

**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

۲۵ ..... فصل اول

۲۵ ..... امنیت سرورهای لینوکس

۲۶ ..... مجوزها (Permission ها)

۲۶ ..... مشاهده مجوزها

۲۷ ..... تغییر مجوزها

۲۸ ..... تنظیم مجوزهای کوتاه

۳۰ ..... مجوز برای دایرکتوری ها

۳۱ ..... مالکان و گروه ها

۳۱ ..... مجوزهای پیشرفته

۳۱ ..... مجوزهای ویژه Setuid/Setgid

۳۱ ..... مجوز ویژه Sticky Bit (بیت چسبنده)

۳۲ ..... مثال هایی از SUID، SGID و Sticky Bit

۳۴ ..... Umask

۳۴ ..... چگونه UMASK را محاسبه کنیم؟

۳۵ ..... su

۳۵ ..... su -

۳۵ ..... su -c

۳۵ ..... sudo در مقابل su

۳۶ ..... استفاده از sudo

۳۶	..... sudo	پیکربندی
۴۲	...../var/log/utmp	فایل
۴۲	...../var/log/wtmp	فایل
۴۳	...../var/log/btmp	فایل
۴۳	...../var/log/secure	فایل
۴۳	.....who و w, uptime	دستورات
۴۴	.....lastlog	دستور
۵۲	.....chage	دستور
۵۳	.....chage	گزینه‌های
۵۴	.....chage	مثال‌هایی از
۵۶	.....Unlock و Lock	کردن کاربران
۷۵	.....chattr و lsattr	دستورهای
۸۲	.....PAM	
۸۲	.....	نحوه خواندن یک فایل پیکربندی
۸۴	.....PAM	Realm‌های مدیریت
۸۵	.....PAM	کنترل‌های ماژول
۸۶	.....optional	
۸۶	.....	کنکاش در سلسه مراتب: چه اتفاقی می‌افتد؟
۸۸	.....su	جلوگیری از استفاده تمامی کاربران از
۸۸	.....wheel	اجازه استفاده از su فقط برای اعضای گروه
۸۹	.....root	غیرفعال کردن ورود مستقیم
۹۰	.....	اجرای کلمات عبور قوی
۹۱	.....root	جلوگیری از خاموش کردن سیستم توسط کاربران غیر
۹۲	.....PAM	ماژول‌های رایج
۹۴	.....PAM	راهنمای ماژول‌های
۱۰۰	.....pam_tally2	ماژول

۱۰۱.....	SSH Login های pam_tally2 برای قفل کردن
۱۰۱.....	نحوه قفل کردن و باز کردن حساب کاربری
۱۰۱.....	پارامترها
۱۰۲.....	بازیابی رمز عبور ریشه (Root Password Recovery)
۱۰۳.....	تنظیم مجدد رمز عبور ریشه
۱۰۴.....	ایمن سازی Grub Boot Loader
۱۰۶.....	ایمن سازی درون inittab
۱۰۹.....	پیگر بندی مناسب motd (Message of the day)
۱۱۲.....	دستور psacct
۱۲۱.....	لیست های کنترل دسترسی (ACL ها)
۱۲۲.....	ACL ها و Mount کردن سیستم فایل ها
۱۲۲.....	تنظیم دسترسی به ACL ها
۱۲۴.....	تنظیم ACL های پیش فرض
۱۲۴.....	بازیابی ACL ها
۱۳۲.....	امنیت و SELinux
۱۳۲.....	مکانیسم های کنترل دسترسی (ACM ها)
۱۳۲.....	کنترل دسترسی اختیاری (DAC)
۱۳۲.....	لیست های کنترل دسترسی (ACLs)
۱۳۳.....	کنترل دسترسی اجباری (Mandatory Access Control/MAC)
۱۳۳.....	کنترل دسترسی مبتنی بر نقش (RBAC)
۱۳۳.....	امنیت چند سطحی (MLS)
۱۳۳.....	امنیت چند طبقه (MCS)
۱۳۴.....	مقدمه ای بر SELinux
۱۳۴.....	بررسی اجمالی SELinux
۱۳۴.....	فرایند تصمیم گیری SELinux
۱۳۵.....	حالت های عملیاتی SELinux

