

امنیت در سیستم‌عامل‌های

یونیکس و لینوکس

www.ketab.ir

مهندس مجید داوری دولت‌آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندار پارس

سرشناسه	:	داوری دولت‌آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور	:	امنیت در سیستم‌عامل‌های یونیکس و لینوکس / مجید داوری دولت‌آبادی.
مشخصات نشر	:	تهران : پندار پارس، ۱۳۹۳.
مشخصات ظاهری	:	۵۵۲ ص.: مصور، جدول.
شابک	:	۲۵۰۰۰۰ ریال ۹۷۸-۶۰۰-۶۵۲۹-۱-۵۶
وضعیت فهرست نویسی	:	فیا
یادداشت	:	کتابنامه.
موضوع	:	سیستم عامل لینوکس
موضوع	:	سیستم عامل یونیکس
موضوع	:	سیستم‌های عامل (کامپیوتر)
موضوع	:	کامپیوترها -- ایمنی اطلاعات
رده بندی نگره	:	۷۴/۷۶QA ۱۳۹۳ ۹۳۵۲/س
رده بندی یی	:	۲۳۲/۰۰۵
شماره ثبت ملی	:	۳۲۵۰۳۲۵

انتشارات پندار پارس

دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شمال ۱۴، حد ۱۶
 تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۱۲۴۵۲۳۴۸
www.pendarepars.com
info@pendarepars.com



نام کتاب : امنیت در سیستم‌عامل‌های یونیکس و لینوکس

ناشر : انتشارات پندار پارس

ترجمه و تالیف : مهندس مجید داوری دولت‌آبادی

چاپ نخست : اردیبهشت ۹۳

شمارگان : ۵۰۰ نسخه

لینوگرافی : ترام‌منج

چاپ، صحافی : فرشیوه، خیام

شابک : ۹۷۸-۶۰۰-۶۵۲۹-۱-۵۶

قیمت : ۳۵۰۰۰ تومان

هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد

فهرست

۳	فصل نخست: مروری بر امنیت در سیستم‌های عامل کدباز.....
۴	۱-۱ مکانیزم‌های مختلف در بهبود امنیت لینوکس.....
۶	۱-۲ بهره‌گیری از خطاها برای امن‌سازی لینوکس.....
۸	۱-۳ توصیه‌های مهم امنیتی در مورد یونیکس و لینوکس.....
۹	۱-۴ مفاهیم پایه‌ای در امنیت سیستم‌های عامل کدباز (لینوکس و یونیکس).....
۱۰	۱-۴-۱ مفهوم TCPwrapper.....
۱۱	۱-۴-۲ مفهوم دایمون xinetd.....
۱۲	۱-۴-۳ مفهوم دایمون identd.....
۱۴	۱-۵ مفهوم سازی، سرورهای لینوکسی.....
۲۲	۱-۶ مفهوم ترافیک اسپیڈیر یونیکس و لینوکس.....
۲۳	۱-۷ امنیت سیستم عامل یونیکس.....
۲۳	۱-۷-۱ امنیت یونیکس.....
۲۳	۱-۷-۲ سیستم حفاظت لینوکس.....
۲۵	۱-۷-۳ تحلیل امنیتی لینوکس.....
۲۷	۱-۷-۴ اسپیڈیری لینوکس.....
۲۹	۱-۸ تفاوت‌های اصلی دو سیستم عامل یونیکس و لینوکس.....
۳۰	۱-۹ مراجع این فصل.....
۳۱	فصل دوم: امن‌سازی ساختارهای مدیریتی سیستم.....
۳۱	۲-۱ بررسی درستی بسته‌های نرم‌افزاری.....
۳۱	۲-۲ پیکربندی TCP Wrapperها.....
۳۳	۲-۳ ابزار Bastille.....
۳۳	۲-۴ انواع هسته‌ها از نظر نوع عملکرد در لینوکس.....
۳۳	۲-۴-۱ هسته‌های نوع پیش‌فرض و سفارشی.....
۳۴	۲-۴-۲ هسته‌های نوع پایدار و در حال توسعه.....
۳۴	۲-۵ ماژول‌ها در هسته‌ی لینوکس.....
۳۶	۲-۶ غیرفعال کردن ماژول‌های هسته غیرضروری.....
۳۶	۲-۷ اسپیڈیری ارتقای سطح دسترسی به‌روز Page Fault در هسته‌ی لینوکس.....
۳۷	۲-۸ امنیت هسته.....
۳۸	۲-۹ ابزارهای امن‌سازی هسته.....
۴۰	۲-۱۰ مفهوم LSM.....
۴۱	۲-۱۱ ماژول‌های امنیتی لینوکس.....
۴۱	۲-۱۱-۱ ساختار امنیتی Flask.....
۴۴	۲-۱۱-۲ اعمال تایپ یا TE (DTE).....
۴۵	۲-۱۱-۳ کنترل دسترسی بر مبنای نقش یا RBAC.....
۴۶	۲-۱۱-۴ ماژول امنیتی SELinux.....
۵۲	۲-۱۱-۵ ماژول امنیتی Capability.....
۵۴	۲-۱۲ استفاده از ماکروها.....
۵۴	۲-۱۳ معرفی ماژول‌های دیگر.....
۵۵	۲-۱۳-۱ ماژول امنیتی Openwall.....
۵۵	۲-۱۳-۲ ماژول امنیتی DTE.....
۵۵	۲-۱۳-۳ ماژول امنیتی LIDS.....
۵۶	۲-۱۴ مفهوم رویه‌ی از راه دور (RPC).....
۵۸	۲-۱۵ ضدویروس در لینوکس.....

