

فهرست مطالب

فصل اول: مقدمه / ۱۳

۱.۱ مفاهیم امنیت کامپیوتر / ۱۴

۲.۱ معماری امنیتی OSI / ۱۸

۳.۱ حملات امنیتی / ۱۹

۴.۱ سرویس‌های امنیتی / ۲۱

۵.۱ مکانیزم‌های امنیتی / ۲۴

۶.۱ یک مدل برای امنیت شبکه / ۲۶

۷.۱ استانداردها / ۲۸

۸.۱ رئوس مطالب کتاب / ۲۹

۹.۱ منابع توصیه شده / ۲۹

۱۰.۱ اصطلاحات کلیدی و اختصارها / ۳۰

پرسش‌ها و سوال‌های فصل اول

بخش اول: رمزنگاری

فصل دوم: رمزگذاری متقارن و محرمانگی پیغام / ۳۳

۱.۲ اصول رمزنگاری متقارن / ۳۳

۲.۲ الگوریتم‌های رمزنگاری بلوکی متقارن / ۳۹

۳.۲ اعداد تصادفی و شبه تصادفی / ۴۵

۴.۲ رمزهای جریانی و RC4 / ۴۹

۵.۲ حالت‌های عملیاتی رمزنگاری بلوکی / ۵۳

۶.۲ منابع توصیه شده / ۵۹

۷.۲ اصطلاحات کلیدی و اختصارها / ۵۹

پرسش‌ها و سوال‌های فصل دوم

فصل سوم: رمزنگاری کلید-عمومی و احراز هویت پیغام / ۶۷

۱.۳ خط‌مشی‌های احراز هویت پیام / ۶۷

۲.۳ توابع امن درهم‌سازی / ۷۲

۳.۳ کدهای احراز هویت پیام یا MAC / ۷۹

۴.۳ اصول رمزنگاری کلید-عمومی / ۸۴

۵.۳ الگوریتم‌های رمزنگاری کلید-عمومی / ۸۷

۶.۳ امضاهای الکترونیکی / ۹۵

۷.۳ منابع توصیه شده / ۹۶

۸.۳ اصطلاحات کلیدی و اختصارها / ۹۶

پرسش‌ها و سوال‌های فصل سوم

بخش دوم: کاربردهای امنیت شبکه

فصل چهارم: توزیع کلید و احراز هویت کاربر / ۱۰۷

۱.۴ توزیع کلید متقارن با استفاده از رمزگذاری متقارن / ۱۰۷

۲.۴ Kerberos / ۱۰۸

۳.۴ توزیع کلید با استفاده از رمزگذاری نامتقارن / ۱۲۲

۴.۴ گواهینامه‌های X.509 / ۱۲۴

۵.۴ زیرساختار کلید-عمومی / ۱۳۲

۶.۴ مدیریت هویت فدرال / ۱۳۴

۷.۴ منابع توصیه شده / ۱۴۰

۸.۴ اصطلاحات کلیدی و اختصارها / ۱۴۰

پرسش‌ها و سوال‌های فصل چهارم

فصل پنجم: کنترل دسترسی شبکه و امنیت محاسبات ابری / ۱۴۷

۱.۵ کنترل دسترسی شبکه / ۱۴۷

۲.۵ پروتکل احراز هویت توسعه‌یافته / ۱۵۰

۳.۵ کنترل دسترسی شبکه مبتنی بر گذرگاه IEEE 802.1X / ۱۵۴

۴.۵ محاسبات ابری / ۱۵۷

۵.۵ ریسک‌های امنیتی ابر و اقدامات متقابل / ۱۶۳

۶.۵ محافظت داده‌ها در ابر / ۱۶۵

۷.۵ امنیت ابر بعنوان یک سرویس / ۱۶۸

۸.۵ منابع توصیه شده / ۱۷۱

۹.۵ اصطلاحات کلیدی و اختصارها / ۱۷۲

پرسش‌ها و سوال‌های فصل پنجم

فصل ششم: امنیت لایه - انتقال / ۱۷۵

۱.۶ ملاحظات امنیت وب / ۱۷۵

۲.۶ لایه سوکت‌های امن یا SSL / ۱۷۸

۳.۶ امنیت لایه انتقال / ۱۹۱

۴.۶ پروتکل HTTPS / ۱۹۶

۵.۶ پورته امن یا SSH / ۱۹۷

۶.۶ منابع توصیه شده / ۲۰۸

۷.۶ اصطلاحات کلیدی و اختصارها / ۲۰۸

پرسش‌ها و سوال‌های فصل ششم

