

# امنیت در

سرورها، سرویس‌ها و شبکه‌های

# لینوکس

**RH413** (پوشش دهنده مدارک امنیت لینوکس

و **EX413** از RedHat)

(Red Hat Security and Server Hardening (RH413)  
and Red Hat Certificate of Expertise in Security  
and Server Hardening Exam (EX413))

مؤلف: مهندس سید حسین رجاء



## فهرست مطالب

پیشگفتار.....	۱۷
فصل اول.....	۲۹
امنیت سرورهای لینوکس.....	۲۹
مجوزها (Permissionها).....	۲۹
مشاهده مجوزها.....	۳۰
تغییر مجوزها.....	۳۱
تنظیم مجوزهای کوتاه.....	۳۳
مجوز برای دایرکتوری‌ها.....	۳۶
مالکان و گروه‌ها.....	۳۷
مجوزهای پیشرفته.....	۳۸
مجوزهای ویژه Setuid/Setgid.....	۳۸
مجوز ویژه Sticky Bit (بیت چسبنده).....	۳۹
مثال‌هایی از SUID، SGID و Sticky Bit.....	۳۹
Umask.....	۴۳
چگونه UMASK را محاسبه کنیم؟.....	۴۳
su.....	۴۴
su -.....	۴۵
su -c.....	۴۵
sudo در مقابل su.....	۴۵

۴۷	استفاده از sudo
۴۸	پیکربندی sudo
۵۷	فایل /var/log/utmp
۵۸	فایل /var/log/wtmp
۵۸	فایل /var/log/btmp
۵۹	فایل /var/log/secure
۵۹	دستورات w و uptime، who
۶۱	دستور lastlog
۷۵	دستور chage
۷۵	گزینه‌های chage
۷۷	مثال‌هایی از chage
۸۰	Lock و Unlock کردن کاربران
۱۰۶	دستورهای Isattr و chatr
۱۱۶	PAM
۱۱۶	نحوه خواندن یک فایل پیکربندی
۱۱۹	Realm‌های مدیریت PAM
۱۲۱	کنترل‌های ماژول PAM
۱۲۲	ماژول‌های پشت‌پشته
۱۲۳	کنکاش در سلسه مراتب: چه اتفاقی می‌افتد؟
۱۲۵	هر کاربر را بدون ارائه رمز عبور، به root، su دهید.
۱۲۶	جلوگیری از استفاده تمامی کاربران از su
۱۲۶	اجازه استفاده از su فقط برای اعضای گروه wheel
۱۲۷	غیرفعال کردن ورود مستقیم root
۱۲۸	اجرای کلمات عبور قوی
۱۳۰	جلوگیری از خاموش کردن سیستم توسط کاربران غیر root
۱۳۱	ماژول‌های PAM رایج
۱۳۶	راهنمای ماژول‌های PAM
۱۴۷	ماژول pam_tally2

۱۴۸	.....SSH Login های pam_tally2 برای قفل کردن
۱۴۸	..... نحوه قفل کردن و باز کردن حساب کاربری
۱۴۸	..... پارامترها
۱۵۰	.....(Root Password Recovery) ریشه رمز عبور ریشه
۱۵۰	.....تنظیم مجدد رمز عبور ریشه
۱۵۲	.....Grub Boot Loader ایمن سازی
۱۵۵	.....inittab ایمن سازی درون
۱۵۸	.....(Message of the day) motd پیکربندی مناسب
۱۶۳	.....psacct دستور
۱۷۷	.....لیست های کنترل دسترسی (ACLها)
۱۷۸	.....ACL ها و Mount کردن سیستم فایل ها
۱۷۹	.....ACL ها و NFS
۱۷۹	.....تنظیم دسترسی به ACL ها
۱۸۱	.....تنظیم ACL های پیش فرض
۱۸۲	.....بازیابی ACL ها
۱۹۳	.....مکانیسم های کنترل دسترسی (ACM ها)
۱۹۳	.....کنترل دسترسی اختیاری (DAC)
۱۹۴	.....لیست های کنترل دسترسی (ACLs)
۱۹۴	.....کنترل دسترسی اجباری (Mandatory Access Control/MAC)
۱۹۴	.....کنترل دسترسی مبتنی بر نقش (RBAC)
۱۹۵	.....امنیت چند سطحی (MLS)
۱۹۵	.....امنیت چند طبقه (MCS)
۱۹۵	.....مقدمه ای بر SELinux
۱۹۶	.....بررسی اجمالی SELinux
۱۹۶	.....فرایند تصمیم گیری SELinux
۱۹۷	.....حالت های عملیاتی SELinux
۱۹۸	.....فایل های مربوط به SELinux
۱۹۸	.....سیستم فایل SELinux