۵۸	۲-۱۵-۱ AVAST ضد ویروس
۵۹	۲-۱۵-۲ BitDefender ضد ویروس
۵۹	۲-۱۵-۳ ClamAV ضد ویروس
۵۹	۲-۱۵-۴ AVG ضد ویروس
۶۰	۲-۱۶ دستور sysctl
۶۲	۲-۱۷ لیست کنترلی امن سازی سیستم عامل لینوکس
۶۶	۲-۱۸ مراجع این فصل
۶۷	فصل سوم: احراز هویت و ساختارهای کنترل دسترسی
۶۷	۳-۱ تعیین سطوح دسترسی و مجوزهای کاربران در لینوکس
۶۹	۳-۲ اجرای دستورها با مجوز دیگر کاربران در لینوکس
۷۱	۳-۳ محدودسازی دسترسی در یونیکس و لینوکس
۷۲	۳-۴ دسترسی متدنخست برای تنظیم و تغییر مجوزها در لینوکس
۷۵	۳-۵ حسابهای کاربری معمولی و مدیر سیستم
۷۶	۳-۶ رولهای تصدیق اصالت در لینوکس
۸۳	۳-۷ ساخت فایل های shadow
۸۴	۳-۸ دستورهای مدیریتی مدیریت کاربران
۸۸	۳-۹ حسابهای رمز عبور ضعیف
۹۲	۳-۱۰ تغییر گذرواژه های حساب کاربری بیشه در لینوکس
۹۳	۳-۱۱ تأمین گذرواژه های در لینوکس
۹۶	۳-۱۲ سیستم حسابرسی در لینوکس
۱۰۲	۳-۱۳ مراجع این فصل
۱۰۳	فصل چهارم: امن سازی سرویس های وب
۱۰۳	۴-۱ امنیت در سرورهای وب
۱۰۴	۴-۲ فرض های امنیتی سرور وب
۱۰۵	۴-۳ انتخاب سیستم عامل پیش از نصب سرور وب
۱۰۵	۴-۴ آماده سازی میزبان برای نصب امن سرور Apache
۱۰۵	۴-۴-۱ امنیت میزبان Apache
۱۰۷	۴-۴-۲ بارگذاری و اعتبارسنجی Apache
۱۰۸	۴-۴-۳ ایجاد گواهی SSL
۱۱۰	۴-۵ نصب امن سرویس دهنده وب Apache
۱۱۰	۴-۵-۱ عملیات مربوط به نصب
۱۱۰	۴-۵-۲ کد منبع یا نسخه اجرای
۱۱۱	۴-۵-۲-۱ دریافت و نصب کد منبع
۱۱۲	۴-۵-۲-۲ دریافت وصله ها
۱۱۳	۴-۵-۳ نسخه اجرای ایستا یا ماژول های پویا
۱۱۳	۴-۵-۴ درهای پشی Apache
۱۱۴	۴-۵-۴-۱ مکان پوشه ها
۱۱۵	۴-۵-۵ نصب سرویس دهنده Apache
۱۱۵	۴-۵-۵-۱ پیکربندی کد منبع
۱۱۶	۴-۵-۵-۲ کامپایل و نصب Apache
۱۱۶	۴-۵-۵-۳ آزمایش درستی نصب Apache
۱۱۶	۴-۵-۵-۴ انتخاب ماژول ها برای نصب
۱۱۸	۴-۵-۶ تنظیم حساب کاربری سرویس دهنده وب
۱۱۹	۴-۵-۷ تنظیم مجوزهای فایل اجرای Apache
۱۱۹	۴-۵-۸ قراردادن Apache در محس
۱۲۱	۴-۵-۸-۱ ابزارهای مورد نیاز chroot

۱۳۱	chroot مثالی از کاربرد	۴-۵-۸-۲
۱۳۲	استفاده از ldd برای مشخص کردن وابستگی‌ها	۴-۵-۸-۳
۱۳۳	استفاده از strace برای مشاهده‌ی پردازش‌ها	۴-۵-۸-۴
۱۳۴	استفاده از chroot برای جای دادن Apache در محبس	۴-۵-۸-۵
۱۳۴	جای دادن فایل‌های کاربر، گروه و تفکیک‌کننده‌ی نام در محبس	۴-۵-۸-۶
۱۳۵	اتمام انتقال Apache به محیط محبس	۴-۵-۸-۷
۱۳۵	آماده کردن php برای کار در محبس	۴-۵-۹
۱۳۶	آماده‌سازی perl برای کار در محیط محبس	۴-۵-۱۰
۱۳۷	مراقبت از مشکلات کوچک محبس	۴-۵-۱۱
۱۳۷	استفاده از وصله‌ی chroot(2)	۴-۵-۱۲
۱۳۸	استفاده از ماژول mod_chroot یا mod_security	۴-۵-۱۳
۱۳۹	۱.x شاخه‌ی Apache سرویس‌دهنده‌ی	۴-۵-۱۳-۱
۱۳۹	۲.x شاخه‌ی Apache سرویس‌دهنده‌ی	۴-۵-۱۳-۲
۱۳۹	فایل‌های حیاتی در بک‌رندینگ سرور وب Apache	۴-۶
۱۴۰	کنترل دسترسی Apache	۴-۷
۱۴۱	فایل پیکربندی httpd.conf	۴-۸
۱۳۴	پیکربندی امن Apache	۴-۹
۱۳۵	۱-۹-۴ پیش‌فرض‌های پیکربندی امن	۴-۹-۱
۱۳۵	۲-۹-۴ گزینه‌های رهنمود	۴-۹-۲
۱۳۶	۱-۹-۲-۱ رهنمود mod_allowoverride	۴-۹-۲-۱
۱۳۷	۳-۹-۴ فعال‌سازی اسکریپت‌های CGI	۴-۹-۳
۱۳۸	۴-۹-۴ واقع‌نگاری	۴-۹-۴
۱۳۸	۵-۹-۴ پیکربندی تنظیمات محدودکننده‌ی سرویس‌دهنده	۴-۹-۵
۱۴۰	۱-۹-۵ محدودیت دسترسی به وسیله‌ی .htaccess	۴-۹-۵-۱
۱۴۰	۶-۹-۴ جلوگیری از فاش شدن اطلاعات	۴-۹-۶
۱۴۲	۷-۹-۴ تغییر هویت سرویس‌دهنده‌ی وب	۴-۹-۷
۱۴۳	۸-۹-۴ تغییر فیلد سرآیند سرویس‌دهنده	۴-۹-۸
۱۴۳	۱-۹-۸-۱ تغییر نام در کد منبع	۴-۹-۸-۱
۱۴۴	۲-۹-۸-۱ تغییر نام به‌وسیله‌ی mod_security	۴-۹-۸-۲
۱۴۵	۳-۹-۸-۱ تغییر نام به‌وسیله‌ی mod_headers در Apache	۴-۹-۸-۳
۱۴۵	۴-۹-۸-۱ حذف محتویات پیش‌فرض	۴-۹-۸-۴
۱۴۶	۱۰-۹-۴ پیکربندی امن سرویس‌دهنده‌ی Apache با پشتیبانی SSL و LDAP	۴-۱۰-۹
۱۴۶	۱-۱۰-۹ پیکربندی امن Apache	۴-۱۰-۱
۱۴۶	۱-۱۰-۱-۱ تغییر نسخه‌ی Apache	۴-۱۰-۱-۱
۱۴۶	۲-۱۰-۱-۱ پیکربندی نرم‌افزار Apache برای کامپایل	۴-۱۰-۱-۲
۱۴۸	۳-۱۰-۱-۱ کامپایل سرور Apache	۴-۱۰-۱-۳
۱۴۹	۴-۱۰-۱-۱ نصب سرور Apache	۴-۱۰-۱-۴
۱۴۹	۲-۱۰-۱ نصب گواهی SSL	۴-۱۰-۲
۱۴۹	۱-۱۰-۲ تنظیم شاخه‌ی گواهی Apache	۴-۱۰-۲-۱
۱۴۹	۳-۱۰-۲ تنظیم سرور Apache	۴-۱۰-۲-۳
۱۴۹	۱-۱۰-۳-۱ پیکربندی httpd.conf	۴-۱۰-۳-۱
۱۵۲	۲-۱۰-۳-۱ پیکربندی ssl.conf	۴-۱۰-۳-۲
۱۵۲	۳-۱۰-۳-۱ حذف فایل‌های پیش‌فرض Apache	۴-۱۰-۳-۳
۱۵۲	۴-۱۰-۳-۱ تنظیم مجوز فایل‌ها و شاخه‌های سرور	۴-۱۰-۳-۴
۱۵۳	۴-۱۰-۴ تنظیمات نهایی و نصب سرور	۴-۱۰-۴
۱۵۳	۱-۱۰-۴ تغییر اسکریپت راه‌اندازی Apache	۴-۱۰-۴-۱

