

به نام خدا

۱۵۹۹۹۹۹
۵۹/۹۹



امنیت در سرورها، سرویس ها و شبکه های لینوکس

(پوشش دهنده مدارک امنیت لینوکس RHEL413 و EX413 از RedHat)

مؤلف

مهندس سید حسین رجاء

هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی
ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق
مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

امنیت در سرورها، سرویس ها و شبکه های لینوکس

(پوشش دهنده مدارک امنیت RH413 و EX413 از RedHat)

سرشناسه: رجاء، سید حسین. ۱۳۶۲-

عنوان و نام پدید آور: امنیت در سرورها، سرویس ها و شبکه
های لینوکس (پوشش دهنده مدارک امنیت لینوکس RH413
و EX413 از REDHAT) مؤلف: سید حسین رجاء

مشخصات نشر: تهران - دیباگران تهران - ۱۳۹۶

مشخصات ظاهری: ۶۴۲ ص. مصور.

شابک: ۹۷۸-۶۰۰-۱۲۴-۷۶۸-۲

وضعیت فهرست نویسی: فیا

دداشت: کتابنامه: ص: ۶۳۹.

موضوع: سیستم عامل لینوکس

موضوع: امنیت

موضوع: سیستم عامل (کامپیوتر) - تدابیر ایمنی

موضوع: Operating systems (computers) - security measures

موضوع: شبکه های کامپیوتری - تدابیر ایمنی

موضوع: computer networks - security measures

موضوع: کامپیوترها - ایمنی اطلاعات

موضوع: Computer security

رده بندی کنگره: ۳۳۵ ۱۳۹۶ ر ۹۴ س ۷۶/۷۶ QA

رده بندی دیویی: ۰۵/۴۳۲

شماره کتابشناسی ملی: ۵۰۳۰۸۲۶

مؤلف: مهین سید حسین رجاء

ناشر: مؤسسه فرهنگ هنری دیباگران تهران

صفحه آرای: شبنم هاشم

طرح روی جلد: دریا علی فردوسی

چاپ: دانشجو

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۶

تیراژ: ۱۰۰ جلد

قیمت: ۳۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۷۶۸-۲

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، رویروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

کد پستی: ۱۳۱۴۹۸۳۱۸۵

فروشگاههای اینترنتی:

www.mftbook.ir

www.mftshop.com

نشانی تلگرام: @mftbook

نشانی اینستاگرام: Dibagaran_publishing

پست الکترونیکی: bookmarket@mftmail.com

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
۴۲		/var/log/btmp	فایل
۴۲		/var/log/secure	فایل
۴۲		who و w, uptime	دستورات
۴۴		lastlog	دستور
۵۲		chage	دسته
۵۳		chage	گزینه‌های
۵۴		chage	مثال‌هایی از
۵۶		Lock و Unlock	کلیدهای کاربر
۷۵		chattr و lsattr	دستورهای
۸۲		PAM	
۸۲			نحوه خواندن یک فایل پیکربندی
۸۴		PAM	Realmd مدیریت
۸۵		PAM	کنترل‌های مازول
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	رایج
۹۴		PAM	راهنمای مازول‌های
۱۰۰		pam_tally2	مازول

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

۱۳۵	فایل‌های مربوط به SELinux
۱۳۵	سیستم فایل SELinux
۱۳۶	فایل‌های پیکربندی SELinux
۱۳۶	فایل پیکربندی <code>/etc/sysconfig/selinux</code>
۱۳۸	دایرکتوری <code>/etc/selinux</code>
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 با سیستم‌های استاندارد کاربران لینوکس
۱۴۲	Login‌های SELinux
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 با اِی‌فایل
۱۶۰	بررسی شناسه یک فرآیند
۱۶۱	بررسی شناسه یک کاربر
۱۶۲	بررسی شناسه فایل
۱۶۳	برچسب‌گذاری مجدد فایل یا دایرکتوری
۱۶۶	ایجاد آرشیهایی 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

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

۱۹۳..... فصل دوم

۱۹۳..... امنیت سرویس‌های لینوکس

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

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

۲۴۰.....	کنترل دسترسی با mod_rewrite
۲۴۰.....	ماژول آپاچی mod_access_compat
۲۴۱.....	Allow Directive
۲۴۳.....	Deny Directive
۲۴۴.....	Order Directive
۲۴۶.....	Satisfy Directive
۲۴۷.....	<Limit> Directive
۲۴۸.....	<LimitExcept> Directive
۲۴۹.....	مثال کاربردی از Access Control در Apache
۲۶۷.....	Authentication و Authorization در Apache
۲۶۸.....	ماژول‌ها و Directive های مرتبط
۲۶۹.....	معرفی
۲۶۹.....	پیش‌نیازها
۲۷۰.....	محافظت 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.....	مثال کاربردی از Authentication و Authorization در Apache
۲۸۲.....	ایجاد گواهینامه‌ها و کلیدهای Self-Signed SSL برای Apache
۲۸۲.....	فعال کردن HTTPS برای Apache
۲۸۲.....	ایجاد گواهینامه SSL برای Apache
۲۹۴.....	امنیت ایمیل سرور
۲۹۴.....	پیکربندی DKIM و DomainKeys
۳۱۲.....	ممانعت از Open Relay و پیکربندی Selective Relay
۳۱۴.....	پیکربندی SMTP Auth

