به نام خدا

امنیت در سرورها،سرویس ها و شبکه های لینوکس

(پوشش دهنده مدارک امنیت لینوکس RH413 و EX413 از RedHat)

مؤلف

مهندس سید حسین رجاء

فهرست مطالب

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی است که بتواند خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت **"مهندس سید حسین رجاء"** و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

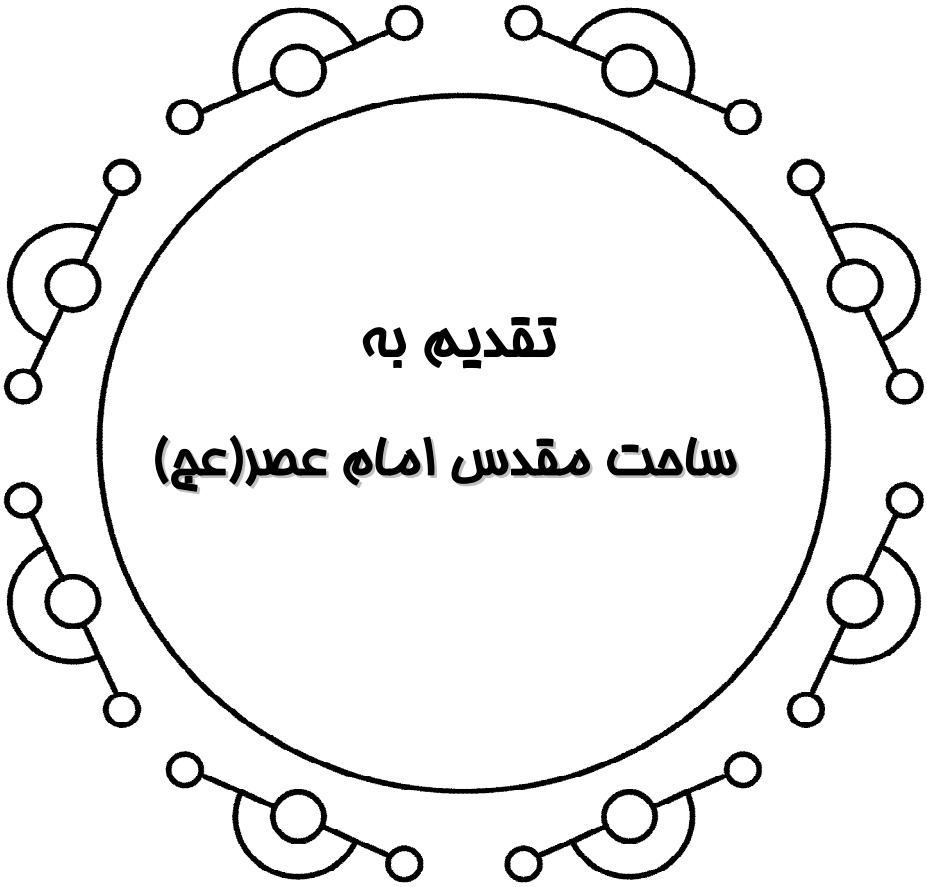
کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
Publishing@mftmail.com


تقدیم به
ساحت مقدس امام عصر(عج)

پیشگفتار

در عصر اطلاعات، بسیاری از تراکنش‌ها چه مالی و چه غیرمالی، به‌صورت الکترونیکی انجام می‌شوند، تبادل داده‌ها از طریق اینترنت صورت می‌گیرد و سرقت و دست‌کاری و لو رفتن داده‌ها می‌تواند هزینه‌ای گزاف از حیث آبرویی، مالی، سیاسی، اقتصادی و فرهنگی داشته باشد.

در حوزه لینوکس، نیز این مسئله که امنیت باشد وجود دارد و بسیار حائز اهمیت است. در این کتاب امنیت در حوزه لینوکس را از سه دیدگاه امنیت سرورهای لینوکس، امنیت سرویس‌های لینوکس و امنیت شبکه‌های لینوکس به‌صورت کاملاً حرفه‌ای و مبتنی بر سناریوهای عملی متعدد بررسی نموده‌ایم.