۱۵۳	۴-۱۰-۲ بررسی پیکربندی سرور با راهاندازی
۱۵۳	۴-۱۰-۳ تنظیم LDAP
۱۵۴	۴-۱۰-۴ اجرای سرور Apache
۱۵۴	۴-۱۱ کنترل دسترسی‌ها در سرویس‌دهنده Apache
۱۵۶	۴-۱۱-۱ کنترل دسترسی به سایت
۱۵۶	۴-۱۱-۱-۱ استفاده از ماژول mod_access
۱۵۷	۴-۱۱-۱-۲ استفاده از ماژول mod_rewrite
۱۵۷	۴-۱۲ فایل پیکربندی modules.conf
۱۵۸	۴-۱۳ ماژول‌های امنیتی سرویس‌دهنده Apache
۱۵۸	۴-۱۳-۱ تنظیمات سرور وب
۱۶۰	۴-۱۳-۱-۱ ماژول mod_rewrite
۱۶۴	۴-۱۳-۱-۲ ماژول mod_security
۱۷۰	۴-۱۴ تنظیم امن سرویس‌دهنده وب Apache با رویکرد اصلاحی
۱۷۱	۴-۱۵ بررسی نقاط آسیب‌پذیر در سرویس‌دهنده وب Apache
۱۷۱	۴-۱۵-۱ آسیب‌پذیری‌ها در معرض تهدید
۱۷۱	۴-۱۵-۲ نقاط ضعف در مقابل نقطه آسیب‌پذیر
۱۷۳	۴-۱۶ حمله به ثبات سرویس‌دهنده Apache
۱۷۴	۴-۱۶-۱ فناوری‌های تصدیق اصالت
۱۷۴	۴-۱۶-۲ ضعف‌های طراحی در مکانیزم‌های تصدیق اصالت
۱۷۵	۴-۱۶-۲-۱ گذرواژه‌ها متناسب با
۱۷۵	۴-۱۶-۲-۲ ورود به روش Fail-Open
۱۷۶	۴-۱۶-۲-۳ پیام‌های خطای طولانی
۱۷۷	۴-۱۶-۲-۴ انتقال آسیب‌پذیر حساب‌های کاربری
۱۷۸	۴-۱۶-۲-۵ مکانیزم تغییر گذرواژه
۱۷۹	۴-۱۶-۲-۶ مکانیزم مربوط به فراموشی گذرواژه
۱۷۹	۴-۱۶-۲-۷ مکانیزم یادآوری حساب کاربری
۱۸۰	۴-۱۶-۲-۸ اعتبارسنجی ناقص حساب‌های کاربری
۱۸۰	۴-۱۶-۲-۹ نام کاربری غیریکتا
۱۸۱	۴-۱۶-۲-۱۰ نام‌های کاربری قابل پیش‌بینی
۱۸۱	۴-۱۶-۲-۱۱ گذرواژه‌های آغازین قابل پیش‌بینی
۱۸۱	۴-۱۶-۲-۱۲ توزیع نام‌ن حساب‌های کاربری
۱۸۲	۴-۱۶-۳ ضعف‌های پیاده‌سازی تصدیق اصالت
۱۸۲	۴-۱۶-۳-۱ مکانیزم ورود Fail-Open
۱۸۳	۴-۱۶-۳-۲ شکست در مکانیزم ورود چندمرحله‌ای
۱۸۵	۴-۱۶-۳-۳ ذخیره نام‌ن حساب‌های کاربری
۱۸۵	۴-۱۶-۴ امن‌سازی تصدیق اصالت
۱۸۵	۴-۱۶-۴-۱ استفاده از حساب‌های کاربری قوی
۱۸۶	۴-۱۶-۴-۲ مدیریت امن حساب‌های کاربری
۱۸۶	۴-۱۶-۴-۳ اعتبارسنجی صحیح حساب‌های کاربری
۱۸۷	۴-۱۶-۴-۴ جلوگیری از افشای اطلاعات
۱۸۸	۴-۱۶-۴-۵ جلوگیری از حمله‌های نوع ورود به‌زور (Brute-force)
۱۸۹	۴-۱۶-۴-۶ جلوگیری از سوءاستفاده از مکانیزم تغییر گذرواژه
۱۹۰	۴-۱۷ تنظیم ثبت وقایع در راستای امن‌سازی Apache
۱۹۱	۴-۱۷-۱ محول کردن ثبت وقایع به برنامه‌های خارجی
۱۹۲	۴-۱۷-۲ ملاحظات امنیتی در فایل‌های ثبت وقایع
۱۹۲	۴-۱۷-۲-۱ ثبت وقایع و دسترسی ریشه (root)

