

امنیت در اینترنت

اصول زیربنایی آن

تألیف: مهندس فاطمه ماندنی خالدي

با همکاری: استاد ارجمند مهندس عابد سلیمی

ماندنی خالدي، فاطمه

امنيت در اينترنت و اصول زيربنائي آن / تاليف فاطمه ماندني خالدي با همكاري عابد
سليمي. - تهران: آصال، ۱۳۸۴.

۵۱۲ ص.: مصور، جدول، نمودار.

ISBN 964-8384-17-7

۵۵۰۰۰ ريال

فهرستنويسی بر اساس اطلاعات فيا.

واژه نامه. کتابنامه: ص. (۵۰۰).

۱. اينترنت -- اقدامات ناميني. ۲. كامپيوترها -- ايمني اطلاعات. ۳. شبكه هاي

كامپيوني -- اقدامات ناميني. الف. سليمي، عابد. ب. عنوان.

۸۴-۸۰۳ م

۰۰۵/۸

TK۵۱۰۵/۵۹/م۲

❖ نام كتاب: امنيت در اينترنت و اصول زيربنائي آن

❖ مؤلف: فاطمه ماندني خالدي با همكاري استاد عابد سليمي

❖ ناشر: انتشارات آصال

❖ نوبت چاپ: اول - ۱۳۸۴

❖ ليتوگرافي: موسسه فرازنگر (۸۸۹۱۵۶۳۱)

❖ ناظر فني چاپ: مريم حنائي اقدم

❖ تيراژ: ۵۰۰۰ نسخه

❖ بهاء: ۵۵۰۰ تومان

❖ طرح جلد: گلرخ عبدالوند (۰۹۱۲۳۵۰۷۰۹۴)

❖ حروفچيني و صفحه آرائي: فاطمه ماندني خالدي

شابك: ۷-۱۷-۸۳۸۴-۹۶۴-۷-۹۶۴-۸۳۸۴-۱۷-۷ ISBN:964-8384-17-7

مرکز پخش: كتاب پايخت

تهران - خيابان انقلاب - خيابان لبافي نژاد - بين خيابان فخررازي و خيابان ۱۲ فروردين

بلاک ۱۷۰ - كتاب پايخت تلفن: ۶۶۹۵۳۰۷۵ - ۶۶۹۶۷۷۶۸

فهرست مطالب

بخش اول: آشنایی با اینترنت و اصول امنیتی آن

فصل ۱: آشنایی با اینترنت

- ۱۷ ☒ مقدمه
- ۱۷ ☒ زیرساخت اینترنت
- ۱۷ ☒ معماری اینترنت
- ۱۹ ☒ پروتکل اینترنت (TCP/IP)
- ۲۰ ☒ جریان اطلاعات در TCP/IP
- ۲۱ ☒ اجزای پروتکل TCP/IP
- ۳۰ ☒ دستورات کمکی TCP/IP
- ۳۵ ☒ کاربردهای اینترنت

فصل ۲: امنیت در اینترنت

- ۳۷ ☒ مقدمه
- ۳۷ ☒ ضرورت تأمین امنیت در اینترنت
- ۳۸ ☒ پارامترهای بنیادی امنیت
- ۴۰ ☒ اهداف نفوذگران
- ۴۱ ☒ انواع حملات
- ۴۴ ☒ انواع آسیب پذیرها
- ۴۵ ☒ آشنایی با سناریوی کلی نفوذ

فصل ۳: مراحل اولیه ایجاد امنیت

- ۴۹ ☒ مقدمه
- ۴۹ ☒ تنظیم سیاستهای امنیتی
- ۴۹ ☒ پارامترهای لازم برای تنظیم و توسعه سیاستهای امنیتی
- ۵۲ ☒ ساختار سیاستهای امنیتی
- ۵۴ ☒ ویژگیهای یک سیاست امنیتی خوب
- ۵۴ ☒ راهکارهای اولیه تأمین امنیت
- ۵۴ ☒ ایمن نمودن سیستم های عامل و برنامه های کاربردی
- ۵۵ ☒ حذف سرویسهای غیرضروری
- ۵۵ ☒ رمز عبور
- ۵۶ ☒ عدم اجرای برنامه هایی که منابع آنها تأیید شده نیست با اجرای سیاست PKI
- ۵۶ ☒ ایجاد محدودیت در برخی از ضمایم E-mail
- ۵۸ ☒ اعطای حداقل امتیاز به کاربران