نکته قابل توجه در این کتاب آن است که سرفصل‌های کتاب به گونه‌ای تنظیم شده است که باعث می‌شود کتاب برای شرکت‌کنندگان در آزمون‌های بین المللی Red Hat Security and Server Hardening (RH413) و Red Hat Certificate of Expertise in Security and Server Hardening Exam (EX413) کاملاً قابل استفاده باشد و مطالب کاربردی مطرح شده در این دو آزمون نیز پوشش داده شوند.

مباحث این کتاب، به اختصار شامل موارد زیر است:

۱- امنیت سرورهای لینوکس

- مجوزها
- مالکان و گروه‌ها
- مجوزهای ویژه Sticky Bit/Setuid/Setgid
- Umask
- sudo و su
- فایل /var/log/utmp
- فایل /var/log/wtmp
- فایل /var/log/btmp
- فایل /var/log/secure
- دستورات uptime، w و who
- دستور lastlog
- دستور chage
- Lock و Unlock کردن کاربران
- دستورهای lsattr و chattr
- PAM
- Realmهای مدیریت PAM
- کنترل‌های ماژول PAM
- ماژول‌های پشته

- ماژول‌های PAM رایج
- مثال‌هایی از PAM
- ماژول pam_tally2
- بازیابی رمز عبور root
- ایمن‌سازی Grub Boot Loader
- ایمن‌سازی درون inittab
- پیکربندی مناسب motd (Message of the day)
- دستور psacct
- لیست‌های کنترل دسترسی (ACLها)
- مکانیسم‌های کنترل دسترسی (ACMها)
- کنترل دسترسی اختیاری (DAC)
- کنترل دسترسی اجباری (MAC/Mandatory Access Control)
- کنترل دسترسی مبتنی بر نقش (RBAC)
- امنیت چند سطحی (MLS)
- امنیت چند طبقه (MCS)
- SELinux
- Loginهای SELinux
- مدل Bell-La Padula (BLP)
- MLS و امتیازات سیستم (System Privileges)
- سطوح امنیت، اشیاء و موضوع
- سیاست MLS
- انواع در SELinux (SELinux Types)
- استفاده از قوانین خط مشی برای تعیین دسترسی انواع
- نقش سیاست در فرایند بوت
- کلاس‌های اشیاء و مجوزها
- سیاست هدف (Targeted Policy)
- سیاست سخت‌گیرانه (Strict Policy)
- کاربران و نقش‌ها در سیاست هدف (Targeted Policy)
- کنترل کاربر انتهایی SELinux
- انتقال و کپی کردن فایل‌ها در SELinux
- بررسی امنیت یک پروسه، کاربر یا شیء فایل
- برچسب‌گذاری مجدد فایل یا دایرکتوری
- ایجاد آرشیوهایی که محتوای امنیتی (Security Context) را حفظ می‌کنند
- کنترل مدیریت SELinux
- برچسب‌گذاری مجدد (Relabling) یک سیستم فایل

- مدیریت Home Directoryهای NFS
- مشخص کردن امنیت پرونده‌های سیستم فایل
- اجرای دستور در یک زمینه امنیتی خاص
- تغییر به یک نقش متفاوت
- تحلیلگر کنترل SELinux
- فعال کردن Kernel Auditing
- سفارشی کردن سیاست SELinux
- سیاست ماژولار
- لیست ماژول‌های خط مشی
- ساخت یک ماژول خط مشی محلی
- تجزیه و تحلیل فایل Type Enforcement (TE)
- بارگذاری بسته سیاست
- مثال‌هایی از SELinux و MAC
- ...