۱۹۳	۴-۱۷-۲-۲ ثبت وقایع در فایل‌های متنی قابل تغییر
۱۹۳	۴-۱۷-۲-۳ مشکل امنیتی در برنامه‌های ثبت وقایع
۱۹۳	۴-۱۷-۲-۴ ثبت وقایع و فضای دیسک
۱۹۴	۴-۱۷-۲-۵ ثبت وقایع غیرقابل اعتماد
۱۹۴	۴-۱۷-۳ خواندن فایل‌های ثبت وقایع
۱۹۴	۴-۱۷-۳-۱ The Error Log ثبت وقایع خطا
۱۹۵	۴-۱۷-۳-۲ The Access Log ثبت وقایع دسترسی یا
۱۹۶	۴-۱۸ مشاهده رویدادها در سرویس‌دهنده Apache
۱۹۷	۴-۱۸-۱ استفاده از دایمون syslogd
۱۹۸	۴-۱۸-۱-۱ استفاده از syslog برای رویدادنگاری error_log
۱۹۹	۴-۱۸-۱-۲ استفاده از syslog برای رویدادنگاری access_log
۲۰۰	۴-۱۸-۱-۳ استفاده از syslog-ng
۲۰۰	۴-۱۹ به‌کارگیری ماژول mod_security در امنیت Apache
۲۰۴	۴-۲۰ تنظیم قوانین فیلتر ماژول mod_security در امنیت Apache
۲۱۱	۴-۲۱ نصب راه‌اندازی mod_security نسخه دو بر روی Apache
۲۱۴	۴-۲۲ مراجع این فصل
۲۱۵	فصل پنجم: امن‌سازی سیستم پست الکترونیکی
۲۱۵	۵-۱ امنیت در پست الکترونیکی
۲۱۵	۵-۱-۱ پست الکترونیکی چگونه کار می‌کند
۲۱۵	۵-۱-۲ فقدان امنیت در پست الکترونیکی
۲۱۶	۵-۱-۳ تهدیدهای امنیتی در ارتباط پست الکترونیکی
۲۱۷	۵-۱-۴ امن‌سازی پست الکترونیکی توسط TLS
۲۱۸	۵-۱-۵ حفاظت از حریم خصوصی توسط MTLS
۲۱۹	۵-۱-۶ رمزگذاری نامتقارن و پست الکترونیکی (PGP و S/MIME)
۲۱۹	۵-۱-۷ معرفی PGP
۲۲۰	۵-۱-۸ مشکلات تعاملی
۲۲۱	۵-۲ آسیب‌پذیری‌های موجود در بسته پست الکترونیکی Sendmail
۲۲۳	۵-۳ بسته پست الکترونیکی Postfix
۲۲۴	۵-۴ ایمن‌سازی سرور پست الکترونیکی
۲۲۴	۵-۴-۱ ایمن‌سازی سرورهای خانواده لینوکس
۲۲۵	۵-۴-۲ ایمن‌سازی بسته‌های پست الکترونیکی (Sendmail)
۲۲۶	۵-۴-۳ ایمن‌سازی بسته پست الکترونیکی (Qmail)
۲۲۶	۵-۴-۴ ایمن‌سازی بسته پست الکترونیکی (Postfix)
۲۲۷	۵-۴-۵ Open Relay پرهیز از
۲۲۸	۵-۴-۶ بلوکه کردن Spamها
۲۲۹	۵-۴-۷ فیلتر کردن ویروس‌ها
۲۳۰	۵-۵ اطلاعات پایه‌ی امنیتی در عامل انتقال نامه الکترونیکی Qmail
۲۳۰	۵-۵-۱ عامل انتقال نامه الکترونیکی Qmail
۲۳۲	۵-۵-۲ نکته‌هایی برای استفاده از Qmail
۲۳۲	۵-۵-۳ اشکالات گزارش شده در Qmail
۲۳۳	۵-۶ پیکربندی عامل انتقال نامه الکترونیکی Qmail
۲۳۳	۵-۶-۱ پیکربندی Qmail
۲۳۷	۵-۷ لیست کنترلی امن‌سازی عامل انتقال نامه الکترونیکی Qmail
۲۳۸	۵-۸ مراجع این فصل
۲۳۹	فصل ششم: امن‌سازی سرویس‌های فایل و به‌اشتراک‌گذاری آن
۲۳۹	۶-۱ اصول آغازین سطوح دسترسی فایل در یونیکس و لینوکس

۲۳۹	۶-۱-۱ مجوزهای دستیابی پرونده‌ها
۲۴۱	۶-۱-۲ نکاتی در مورد مجوز دسترسی به برخی فایل‌های کلیدی
۲۴۱	۶-۱-۳ ویژگی‌های پرونده‌ها
۲۴۴	۶-۲ کنترل دسترسی به فایل‌ها و ویژگی‌های آنها
۲۴۵	۶-۳ ابزار Tripwire
۲۴۶	۶-۳-۱ Tripwire چگونه کار می‌کند؟
۲۴۷	۶-۴ سیستم‌های فایل رمزنگاری شده
۲۴۸	۶-۵ امن‌سازی سرویس‌دهنده‌ی FTP
۲۵۰	۶-۵-۱ ابزارهای مرتبط برای آزمایش FTP
۲۵۰	۶-۵-۲ حمله‌های محتمل بر علیه FTP
۲۵۱	۶-۵-۳ vsftpd
۲۵۲	۶-۵-۴ نصب و استفاده از vsftpd
۲۵۲	۶-۵-۵ پیکربندی vsftpd
۲۵۴	۶-۵-۶ نکات امنیتی تکمیلی
۲۵۴	۶-۶ لیست سرورهای سرویس‌دهنده‌ی FTP
۲۵۵	۶-۷ پروتکل SFTP و SPS
۲۵۵	۶-۷-۱ SFTP یا SPS (SFTP)
۲۵۵	۶-۷-۲ استفاده از SPS برای امن کردن سرویس‌دهنده‌های FTP
۲۵۶	۶-۷-۳ تفاوت FTP و FTPS
۲۵۶	۶-۸ پروتکل ساده انتقال فایل (TFTP)
۲۵۷	۶-۹ سرویس‌دهنده‌ی اشتراک فایل Samba
۲۵۷	۶-۹-۱ فایل پیکربندی smb.conf
۲۶۱	۶-۹-۲ کار با سرویس‌دهنده‌ی Samba
۲۶۲	۶-۱۰ سیستم‌فایل شبکه (NFS)
۲۶۲	۶-۱۱ عدم پیکربندی مناسب سرویس‌های NFS
۲۶۵	۶-۱۲ مراجع این فصل
۲۶۷	فصل هفتم: امن‌سازی پایگاه‌های داده‌ی رایج در یونیکس و ونوکس
۲۶۷	۷-۱ ضعف‌های امنیتی در پایگاه‌های داده
۲۷۰	۷-۲ محافظت از پایگاه‌های داده
۲۷۲	۷-۳ معماری پایگاه‌داده‌ی MySQL
۲۷۳	۷-۴ امن‌سازی پایگاه‌داده‌ی MySQL
۲۷۴	۷-۴-۱ نصب سرور MySQL به‌فرم امن
۲۷۶	۷-۴-۲ پیکربندی سرور MySQL به‌فرمی امن
۲۷۸	۷-۴-۳ حذف اشیاء غیرضروری در پایگاه‌های داده‌ی MySQL
۲۷۹	۷-۴-۴ ایمن‌سازی حساب‌های کاربری
۲۸۰	۷-۴-۵ استفاده از احراز هویت ایمن برای تصدیق هویت کاربران
۲۸۲	۷-۴-۶ کنترل دسترسی کاربران
۲۸۴	۷-۴-۷ ذخیره‌سازی امن اطلاعات
۲۸۴	۷-۴-۸ پشتیبان‌گیری منظم از اطلاعات
۲۸۷	۷-۴-۹ فعال‌سازی گزارش‌های ثبت وقایع
۲۸۹	۷-۵ ملاحظات امنیتی در پایگاه‌داده‌ی MySQL
۲۹۳	۷-۶ پیاده‌سازی مکانیزم‌های امنیتی در MySQL
۲۹۶	۷-۷ بهره‌گیری از ابزارهای امنیتی برای MySQL
۲۹۸	۷-۸ دیواره‌آتش پایگاه‌داده‌ی MySQL
۲۹۹	۷-۹ مکانیزم‌های امنیتی در PostgreSQL
۳۰۳	۷-۱۰ کنترل دسترسی از طریق فایل‌های مخصوص پیکربندی

