

امنیت شبکه‌های کامپیوتری

- مفاهیم امنیت شبکه
- امنیت در شبکه‌های بی سیم
- عدم پذیرش سرویس یا DoS
- پروتکل‌های انتقال فایل امن
- رمزنگاری
- ویروس و ضدویروس
- امنیت شبکه لایه بندی شده

مؤلف و مترجم:

مهندس سعیده دانا

سر شناسنامه : دانا، سعیده، ۱۳۶۶-

عنوان و نام پدید آورنده : امنیت شبکه‌های کامپیوتری: مفاهیم امنیت شبکه، امنیت در شبکه‌های بی سیم، ...، امنیت شبکه لایه‌بندی شده / مولف و مترجم سعیده دانا.

مشخصات نشر : مشهد/ خاتم توس/ ۱۳۹۹

شابک: ۹۵۵۷۲-۹-۵-۹۷۸-۶۰۰-۴۰۰۰۰۰۰ ریال

موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی

رده بندی کنگره: TK۵۱۰۵/۵۹

رده بندی دیودی: ۰۰۵/۸

شماره کتابشناسی ملی: ۷۳۳۳۱۲۴

www.Khatamtoos.ir

انتشارات خاتم توس

عنوان کتاب: امنیت شبکه‌های کامپیوتری = Computer security networks

مولف و مترجم: مهندس سعیده دانا

ناشر: انتشارات خاتم توس

نوبت چاپ: چاپ اول

تیراژ: ۱۰۰۰ جلد

قیمت: ۴۰۰۰۰۰ ریال

شابک: ۹۵۵۷۲-۹-۵-۹۷۸-۶۰۰

ISBN: 978-600-95572-9-5



فهرست مطالب

عنوان

صفحه

۸	مقدمه :
۹	مفاهیم امنیت شبکه
۱۰	۱- مفاهیم امنیت شبکه
۱۳	۲- اولین اتصال یک کامپیوتر به اینترنت
۱۴	۱-۲ انگیزه
۱۴	۲-۲ توصیه ها
۱۵	راهنمایی عمومی
۱۵	اینها مراحل هستند که توصیه می شوند:
۱۷	۳-۲ ویندوز XP
۱۸	۴-۲ Apple Macintosh OSX
۱۹	۵-۲ سایر سیستم عامل ها
۲۱	۳- رویدادهای امنیتی و اقدامات لازم در برخورد با آنها (Incident Handling)
۲۱	۱-۳ برخورد با رویداد
۲۱	مثالی از واکنش به یک رویداد در یک سازمان بزرگ
۲۴	۴- امنیت در تولید نرم افزارها
۲۴	نرم افزار
۲۶	۵- تشخیص نفوذ (Intrusion Detection)
۲۶	۱-۵ انواع حملات شبکه ای با توجه به طریقه حمله
۲۷	۲-۵ حملات از کار انداختن سرویس
۲۷	۳-۵ حملات دسترسی به شبکه
۲۸	۴-۵ انواع حملات شبکه ای با توجه به حمله کننده
۲۸	۵-۵ برداره تشخیص نفوذ
۲۹	۶-۵ مقایسه تشخیص نفوذ و پیش گیری از نفوذ
۲۹	۱-۶ تفاوت شکلی تشخیص با پیش گیری
۳۰	۲-۶ تشخیص نفوذ
۳۱	۳-۶ پیش گیری از نفوذ
۳۲	۴-۶ نتیجه نهایی
۳۲	۶- ویروس و ضدویروس
۳۳	۱-۶ ویروس چیست؟
۳۳	۲-۶ انواع ویروس
۳۳	۱-۲-۶ boot sector :

۳۴	Macro viruses: ۲-۲-۶
۳۴	File infecting viruses: ۳-۲-۶
۳۴	ویروس های چندریخت (Polymorphic): ۴-۲-۶
۳۴	ویروس های مخفی: ۵-۲-۶
۳۵	ویروس های چندبخشی: ۶-۲-۶
۳۵	سایر برنامه های مختل کننده امنیت: ۳-۶
۳۵	اسب های تروا: ۱-۳-۶
۳۵	کرم ها: ۲-۳-۶
۳۵	بمب های منطقی: ۳-۳-۶
۳۶	قابلیت های نرم افزار های ضد ویروس: ۴-۶
۳۶	تفاوت بین نسخه های ضد ویروس: ۱-۴-۶
۳۶	حافظت E-mail: ۲-۴-۶
۳۷	بروز رسانی نرم افزار های ضد ویروس: ۵-۶
۳۸	امنیت تجهیزات شبکه: ۷-۱
۳۸	امنیت فیزیکی: ۱-۷
۳۹	افزودگی در محل استقرار شبکه: ۲-۷
۳۹	توپولوژی شبکه: ۳-۷
۴۰	محل های امن برای تجهیزات: ۴-۷
۴۱	انتخاب لایه کانال ارتباطی امن: ۱-۴-۷
۴۱	منابع تغذیه: ۲-۴-۷
۴۱	عوامل محیطی: ۳-۴-۷
۴۲	امنیت منطقی: ۵-۷
۴۲	امنیت مسیریاب ها: ۱-۵-۷
۴۳	مدیریت پیکربندی: ۲-۵-۷
۴۳	کنترل دسترسی به تجهیزات: ۳-۵-۷
۴۴	امن سازی دسترسی: ۴-۵-۷
۴۴	مدیریت رمز های عبور: ۵-۵-۷
۴۴	ملزومات و مشکلات امنیتی ارائه دهندگان خدمات: ۶-۷
۴۴	قابلیت های امنیتی: ۱-۶-۷
۴۵	مشکلات اعمال ملزومات امنیتی: ۲-۶-۷
۴۵	رویکردی عملی به امنیت شبکه لایه بندی شده: ۸-۱
۴۶	افزودن به ضریب عملکرد هر ها: ۱-۸
۴۷	مدل امنیت لایه بندی شده: ۲-۸
۴۸	امنیت پیرامون: ۱-۲-۸
۴۸	فایروال: ۱-۱-۲-۸
۴۹	آنتی ویروس شبکه: ۲-۱-۲-۸
۴۹	VPN: ۳-۱-۲-۸