۱۹۹	فایل‌های پیکربندی SELinux
۱۹۹	فایل پیکربندی /etc/sysconfig/selinux
۲۰۲	دایرکتوری /etc/selinux
۲۰۲	ابزارهای کاربردی SELinux
۲۰۴	امنیت چند طبقه (MCS)
۲۰۵	برنامه‌های کاربردی برای امنیت چند طبقه‌ای
۲۰۵	محتوای امنیتی SELinux (SELinux Security Contexts)
۲۰۶	شروع کار با امنیت چند طبقه‌ای
۲۰۷	مقایسه SELinux و تأیید هویت استاندارد کاربران لینوکس
۲۰۸	Login‌های SELinux
۲۱۰	پیکربندی دسته‌ها
۲۱۱	اختصاص دسته به کاربران
۲۱۴	اختصاص دادن دسته به فایل‌ها
۲۱۶	امنیت چند سطحی (MLS)
۲۱۷	مدل Bell-La Padula (BLP)
۲۱۹	MLS و امتیازات سیستم (System Privileges)
۲۱۹	سطوح امنیت، اشیاء و موضوع
۲۲۰	سیاست MLS
۲۲۱	مرور کلی سیاست SELinux
۲۲۱	سیاست SELinux چیست؟
۲۲۱	انواع در SELinux (SELinux Types)
۲۲۲	استفاده از قوانین خط مشی برای تعیین دسترسی انواع
۲۲۳	SELinux و کنترل دسترسی اجباری (MAC)
۲۲۴	خط مشی کجاست؟
۲۲۴	فایل‌های درختی باینری
۲۲۵	فایل‌های درخت منبع
۲۲۶	نقش سیاست در فرایند بوت
۲۲۸	کلاس‌های اشیاء و مجوزها

سیاست هدف (Targeted Policy)	۲۲۹
سیاست سخت‌گیرانه (Strict Policy)	۲۳۰
کاربران و نقش‌ها در سیاست هدف (Targeted Policy)	۲۳۰
کنترل کاربر انتهایی SELinux	۲۳۴
انتقال و کپی کردن فایل‌ها در SELinux	۲۳۵
کپی کردن فایل‌ها: گزینه‌های SELinux برای cp	۲۳۵
انتقال دادن فایل‌ها: گزینه‌های SELinux برای mv	۲۳۶
بررسی امنیت یک پروسه، کاربر یا شیء فایل	۲۳۸
بررسی شناسه یک فرآیند	۲۳۸
بررسی شناسه یک کاربر	۲۳۹
بررسی شناسه فایل	۲۴۰
برچسب‌گذاری مجدد فایل یا دایرکتوری	۲۴۱
ایجاد آرشیوهایی که محتوای امنیتی (Security Context) را حفظ می‌کنند	۲۴۸
کنترل مدیریت SELinux	۲۵۱
مشاهده وضعیت SELinux	۲۵۲
برچسب‌گذاری مجدد (Relabing) یک سیستم فایل	۲۵۴
برچسب‌گذاری مجدد (Relabing) یک سیستم فایل با استفاده از init	۲۵۵
برچسب‌گذاری مجدد (Relabing) یک سیستم فایل با استفاده از fixfiles	۲۵۵
مدیریت Home Directory های NFS	۲۵۶
دسترسی دادن به یک دایرکتوری یا یک درخت	۲۵۷
فعال یا غیرفعال سازی Enforcement	۲۵۸
تغییر بولین در زمان اجرا	۲۶۰
فعال یا غیرفعال کردن SELinux	۲۶۲
تغییر حالت SELinux با استفاده از GUI	۲۶۴
تغییر سیاست	۲۶۴