- ۵۸ ■ فایل‌های ثبت رخداد
- ۶۰ ■ چاپگر شبکه
- ۶۰ ■ پروتکل SNMP
- ۶۱ ■ تست امنیت شبکه
- ۶۱ ○ آشنایی با Netstat و سرنیچ های آن

فصل ۴: تعیین استراتژی دفاعی

- ۶۷ ☒ مقدمه
- ۶۷ ☒ بهره گیری از استراتژی دفاع در عمق "Defense In Depth"
- ۶۷ ☒ ارکان اصلی این استراتژی
- ۷۰ ☒ امنیت لایه ای "Layered Security" رهیافتی از این استراتژی
- ۷۱ ■ لایه ۱: Perimeter Security
- ۷۳ ■ لایه ۲: Network Security
- ۷۶ ■ لایه ۳: Host Security
- ۷۷ ■ لایه ۴: Application Security
- ۷۸ ■ لایه ۵: Data Security
- ۷۹ ☒ مجموعه آمار منتشر شده در مورد حملات و آسیب پذیریها

بخش دوم: ابزارها و سرویس های امنیتی

فصل ۵: Firewall

- ۸۳ ☒ مقدمه
- ۸۳ ☒ فایروال ها چه وظایفی بر عهده دارند
- ۸۴ ☒ نواحی خطر و نکاتی که بایستی لحاظ نمود
- ۸۵ ☒ خصوصیات برجسته فایروال های امروزی
- ۸۷ ☒ پارامترهایی که در عملکرد فایروال ها تأثیر گذارند
- ۸۷ ☒ مزایا و معایب استفاده از فایروال
- ۸۸ ☒ انواع فایروال از حیث ساختاری
- ۸۹ ■ فایروال های Packet Filter
- ۹۳ ■ فایروال های Stateful Inspection
- ۹۶ ■ فایروال های Application Gateway / Proxy
- ۹۹ ■ فایروال های Hybrid
- ۱۰۰ ■ فایروال های شخصی
- ۱۰۱ ☒ انواع پلت فرم قابل اجرا
- ۱۰۱ ☒ توپولوژی فایروال
- ۱۰۱ ■ محیط هایی با امکانات امنیتی محدود
- ۱۰۵ ■ محیط هایی با امکانات امنیتی مناسب
- ۱۱۰ ☒ سیاست امنیتی فایروال
- ۱۱۵ ☒ نمونه ای از توپولوژی فایروال به همراه Rule-base پیاده سازی شده
- ۱۱۸ ☒ توصیه های اجرایی
- ۱۱۹ ☒ ابزارهای لازم برای تست نفوذ و ارزیابی فایروال
- ۱۲۴ ☒ آیا پورت ۸۰ برای ارتباطات http ایمن میباشد؟
- ۱۲۵ ☒ آشنایی با NAT
- ۱۲۵ ■ انواع NAT

۱۲۷	▪ نحوه عملکرد NAT
۱۳۳	▪ امنیت
۱۳۴	✓ آشنایی با Cisco IOS Firewall (CBAC)
۱۳۷	▪ عملکرد CBAC
۱۳۷	▪ مزایا و معایب CBAC
۱۳۸	▪ پیکربندی CBAC

فصل ۶: IDS

۱۴۹	✓ مقدمه
۱۵۰	✓ انواع IDS
۱۵۱	▪ معماری
۱۵۲	▪ استراتژی کنترل
۱۵۴	▪ زمانبندی
۱۵۴	▪ سرچشمه اطلاعات
۱۵۷	▪ نوع آنالیز
۱۵۸	▪ نوع پاسخ
۱۵۸	✓ ابزارهای مکمل
۱۵۹	▪ Vulnerability Assessment
۱۶۰	▪ File Integrity Checkers
۱۶۰	▪ Honeypot Systems
۱۶۱	✓ استقرار IDS ها
۱۶۱	▪ استقرار Network-Based IDS
۱۶۲	▪ استقرار Host-Based IDS
۱۶۳	✓ نقاط قوت و محدودیت IDS ها
۱۶۵	✓ مقایسه ای بین چند IDS موجود

