

《网络安全项目实践》

书籍信息

版次：1

页数：156

字数：231000

印刷时间：2017年06月01日

开本：16开

纸张：胶版纸

包装：平装-胶订

是否套装：否

国际标准书号ISBN：9787111563969

丛书名：教育部师资实践基地系列教材

内容简介

本书由徐雪鹏主编、岳大安（神州学知教育咨询有限公司CSO兼CEO）撰写，是神州数码技能教室项目的配套指导教材，也是信息安全实践基地的指定训练教材。全书共设4章，分别为网络安全基本理论、局域网安全、防火墙、虚拟专用网络安全。以培养学生的职业能力为核心，以工作实践为主线，以项目为导向，采用任务驱动、场景教学的方式，面向企业信息安全工程师人力资源岗位能力模型设置教材内容，建立以实际工作过程为框架的职业教育课程结构。本书可作为职业技术学院信息安全专业教材，也可作为信息安全从业人员的参考用书。本书配有授课用电子课件，可到机械工业出版社教材服务网www.cmpedu.com免费注册下载。

目录

前言

第1章 网络安全基本理论.1	
1.1 网络安全的重要性 .1	
1.2 网络安全CIA模型 4	
1.3 网络攻击的分类 .5	
1.4 黑客的分类 .6	
1.5 黑客入侵思路 .8	
第2章 局域网安全.14	
2.1 MAC攻击及其解决方案 15	
2.1.1 MAC攻击介绍 .15	
2.1.2 MAC攻击解决方案1：Port-Security .20	
2.1.3 MAC攻击解决方案2：AM 22	
2.2 DHCP攻击及其解决方案 .23	
2.2.1 DHCP攻击介绍：DHCP Starvation 23	
2.2.2 DHCP攻击介绍：DHCP Spoofing 26	
2.2.3 DHCP攻击解决方案：DHCP Snooping .27	
2.3 ARP攻击及其解决方案29	
2.3.1 ARPI攻击介绍：ARP DoS .29	
2.3.2 ARP攻击介绍：The Man in the Middle ARP .30	
2.3.3 ARP攻击解决方案1：AM32	
2.3.4 ARP攻击解决方案2：DAI .33	
2.3.5 ARP攻击解决方案3：Isolated VLAN .34	
2.4 生成树攻击及其解决方案 36	
2.4.1 STP攻击介绍：STP Spoofing 36	
2.4.2 STP攻击介绍：STP BPDU DoS .39	
2.4.3 STP攻击解决方案1：Root Guard 40	

2.4.4 STP攻击解决方案2 : BPDU Guard	.42
2.4.5 STP攻击解决方案3 : BPDU Filter	.43
2.5 VLAN攻击及其解决方案	45
2.5.1 VLAN攻击介绍 : Nested VLAN Hopping	45
2.5.2 VLAN攻击解决方案 : Native VLAN	.48
2.6 Routing Protocol攻击及解决方案	49
2.6.1 Routing Protocol攻击介绍 : Routing Protocol Spoofing	49
2.6.2 Routing Protocol攻击解决方案 : Routing Protocol Strong Authentication	51
2.7 LAN非授权访问攻击及其解决方案	.53
2.7.1 LAN非授权访问攻击介绍	.53
2.7.2 LAN非授权访问攻击解决方案 : IEEE 802.1x	57
第3章 防火墙	.69
3.1 IP应用非授权访问攻击及其解决方案	69
3.1.1 IP应用非授权访问攻击介绍	.69
3.1.2 IP应用非授权访问攻击解决方案1 : Packet Filter Firewall	72
3.1.3 IP应用非授权访问攻击解决方案2 : Stateful Packet Filter Firewall	74
3.2 DoS/DDoS攻击及其解决方案	.77
3.2.1 SYN Flood攻击介绍	77
3.2.2 SYN Flood攻击解决方案 : SYN Proxy	80
3.2.3 SYN Flood攻击解决方案 : Unicast Reverse Path Forwarding	.82
3.2.4 Land攻击和解决方案	.83
3.2.5 Smurf/Fraggle攻击和解决方案	.86
第4章 虚拟专用网络安全	88
4.1 网络被动监听攻击及其解决方案	88
4.1.1 网络被动监听攻击介绍	88
4.1.2 密码学原理	.89
4.2 IPSec VPN	.103
4.2.1 IPSec介绍	103
4.2.2 IPSec Transport Mode	107
4.2.3 IPSec Tunnel Mode : L2L IPSec VPN	108
4.2.4 GRE Over IPSec	.114
4.3 IKE	.119
4.3.1 IKE介绍	.119
4.3.2 PKI介绍	.129
4.4 SSL VPN	139
4.4.1 SSL	139
4.4.2 SSL VPN的访问模式	.147
参考文献	.156