۱۳۵.....	فایل‌های مربوط به SELinux
۱۳۵.....	سیستم فایل SELinux
۱۳۶.....	فایل‌های پیکربندی SELinux
۱۳۶.....	فایل پیکربندی /etc/sysconfig/selinux
۱۳۸.....	دایرکتوری /etc/selinux
۱۳۸.....	ابزارهای کاربردی SELinux
۱۳۹.....	امنیت چند طبقه (MCS)
۱۴۰.....	برنامه‌های کاربردی برای امنیت چند طبقه‌ای
۱۴۰.....	محتوای امنیتی SELinux (SELinux Security Contexts)
۱۴۰.....	شروع کار با امنیت چند طبقه‌ای
۱۴۱.....	مقایسه SELinux و تأیید هویت استاندارد کاربران لینوکس
۱۴۲.....	SELinux های Login
۱۴۳.....	پیکربندی دسته‌ها
۱۴۴.....	اختصاص دسته به کاربران
۱۴۵.....	اختصاص دادن دسته به فایل‌ها
۱۴۷.....	امنیت چند سطحی (MLS)
۱۴۸.....	مدل Bell-La Padula (BLP)
۱۴۸.....	MLS و امتیازات سیستم (System Privileges)
۱۴۹.....	سطوح امنیت، اشیاء و موضوع
۱۴۹.....	سیاست MLS
۱۵۰.....	مرور کلی سیاست SELinux
۱۵۰.....	سیاست SELinux چیست؟
۱۵۰.....	انواع در SELinux (SELinux Types)
۱۵۱.....	استفاده از قوانین خط مشی برای تعیین دسترسی انواع
۱۵۱.....	SELinux و کنترل دسترسی اجباری (MAC)
۱۵۲.....	خط مشی کجاست؟

۱۵۲.....	فایل‌های درختی باینری
۱۵۲.....	فایل‌های درخت منبع
۱۵۳.....	نقش سیاست در فرایند بوت
۱۵۴.....	کلاس‌های اشیاء و مجوزها
۱۵۵.....	سیاست هدف (Targeted Policy)
۱۵۶.....	سیاست سخت‌گیرانه (Strict Policy)
۱۵۶.....	کاربران و نقش‌ها در سیاست هدف (Targeted Policy)
۱۵۸.....	کنترل کاربر انتهایی SELinux
۱۵۹.....	انتقال و کپی کردن فایل‌ها در SELinux
۱۵۹.....	کپی کردن فایل‌ها: گزینه‌های SELinux برای cp
۱۶۰.....	انتقال دادن فایل‌ها: گزینه‌های SELinux برای mv
۱۶۰.....	بررسی امنیت یک پروسه، کاربر یا شیء فایل
۱۶۰.....	بررسی شناسه یک فرآیند
۱۶۱.....	بررسی شناسه یک کاربر
۱۶۲.....	بررسی شناسه فایل
۱۶۳.....	برچسب‌گذاری مجدد فایل یا دایرکتوری
۱۶۶.....	ایجاد آرشیوهای که محتوای امنیتی (Security Context) را حفظ می‌کنند
۱۶۹.....	کنترل مدیریت SELinux
۱۶۹.....	مشاهده وضعیت SELinux
۱۷۱.....	برچسب‌گذاری مجدد (Relabing) یک سیستم فایل
۱۷۱.....	برچسب‌گذاری مجدد (Relabing) یک سیستم فایل با استفاده از init
۱۷۱.....	برچسب‌گذاری مجدد (Relabing) یک سیستم فایل با استفاده از fixfiles
۱۷۲.....	مدیریت Home Directory های NFS
۱۷۲.....	دسترسی دادن به یک دایرکتوری یا یک درخت
۱۷۳.....	فعال یا غیرفعال سازی Enforcement
۱۷۵.....	تغییر بولین در زمان اجرا