فصل ۷: VPN

۱۶۷	✓ مقدمه
۱۶۷	✓ انواع ارتباطات VPN
۱۶۹	✓ ساختار VPN
۱۷۱	✓ Tunneling
۱۷۴	✓ مزایا و معایب VPN
۱۷۴	✓ اینترفیس های رایج VPN
۱۷۵	✓ پیکربندی VPN

فصل ۸: پروتکل ها و سرویس های امنیتی

۱۸۱	✓ مقدمه
۱۸۱	✓ IPSec
۱۸۲	▪ پروتکل ها و مدهای IPSec
۱۸۵	▪ پیکربندی IPSec در ویندوز
۱۸۸	▪ ایجاد یک IPSec Policy
۱۹۳	✓ SSL
۱۹۵	▪ اهداف SSL و معماری آن
۱۹۶	▪ پارامترهای مهم ارتباطی SSL
۱۹۷	▪ پروتکل SSL Record

- ۱۹۸ پروتکل های Alert، Cipher change و Handshake
- ۱۹۹ نحوه احراز هویت در SSL
- ۱۹۹ تکنیک های رمزنگاری در SSL
- ۲۰۲ چگونگی ایجاد یک ارتباط ایمن از طریق SSL
- ۲۰۴ مشکلات امنیتی موجود در SSL
- ۲۰۴ پیکر بندی SSL در وب سرور IIS
- ۲۰۹ SSH ☒
- ۲۱۰ عملکرد SSH
- ۲۱۱ ویژگی های SSH
- ۲۱۲ استفاده از SSH در ویندوز

بخش سوم: برخی از روش های نفوذ و راه های مقابله با آن

فصل ۹: Scan

- ۲۱۷ مقدمه ☒
- ۲۱۷ (War-Dialing) Modem Scan ☒
- ۲۱۸ War-Dialing در برابر حملات ☒
- ۲۱۹ Mapping Scan ☒
- ۲۲۰ مقابله جهت یافتن توپولوژی شبکه
- ۲۲۰ Port Scan ☒
- ۲۲۱ Nmap
- ۲۲۵ مقابله با پوش پورتهای شبکه
- ۲۲۶ Vulnerability Scan ☒
- ۲۲۷ Nessus
- ۲۲۹ مقابله با پوش نقاط آسیب پذیر
- ۲۳۰ ارزیابی Nessus در مورد آسیب پذیری های موجود در یک شبکه فرضی
- ۲۳۰ (War Driving) Wireless Scan ☒
- ۲۳۰ مقابله با War Driving

فصل ۱۰: Sniff

- ۲۳۳ مقدمه ☒
- ۲۳۴ Eavesdropping با Sniffing ☒
- ۲۳۵ استراق سمع از Hub (Passive Sniffing) ☒
- ۲۳۵ نرم افزار Snort
- ۲۳۵ نرم افزار Sniffit
- ۲۳۶ استراق سمع از Switch (Active Sniffing) ☒
- ۲۳۷ نرم افزار Dsniff
- ۲۳۸ جلوه گیری از کار Switch ها با تکنیک MAC Flood
- ۲۳۸ جلوه گیری از کار Switch ها با تکنیک ARP Spoof
- ۲۳۹ استفاده از تکنیک DNS Spoof
- ۲۴۰ استفاده از تکنیک استراق سمع از SSH و HTTPS
- ۲۴۳ مایر امکانات موجود در Dsniff
- ۲۴۳ مقابله با Sniffer ها ☒

فصل ۱۱: DoS & DDoS

۲۴۷	مقدمه ☒
۲۴۸	Stopping Services from Local Network ☒
۲۴۹	▪ روش پیشگیری و مقابله
۲۴۹	Exhausting Resources from Local Network ☒
۲۵۰	▪ روش پیشگیری و مقابله
۲۵۰	Stopping Services from Internet ☒
۲۵۲	▪ روش پیشگیری و مقابله
۲۵۲	Exhausting Resources from Internet ☒
۲۵۲	▪ حمله SYN Flood
۲۵۴	○ روش پیشگیری و مقابله
۲۵۴	▪ حمله Smurf
۲۵۵	▪ حمله Fraggle
۲۵۵	○ روش پیشگیری و مقابله با حملات Sinurf و Fraggle
۲۵۵	▪ حمله DDoS
۲۵۶	○ حمله TFN\TK
۲۵۸	○ روش پیشگیری و مقابله با حملات DDoS
۲۵۹	▪ مجموعه‌ای آماری از کشف حملات DoS ☒