۲- امنیت سرویس‌های لینوکس

- غیرفعال کردن سرویس‌های غیرضروری سیستم/بستن پورت‌های باز
- فرمان fuser
- یافتن فرایندی که به یک دایرکتوری دسترسی دارد
- نحوه خاتمه دادن به فرآیندها و ارسال سیگنال به آن‌ها با استفاده از fuser
- fuser و گرفتن اطلاعاتی از پروسه‌ها و سوکت ها
- پیدا کردن فرآیندهای در حال اجرا در پورت خاص
- لیست فایل‌های باز IPv4 و IPv6
- فهرست فایل‌های باز پورت TCP در دامنه ۱-۱۰۲۴
- پیدا کردن اینکه افراد چه فایل‌ها و دستوراتی را استفاده می‌کنند
- لیست تمام اتصالات شبکه
- Jail یا chroot کردن DNS Server
- بهترین روش‌های ایمن‌سازی سرور OpenSSH
- فایل‌های known_hosts و authorized keys در SSH
- احراز هویت بدون ارائه گذرواژه در SSH (SSH PasswordLess Authentication)
- Access Control در Apache
- کنترل دسترسی توسط میزبان
- کنترل دسترسی با متغیرهای دلخواه
- کنترل دسترسی با mod_rewrite
- ماژول آپاچی mod_access_compat

- Allow Directive
- Deny Directive
- Order Directive
- Satisfy Directive
- Limit Directive
- LimitExcept Directive
- Authentication وAuthorization درApache
- محافظت از دایرکتوری درون وب سرور توسط رمز عبور
- اجازه دادن به بیش از یک نفر برای دسترسی
- جایگزین‌هایی برای ذخیره‌سازی رمز
- استفاده از ارائه‌دهندگان متعدد
- استفاده از ارائه‌دهندگان مجوز (authorization providers) برای کنترل دسترسی
- ایجاد گواهینامه‌ها و کلیدهای Self-Signed SSL برای Apache
- فعال کردن HTTPS برای Apache
- ایمن‌سازی وب سرور توسط SSL/TLS (HTTPS وApache)
- امنیت ایمیل سرور
- پیکربندی DomainKeys و DKIM
- ممانعت از Open Relay و پیکربندی Selective Relay
- پیکربندی SMTP Auth
- پیکربندی Courier Auth، Courier IMAP و Coureir POP
- پیکربندی SSL Courier POP3
- پیکربندی Courier IMAP SSL
- پیکربندی SMTPSD یا ایمن کردن SMTP (SMTP همراه با SSL / TLS)
- استفاده از SSL در SquirrelMail
- مقابله با ویروس در سرور ایمیل
- مقابله با Spam در سرور ایمیل
- نصب و پیکربندی Mailscanner
- نصب و پیکربندی maildrop
- ایمن‌سازی NFS
- دسترسی میزبان
- مدهای امنیتی در سرویس Samba
- پروکسی معمولی (Regular Proxy)
- پروکسی معکوس (Reverse Proxy)
- اسکوئید (Squid)
- نصب و پیکربندی Squid

- پیکربندی squid proxy به عنوان فیلتر وب
- محدود کردن دسترسی به وب‌سایت‌های خاص
- محدود کردن دسترسی به کلمات کلیدی خاص
- محدود کردن دسترسی به آدرس‌های IP خاص
- محدود کردن حجم دانلود توسط Squid
- پیکربندی Squid به عنوان Transparent Proxy
- ...

۳- امنیت شبکه‌های لینوکس

- فایروال در لینوکس
- مدیریت سرور iptables
- پردازش بسته در iptables
- مقاصد و جهش‌ها (Targets And Jumps)
- عملیات سوئیچ‌های مهم Iptables
- معیارهای رایج مطابقت در Iptables
- شرایط مطابقت مشترک TCP و UDP
- شرایط مطابقت مشترک ICMP (Ping)
- استفاده از زنجیره‌های تعریف شده توسط کاربر
- ذخیره و بازگرداندن اسکریپت iptables
- بازیابی از یک اسکریپت از دست رفته
- دفاع ابتدایی از سیستم عامل
- مقداردهی اولیه iptables به صورت پیشرفته
- اجازه دسترسی DNS به فایروال شما
- اجازه دسترسی WWW و SSH به فایروال شما
- اجازه دسترسی دادن به فایروال برای دسترسی به اینترنت
- اجازه دسترسی به شبکه خانگی خود برای دسترسی به فایروال
- Masquerading (NAT چند به یک)
- Port Forwarding (DHCP DSL) NAT از نوع
- NAT استاتیک
- عیب‌یابی iptables
- بررسی LOG های فایروال
- مدیریت و پیکربندی Audit
- جستجو در Logهای Audit رویدادها
- ایجاد گزارش‌های Audit
- تجزیه و تحلیل یک فرآیند با استفاده از autrace

