

فهرست مطالب

۱۳	فصل اول: مفاهیم پایه و اساس امنیت در تجارت الکترونیک
۱۴	۱-۱ سیستم مدیریت امنیت اطلاعات
۱۵	۲-۱ مفاهیم امنیت شبکه
۲۰	۳-۱ اهمیت امنیت برای سازمان های کوچک و متوسط در کشورهای در حال توسعه
۲۲	۴-۱ خصوصیات یا سرویس هایی برای پروتکل های امنیتی
۲۲	۵-۱ محرمانگی
۲۳	۶-۱ احراز اصالت مبدأ
۲۴	۷-۱ احراز اصالت وجودی
۲۵	۸-۱ جامعیت
۲۵	۹-۱ تبادل کلید احراز اصالت شده
۲۶	۱۰-۱ عدم انکار
۲۷	۱۱-۱ اختفاء
۲۸	۱۲-۱ در دسترس بودن
۲۹	۱۳-۱ آشنایی با حملات pharming
۲۹	۱۴-۱ گونه ای جدید از حمله
۳۳	۱۵-۱ بررسی دنیای واقعی
۳۳	۱۶-۱ امضا
۳۵	۱۷-۱ انصاف (fairness)
۳۵	۱۸-۱ اثر انگشت منحصر به فرد
۳۷	فصل دوم: رمز نگاری و الگوریتمهای آن
۳۸	۱-۲ معرفی و اصطلاحات

۳۹	۲-۲ الگوریتم‌ها
۴۲	۳-۲ کلیدها در رمزنگاری
۴۵	۴-۲ شکستن کلیدهای رمزنگاری
۴۵	۵-۲ الگوریتمهای متقارن
۴۶	۶-۲ الگوریتم‌های نامتقارن
۴۷	۷-۲ رمزنگاری در پروتکل‌های انتقال
۴۷	۸-۲ پروتکل‌ها
۴۸	۹-۲ پروتکل‌های رمزنگاری انتقال
۶۴	۱۰-۲ رمز گذاری با IPSEC
۷۵	فصل سوم: رویکردی عملی به امنیت شبکه لایه بندی شده
۷۷	۱-۳ افزودن به ضریب عملکرد هکرها
۷۷	۲-۳ مدل امنیت لایه بندی شده
۹۳	فصل چهارم: بیومتریک و تجهیزات مربوطه
۹۴	۱-۴ Behavioral and Physiometric (خصوصیات رفتاری و فیزیکی).
۱۰۰	۲-۴ امنیت فیزیکی در مراکز حساس IT
۱۰۴	۳-۴ امنیت فیزیکی
۱۱۱	فصل پنجم: آشنایی با ویروسها و ...
۱۱۲	۱-۵ اولین نکته چگونگی امکان ویروسی شدن کامپیوترها
۱۱۳	۲-۵ راه مقابله با ویروسی شدن کامپیوتر با ایمیل
۱۱۸	۳-۵ نمونه‌هایی از حملات اینترنتی توسط نامه‌های الکترونیکی
۱۱۹	۴-۵ ترفندهای هکری
۱۲۲	۵-۵ Subseven چیست؟
۱۲۸	۶-۵ آموزش کامل تروجان subseven , pars seven

۱۳۵	۷-۵ آموزش هک با نرم افزار PS - Magic
۱۳۶	۸-۵ آشنایی با یک ویروس ساده
۱۳۷	۹-۵ سوزاندن سخت افزارهای دارای هد
۱۳۷	۱۰-۵ نحوه بدست آوردن IP افراد در Yahoo Messenger بدون ابزار
۱۳۹	۱۱-۵ ویروس و علائم آن در یک نگاه
۱۴۰	۱۲-۵ ساخت یک ویروس
۱۴۱	۱۳-۵ Rootkit چیست؟
۱۴۵	۱۴-۵ تروجان Banker - AML
۱۴۶	۱۵-۵ تروجان Haxdoor - BC
۱۴۷	۱۶-۵ تروجان PeepVie - W
۱۴۹	۱۷-۵ تروجان PWS - KI
۱۵۰	۱۸-۵ تروجان Sickbt - D
۱۵۱	۱۹-۵ تروجان Banload-TI
۱۵۲	۲۰-۵ کرم Bagle - DM
۱۵۵	۲۱-۵ کرم USKAF - A
۱۵۷	۲۲-۵ Spam چیست؟
۱۶۰	۲۳-۵ Spyware چیست؟
۱۶۶	۲۴-۵ ویروس W32/NetSky.B
۱۶۹	۲۵-۵ معرفی سه گروه اینترنتی Zar.A , Bropia.A و Mydoom.AE
۱۷۰	۲۶-۵ ویروس استاکس نت
۱۷۱	۲۷-۵ ویروس شناسی
۱۷۵	۲۸-۵ تحلیل کد ویروس
۱۸۳	۲۹-۵ ویروس Flame

