



امنیت شبکه‌های کامپیوتری

منطبق بر سرفصل ابلاغی شورای برنامه‌ریزی

دانشگاه فنی و حرفه‌ای کشور مورخ ۱۳۹۸/۲/۹

تألیف و گردآوری:

مهندس امیرحسین حریری

مهندس مهدی احمدی

سرشناسه	حریری، امیرحسین، ۱۳۷۲-
عنوان و نام پدیدآور	امنیت شبکه‌های کامپیوتری منطبق بر سرفصل ابلاغی شورای برنامه‌ریزی دانشگاه فنی و حرفه‌ای کشور مورخ ۱۳۹۸/۲/۹/تالیف و گردآوری امیرحسین حریری، مهدی احمدی.
مشخصات نشر	تهران: دانشگاه فنی و حرفه‌ای، ۱۴۰۰.
مشخصات ظاهری	۱۷۱ ص.: مصور (بخشی رنگی)، نمودار (بخشی رنگی).
شابک	۹۷۸-۶۰۰-۸۸۲۰-۹۳-۲
وضعیت فهرست نویسی	فیبا
یادداشت	واژه‌نامه.
یادداشت	کتابنامه.
موضوع	شبکه‌های کامپیوتری -- تدابیر امنیتی -- راهنمای آموزشی (عالی)
موضوع	Computer networks -- Security measures -- Study and teaching (Higher)
موضوع	شبکه‌های کامپیوتری -- راهنمای آموزشی (عالی)
موضوع	Computer networks -- Study and teaching (Higher)
شناسه افزوده	احمدی، مهدی، ۱۳۸۱ - (مهندس)
شناسه افزوده	دانشگاه فنی و حرفه‌ای
شناسه افزوده	Technical and Vocational University
رده بندی کنگره	۵۹/TK۵۱۰۵
رده بندی دیویی	۸/۰۰۵
شماره کتابشناسی ملی	۸۴۵۲۶۷۵
اطلاعات رکورد کتابشناسی	فیبا

عنوان کتاب	امنیت شبکه‌های کامپیوتری
تالیف و گردآوری	امیرحسین حریری / مهدی احمدی
ناشر	دانشگاه فنی و حرفه‌ای
سال و نوبت چاپ	۱۴۰۰ / چاپ اول
شمارگان	۵۰۰ جلد
قیمت	۳۵،۰۰۰ تومان
شابک	ISBN: 978-600-8820-93-2 ۹۷۸-۶۰۰-۸۸۲۰-۹۳-۲

کلیه حقوق این اثر برای مؤلفین و دانشگاه فنی و حرفه‌ای محفوظ است.

آدرس: تهران میدان ونک خیابان بزرگ شرقی پلاک ۴ - تلفن: ۴۲۳۵۰۰۰۰-۲۱

پست الکترونیک: Entesharat@tvu.ac.ir، وب سایت: Tvu.ac.ir



دانشگاه فنی و حرفه‌ای

فهرست مطالب

فصل اول: تعاریف اولیه امنیت شبکه

۱-۱- مقدمه	۲
۲-۱- عدم انکار	۲
۳-۱- شناسایی هویت	۳
۴-۱- کنترل دسترسی	۳
۵-۱- تفاوت شناسایی هویت و کنترل دسترسی	۴
۶-۱- قابلیت اعتماد	۴
۱-۶-۱- مدیریت ریسک	۴
۲-۶-۱- خط مشی امنیتی	۴
۳-۶-۱- دارائی ارزشمند	۵
۴-۶-۱- آسیب پذیری	۵
۵-۶-۱- تهدید	۵
۶-۶-۱- حمله	۶
۷-۶-۱- Cyber	۶
۸-۶-۱- Cyber Space	۶
۷-۱- طبقه بندی حملات	۸
۱-۷-۱- وقفه	۸
۲-۷-۱- شنود	۸
۳-۷-۱- تغییر	۹
۴-۷-۱- ایجاد اطلاعات	۹
۵-۷-۱- حملات فعال	۱۰
۶-۷-۱- حملات منفعل	۱۰
۷-۷-۱- تفاوت حملات فعال و غیر فعال	۱۱
۸-۱- مدل پیشنهادی برای امنیت شبکه	۱۲
۱-۸-۱- ویژگیهای لازم مدل امنیت شبکه	۱۳
۹-۱- خلاصه فصل	۱۴
۱۰-۱- سؤالات فصل اول	۱۴