- Port Scanner قدرتمند nmap
- کارت راهنمای nmap
- مشخصات هدف
- کشف میزبان
- تکنیک‌های اسکن
- مشخصات پورت و ترتیب اسکن
- تشخیص نسخه سرویس
- اسکن نوع اسکریپت
- تشخیص OS
- زمان‌بندی و کارایی
- Evasion و Spoofing فایروال IDS
- گزینه‌های خروجی Nmap
- پیکربندی iptables برای ممانعت از حملات Nmap
- Packet Capturing و تحلیل آن توسط دستور tcpdump
- ...

مخاطبین اصلی کتاب، متخصصین لینوکس، کارشناسان امنیت، مدیران شبکه، متخصصین حوزه نرم‌افزارهای متن باز، برنامه نویسان، متقاضیان و شرکت‌کنندگان در آزمون‌های بین المللی Red Hat Security and Server Hardening (RH413) و Red Hat Certificate of Expertise in Security and Server Hardening Exam (EX413)، دانشجویان رشته نرم‌افزار و فناوری اطلاعات و تمامی افراد علاقه‌مند به حوزه امنیت لینوکس و مباحث پیرامونی آن می‌باشند.

سید حسین رجاء کارشناس ارشد فناوری اطلاعات (IT) می‌باشد که حدوداً ۱۸ سال فعالیت در زمینه‌های مختلف IT، من جمله تدریس، برنامه‌نویسی، شبکه، امنیت شبکه، پایگاه داده، مجازی سازی، سیسکو، لینوکس، ویندوز و ایمیل سرور را تجربه کرده است. از جمله مدارک علمی ایشان می‌توان به CCIE R&S، CCIE Service Provider و LPIC-1,2,3(300,301,302,303,305) اشاره کرد.

قابل ذکر است، کتاب‌ها و آموزش‌های تصویری (ویدیویی) زیر در زمینه لینوکس و مدارک آن از اینجانب تاکنون منتشر شده است:

- امنیت در سروها، سرویس‌ها و شبکه‌های لینوکس (مدارک امنیت لینوکس RH413 و EX413 از RedHat)، سید حسین رجاء، انتشارات دیباگران، ۱۳۹۶
- آموزش جامع لینوکس (سطوح مقدماتی و متوسط)، سید حسین رجاء، انتشارات دیباگران، ۱۳۹۶
- آموزش جامع لینوکس (سطح پیشرفته)، سید حسین رجاء، انتشارات دیباگران، ۱۳۹۶
- آموزش تصویری Linux LPIC-3 303 Security، مؤلف سید حسین رجاء، رایکا امپرا (گروه آموزشی رایکا)، ۱۳۹۶
- آموزش تصویری Linux LPIC-3 305 Mail (Based on Qmail MTA)، مؤلف سید حسین رجاء، گروه آموزشی رایکا، ۱۳۹۵
- آموزش تصویری Linux LPIC-1 101، مؤلف سید حسین رجاء، گروه آموزشی رایکا، ۱۳۹۵