۱۹۳	فصل ششم: چگونگی فعالیت دیوارهای آتش در لایه‌های مختلف و انواع آنها
۱۹۴	۱-۶ چگونگی فعالیت دیوارهای آتش در لایه‌های مختلف و انواع آنها
۱۹۶	۲-۶ انواع دیوارهای آتش
۱۹۸	۳-۶ صندوق پستی خود را ضد اسپم بسازید
۲۰۳	۴-۶ مدیریت پورتهای و جلوگیری از بروز مشکل به وسیله Firewall
۲۰۴	۵-۶ آموزش نرم افزار Zone Alarm 5.5
۲۰۶	۶-۶ تنظیم برنامه فایروال Zone Alarm
۲۱۰	۷-۶ شمای کلی از نرم افزار
۲۱۵	۸-۶ نگاهی تخصصی تر
۲۱۶	۹-۶ نوشتن یک سناریوی امنیتی
۲۲۳	۱۰-۶ راهنمای نصب Norton Antivirus
۲۲۶	۱۱-۶ آنتی ویروس و دیوار آتش Microsoft Security Essential
۲۳۱	فصل هفتم: امنیت تجارت و بانکداری الکترونیک
۲۳۳	۱-۷ دیدگاه توسعه بانکداری الکترونیک
۲۳۴	۲-۷ حمله به شبکه های بانکی
۲۳۶	۳-۷ حمله به برنامه های بانکی موجود در گوشی های هوشمند
۲۳۷	۴-۷ اینترنت بانک؛ هدف جدید تروجان
۲۴۰	۵-۷ بدافزاری برای تخلیه ی حساب بانکی
۲۴۱	۶-۷ بدافزاری بنام Ghost Push
۲۴۲	۷-۷ راه حل های رمز گذاری اطلاعات در سیستم های بانکی
۲۴۳	۸-۷ زیرساخت های امنیتی مدرن برای مبادلات در شبکه اینترنت
۲۵۴	۹-۷ امنیت در اینترنت و شبکه های ارتباطی
۲۵۹	۱۰-۷ بررسی نقاط ضعف امنیتی شبکه های وب

۲۶۳	۱۱-۷ حمله به برنامه‌های وبی
۲۷۴	۱۲-۷ ایجاد یک ارتباط ایمن در برنامه های وب
۲۹۱	۱۳-۷ امنیت اطلاعات در Web 2.0
۲۹۲	۱۴-۷ خرد جمعی در دهکده ای به نام Web 2.0
۲۹۲	۱۵-۷ خرد جمعی در دهکده ای به نام Web 2.0
۲۹۴	۱۶-۷ امنیت معاملات اینترنتی تا چه اندازه است.
۲۹۶	۱۷-۷ امنیت تعاملات الکترونیکی
۲۹۹	۱۸-۷ امنیت در معاملات اینترنتی
۳۰۱	۱۹-۷ امنیت و ضد امنیت در داد و ستدهای الکترونیک
۳۱۰	۲۰-۷ ارزش تجاری امنیت
۳۱۳	۲۱-۷ ایمنی و داد و ستد در اینترنت با کارت SIGN TRUST
۳۱۷	۲۲-۷ حفاظت از حریم شخصی در اینترنت
۳۲۱	۲۳-۷ یک اساس نامه امنیتی (Security Policy) چیست؟
۳۲۵	۲۴-۷ کوکی‌ها و مسائل امنیتی آنها در سایت های تجاری و همراه کامپیوترها
۳۳۱	۲۵-۷ کوکی، راز پنهان در مرورگرهای اینترنتی
۳۳۵	۲۶-۷ کلیدهای امنیتی جدید و رمزهای یک دقیقه‌ای!
۳۳۷	۲۷-۷ سایت‌های دولتی نیاز به امنیت دارند
۳۴۷	فصل هشتم: نفوذ و تشخیص نفوذ
۳۴۸	۱-۸ مقایسه تشخیص نفوذ و پیشگیری از نفوذ
۳۵۲	۲-۸ مقایسه امنیت در ویندوز و لینوکس بعنوان سیستمهای عامل سرور
۳۶۱	فصل نهم: تعریف، تحلیل، پیاده سازی و مقابله با تزریق کدهای SQL
۳۶۲	۱-۹ مقدمه
۳۶۳	۲-۹ تزریق SQL چیست؟