فصل ۱۲: Trojan & Backdoors

۲۶۳	مقدمه ☒
۲۶۳	Trojan ها ☒
۲۶۴	Backdoor ها ☒
۲۶۵	Backdoor های پنهان شده درون Trojan ها ☒
۲۶۵	▪ تروجان در سطح برنامه‌های کاربردی
۲۶۶	○ چگونه میتوان متوجه آلوده شدن سیستم به یک تروجان شد
۲۶۸	○ روشهای پیشگیری و مقابله با تروجانها در سطح برنامه‌های کاربردی
۲۶۹	▪ Rootkit های معمولی
۲۷۲	○ روشهای پیشگیری و مقابله با Rootkit های معمولی
۲۷۳	▪ Rootkit های سطح Kernel
۲۷۵	○ روشهای پیشگیری و مقابله با Rootkit های سطح هسته سیستم عامل

بخش چهارم: بیکربندی ایمن سیستم های عامل و برخی از Application ها

فصل ۱۳: ایمن نمودن سیستم های عامل

۲۷۹	مقدمه ☒
۲۸۰	مهمترین نقاط آسیب پذیر ویندوز ☒
۲۸۰	▪ اولین نقطه آسیب پذیر: Internet Information Services
۲۸۱	○ سیستم های عامل در معرض تهدید
۲۸۱	○ نحوه تشخیص آسیب پذیری سیستم
۲۸۲	○ نحوه حفاظت در مقابل نقطه آسیب پذیر
۲۸۳	▪ دومین نقطه آسیب پذیر: Microsoft SQL Server
۲۸۵	○ سیستم های عامل در معرض تهدید
۲۸۵	○ نحوه تشخیص آسیب پذیری سیستم

- ۲۸۵ ○ نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۲۸۷ ■ سومین نقطه آسیب پذیر: Windows Authentication
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۲۹۰ ○ نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۲۹۰ ○ چهارمین نقطه آسیب پذیر: Internet Explorer
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۲۹۷ ○ نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۲۹۷ ■ پنجمین نقطه آسیب پذیر: Windows Remote Access Services
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۲۹۸ ○ ششمین نقطه آسیب پذیر: Microsoft Data Access Components
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۰۰ ○ هفتمین نقطه آسیب پذیر: Windows Scripting Host
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۰۱ ○ هشتمین نقطه آسیب پذیر: Outlook Express و Outlook Messenger ها
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۰۳ ○ نهمین نقطه آسیب پذیر: File-Sharing Applications
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۰۹ ○ دهمین نقطه آسیب پذیر: Simple Network Management Protocol
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۱۰ ○ یازدهمین نقطه آسیب پذیر: اولین نقطه آسیب پذیر یونیکس (و لینوکس)
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۱۰ ○ دوازدهمین نقطه آسیب پذیر: BIND Domain Name System
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۱۱ ○ سیزدهمین نقطه آسیب پذیر: Remote Procedure Calls
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۱۱ ○ چهاردهمین نقطه آسیب پذیر: Apache Web Server
 - سیستم های عامل در معرض تهدید
 - نحوه تشخیص آسیب پذیری سیستم
- ۳۱۱ ○ پانزدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۱۲ ○ شانزدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۱۳ ○ هجدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۱۴ ○ نوزدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۱۵ ○ بیستمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۱۵ ○ بیست و یکمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۱۹ ○ بیست و دومین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۰ ○ بیست و سومین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۰ ○ بیست و چهارمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۱ ○ بیست و پنجمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۲ ○ بیست و ششمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۲ ○ بیست و هفتمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۳ ○ بیست و هشتمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۵ ○ بیست و نهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۵ ○ بیست و دهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۶ ○ بیست و یازدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۶ ○ بیست و دهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۶ ○ بیست و هفتمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۷ ○ بیست و ششمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۷ ○ بیست و پنجمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۷ ○ بیست و چهارمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۸ ○ بیست و سومین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ بیست و دومین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ بیست و یکمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ بیستمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ نوزدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ هجدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ شانزدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ پانزدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ چهاردهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ سیزدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ دوازدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ یازدهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ دهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ نهمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ هشتمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ هفتمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ ششمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ پنجمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ چهارمین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ سومین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ دومین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۳۲۹ ○ اولین نقطه آسیب پذیر:
 - نحوه حفاظت در مقابل نقطه آسیب پذیر