- آموزش تصویری Linux LPIC-1 102، مؤلف سید حسین رجاء، گروه آموزشی رایکا، ۱۳۹۵
- آموزش تصویری Linux LPIC-2 201، مؤلف سید حسین رجاء، گروه آموزشی رایکا، ۱۳۹۵
- آموزش تصویری Linux LPIC-2 202، مؤلف سید حسین رجاء، گروه آموزشی رایکا، ۱۳۹۵
- راهنمای جامع مدرک بین‌المللی Linux LPIC-3(302 Samba 3x)، سید حسین رجاء، انتشارات کانون نشر علوم، ۱۳۹۶
- راهنمای جامع مدرک بین‌المللی Linux LPIC-3(301 OpenLDAP 2.3)، سید حسین رجاء، انتشارات کانون نشر علوم، ۱۳۹۵
- راهنمای جامع مدرک بین‌المللی Linux LPIC-3(300 Part1: OpenLDAP 2.4)، سید حسین رجاء، کانون نشر علوم، ۱۳۹۵
- راهنمای کاربردی مدارک بین‌المللی LPIC-3(303 Security) و RHCSS، مؤلف سید حسین رجاء، کانون نشر علوم، ۱۳۹۵
- راهنمای کاربردی مدرک بین‌المللی لینوکس RHCE، مؤلف سید حسین رجاء، انتشارات کانون نشر علوم، ۱۳۹۵
- راهنمای کاربردی مدرک بین‌المللی لینوکس RHCSA، مؤلف سید حسین رجاء، انتشارات کانون نشر علوم، ۱۳۹۵
- برنامه‌نویسی به زبان PYTHON (مبتدی تا پیشرفته)، مؤلف سید حسین رجاء، انتشارات کانون نشر علوم و کاتوزی، ۱۳۹۶
- برنامه‌نویسی پوسته در لینوکس توسط Bash، مؤلف سید حسین رجاء، انتشارات کانون نشر علوم، ۱۳۹۵
- دستورات، کدها، مثال‌ها و سناریوهای عملی اجرا شده در مدرک بین‌المللی Linux LPIC-1(101,102) (به همراه نمونه سؤالات آزمون)، انتشارات کانون نشر علوم، ۱۳۹۶
- دستورات، کدها، مثال‌ها و سناریوهای عملی اجرا شده در مدرک بین‌المللی Linux LPIC-2(201,202) (به همراه نمونه سؤالات آزمون)، انتشارات کانون نشر علوم، ۱۳۹۶
- دستورات، کدها، مثال‌ها و سناریوهای عملی اجرا شده در مدرک بین المللی Linux LPIC-3 305 Mail (Based on Qmail MTA)، انتشارات کانون نشر علوم، ۱۳۹۶
- دستورات، کدها، مثال‌ها و سناریوهای عملی اجرا شده در مدرک بین المللی RHCSA، انتشارات کانون نشر علوم، ۱۳۹۶
- دستورات، کدها، مثال‌ها و سناریوهای عملی اجرا شده در مدرک بین المللی RHCE، انتشارات کانون نشر علوم، ۱۳۹۶
- راهنمای جامع لینوکس (دوره دو جلدی)، مؤلف سید حسین رجاء، انتشارات آترا و کانون نشر علوم، ۱۳۹۴
- راهنمای جامع مدرک بین‌المللی Linux LPIC-3(305 Mail and Messaging)، مؤلف سید حسین رجاء، انتشارات کانون نشر علوم، ۱۳۹۴
- راهنمای جامع مدرک بین‌المللی Linux LPIC-1(101,102)، مؤلف سید حسین رجاء، انتشارات آترا و کانون نشر علوم، ۱۳۹۴

- راهنمای جامع مدرک بین‌المللی Linux LPIC-2(201,202)، مؤلف سید حسین رجاء، انتشارات آترا و کانون نشر علوم، ۱۳۹۴
- Qmail (راه‌اندازی، پیکربندی و مدیریت)، مؤلف سید حسین رجاء، انتشارات افق دور و ریواس، ۱۳۹۳
- امنیت پست الکترونیکی، سید حسین رجاء، انتشارات پندار پارس، ۱۳۹۰

کتاب حاضر با توجه به مطالعات علمی و سال‌ها تجربه فنی نگارنده در زمینه امنیت لینوکس و مباحث پیرامونی تألیف شده است. بدیهی است که مطالب این کتاب، خالی از اشکال نمی‌باشد و انتقادات و پیشنهادات خوانندگان، ما را در بهبود سطح علمی و فنی کتاب، یاری خواهد کرد؛ از خوانندگان محترم درخواست می‌شود هر گونه پیشنهاد و انتقادی که در جهت بهبود و اصلاح محتویات کتاب دارند را، به نشانی الکترونیکی hosseinraja@dspri.com ارسال نمایند.

در نهایت این کتاب را در وهله اول، به ساحت مقدس چهارده معصوم علیهم السلام و در وهله دوم، به پدر و مادرم، همسرم نرگس سادات و فرزندانم، زهرا سادات و سید محمد مهدی تقدیم می‌نمایم.

سید حسین رجاء

زمستان ۱۳۹۶