۳۶۵	۳-۹ دسته بندی حملات تزریق
۳۶۶	۴-۹ شاخصهای حملات تزریق SQL
۳۷۰	۵-۹ استنتاج
۳۷۱	۶-۹ پرس و جوهای نادرست غیر مجاز/غیر منطقی
۳۷۲	۷-۹ پرس و جوی Union
۳۸۶	۸-۹ دسته بندی نهایی حمله ها با کمک چند مثال متداول
۳۹۰	۹-۹ تکنیک های تشخیص و جلوگیری
۳۹۲	۱۰-۹ تکنیکهای خود کار تشخیص و جلوگیری از تزریق کد متداول
۳۹۲	۱۱-۹ بررسی کننده های کد استاتیک
۳۹۳	۱۲-۹ تحلیل ترکیبی استاتیک و پویا
۳۹۴	۱۳-۹ یک نمونه دیگر از حمله تزریق کد اس کیو ال
۳۹۴	۱۴-۹ تکنیکها و مکانیزهای حفاظتی در برابر تزریق کد
۳۹۵	۱۵-۹ نحوه تشخیص سایتهای آسیب پذیر
۳۹۶	۱۶-۹ مقایسه الگوریتم ها و ابزارهای ارائه شده
۴۰۰	۱۷-۹ ارائه ایده تحقیق و بررسی آن
۴۰۴	۱۸-۹ آزمایش حملات رویه های ذخیره شده با تکنولوژی لینک
۴۰۴	۱۹-۹ برتری هایی لینک در برابر تکنولوژی های ارتباطی سنتی
۴۰۵	فصل دهم: ترفندها و نکات عملیاتی مهم
۴۰۶	۱-۱۰ ابزارهای ناشناخته اما کارآمد برای مسلح سازی سیستم در برابر هکرها
۴۰۶	۲-۱۰ کشف حفره های امنیتی
۴۰۷	۳-۱۰ برنامه های رفع مشکلات امنیتی
۴۰۸	۴-۱۰ امنیت سیستم شخصی
۴۰۹	۵-۱۰ رد ایمیل های دریافتی خود را بگیرید!



۴۱۰	۶-۱۰ ده ترفند برای افزایش امنیت سیستم عامل لینوکس
۴۱۴	۷-۱۰ فعال سازی قابلیت مقابله با هکرها در ویندوز XP
۴۱۵	۸-۱۰ اسکن کردن کامپیوتر توسط خودتان، بدون استفاده از آنتی ویروس!
۴۱۷	۹-۱۰ جلوگیری از تشخیص اشتباه هرزنامه ها در Gmail
۴۱۸	۱۰-۱۰ افزایش سرعت باز شدن صفحات اینترنتی در تمام مرورگرها
۴۲۱	۱۱-۱۰ جلوگیری از دسترسی بدون اجازه ی اپلیکیشن ها به اینترنت در اندروید
۴۲۲	۱۲-۱۰ ذخیره ی نقشه های Google Maps برای استفاده ی آفلاین در اندروید
۴۲۳	۱۳-۱۰ پی بردن به روت بودن گوشی های دارای سیستم عامل اندروید
۴۲۴	۱۴-۱۰ دستیابی به لینک مستقیم حساب کاربری در لاین
۴۲۵	۱۵-۱۰ بازگشت به گروهی که از آن خارج شده اید در تلگرام
۴۲۶	۱۶-۱۰ دو راه برای پی بردن به رمز عبور ذخیره شده ی شبکه ی بی سیم در محیط ویندوز
۴۲۸	۱۷-۱۰ نمایان کردن فایل های مخفی شده توسط ویروس ها با یک کلیک!
۴۳۱	منابع و مراجع