فعال یا غیرفعال کردن SELinux	۱۷۶
تغییر حالت SELinux با استفاده از GUI	۱۷۷
تغییر سیاست	۱۷۷
مشخص کردن امنیت پرونده‌های سیستم فایل	۱۷۸
اجرای دستور در یک زمینه امنیتی خاص	۱۷۹
دستورات مفید برای اسکریپت‌ها	۱۷۹
تغییر به یک نقش متفاوت	۱۸۰
زمانی که به راه‌اندازی مجدد نیاز دارید	۱۸۰
تحلیلگر کنترل SELinux	۱۸۱
فعال کردن Kernel Auditing	۱۸۱
مشاهده Logها	۱۸۲
سفارشی کردن سیاست SELinux	۱۸۲
سیاست ماژولار	۱۸۲
لیست ماژول‌های خط مشی	۱۸۳
ساخت یک ماژول خط مشی محلی	۱۸۳
استفاده از audit2allow برای ساخت یک ماژول خط مشی محلی	۱۸۴
تجزیه و تحلیل فایل Type Enforcement (TE)	۱۸۵
بارگذاری بسته سیاست	۱۸۵
مثال‌هایی از SELinux و MAC	۱۸۶

---

## فصل دوم ۱۹۳

### امنیت سرویس‌های لینوکس ۱۹۳

غیرفعال کردن سرویس‌های غیرضروری سیستم/بستن پورت‌های باز	۱۹۴
فرمان fuser	۱۹۶
نحوه استفاده از fuser در سیستم‌های لینوکسی	۱۹۶

۱۹۷.....	یافتن فرایندی که به یک دایرکتوری دسترسی دارد
۱۹۸.....	یافتن فرایندهایی که به یک سیستم فایل دسترسی دارند
۲۰۳.....	نحوه خاتمه دادن به فرایندها و ارسال سیگنال به آنها با استفاده از fuser
۲۰۳.....	fuser و گرفتن اطلاعاتی از پروسه‌ها و سوکت‌ها
۲۰۴.....	مثال‌های بیشتر از fuser
۲۰۷.....	فرمان Isof
۲۰۷.....	مثال‌هایی از فرمان Isof
۲۰۷.....	۱. لیست تمام فایل‌های باز با فرمان Isof
۲۰۹.....	۲. فهرست فایل‌های باز شده توسط کاربری خاص
۲۰۹.....	۳. پیدا کردن فرایندهای در حال اجرا در پورت خاص
۲۰۹.....	۴. لیست فایل‌های باز IPv6 و IPv4
۲۱۰.....	۵. فهرست فایل‌های باز پورت TCP در دامنه ۱-۱۰۲۴
۲۱۰.....	۶. کاربر را با کاراکتر "^" exclude کنید
۲۱۱.....	۷. پیدا کردن اینکه افراد چه فایل‌ها و دستوراتی را استفاده می‌کنند
۲۱۱.....	۸. لیست تمام اتصالات شبکه
۲۱۲.....	۹. جستجو توسط PID
۲۱۲.....	۱۰. تمام فعالیت‌های کاربر خاص را خاتمه می‌دهد
۲۱۳.....	۱۱. لیست کردن فایل‌های باز شده در زیر یک دایرکتوری
۲۱۳.....	۱۲. لیست کردن فایل‌های باز شده توسط پروسه‌هایی که با یک رشته خاص شروع می‌شوند
۲۱۴.....	Jail یا chroot کردن DNS Server
۲۲۶.....	بهترین روش‌های ایمن سازی سرور OpenSSH
۲۳۵.....	فایل‌های known_hosts و authorized keys در SSH
۲۳۶.....	احراز هویت بدون ارائه گذرواژه در SSH (SSH PasswordLess Authentication)
۲۳۹.....	Access Control در Apache
۲۳۹.....	کنترل دسترسی توسط میزبان
۲۴۰.....	کنترل دسترسی با متغیرهای دلخواه