۴۹	مزایا
۵۰	معایب
۵۰	ملاحظات
۵۰	۲-۲-۸ امنیت شبکه
۵۱	۲-۲-۸ مدیریت آسیب پذیری
۵۱	۳-۲-۸ تابعیت امنیتی کاربر انتهایی
۵۲	۴-۲-۸ کنترل دسترسی/تأیید هویت
۵۲	مزایا
۵۳	معایب
۵۴	ملاحظات
۵۴	۳-۲-۸ امنیت میزبان
۵۵	۱-۳-۲-۸ IDS در سطح میزبان
۵۵	۲-۳-۲-۸ VA (تخمین آسیب پذیری) سطح میزبان
۵۵	۳-۳-۲-۸ تابعیت امنیتی کاربر انتهایی
۵۵	۴-۳-۲-۸ آنتی ویروس
۵۵	۵-۳-۲-۸ کنترل دسترسی/تصدیق هویت
۵۶	مزایا
۵۶	معایب
۵۶	ملاحظات
۵۷	۴-۲-۸ امنیت برنامه کاربردی
۵۷	۱-۴-۲-۸ پوشش محافظ برنامه
۵۷	۲-۴-۲-۸ کنترل دسترسی/تصدیق هویت
۵۷	۳-۴-۲-۸ تعیین صحت ورودی
۵۸	مزایا
۵۸	معایب
۵۸	ملاحظات
۵۹	۵-۲-۸ امنیت دیتا
۵۹	۱-۵-۲-۸ رمزنگاری
۵۹	۲-۵-۲-۸ کنترل دسترسی / تصدیق هویت
۶۰	مزایا
۶۰	معایب
۶۰	ملاحظات
۶۰	۳-۸ دفاع در مقابل تهدیدها و حملات معمول
۶۰	۱-۳-۸ حملات به وب سرور
۶۰	۲-۳-۸ بازپخش ایمیل ها بصورت نامجاز
۶۱	۳-۳-۸ دستکاری میزبان دور در سطح سیستم
۶۱	۴-۳-۸ فراهم بودن سرویس های اینترنتی غیر مجاز

مقدمه :

دو تا سه دهه قبل شبکه های کامپیوتری معمولاً در دو محیط وجود خارجی داشت :

- محیط های نظامی که طبق آئین نامه های حفاظتی ویژه به صورت فیزیکی حراست میشد و چون سایتها و تجهیزات شبکه نیز در محیط حفاظت شده نظامی مستقر بود و هیچ ارتباط مستقیم با دنیای خارج نداشتند لذا دغدغه کمتری برای حفظ اسرار و اطلاعات وجود داشت . نمونه بارز این شبکه APARNET در وزارت دفاع آمریکا بود

- محیطهای علمی و دانشگاهی که برای مبادله دستاوردهای تحقیقی و دستذسی به اطلاعات علمی از شبکه استفاده می کردند و معمولاً بر روی چنین شبکه هایی اطلاعاتی مبادله می شد که آشکار شدن آنها لطمه چندانی به کسی وارد نمی کرد

با گسترش روز افزون شبکه های بهم پیوسته و ازیاد حجم اطلاعات مورد مبادله و متکی شدن قسمت زیادی از امور روز مره به شبکه های کامپیوتری و ایجاد شبکه های جهانی چالش بزرگی برای صاحبان اطلاعات پدید آمده است امروزه سرعت دانشی که برای آن وقت و هزینه صرف شده یکی از خطرات بالقوه شبکه های کامپیوتری به شمار می آید

در جهان امروز با محول شدن امور اداری و مالی به شبکه های کامپیوتری زنگ خطر برای تمام مردم به صدا در آمده است و بر خلاف گذشته که خطراتی نیز دزدی و راهزنی معمولاً توسط افراد کم سواد و ولگرد متوجه مردم بود امروزه این خطر توسط افرادی تحصیل میشود که باهوش و باسواد و قدرت نفوذ و ضربه به شبکه را دارند معمولاً هدف افرادی که به شبکه های کامپیوتری نفوذ یا حمله میکنند یکی از موارد زیر است:

۱. تفریخ یا اندازه گیری ضریب توانایی فردی یا کنجکاوی (معمولاً دانشجویان)
۲. دزدین دانشی که برای تهیه آن بایستی صرف هزینه کرد (راهزنان دانش)
۳. انتقام جوئی و ضربه زدن به رقیب
۴. آزار رسانی و کسب شهرت از طریق مردم آزاری
۵. جاسوسی و کسب اطلاعات از وضعیت نظامی و سیاسی یک کشور یا منطقه
۶. جابجا کردن مستقیم پول و اعتبار از حسابهای بانکی و دزدیدن شماره کارتهای اعتبار
۷. رقابت ناسالم در عرصه تجارت و اقتصاد