۳۰۵	۷-۱۱ مکانیزم SSL در PostgreSQL
۳۰۶	۷-۱۲ برقراری ارتباط محلی امن در PostgreSQL
۳۰۸	۷-۱۳ امن سازی پایگاه های داده PostgreSQL
۳۱۳	۷-۱۴ امنیت در پایگاه های داده Oracle
۳۱۶	۷-۱۵ کنترل دسترسی در پایگاه داده Oracle
۳۲۰	۷-۱۶ محافظت از پایگاه های داده Oracle
۳۲۱	۷-۱۷ ایمن سازی ساختاری در پایگاه داده Oracle
۳۲۵	۷-۱۸ بهره گیری از مکانیزم های امنیتی در پایگاه داده Oracle
۳۳۰	۷-۱۹ امن سازی پایگاه داده Berkeley DB
۳۳۲	۲۰-۴ مراجع این فصل
۳۳۳	فصل هشتم: اصول امنیت در DNS
۳۳۴	۸-۱ آسیب پذیری های موجود در BIND DNS
۳۳۶	۸-۲ آسیب پذیری عدم سرویس دهی در BIND
۳۳۶	۸-۳ آسیب پذیری در سرویس DNS
۳۳۸	۸-۴ لیست کد های آسیب پذیری در سرویس نام دامنه (DNS)
۳۴۰	۸-۵ مراجع این فصل
۳۴۱	فصل نهم: امن سازی سیستم های سرویس ها و پروتکل های رایج
۳۴۱	۹-۱ پروتکل آسان مدیریت شبکه (SNMP) و امن سازی آن
۳۴۵	۹-۲ مدیریت سیستم گزارش گیری امنیت (syslog)
۳۴۶	۹-۲-۱ تفاوت Syslog با SIEM در جمعیت کنترل و نظارت
۳۴۶	۹-۲-۲ اجزای یک سرور Syslog
۳۴۷	۹-۲-۳ آشنایی با ساختار پیغام های Syslog
۳۵۰	۹-۲-۴ فایل های مهم مخصوص ثبت وقایع (log)
۳۵۳	۹-۲-۵ بهره گیری از دستورهای logger و faillog
۳۵۳	۹-۳ پیکربندی و مدیریت تحلیل Log
۳۵۳	۹-۳-۱ تحلیل گر Syslog
۳۵۴	۹-۳-۱-۱ پیکربندی Syslog برای ورودهای محلی و دور
۳۵۵	۹-۳-۲ بسته های باز مفید برای بازرسی فایل های ثبت وقایع Log
۳۵۵	۹-۳-۳ گردش Log
۳۵۶	۹-۳-۴ تحلیل گر Log
۳۵۷	۹-۴ بررسی Log های ورودهای نهایی
۳۵۸	۹-۵ امن سازی در پروتکل DHCP
۳۵۸	۹-۵-۱ حمله های نوع DHCP Starvation
۳۵۸	۹-۵-۲ حمله های نوع DHCP Spoofing
۳۵۹	۹-۶ شناسایی DHCP در لینوکس
۳۶۰	۹-۷ امن سازی پروتکل NTP
۳۶۰	۹-۷-۱ جعل و دست کاری بسته های NTP
۳۶۰	۹-۷-۲ حمله ی سرریز بافر
۳۶۱	۹-۷-۳ حمل تکرار
۳۶۱	۹-۸ پیشنهاد برای امن سازی سیستم عامل لینوکس
۳۶۴	۹-۹ شناسایی آسیب پذیری ها و حفره های امنیتی در لینوکس
۳۶۷	۹-۱۰ مدیریت آسیب پذیری ها و وصله ها در لینوکس
۳۶۷	۹-۱۱ مراجع این فصل
۳۶۹	فصل دهم: بهره گیری از دیوارهای آتش
۳۶۹	۱۰-۱ سرویس های دیوار آتش
۳۷۰	۱۰-۲ انواع دیوار آتش

۳۷۰	۱۰-۳	IPTables ابزار
۳۷۱	۱۰-۴	IPTables مفاهیم پایه در
۳۷۳	۱۰-۵	IPTables عبارات و اصطلاحات
۳۷۵	۱۰-۶	IPTables ساختار
۳۷۶	۱۰-۶-۱	حرکت در میان جدول ها و زنجیره ها
۳۸۰	۱۰-۶-۲	Conntrack مفهوم ماشین وضعیت و ورودی های
۳۸۱	۱۰-۶-۳	وضعیت های مختلف یک بسته
۳۸۲	۱۰-۶-۳-۱	TCP اتصال های نوع
۳۸۳	۱۰-۶-۳-۲	UDP اتصال های نوع
۳۸۳	۱۰-۶-۳-۳	ICMP اتصال های نوع
۳۸۴	۱۰-۶-۴	IPTables امکانات ابزار
۳۸۴	۱۰-۶-۴-۱	iptables-save دستور
۳۸۶	۱۰-۶-۴-۲	iptables-restore دستور
۳۸۶	۱۰-۶-۵	ایجاد قوانین در دیوار آتش
۳۹۴	۱۰-۶-۶	IPChains تفاوت و
۳۹۴	۱۰-۶-۷	مسئله کردن یک آدرس IP
۳۹۵	۱۰-۷	راه اندازی و راه اندازی دیوار آتش در محیط گرافیکی
۳۹۶	۱۰-۷-۱	بهره گیری از محیط گرافیکی دیوار آتش برای تنظیم
۳۹۶	۱۰-۷-۱-۱	عبارت های فعال کردن دیوار آتش
۳۹۷	۱۰-۷-۱-۲	گزینه های برای اعتماد (Trusted Services)
۳۹۷	۱۰-۷-۱-۳	گزینه های دیگر (Other ports)
۳۹۷	۱۰-۷-۱-۴	گزینه های واسطه های قابل اعتماد (Trusted Interface)
۳۹۷	۱۰-۷-۱-۵	گزینه های masquerading
۳۹۷	۱۰-۷-۱-۶	گزینه های Port forwarding
۳۹۷	۱۰-۷-۱-۷	گزینه های ICMP Filter
۳۹۸	۱۰-۸	استفاده از IPTables برای تنظیمات خاص
۴۰۰	۱۰-۹	جدول های موجود در IPTables
۴۰۱	۱۰-۱۰	آزمون نفوذ پذیری دیوارهای آتش با ابزار FTester
۴۰۲	۱۰-۱۰-۱	FTester نصب
۴۰۲	۱۰-۱۰-۲	پیکربندی آغازین
۴۰۳	۱۰-۱۰-۳	استفاده از FTester در آزمون دیوار آتش
۴۰۴	۱۰-۱۰-۳-۱	گام نخست
۴۰۴	۱۰-۱۰-۳-۲	گام دوم
۴۰۵	۱۰-۱۰-۳-۳	گام سوم
۴۰۷	۱۰-۱۱	FreeBSD در IPFW دیوار آتش
۴۰۷	۱۰-۱۱-۱	پیکربندی در هسته
۴۰۷	۱۰-۱۱-۲	فایل /etc/rc.conf
۴۰۹	۱۰-۱۱-۳	ipfw دستور
۴۱۰	۱۰-۱۱-۴	نحوه نوشتن قوانین
۴۱۰	۱۰-۱۱-۴-۱	فیلد CMD
۴۱۰	۱۰-۱۱-۴-۲	فیلد RULE_NUMBER
۴۱۰	۱۰-۱۱-۴-۳	فیلد ACTION
۴۱۰	۱۰-۱۱-۴-۴	فیلد LOGGING
۴۱۱	۱۰-۱۱-۴-۵	فیلد SELECTION
۴۱۲	۱۰-۱۱-۵	جدول ها
۴۱۵	۱۰-۱۲	ipf دیوار آتش

