sensitive information or dispose of it in an approved way.

Don't think that you are secure if you take adequate precautions with paper docu-



ments. Another favorite of the hacker is social engineering. A social engineer is a person who can smooth talk other individuals into revealing sensitive information. This might be accomplished by calling the help desk and asking someone to reset a password or by sending an E-mail to an insider telling him he needs to reset an account.

If the hacker is still struggling for information, he can turn to what many consider the hacker's most valuable reconnaissance tool, the Internet. That's right; the Internet offers the hacker a multitude of possibilities for gathering information. Let's start with the company website. The company website might have key employees listed, technologies used, job listings probably detailing software and hardware types used, and some sites even have databases with employee names and E-mail addresses.

TIP: Good security policies are the number one defense against reconnaissance attacks. They are discussed in more detail in later section "Social Engineering".

1.2.2 Scanning and Enumeration

Scanning and enumeration are considered the second pre-attack phase. Scanning is the active step of attempting to connect to systems to elicit a response. Enumeration is used to gather more in-depth information about the target, such as open shares and user account information. At this step in the methodology, the hacker is moving from passive information gathering to active information gathering. Hackers begin injecting packets into the network and might start using scanning tools such as Nmap. The goal is to map open ports and applications. The hacker might use techniques to lessen the chance that he will be detected by scanning at a very slow rate. As an example, instead of checking for all potential applications in just a few minutes, the scan might take days to verify what applications are running. Many organizations use Intrusion Detection Systems (IDS) to detect just this type of activity. Don't think that the hacker will be content with just mapping open ports. He will soon turn his attention to grabbing banners. He will want to get a good idea of what type of version of software applications you are running. And, he will keep a sharp eye out for down-level software and applications that have known vulnerabilities. An example of down-level software would be Windows 95.

One key defense against the hacker is the practice of deny all. The practice of deny all rule can help reduce the effectiveness of the hacker's activities at this step. Deny all means that all ports and applications are turned off, and only the minimum number of applications and services are turned on that are needed to accomplish the organization's goals.

NOTE: Practice of deny all rule can help reduce the effectiveness of the hacker's



activities at this step. Deny all means that all ports and applications are turned off and only the minimum number of applications and services are turned on that are needed to accomplish the organization's goals.

Unlike the elite blackhat hacker who attempts to remain stealth, script kiddies might even use vulnerability scanners such as Nessus to scan a victim's network. Although the activities of the blackhat hacker can be seen as a single shot in the night, the script kiddies scan will appear as a series of shotgun blasts, as their activity will be loud and detectable. Programs such as Nessus are designed to find vulnerabilities but are not designed to be hacking tools; as such, they generate a large amount of detectable network traffic.

TIP: The greatest disadvantage of vulnerability scanners is that they are very noisy.

1.2.3 Gaining Access

As far as potential damage, this could be considered one of the most important steps of an attack. This phase of the attack occurs when the hacker moves from simply probing the network to actually attacking it. After the hacker has gained access, he can begin to move from system to system, spreading his damage as he progresses.

Access can be achieved in many different ways. A hacker might find an open wireless access point that allows him a direct connection or the help desk might have given him the phone number for a modem used for out-of-band management. Access could be gained by finding vulnerability in the web server's software. If the hacker is really bold, he might even walk in and tell the receptionist that he is late for a meeting and will wait in the conference room with network access. Pity the poor receptionist who unknowingly provided network access to a malicious hacker. These things do happen to the company that has failed to establish good security practices and procedures.

The factors that determine the method a hacker uses to access the network ultimately comes down to his skill level, amount of access he achieves, network architecture, and configuration of the victim's network.

1.2.4 Escalation of Privilege

Although the hacker is probably happy that he has access, don't expect him to stop what he is doing with only a "Joe user" account. Just having the access of an average user probably won't give him much control or access to the network. Therefore, the attacker will attempt to escalate himself to administrator or root privilege. After all,