۲۴۰	.....mod_rewrite کنترل دسترسی با
۲۴۰	.....mod_access_compat ماژول آپاچی
۲۴۱	.....Allow Directive
۲۴۳	.....Deny Directive
۲۴۴	.....Order Directive
۲۴۶	.....Satisfy Directive
۲۴۷	.....<Limit> Directive
۲۴۸	.....<LimitExcept> Directive
۲۴۹	..... Apache در Access Control مثال‌های کاربردی از
۲۶۷	..... Apache در Authorization و Authentication
۲۶۸	..... ماژول‌ها و Directive‌های مرتبط
۲۶۹	..... معرفی
۲۶۹	.....پیش‌نیازها
۲۷۰	.....محافظةت از دایرکتوری درون وب سرور توسط رمز عبور
۲۷۱	.....اجازه دادن به بیش از یک نفر برای دسترسی
۲۷۲	.....جایگزین‌هایی برای ذخیره‌سازی رمز
۲۷۳	.....استفاده از ارائه‌دهندگان متعدد
۲۷۴	.....استفاده از ارائه‌دهندگان مجوز (authorization providers) برای کنترل دسترسی
۲۷۵	..... Apache در Authorization و Authentication مثال کاربردی از
۲۸۲	..... Apache برای Self-Signed SSL ایجاد گواهی‌نامه‌ها و کلیدهای
۲۸۲	..... Apache برای HTTPS فعال کردن
۲۸۲	..... Apache برای SSL ایجاد گواهی‌نامه
۲۹۴	.....امنیت ایمیل سرور
۲۹۴	.....DKIM و DomainKeys پی‌کربندی
۳۱۲	.....Selective Relay و Open Relay پی‌کربندی ممانعت از
۳۱۴	.....SMTP Auth پی‌کربندی

۳۳۲.....	پیکربندی Courier Auth، Courier IMAP و Coureir POP
۳۴۴.....	پیکربندی Courier POP3 SSL
۳۶۳.....	پیکربندی Courier IMAP SSL
۳۷۱.....	پیکربندی SMTPSD یا ایمن کردن SMTP (SMTP همراه با TLS / SSL)
۳۹۲.....	استفاده از SSL در SquirrelMail
۳۹۵.....	مقابله با ویروس در سرور ایمیل
۴۲۸.....	مقابله با Spam در سرور ایمیل
۴۴۹.....	نصب و پیکربندی Mailscanner
۴۶۰.....	نصب و پیکربندی maildrop
۴۷۴.....	ایمن‌سازی NFS
۴۷۴.....	دسترسی میزبان
۴۷۵.....	استفاده از NFSv2 یا NFSv3
۴۷۵.....	استفاده از NFSv4
۴۷۶.....	مجوزهای فایل
۴۷۶.....	پیکربندی Firewal برای NFS
۴۸۰.....	مدهای امنیتی در سرویس Samba
۴۹۱.....	چرا باید از پروکسی استفاده نماییم؟
۴۹۱.....	مزایای پروکسی معمولی (Regular Proxy)
۴۹۱.....	مزایای پروکسی معکوس (Reverse Proxy)
۴۹۱.....	اسکوئید (Squid)
۴۹۱.....	نصب و پیکربندی Squid
۵۰۱.....	پیکربندی squid proxy به عنوان فیلترینگ وب
۵۰۱.....	محدود کردن دسترسی به وبسایت‌های خاص
۵۰۴.....	محدود کردن دسترسی به کلمات کلیدی خاص
۵۰۷.....	محدود کردن دسترسی به آدرس‌های IP خاص
۵۱۰.....	محدود کردن دسترسی به آدرس‌های IP خاص

۵۱۱.....	تغییر شماره پورت پروکسی Squid
۵۱۱.....	محدود کردن حجم دانلود توسط Squid
۵۱۲.....	پیکربندی Squid به عنوان Transparent Proxy