۴۱۶	۱۰-۱۳ مراجع این فصل
۴۱۷	فصل یازدهم: سیستم‌های تشخیص نفوذ، Honeypot و مانیتورینگ
۴۱۷	۱۱-۱ سیستم‌های تشخیص نفوذ
۴۱۸	۱۱-۱-۱ سیستم‌های تشخیص نفوذ تحت شبکه (NIDS)
۴۱۹	۱۱-۱-۲ سیستم‌های تشخیص نفوذ تحت میزبان (HIDS)
۴۲۰	۱۱-۱-۳ طبقه‌بندی IDSها برپایه‌ی قابلیت‌ها
۴۲۲	۱۱-۲ سیستم تشخیص نفوذ Snort
۴۲۳	۱۱-۲-۱ اجزای نرم‌افزار Snort
۴۲۳	۱۱-۲-۱-۱ بخش گردآوری اطلاعات
۴۲۳	۱۱-۲-۱-۲ بخش تجزیه و تحلیل کننده‌ی آغازین
۴۲۳	۱۱-۲-۱-۳ بخش موتور شناسایی
۴۲۴	۱۱-۲-۱-۴ بخش خروجی هشدار
۴۲۴	۱۱-۳ نصب پیکربندی Snort
۴۲۵	۱۱-۳-۱ نرم‌افزارهای پیش‌نیاز Snort
۴۲۵	۱۱-۳-۱-۱ libpcap
۴۲۶	۱۱-۳-۱-۲ PCRE
۴۲۶	۱۱-۳-۱-۳ libpcre
۴۲۶	۱۱-۳-۱-۴ libsnort
۴۲۶	۱۱-۳-۲ نصب Snort
۴۲۶	۱۱-۳-۲-۱ نصب Snort استفاده از بسته‌ی RPM
۴۲۷	۱۱-۳-۲-۲ راه‌اندازی، متوقف‌سازی و راه‌اندازی دوباره‌ی Snort
۴۲۷	۱۱-۳-۲-۳ نصب Snort با استفاده از کد منبع
۴۲۷	۱۱-۳-۲-۴ کامپایل و نصب
۴۲۹	۱۱-۳-۳ پیکربندی Snort
۴۳۲	۱۱-۳-۴ واسطه‌های کاربری Snort
۴۳۷	۱۱-۴ معماری و امنیت در ابزار Snort
۴۳۷	۱۱-۴-۱ تأمین امنیت Snort
۴۳۷	۱۱-۴-۲ تشخیص سیستم Snort روی شبکه
۴۳۸	۱۱-۴-۳ حمله‌های تهدیدکننده‌ی Snort
۴۳۹	۱۱-۴-۴ معماری Snort در شبکه
۴۴۰	۱۱-۵ سیستم‌های تشخیص نفوذ معروف
۴۴۱	۱۱-۶ ابزارهای مفید و رایج برای کار با Snort
۴۴۱	۱۱-۶-۱ ابزار SnortSnarf
۴۴۲	۱۱-۶-۲ ابزار Snort Alert Monitor
۴۴۳	۱۱-۶-۳ ابزار Guardian (Active Response for Snort)
۴۴۴	۱۱-۶-۴ ابزار BASE
۴۴۴	۱۱-۷ Honeypot چیست؟
۴۴۵	۱۱-۸ انواع Honeypot
۴۴۵	۱۱-۸-۱ Honeypot‌های با تعامل کم
۴۴۷	۱۱-۸-۲ Honeypot‌های با تعامل متوسط
۴۴۷	۱۱-۸-۳ Honeypot‌های با تعامل زیاد
۴۴۹	۱۱-۸-۴ تقسیم‌بندی Honeypot‌ها از نظر کاربرد
۴۴۹	۱۱-۸-۴-۱ Production Honeypot
۴۵۰	۱۱-۸-۴-۲ Research Honeypot
۴۵۰	۱۱-۹ مکانیزم‌های تحلیل اطلاعات در Honeypot‌ها
۴۵۱	۱۱-۹-۱ فایل‌های Log مخصوص دیوار آتش