前言

当前，信息技术产业欣欣向荣，处于空前繁荣的阶段，但是危害信息安全的事件也在不断发生，信息安全的形势非常严峻，黑客入侵、利用计算机实施犯罪、恶意软件侵扰、隐私泄露等，是我国信息网络空间面临的主要威胁和挑战。我国已经成为世界信息产业大国，但是还不是信息产业强国，在信息产业的基础性产品研制、生产方面还比较薄弱，例如，现在我国计算机操作系统等基础软件和CPU等关键性集成电路还部分依赖国外的产品，这就使得我国的信息安全基础不够牢固。

随着计算机和网络在军事、政治、金融、工业、商业等行业部门的广泛应用，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的安全受到破坏，不仅会带来巨大的经济损失，还会引起社会的混乱。因此，确保以计算机和网络为主要基础设施的信息系统的安全已成为世人关注的社会问题和信息科学技术领域的研究热点。当前，我国正处在全面建成小康社会的决定性阶段，实现我国社会信息化并确保信息安全是我国全面建成小康社会的必要条件之一。而要实现我国社会信息化并确保信息安全的关键是人才，这就需要我们培养规模宏大，素质优良的信息化和信息安全人才队伍。

2014年，习近平主席在中央网络安全与信息化领导小组会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建成网络强国。

当前，信息技术产业欣欣向荣，处于空前繁荣的阶段，但是危害信息安全的事件也在不断发生，信息安全的形势非常严峻，黑客入侵、利用计算机实施犯罪、恶意软件侵扰、隐私泄露等，是我国信息网络空间面临的主要威胁和挑战。我国已经成为世界信息产业大国，但是还不是信息产业强国，在信息产业的基础性产品研制、生产方面还比较薄弱，例如，现在我国计算机操作系统等基础软件和CPU等关键性集成电路还部分依赖国外的产品，这就使得我国的信息安全基础不够牢固。随着计算机和网络在军事、政治、金融、工业、商业等行业部门的广泛应用，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的安全受到破坏，不仅会带来巨大的经济损失，还会引起社会的混乱。因此，确保以计算机和网络为主要基础设施的信息系统的安全已成为世人关注的社会问题和信息科学技术领域的研究热点。当前，我国正处在全面建成小康社会的决定性阶段，实现我国社会信息化并确保信息安全是我国全面建成小康社会的必要条件之一。而要实现我国社会信息化并确保信息安全的关键是人才，这就需要我们培养规模宏大，素质优良的信息化和信息安全人才队伍。2014年，习近平主席在中央网络安全与信息化领导小组会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建成网络强国。“十三五”时期，我国要积极推动网络强国建设。网络强国涉及技术、应用、文化、安全、立法、监管等诸多方面，不仅要突出抓好核心技术突破，还要提供更加安全可靠的软硬件支撑，加快建设高速、移动、安全、泛在的新一代信息基础设施，在不断推进新技术新业务应用，繁荣发展互联网经济的同时，要强化网络和信息安全，而培育高素质人才队伍是实施网络强国战略的重要措施。2015年，国务院学位委员会和教育部增设“网络空间安全”一级学科。

我国信息安全学科建设和人才培养，迎来了全面高速发展的新阶段。本书以培养学生的职业能力为核心，以工作实践为主线，以项目为导向，采用任务驱动、场景教学的方式，面向企业信息安全工程师人力资源岗位设置教材内容，建立以实际工作过程为框架的职业教育课程结构。本书共有4章，分别为网络安全基本理论、局域网安全、防火墙、虚拟专用网络安全。第1章：网络安全基本理论，主要介绍了网络安全模型、网络攻击的分类、黑客的分类以及黑客入侵思路。

第2章：局域网安全，主要介绍了MAC攻击及其解决方案、DHCP攻击及其解决方案、ARP攻击及其解决方案、生成树攻击及其解决方案、VLAN攻击及其解决方案、Routing Protocol攻击及其解决方案、LAN非授权访问攻击及其解决方案。第3章：防火墙，主要介绍了IP应用非授权访问攻击及其解决方案、DoS/DDoS攻击及其解决方案。第4章：虚拟专用网络安全，主要介绍了网络被动监听攻击及其解决方案、IPSecVPN、IKE、SSL VPN。本书由徐雪鹏担任主编，岳大安和孙雨春任副主编，参加本书编写的还有赵飞、包楠、张鹏和李晓隆。由于编者水平有限，书中难免存在不当和疏漏之处，敬请读者批评指正。联系方式ceo@knowskill.com。编者

[显示全部信息](#)

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

[更多资源请访问www.tushupdf.com](http://www.tushupdf.com)