---

## فصل سوم..... ۵۱۵

### امنیت شبکه‌های لینوکس..... ۵۱۵

---

۵۱۶.....	فایروال در لینوکس
۵۱۶.....	Iptables چیست؟
۵۱۷.....	دانلود و نصب بسته Iptables
۵۱۷.....	مدیریت سرور iptables
۵۱۷.....	پردازش بسته در iptables
۵۱۹.....	پردازش برای بسته‌های هدایت شده توسط فایروال
۵۲۱.....	مقاصد و جهش‌ها (Targets And Jumps)
۵۲۴.....	عملیات سوئیچ‌های مهم Iptables
۵۲۴.....	جدول معیارهای رایج مطابقت در Iptables
۵۲۵.....	جدول شرایط مطابقت مشترک TCP و UDP
۵۲۶.....	جدول شرایط مطابقت مشترک ICMP (Ping)
۵۲۷.....	جدول شرایط مطابقت اضافه
۵۲۸.....	استفاده از زنجیره‌های تعریف شده توسط کاربر
۵۲۹.....	ذخیره و بازگرداندن اسکریپت iptables
۵۳۱.....	بازیابی از یک اسکریپت از دست رفته
۵۳۲.....	بارگذاری ماژول‌های هسته مورد نیاز توسط iptables
۵۳۳.....	نمونه اسکریپت iptables
۵۳۳.....	دفاع ابتدایی از سیستم عامل
۵۳۶.....	مقدار دهی اولیه iptables به صورت پیشرفته

۵۳۸.....	اجازه دسترسی DNS به فایروال شما
۵۳۹.....	اجازه دسترسی WWW و SSH به فایروال شما
۵۴۰.....	دادن اجازه دسترسی به فایروال برای دسترسی به اینترنت
۵۴۱.....	اجازه دسترسی به شبکه خانگی خود برای دسترسی به فایروال
۵۴۱.....	Masquerading (NAT چند به یک)
۵۴۴.....	NAT از نوع Port Forwarding (DHCP DSL)
۵۴۶.....	NAT استاتیک
۵۵۰.....	عیب‌یابی iptables
۵۵۱.....	بررسی LOG های فایروال
۵۵۲.....	iptables شروع نمی‌شود!
۵۵۳.....	مدیریت و پیکربندی سیستم حسابرسی لینوکس (Auditing)
۵۵۳.....	پیش‌نیازها
۵۵۴.....	بررسی نصب Audit
۵۵۴.....	پیکربندی Audit
۵۵۸.....	جستجو در Log های Audit رویدادها
۵۵۹.....	ایجاد گزارش‌های Audit
۵۶۱.....	تجزیه و تحلیل یک فرآیند با استفاده از autrace
۵۶۲.....	Port Scanner قدرتمند nmap
۵۶۳.....	مثال‌هایی از nmap
۵۹۱.....	کارت راهنمای nmap
۵۹۱.....	مشخصات هدف
۵۹۱.....	کشف میزبان
۵۹۲.....	تکنیک‌های اسکن
۵۹۳.....	مشخصات پورت و ترتیب اسکن
۵۹۳.....	تشخیص نسخه سرویس
۵۹۴.....	اسکن نوع اسکریپت

۵۹۴.....	تشخیص OS
۵۹۵.....	زمان‌بندی و کارایی
۵۹۶.....	IDS و Spoofing فایروال
۵۹۷.....	Nmap گزینه‌های خروجی
۵۹۸.....	Nmap سایر گزینه‌های
۵۹۹.....	پیکربندی iptables برای ممانعت از حملات Nmap
۶۰۶.....	Packet Capturing و تحلیل آن توسط tcpdump

---

۶۳۹.....	مراجع و منابع
----------	---------------

---

## خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی است که بتواند خواسته‌هایی 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.

گسترده‌گی 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 پُر بار، 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.

