

امنیت شبکه پیشرفته

مؤلف:

عین‌اله جعفر نژاد قمی

(عضو هیأت علمی جهاد دانشگاهی)



علوم رایانه

تهران، خیابان انقلاب، خیابان منیری جاوید، نبش وحید نظری، شماره ۱۴۲ - تلفکس: ۶۶۴۰۰۲۲۰ - ۶۶۴۰۰۱۴۴

فهرست مطالب

فصل ۱: مفهوم امنیت شبکه، تهدیدها و حمله‌ها

۱۱	تعریف امنیت کا بیوتر	۱-۱
۱۳	اثرات رخنه‌های امنیتی	۲-۱
۱۴	چالش‌های امنیت کامپیوتر	۳-۱
۱۵	معماری امنیت OSI	۴-۱
۱۶	حمله‌های امنیتی	۵-۱
۱۹	سرویس‌های امنیتی	۶-۱
۲۰	مکانیزم‌های امنیتی	۷-۱
۲۱	تهدیدها، حمله‌ها و دارایی‌ها	۸-۱
۲۱	سطوح حمله و درختان حمله	۹-۱
۲۶	مدلی برای امنیت شبکه	۱۰-۱
۲۸	پرسش‌های مروری	۱۱-۱
۲۹	مسئله‌ها	۱۲-۱

فصل ۲: دیوار آتش (فایروال)

۳۰	نیاز به دیوارهای آتش	۱-۲
۳۱	ویژگی‌های دیوار آتش و سیاست دسترسی	۲-۲
۳۴	انواع دیوارهای آتش	۳-۲
۴۲	استقرار دیوار آتش	۴-۲
۴۶	پیکربندی و تعیین مکان دیوار آتش	۵-۲
۵۰	پرسش‌های مروری	۶-۲
۵۱	مسئله‌ها	۷-۲

فصل ۳: سیستم‌های تشخیص نفوذ و امنیت شبکه

۱-۳	تاریخچه سیستم‌های تشخیص نفوذ.....	۵۳
۲-۳	مروری بر IDS.....	۵۳
۳-۳	سیستم‌های تشخیص نفوذ مبتنی بر شبکه.....	۵۹
۴-۳	IDS های مبتنی بر میزبان.....	۶۶
۵-۳	سیستم‌های پیشگیری از نفوذ.....	۷۱
۶-۳	ظرف‌های غسل و شبکه‌های غسل.....	۷۱
۷-۳	پرسش‌های مروری.....	۷۳
۸-۳	مسئله.....	۷۴

فصل ۴: امنیت شبکه‌های بی‌سیم

۱-۴	امنیت بی‌سیم.....	۷۵
۲-۴	تهدیدهای شبکه‌ی بی‌سیم.....	۷۶
۳-۴	امنیت دستگاه‌های سیار.....	۷۹
۴-۴	مروری بر شبکه‌ی محلی بی‌سیم IEEE 802.11.....	۸۳
۵-۴	امنیت شبکه‌ی محلی بی‌سیم IEEE 802.11.....	۹۰
۶-۴	پرسش‌های مروری.....	۹۴
۷-۴	مسئله‌ها.....	۹۴

فصل ۵: انواع حمله‌ها و بدافزارها

۱-۵	راه‌های حمله.....	۹۷
۲-۵	کد بدخواه.....	۹۸
۳-۵	حمله به سیستم‌های کامپیوتری و شبکه‌ها.....	۱۰۶
۴-۵	ساخت شبکه‌ی حمله.....	۱۱۱
۵-۵	اقدامات متقابل حمله‌های DDOS.....	۱۱۲
۶-۵	فیشینگ.....	۱۱۳
۷-۵	ویشینگ.....	۱۱۳
۸-۵	پرسش‌های مروری.....	۱۱۴

فصل ۶: امنیت شبکه VoIP

۱-۶	مروری بر شبکه‌ی VoIP	۱۱۵
۲-۶	پروتکل‌های VoIP	۱۱۷
۳-۶	سناریوهای تهدید امنیت VoIP	۱۲۲
۴-۶	نگرانی‌های امنیتی H.323	۱۲۷
۵-۶	نگرانی‌های امنیتی SIP	۱۳۲
۶-۶	دبوارهای آتش، ترجمه‌ی آدرس شبکه و برقراری تماس	۱۳۷
۷-۶	پرسش‌های مروری	۱۴۲

فصل ۷: تحلیل ترافیک شبکه

۱-۷	تحلیل ترافیک شبکه	۱۴۳
۲-۷	پیشگویی ترافیک شبکه	۱۴۹
۳-۷	پرسش‌های مروری	۱۵۲
	واژه‌نامه انگلیسی به فارسی	۱۵۳
	مراجع	۱۵۶

مقدمه

در عصر حاضر که ارتباطات الکترونیکی به طور فزاینده‌ای در حال رواج است، ویروس‌ها و هکرها بسیار متنوع و گسترده شده‌اند، استراق سمع الکترونیکی و کلاهبرداری الکترونیکی به امور عادی تبدیل شده‌اند، امنیت اهمیت ویژه‌ای پیدا کرده است. دو موضوع مهم در این حیطه مطرح است و به اهمیت موضوع امنیت افزوده است. اولی، رشد انفجاری سیستم‌های کامپیوتری و ارتباط آن‌ها از طریق شبکه، موجب وابستگی شدید سازمان‌ها و افراد به اطلاعات ذخیره شده در سیستم شده است. دوم، تکامل اصول رمزنگاری شبکه و امنیت است که منجر به توسعه‌ی الگوریتم‌های واقعی برای تأمین امنیت شبکه شده است.

این کتاب براساس فصل‌های وزارت علوم، تحقیقات و فناوری برای درس امنیت شبکه پیشرفته و با استفاده از معتبرترین منابع در این حوزه تدوین شده است. در فصل اول، مفهوم امنیت شبکه، تهدیدها و حملات، طول مفصل مورد بحث قرار گرفته‌اند. در فصل دوم، به دیوار آتش (فایروال) پرداخته شد و انواع مختلف دیوارهای آتش و محل استقرار آن‌ها مورد بحث قرار گرفت.

فصل سوم سیستم‌های تشخیص نفوذ را در بحث مورد بحث قرار داد. انواع سیستم‌های تشخیص نفوذ و مزایا و معایب هر کدام نیز بررسی شده‌اند. در فصل چهارم به جنبه‌های مختلف امنیت شبکه‌های بی‌سیم پرداخته شده است. فصل پنجم به موضوع مهم انواع حمله‌ها و بدافزارها و روش‌های مقابله با آن‌ها می‌پردازد. فصل ششم امنیت شبکه‌ی VoIP و فصل هفتم تحلیل ترافیک شبکه را مورد بحث قرار می‌دهد.

نگارنده امیدوار است کتاب حاضر همچون سایر آثار انتشارات علوم رایانه مورد استفاده اساتید محترم و دانشجویان گرامی قرار گیرد.