۴۵۱		۱۱-۹-۲ سیستم تشخیص نفوذ (IDS)
۴۵۱		۱۱-۹-۳ فایل های Log سیستم
۴۵۲		۱۱-۹-۴ جرم شناسی سیستم قربانی
۴۵۲		۱۱-۹-۵ جرم شناسی پیشرفته سیستم قربانی
۴۵۲		۱۱-۱۰ مکانیزم های گردآوری اطلاعات در Honeypot ها
۴۵۳		۱۱-۱۰-۱ مبتنی بر میزبان
۴۵۳		۱۱-۱۰-۲ مبتنی بر شبکه
۴۵۳		۱۱-۱۰-۳ مبتنی بر مسیر یاب / دروازه (Gateway)
۴۵۴		۱۱-۱۱ گام های راه اندازی و به کار گیری یک Honeypot
۴۵۴		۱۱-۱۲ انتخاب سخت افزار برای میزبان
۴۵۴		۱۱-۱۱ نصب سیستم عامل
۴۵۵		۱۱-۱۱ معماری شبکه
۴۵۵		۱۱-۱۴ هشدارها و تشخیص نفوذ
۴۵۵		۱۱-۱۲ ابزار های کنترلی نظارت شبکه
۴۵۹		۱۱-۱۳ مربع اتصال
۴۶۱		فصل دوازدهم: سیستم های دفاعی
۴۶۲		۱۲-۱ نصب سرویس دهنده Squid
۴۶۳		۱۲-۲ برخی از پارامترهای Squid
۴۶۴		۱۲-۳ پیکربندی سرویس دهنده Squid
۴۶۵		۱۲-۳-۱ تنظیم پورت سرویس دهنده Squid
۴۶۵		۱۲-۳-۲ تنظیم محل ذخیره سازی Cache شده
۴۶۵		۱۲-۳-۳ شناسه های گروه و کاربر
۴۶۶		۱۲-۳-۴ ارسال نامه الکترونیکی برای Cache
۴۶۶		۱۲-۳-۵ اطلاعات ورود به سرویس FTP
۴۶۶		۱۲-۳-۶ تنظیمات کنترل دسترسی
۴۶۸		۱۲-۳-۷ ثبت وقایع در سرویس دهنده Squid
۴۶۹		۱۲-۳-۸ مفهوم upstream Proxy در سرویس دهنده Squid
۴۶۹		۱۲-۳-۹ به اشتراک گذاری سرورهای Cache با کمک Squid
۴۶۹		۱۲-۳-۱۰ پیاده سازی سرور پراکسی به فرم شفاف
۴۷۰		۱۲-۴ راه اندازی سرویس دهنده Squid
۴۷۰		۱۲-۵ امن سازی سرویس دهنده Squid
۴۷۲		۱۲-۶ سرویس دهنده Squid در FreeBSD
۴۷۲		۱۲-۶-۱ پیکربندی Squid
۴۷۳		۱۲-۶-۲ راه اندازی و متوقف کردن سرور Squid
۴۷۳		۱۲-۶-۳ تنظیم کلاینت ها
۴۷۳		۱۲-۶-۴ بررسی فایل پیکربندی
۴۸۰		۱۲-۶-۵ قابلیت لیست های کنترل دسترسی در Squid و FreeBSD
۴۸۳		۱۲-۶-۶ برچسب های cache_access_log, cache_store_log و cache_log
۴۸۳		۱۲-۶-۷ برچسب ftp_user
۴۸۳		۱۲-۶-۸ برچسب dns_nameservers
۴۸۳		۱۲-۶-۹ برچسب auth_param
۴۸۴		۱۲-۶-۱۰ پارامتر authenticate_ttl
۴۸۴		۱۲-۶-۱۱ پارامتر request_header_max_size
۴۸۴		۱۲-۶-۱۲ بررسی برچسب هایی با تعیین مدت زمان
۴۸۴		۱۲-۶-۱۳ برچسب های امنیتی در Squid
۴۸۵		۱۲-۶-۱۴ اجرای Squid در حالت Intercept یا Transparent

۴۸۶	۱۲-۷ مراجع این فصل
۴۸۷	فصل سیزدهم: کانال‌های امن و امن‌سازی ساختار آنها
۴۸۷	۱۳-۱ OpenSSL و عملیات مربوط به گواهینامه‌ها
۴۸۷	۱۳-۱-۱ تولید درخواست امضای گواهینامه
۴۸۸	۱۳-۱-۲ تولید گواهینامه‌ی self-signed با در اختیار داشتن CSR
۴۸۹	۱۳-۱-۳ مشاهده‌ی محتوای CSR
۴۸۹	۱۳-۱-۴ مشاهده‌ی محتوای یک گواهینامه
۴۸۹	۱۳-۱-۵ مشاهده‌ی امضا کننده‌ی یک گواهینامه
۴۹۰	۱۳-۱-۶ تولید کلید خصوصی و رمزنگاری/رمزگشایی آن
۴۹۰	۱۳-۱-۷ تبدیل گواهینامه با فرمت PEM به گواهینامه با فرمت PKCS12
۴۹۱	۱۳-۱-۸ تبدیل گواهینامه با فرمت PKCS12 به گواهینامه با فرمت PEM
۴۹۱	۱۳-۱-۹ ابطال کردن OpenSSL به‌عنوان سرویس‌دهنده
۴۹۲	۱۳-۱-۱۰ فعال کردن OpenSSL به‌عنوان سرویس‌گیرنده
۴۹۲	۱۳-۲ راه‌های برقراری SSL و امن‌سازی آن در لینوکس
۴۹۲	۱۳-۲-۱ حمله‌ی MITM به SSL
۴۹۲	۱۳-۲-۱-۱ حمله‌ی Man in the Middle
۴۹۲	۱۳-۲-۱-۲ حمله‌ی Brute force بر روی کلید نشست
۴۹۲	۱۳-۲-۱-۳ حمله‌ی انبساط سرویس
۴۹۲	۱۳-۲-۱-۴ حمله‌ی نفیل فیک
۴۹۴	۱۳-۲-۱-۵ آسیب‌پذیری در Debian OpenSSH در مکانیزم تولید اعداد تصادفی
۴۹۴	۱۳-۲-۲ نحوه‌ی تشخیص آسیب‌پذیری‌های OpenSSH و حفاظت از آن
۴۹۵	۱۳-۳ ساختار VPN در یونیکس و لینوکس
۴۹۵	۱۳-۳-۱ نصب PPTP
۴۹۶	۱۳-۳-۲ نصب L2TP
۴۹۶	۱۳-۳-۳ نصب OpenVPN
۴۹۸	۱۳-۴ نصب امن سرویس‌دهنده‌ی SSH
۴۹۸	۱۳-۴-۱ انواع بسته
۴۹۸	۱۳-۴-۱-۱ بسته‌های دودویی
۴۹۹	۱۳-۴-۱-۲ بسته‌های کد منبع
۴۹۹	۱۳-۴-۲ پیش‌نیازها
۴۹۹	۱۳-۴-۳ دریافت بسته
۴۹۹	۱۳-۴-۴ نصب بسته‌ی دودویی
۴۹۹	۱۳-۴-۴-۱ بررسی درستی بسته
۵۰۰	۱۳-۴-۴-۲ نصب بسته
۵۰۰	۱۳-۴-۵ نصب بسته‌ی کد منبع
۵۰۱	۱۳-۴-۵-۱ خارج کردن بسته از حالت فشرده
۵۰۱	۱۳-۴-۵-۲ پیکربندی برای کامپایل
۵۰۵	۱۳-۴-۵-۳ کامپایل
۵۰۶	۱۳-۴-۵-۴ نصب بسته
۵۰۶	۱۳-۴-۶ جایگاه فایل‌ها
۵۰۶	۱۳-۴-۶-۱ فایل‌های پیکربندی
۵۰۶	۱۳-۴-۶-۲ فایل‌های اجرایی
۵۰۷	۱۳-۵ امن‌سازی سرویس‌دهنده‌ی SSH در لینوکس
۵۰۸	۱۳-۵-۱ بهره‌گیری از SSH به‌عنوان یک سرویس امن
۵۰۸	۱۳-۵-۲ تولید کلیدهای RSA
۵۰۹	۱۳-۵-۳ بهره‌گیری از دستور ssh-agent