فصل دوم: آشنایی با بدافزارها

۱-۲- مقدمه	۱۶
۲-۲- بدافزار چیست؟	۱۶

۱۷	۳-۲- ویژگی بدافزارها
۱۸	۴-۲- مهمترین روشها و راههای ورود بدافزارها به کامپیوتر
۱۹	۵-۲- نحوه تشخیص آلوده شدن سیستم به یک بدافزار
۱۹	۶-۲- خسارات ناشی از بدافزارها
۲۰	۷-۲- انواع بدافزار
۲۰	۸-۲- طبقه بندی نوع نخست
۲۱	۸-۲-۱- بدافزارهای بد
۲۱	۸-۲-۲- بدافزارهای خوب
۲۱	۹-۲- طبقه بندی نوع دوم
۲۱	۹-۲-۱- Rootkit
۲۲	۹-۲-۲- Spyware
۲۳	۱۰-۲- طبقه بندی نوع سوم
۲۳	۱۰-۲-۱- Virus
۲۴	۱۰-۲-۲- Worm
۲۵	۱۰-۲-۳- Trojan
۲۵	۱۰-۲-۴- Logical Bomb
۲۶	۱۰-۲-۵- Hoax
۲۶	۱۱-۲- طبقه بندی نوع چهارم
۲۷	۱۱-۲-۱- Adware
۲۷	۱۱-۲-۲- Dialer
۲۸	۱۱-۲-۳- Downloader
۲۸	۱۱-۲-۴- Keylogger
۲۸	۱۱-۲-۵- Ransomware
۲۹	۱۱-۲-۶- Social Networks
۲۹	۱۱-۲-۷- Stealer
۳۰	۱۲-۲- طبقه بندی نوع پنجم
۳۰	۱۳-۲- طبقه بندی نوع ششم
۳۱	۱۳-۲-۱- نوین
۳۱	۱۳-۲-۲- ماکرو
۳۱	۱۳-۲-۳- مفید در حافظه
۳۲	۱۳-۲-۴- تغییر دهنده فایل
۳۲	۱۳-۲-۱-۴- بدافزارهای همراه
۳۲	۱۳-۲-۲-۴- بدافزارهای اسکریپتی

چرا باید مفاهیم بنیادی امنیت شبکه را بدانیم؟

با توسعه فناوری اطلاعات و پیاده‌سازی سیستم‌های اطلاعاتی در سراسر دنیا، تأمین امنیت آن به عنوان دغدغه‌ای مهم در مجامع علمی، دولتی و خصوصی مطرح شده است. از آنجا که شبکه به عنوان بستری اساسی برای انتقال اطلاعات به حالتی فراگیر نزدیک می‌شود، حفظ امنیت در انتقال اطلاعات و عدم نفوذپذیری از طریق شبکه، به عنوان حالت خاصی از امنیت اطلاعات، نیاز به بررسی بسیار دارد و البته کارهای ارزشمندی هم در این زمینه انجام گرفته و محصولات مختلفی ارائه شده است. آشنایی مدیران سازمان‌ها، مراکز دولتی، نظامی، تجاری و هر جایی که امنیت اطلاعات برای آن‌ها مطرح است، با مبانی امنیت شبکه، مخاطرات امنیتی، راه‌حل‌ها و نحوه سیاست‌گذاری صحیح برای این موضوع، امری اجتناب‌ناپذیر محسوب می‌شود. اگر همچنین مدیران شبکه، به مسایل امنیتی شبکه خود آگاه نباشند، ممکن است به صورت‌های مختلفی مورد حمله افراد نفوذگر قرار گیرند.

این کتاب سعی دارد با ارائه مفاهیم بنیادی امنیت شبکه، دانشجویان کاردانی کامپیوتر را با مسایل مطرح در امنیت شبکه آشنا سازد تا بدین وسیله قادر به وضع سیاست‌های خاص برای حفظ امنیت اطلاعات و به‌طور خاص امنیت شبکه، شناسایی افراد خاطی و برخورد با آن‌ها باشند. همچنین، در سطحی پیشرفته‌تر و البته نه صرفاً تکنیکی، مسئولین شبکه‌های شرکت‌ها و سازمان‌ها را با امنیت شبکه و تجهیزات آن، مخاطرات امنیتی، راه‌حل‌ها و سایر مسائل مربوط به امنیت یک شبکه در مقابله با نفوذگران داخلی و خارجی آشنا می‌گرداند. گفتنی است که مطالعه کامل این کتاب نیاز به آشنایی با مفاهیم شبکه و دانستن اطلاعات پایه‌ای در زمینه امنیت شبکه دارد و بر اساس سرفصل‌های مصوب درس «امنیت شبکه‌های کامپیوتری» تالیف گردیده است.