فصل هفتم: امنیت شبکه‌های بی سیم / ۲۱۱

۱.۷ امنیت بی سیم / ۲۱۱

۲.۷ امنیت تجهیزات سیار / ۲۱۴

۳.۷ مروری بر شبکه‌های محلی بی سیم IEEE 802.11 / ۲۱۹

۴.۷ امنیت شبکه محلی بی سیم IEEE 802.11i / ۲۲۵

۵.۷ منابع توصیه شده / ۲۴۰

۶.۷ اصطلاحات کلیدی و اختصارها / ۲۴۱

پرسش‌ها و سوال‌های فصل هفتم

فصل هشتم: امنیت پست الکترونیکی / ۲۴۵

۱.۸ حریم خصوصی مناسب / ۲۴۵

۲.۸ S/MIME / ۲۵۲

۳.۸ دامنه‌های کلیدی پست الکترونیکی شناخته شده / ۲۷۰

۴.۸ منابع توصیه شده / ۲۷۸

۵.۸ اصطلاحات کلیدی و اختصارها / ۲۷۸

پرسش‌ها و سوال‌های فصل هشتم

فصل نهم: امنیت IP / ۲۸۱

۱.۹ بازنگری امنیت IP / ۲۸۲

۲.۹ سیاست امنیت IP / ۲۸۵

۳.۹ کپسوله کردن بار مفید امنیتی / ۲۹۳

۴.۹ ترکیب اجتماعات امنیتی / ۳۰۱

۵.۹ تبادل کلید اینترنتی / ۳۰۴

۶.۹ مجموعه روش‌های رمزگذاری / ۳۱۲

۷.۹ منابع توصیه شده / ۳۱۴

۸.۹ اصطلاحات کلیدی و اختصارها / ۳۱۵

پرسش‌ها و سوال‌های فصل نهم

بخش سوم: امنیت سیستم

فصل دهم: نرم‌افزار بد اندیش / ۳۱۹

۱.۱۰ انواع نرم‌افزارهای بداندیش (بدافزار) / ۳۲۰

۲.۱۰ ویروس‌ها - محتوای آلوده شده - انتشار / ۳۲۲

۳.۱۰ کرم‌ها - استفاده از آسیب‌پذیری - انتشار / ۳۲۸

۴.۱۰ تروجان‌ها و اسپم‌ها - مهندسی اجتماعی - انتشار / ۳۳۳

۵.۱۰ ظرفیت - خرابی سیستم / ۳۳۵

۶.۱۰ ظرفیت - عامل حمله - بات‌ها و زامبی / ۳۳۷

۷.۱۰ ظرفیت - دزدی اطلاعات - ثبت کلیدها، جعل صفحات، جاسوس‌افزار / ۳۳۹

۸.۱۰ ظرفیت - سرقت - روت‌کیت و درب‌های مخفی / ۳۴۰

۹.۱۰ اقدامات متقابل / ۳۴۲

۱۰.۱۰ حملات محرومیت - از - خدمات گسترش‌یافته / ۳۴۹

۱۱.۱۰ منابع توصیه شده / ۳۵۴

۱۲.۱۰ اصطلاحات کلیدی و اختصارها / ۳۵۵

پرسش‌ها و سوال‌های فصل دهم

فصل یازدهم: نفوذگران / ۳۵۹

۱.۱۱ نفوذگران / ۳۶۰

۲.۱۱ کشف نفوذ / ۳۶۴

۳.۱۱ مدیریت رمزعبور / ۳۷۹

۴.۱۱ منابع توصیه شده / ۳۹۰

۵.۱۱ اصطلاحات کلیدی و اختصارها / ۳۹۰

پرسش‌ها و سوال‌های فصل یازدهم

فصل دوازدهم: دیوارهای آتش / ۳۹۵

۱.۱۲ نیاز به دیوارهای آتش / ۳۹۵

۲.۱۲ خصوصیات دیوار آتش / ۳۹۶

۳.۱۲ انواع دیوارهای آتش / ۳۹۸

۴.۱۲ دیوار آتش مبنا / ۴۰۴

۵.۱۲ تنظیمات و محل استقرار دیوار آتش / ۴۰۶

۶.۱۲ منابع توصیه شده / ۴۱۱

۷.۱۲ اصطلاحات کلیدی و اختصارها / ۴۱۱

پرسش‌ها و سوال‌های فصل دوازدهم

ضمایم / ۴۱۹

ضمیمه الف: اعداد تصادفی و شبه تصادفی / ۴۲۰

ضمیمه ب: رمز جابجایی مضاعف / ۴۲۲

ضمیمه پ: لیست رمزهای عبور کرم موریس / ۴۲۴

ضمیمه ت: پاسخ تشریحی پرسش‌ها و مسائل / ۴۲۶