۳۳۱	چهارمین نقطه آسیب پذیر: Authentication
۳۳۲	○ سیستم های عامل در معرض تهدید
۳۳۲	○ نحوه تشخیص آسیب پذیری سیستم
۳۳۳	○ نحوه حفاظت در مقابل نقطه آسیب پذیر
۳۳۵	پنجمین نقطه آسیب پذیر: Clear Text Services
۳۳۶	○ سیستم های عامل در معرض تهدید
۳۳۶	○ نحوه تشخیص آسیب پذیری سیستم
۳۳۶	○ نحوه حفاظت در مقابل نقطه آسیب پذیر
۳۳۷	ششمین نقطه آسیب پذیر: Sendmail
۳۳۷	○ سیستم های عامل در معرض تهدید
۳۳۷	○ نحوه تشخیص آسیب پذیری سیستم
۳۳۸	○ نحوه حفاظت در مقابل نقطه آسیب پذیر
۳۳۹	هفتمین نقطه آسیب پذیر: Simple Network Management Protocol
۳۳۹	○ سیستم های عامل در معرض تهدید
۳۳۹	○ نحوه تشخیص آسیب پذیری سیستم
۳۴۰	○ نحوه حفاظت در مقابل نقطه آسیب پذیر
۳۴۱	هشتمین نقطه آسیب پذیر: Secure Shell
۳۴۱	○ سیستم های عامل در معرض تهدید
۳۴۱	○ نحوه تشخیص آسیب پذیری سیستم
۳۴۲	○ نحوه حفاظت در مقابل نقطه آسیب پذیر
۳۴۲	نهمین نقطه آسیب پذیر: عدم پیکربندی صحیح سرویس های NIS/NFS
۳۴۳	○ سیستم های عامل در معرض تهدید
۳۴۳	○ نحوه تشخیص آسیب پذیری سیستم
۳۴۴	○ نحوه حفاظت در مقابل نقطه آسیب پذیر
۳۴۵	دهمین نقطه آسیب پذیر: Open Secure Sockets Layer
۳۴۶	○ سیستم های عامل در معرض تهدید
۳۴۶	○ نحوه تشخیص آسیب پذیری سیستم
۳۴۶	○ نحوه حفاظت در مقابل نقطه آسیب پذیر

فصل ۱۴: ایمن نمودن E-mail و مرورگر IE

۳۴۹	☑ مقدمه
۳۵۰	☑ تهدیدات موجود
۳۵۱	☑ روشهای پیشگیری و مقابله
۳۵۱	○ پیشگیری اول: نصب Patch های سرویس گیرندگان پست الکترونیکی و IE
۳۵۴	○ پیشگیری دوم: تنظیمات ایمن IE
۳۶۱	○ پیشگیری سوم: حفظ محرمانگی یا Privacy
۳۶۱	○ رویکرد اول: مقابله با کوکی ها
۳۶۴	○ رویکرد دوم: رمزگذاری
۳۶۵	○ رویکرد سوم: مقابله با Web bug (Web Beacons) ها
۳۶۸	○ رویکرد چهارم: مقابله با IFrame ها
۳۶۸	○ رویکرد پنجم: غیرفعال نمودن ویژگی AutoComplete
۳۷۰	○ رویکرد ششم: استفاده از نرم افزارهای ضد جاسوسی
۳۷۲	○ پیشگیری چهارم: مقابله با Spam ها
۳۷۲	○ ابزارهای مورد استفاده
۳۷۴	○ شناسایی هویت فرستنده Spam
۳۷۸	○ راههای مقابله با Spam