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

۵۱۱	تغییر شماره پورت پروکسی Squid
۵۱۱	محدود کردن حجم دانلود توسط Squid
۵۱۲	پیکربندی Squid به عنوان Transparent Proxy
۵۱۵	فصل سوم
۵۱۵	امنیت شبکه‌های لینوکس
۵۱۶	فایروال 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	بازبایی 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

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

۵۹۴.....تشخیص OS

۵۹۵.....زمان‌بندی و کارایی

۵۹۶.....IDS و Evasion فایروال

۵۹۷.....Nmap گزینه‌های خروجی

۵۹۸.....Nmap سایر گزینه‌های

۵۹۹.....Nmap پیکربندی iptables برای ممانعت از حملات

۶۰۶.....Packet Capturing و تحلیل آن توسط دستور tcpdump

۶۳۹.....مراجع و منابع

www.ketaboo.ir

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 هزینه‌های 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 اختصارشان مراد 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 who و w و uptime
- دستور lastlog
- دستور chage
- Lock و Unlock کردن کاربران
- دستورهای lsattr و chattr
- PAM
- Realm‌های مدیریت PAM
- کنترل‌های مازول PAM
- مازول‌های پشته

- مازول‌های PAM رایج
- مثال‌هایی از PAM
- pam_tally2 مازول
- باز یابی 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 سطوح (MLS)
- امنیت چندقدر (MLS)
- 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 (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
- تهیه و تحلیل فایل Type Enforcement (TE)
- ایجاد بسته سیاست
- مثال‌هایی از SELinux و MAC
- ...

۲- امنیت سرویس‌های لینوکس

- غیرفعال کردن سرویس‌های غیر ضروری سیستم‌ایستن پورت‌های باز
- فرمان fuser
- یافتن فرایندی که به یک دایرکتوری دسترسی دارد
- نحوه خاتمه دادن به فرایندها و ارسال سیگنال آن‌ها با استفاده از fuser
- fuser و گرفتن اطلاعاتی از پروسه‌ها و سیستم‌ها
- پیدا کردن فرایندهای 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
- 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
- این گواهینامه ها و کلیدهای Self-Signed SSL برای Apache
- فعال کردن HTTPS برای Apache
- ایمن‌سازی وب سرور توسط SSL/TLS (Apache, HTTPS)
- امنیت ایمیل سرور
- پیکربندی DKIM و Domain Keys
- ممنوعیت از Open Relay و پیکربندی Selective Relay
- پیکربندی SMTP Auth
- پیکربندی Courier Auth, Courier IMAP, Courier POP
- پیکربندی SSL Courier POP3
- پیکربندی Courier IMAP SSL
- پیکربندی SMTPSD یا ایمن کردن SMTP (SSL / TLS همراه)
- 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)
- اسکویید (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
- راه‌اندازی بسته در iptables
- مت‌م‌د و جهش‌ها (Targets And Jumps)
- عملیات سیج‌ها در Iptables
- معیارهای رایج امنیت در Iptables
- شرایط مطابقت مشهور TCP و UDP
- شرایط مطابقت مشهور ICMP (Ping)
- استفاده از زنجیره‌های ترتیب شده توسط کاربر
- ذخیره و بازگرداندن اسکریپت Iptables
- بازبینی 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 Port Forwarding (DHCP DSL)
- 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 autrace

- 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
- IDS و Evasion، Spoofing و فایروال
- 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، معلمان و شرکت‌کنندگان در آزمون‌های بین‌المللی Red Hat Red Hat Certificate of Expertise in Security and Server Hardening (RH413) و Security and Server Hardening Exam (EX413)، دانشجویان رشته نرم‌افزار و فناوری اطلاعات و تمامی افراد علاقه‌مند به حوزه امنیت لینوکس و مباحث پیرامون آن می‌باشند.

سید حسین رجاء کارشناس ارشد فناوری اطلاعات (T) می‌باشد که حدوداً ۱۸ سال فعالیت در زمینه‌های مختلف IT، من جمله تدریس، برنامه‌نویسی، شبکه، امنیت شبکه، ایجاد داده، مجازی سازی، سیسکو، لینوکس، ویندوز و ایمیل سرور را تجربه کرده است. از جمله مدارک علمی ایشان می‌توان به CCIE، CCIE R&S، 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 102 Linux LPIC-1، مؤلف سید حسین رجاء، گروه آموزشی رایکا، ۱۳۹۵
- آموزش تصویری 201 Linux LPIC-2، مؤلف سید حسین رجاء، گروه آموزشی رایکا، ۱۳۹۵
- آموزش تصویری 202 Linux LPIC-2، 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 با 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 (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 (201,202) Linux LPIC-2. 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@d-pri.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. همسر، نرگس سادات و فرزندانم، زهرا سادات و سید محمد مهدی تقدیم می‌نمایم.

سید حسین رجاء

زمستان ۱۳۹۶