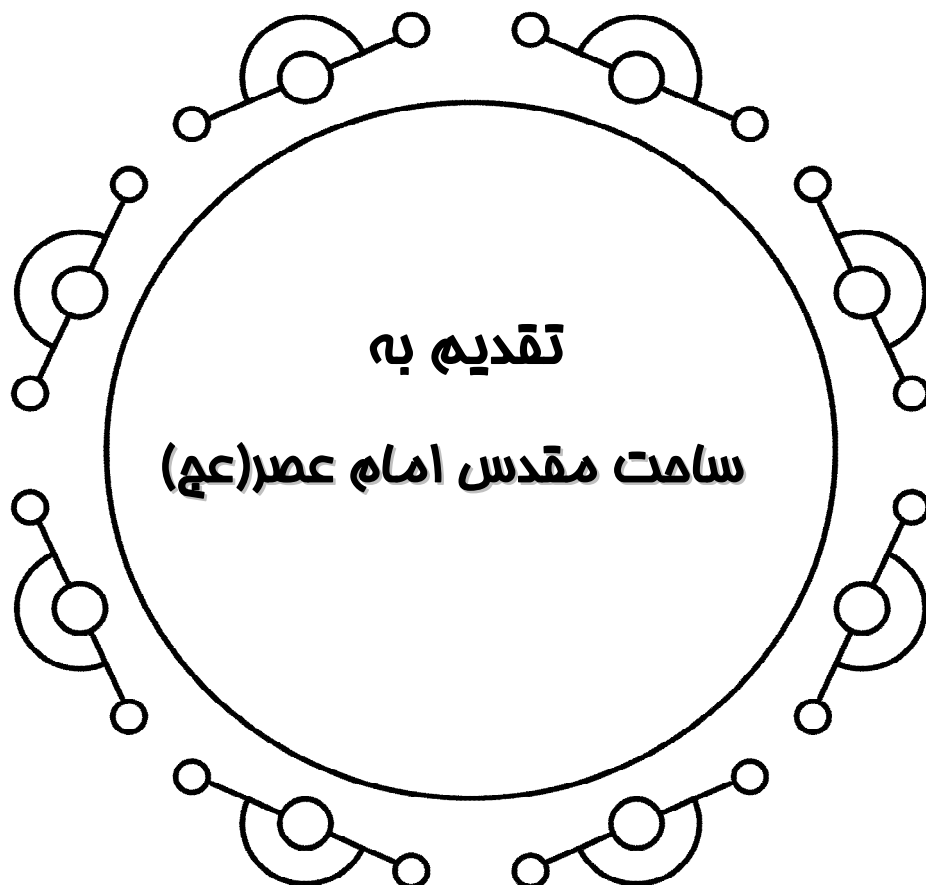
### کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس [dibagaran.mft.info](mailto: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](mailto:Publishing@mftmail.com)



## پیشگفتار

در عصر اطلاعات، بسیاری از تراکنش‌ها چه مالی و چه غیرمالی، به صورت 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 به صورت 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 بین‌المللی 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
- su و sudo
- فایل /var/log/utmp
- فایل /var/log/wtmp
- فایل /var/log/btmp
- فایل /var/log/secure
- دستورات w, uptime و who
- دستور lastlog
- دستور chage
- Lock و Unlock کردن کاربران
- دستوره‌های lsattr و chattr
- PAM
- Realm‌های مدیریت PAM
- کنترل‌های ماژول PAM
- ماژول‌های پشته



- ماژول‌های PAM رایج
- مثال‌هایی از PAM
- pam\_tally2
- بازبینی 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
- SELinux های Login
- 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 (Relabing) یک سیستم فایل

- مدیریت Home Directory های 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 (TE) Type Enforcement
- 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 سوکت‌ها
- 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 PasswordLess Authentication) SSH
- Apache در Access Control
- 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
- Apache Authorization, Authentication در
- 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 (Apache و HTTPS)
- 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)
- NAT از نوع (DHCP DSL) Port Forwarding
- NAT استاتیک
- عیب‌یابی iptables
- بررسی LOG های فایروال
- مدیریت و پیکربندی Audit
- جستجو در Log های Audit رویدادها
- ایجاد گزارش‌های Audit
- تجزیه و تحلیل یک فرآیند با استفاده از atrace

- nmap Port Scanner قدرتمند
- 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 tcpdump
- ...

مخاطبین اصلی کتاب، متخصصین لینوکس، کارشناسان امنیت، مدیران شبکه، متخصصین حوزه نرم‌افزارهای متن باز، برنامه نویسان، متقاضیان و شرکت‌کنندگان در آزمون‌های بین‌المللی 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 و 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 بین‌المللی Linux LPIC-3 305 (Mail (Based on Qmail MTA)، انتشارات کانون نشر علوم، ۱۳۹۶
- دستورات، کدها، مثال‌ها و سناریوهای عملی اجرا شده در مدرک بین‌المللی RHCSA، انتشارات کانون نشر علوم، ۱۳۹۶
- دستورات، کدها، مثال‌ها و سناریوهای عملی اجرا شده در مدرک بین‌المللی 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](mailto: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