- ۳۷۸ پیشگیری پنجم: استفاده از نرم افزارهای آنتی ویروس و فایروالهای شخصی
- ۳۸۱ پیشگیری ششم: تغییر فایل مرتبط و یا غیرفعال نمودن WSH
- ۳۸۳ پیشگیری هفتم: حفاظت در مقابل ماکروهای Office و آموزش کاربران
- ۳۸۴ پیشگیری هشتم: نمایش پسوند فایل‌های اجرایی
- ۳۸۴ پیشگیری نهم: رعایت و پایبندی به اصل حداقل امتیاز
- ۳۸۶ پیشگیری دهم: امنیت سیستم عامل
- ۳۸۶ ☐ رویکرد اول: ایمن سازی رجیستری سیستم
- ۳۸۶ ☐ رویکرد دوم: ایمن سازی اشیاء پایه
- ۳۸۸ ☐ رویکرد سوم: ایمن سازی دایرکتوریهای سیستم

فصل ۱۵: پیکربندی ایمن IIS

- ۳۸۹ ☒ مقدمه
- ۳۹۰ ☒ مواردیکه در زمان نصب IIS پیشنهاد میگردد
- ۳۹۲ ☒ سرویسهای IIS
- ۳۹۳ ☒ ایمن سازی Metabase
- ۳۹۴ ☒ روشهای کنترل دسترسی
- ۳۹۵ ☐ Authentication Methods
- ۳۹۷ ☐ Application level Permission
- ۳۹۸ ☐ اعمال محدودیت در رابطه با سرویس دهنده‌ها و دایرکتوریهای مجزای
- ۳۹۸ ☒ نحوه پیکربندی ایمن وب سایتها
- ۴۰۸ ☒ مقایسه ورژنهای مختلف IIS

فصل ۱۶: پیکربندی یک Personal Firewall

- ۴۰۹ ☒ مقدمه
- ۴۰۹ ☒ McAfee
- ۴۱۵ ☒ اعمال مجموعه قوانین فیلترینگ بر روی یک برنامه
- ۴۱۶ ☒ امکان برقراری ارتباط یا عدم برقراری آن بر اساس آدرس IP
- ۴۱۸ ☒ پیکربندی آدپتور شبکه
- ۴۱۸ ☒ سایر امکانات موجود در McAfee

بخش پنجم: متولوژی چند نوع حمله و بررسی آینده امنیت

فصل ۱۷: متولوژی چند نوع حمله و درسهایی که میتوان از آن آموخت

- ۴۲۳ ☒ مقدمه
- ۴۲۳ ☒ حمله از طریق مودم به یک شبکه تجاری
- ۴۳۰ ☒ حمله از طریق ماشینهای زامبی
- ۴۳۵ ☒ حمله از طریق پرسنل داخلی شبکه

فصل ۱۸: آینده امنیت و نقش عوامل انسانی

- ۴۴۳ ☒ مقدمه
- ۴۴۳ ☒ محدودیت راه حل‌های موجود
- ۴۴۴ ☒ وظایف مدیران سیستم
- ۴۴۶ ☒ وظایف ارائه دهندگان تکنولوژی

۴۴۷	وظایف تصمیم گیرندگان	✓
۴۴۹	نظرات یک هکر در مورد امنیت	✓

ضمائم:

۴۵۳	فهرست پورت‌های شناخته شده (Well-Known Ports)	✓
۴۶۰	پورت‌های مورد استفاده در برخی از برنامه‌ها (Special Application Ports)	✓
۴۶۹	آسیب پذیرترین پورت‌های موجود (Common Vulnerable Ports)	✓
۴۷۱	پورت‌های مورد استفاده در تروجان‌ها (Trojan & Remote Access Services Ports)	✓
۴۷۷	آلگویی از تنظیمات ایمن بر روی ویندوز XP (Security Template Settings on Windows XP)	✓
۴۸۹	بهترین ابزارهای امنیتی (Best Security Tools)	✓
۴۹۱	بهترین لینک‌های امنیتی (Best Security Links)	✓
۴۹۲	نتایج سرشماری در مورد برقراری امنیت در شبکه‌ها و اینترنت	✓
	(Network & Internet Security Poll Results)	

واژه‌نامه

۴۹۳	فهرست علائم اختصاری
۵۰۳	فهرست منابع و مراجع
۵۰۸	