۵۱۰	۱۳-۵-۴ پی‌یکربندی امن سرویس‌دهنده‌ی SSH
۵۱۱	۱۳-۵-۴-۱ تغییر دادن فایل شنود SSH
۵۱۱	۱۳-۵-۴-۲ مجاز دانستن پروتکل شماره دو برای SSH
۵۱۱	۱۳-۵-۴-۳ تنها مجاز دانستن کاربران خاص برای ورود به سیستم از طریق SSH
۵۱۲	۱۳-۵-۴-۴ ایجاد یک نشان سفارشی SSH
۵۱۲	۱۳-۵-۴-۵ تصدیق اصالت با استفاده از کلید عمومی DSA
۵۱۳	۱۳-۵-۵ برقراری یک نشست SSH با سرویس راه دور
۵۱۳	۱۳-۵-۶ انتقال فایل با برنامه‌های scp و sftp
۵۱۴	۱۳-۵-۷ راه‌اندازی سرویس‌دهنده‌ی SSH
۵۱۴	۱۳-۵-۸ نمایش یا عدم نمایش آدرس IP نهایی متصل شده به SSH
۵۱۵	۱۳-۵-۹ پیاده‌سازی تنظیمات امنیتی بیشتر در SSH
۵۱۶	۱۳-۵-۱۰ نحوه‌ی حفاظت درمقابل نقاط آسیب‌پذیر سرویس‌دهنده‌ی SSH
۵۱۷	۱۳-۶ سرویس‌های متن‌ساده در لینوکس
۵۱۹	۱۳-۷ ساختار ابزار GPG
۵۲۰	۱۳-۷-۱ نصب GPG
۵۲۰	۱۳-۷-۲ ایجاد کلیدهای رمزنگاری
۵۲۳	۱۳-۷-۳ کار با کلیدهای رمزنگاری تولید شده
۵۲۶	۱۳-۷-۴ امضای کلیدهای رمزنگاری
۵۲۹	۱۳-۷-۵ رمزنگاری و امضای فایل‌ها
۵۳۰	۱۳-۷-۶ ابزارها برای کار با GPG
۵۳۰	۱۳-۷-۶-۱ ابزارهای گرافیکی
۵۳۰	۱۳-۷-۶-۲ سرویس‌گیرنده‌های پس‌زمینه
۵۳۱	۱۳-۷-۶-۳ ابزارهای دیگر برای کار با GPG
۵۳۱	۱۳-۷-۷ محل قرارگیری فایل‌های ابزار GPG
۵۳۲	۱۳-۸ مراجع این فصل

سخنی با خوانندگان

این روزها امنیت اطلاعات در هر شاخه‌ای از علم، دارای جایگاه ویژه‌ای می‌باشد که روز به روز بر ارزش آن افزوده می‌شود. هم اینک تقریباً تمامی صنایع و حرفه‌ها به نوعی نیازمند امنیت اطلاعات و ایجاد مکانیزم‌هایی جهت محرمانگی آنها هستند. امنیت در یک سیستم‌عامل نیز جزو موارد اساسی و پایه‌ای در یک شبکه‌ی کامپیوتری است که هر مدیر سیستمی باید به آن توجه ویژه داشته باشد. هم اکنون سیستم‌های عامل یونیکس و لینوکس از نظر امنیت نسبت به سیستم‌های عامل ویندوز در جایگاه بهتری قرار دارند، اما باز هم دارای نقاط ضعف و آسیب‌پذیری‌های خاص خود می‌باشند. به امن‌سازی آنها می‌تواند یک سیستم‌عامل قابل قبول را از دیدگاه امنیتی پدید آورد؛ هرچند همان‌گونه که می‌دانیم امنیت یک موضوع نسبی است و به هیچ‌عنوان ساختاری مطلق به‌خود نخواهد گرفت، اما می‌توان تا حد امکان و قابل قبول و با کمک ساختارها و اصول امنیتی، بستر اصلی آن یعنی سیستم‌عامل را امن ساخت. همان‌گونه که گفته شد، امروزه وجهی که یک سیستم‌عامل امن و پایدار، از ارکان اصلی و پایه‌ای یک بستر و شبکه‌ی کامپیوتری محسوب می‌شود که به گونه‌ی مکرر در آن حتی جزئی، ممکن است موجب تخریب و سرقت داده‌ها و یا از بین رفتن همه‌ی اطلاعات موجود بر روی آن سیستم گردد. از این‌رو استفاده از یک سیستم‌عامل پایدار، مطمئن و امن می‌تواند در بسترهای مختلف کامپیوتری، گستران، گستران و متخصصان فناوری اطلاعات کمک به‌سزایی نماید و آنها را در مسیر سرویس‌دهی و نگهداری از اسنادات اساسی سازمان‌ها یاری کند.

اینجانب به‌عنوان عضو کوچکی از خانواده‌ی بزرگ سیستم‌های عامل کدباز، درصدد گردآوری و تألیف کتابی مرجع به‌منظور آشنایی کامل برخی متخصصان، دانش‌آموزان و مدیران شبکه با اصول امن‌سازی و امنیت سیستم‌های عامل مبتنی بر یونیکس و لینوکس بودم تا آنها را با اصول امنیتی سیستم‌های عامل کدباز و همچنین اهمیت امنیت در آنها آشنا و آگاه سازم. (گرچه مدیران و متخصصان، حکم اساتید اینجانب را دارند، اما به حکم وظیفه بر خود لازم دانستم که این آگاه‌سازی را انجام دهم). پیشاپیش تمام کاستی‌های آنرا می‌بخشیدم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه‌ی آنها را دایمی منت پذیرا هستم.

(m_Davari@TOP-co.ir)

(m_Davary@Parshack.zan.co.ir)

درباره‌ی این کتاب

شیرازه‌ی اصلی این کتاب برگرفته از کتاب‌ها و منابع معتبر درباره‌ی امنیت و امن‌سازی سیستم‌های عامل یونیکس و لینوکس است که با تجربیات اینجانب آمیخته شده است، که دخل و تصرفی نیز با آن همراه بوده است. هدف از تألیف این کتاب آشنایی بیشتر کارشناسان و مدیران فناوری اطلاعات با آسیب‌پذیری‌های موجود در سیستم‌های عامل کدباز (یونیکس و لینوکس) است. همچنین راه کارهای مقابله با این نوع آسیب‌پذیری‌ها که موجب بروز حملات مختلف بر علیه این نوع سیستم‌های عامل می‌شوند، در قالب فصل‌های این کتاب بررسی و ارائه شده است. این کتاب اطلاعات مفیدی در اختیار راهبر سیستم‌های یونیکسی و لینوکسی می‌گذارد و وی با کمک این کتاب می‌تواند سیستم‌عامل خود را که معمولاً برای برآوردی چون سرور و سامانه‌های امنیتی مورد استفاده قرار می‌گیرد، امن نماید تا در مقابل انواع حملات اول غیرمتداول ایمن گردد.

پس از سپاس و ستایش به درگاه پروردگار، از همه‌ی دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر و قدردانی می‌کنم. برخورد لازم می‌دانم از زحمات بی‌دریغ استاد محترم سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانه‌ی ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است. در پایان از جناب آقای مهندس حسن مسویی و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یارب چو به وحدت یقین می‌دارم

ایمان به توحید آئین می‌دارم

دارم لب خشک و دیده‌ی تر بپذیر

کز خشک و تر جهان هستی می‌دارم

(مجید داوری دولت آبادی - زمستان ۱۳۹۴)