۲۶۶	مشخص کردن امنیت پرونده‌های سیستم فایل
۲۶۷	اجرای دستور در یک زمینه امنیتی خاص
۲۶۸	دستورات مفید برای اسکریپت‌ها
۲۶۹	تغییر به یک نقش متفاوت
۲۶۹	زمانی که به راه‌اندازی مجدد نیاز دارید
۲۷۰	تحلیلگر کنترل SELinux
۲۷۰	فعال کردن Kernel Auditing
۲۷۲	مشاهده Logها
۲۷۲	سفارشی کردن سیاست SELinux
۲۷۳	سیاست ماژولار
۲۷۳	لیست ماژول‌های خط مشی
۲۷۴	ساخت یک ماژول خط مشی محلی
۲۷۵	استفاده از audit2allow برای ساخت یک ماژول خط مشی محلی
۲۷۶	تجزیه و تحلیل فایل Type Enforcement (TE)
۲۷۷	بارگذاری بسته سیاست
۲۷۸	مثال‌هایی از SELinux و MAC

## ۲۸۹ فصل دوم

۲۸۹	امنیت سرویس‌های لینوکس
۲۸۹	غیرفعال کردن سرویس‌های غیرضروری سیستم/بستن پورت‌های باز
۲۹۳	فرمان fuser
۲۹۳	نحوه استفاده از fuser در سیستم‌های لینوکسی
۲۹۴	یافتن فرآیندی که به یک دایرکتوری دسترسی دارد
۲۹۶	یافتن فرآیندهایی که به یک سیستم فایل دسترسی دارند نحوه خاتمه دادن به فرآیندها و ارسال سیگنال به آنها با استفاده از
۳۰۳	fuser
۳۰۴	fuser و گرفتن اطلاعاتی از پروسه‌ها و سوکت‌ها
۳۰۴	مثال‌های بیشتر از fuser



فرمان Isuf.....	۳۰۸
مثال‌هایی از فرمان Isuf.....	۳۰۹
۱. لیست تمام فایل‌های باز با فرمان Isuf.....	۳۰۹
۲. فهرست فایل‌های باز شده توسط کاربری خاص.....	۳۱۱
۳. پیدا کردن فرآیندهای در حال اجرا در پورت خاص.....	۳۱۲
۴. لیست فایل‌های باز IPv4 و IPv6.....	۳۱۳
۵. فهرست فایل‌های باز پورت TCP در دامنه ۱-۱۰۲۴.....	۳۱۴
۶. کاربر را با کاراکتر "^^" exclude کنید.....	۳۱۵
۷. پیدا کردن اینکه افراد چه فایل‌ها و دستوراتی را استفاده می‌کنند.....	۳۱۶
۸. لیست تمام اتصالات شبکه.....	۳۱۷
۹. جستجو توسط PID.....	۳۱۸
۱۰. تمام فعالیت‌های کاربر خاص را خاتمه می‌دهد.....	۳۱۹
۱۱. لیست کردن فایل‌های باز شده در زیر یک دایرکتوری.....	۳۱۹
۱۲. لیست کردن فایل‌های باز شده توسط پروسه‌هایی که با یک رشته خاص شروع می‌شوند.....	۳۲۰
Jail یا chroot کردن DNS Server.....	۳۲۲
بهترین روش‌های ایمن سازی سرور OpenSSH.....	۳۴۰
فایل‌های known_hosts و authorized keys در SSH.....	۳۵۴
احراز هویت بدون ارائه گذرواژه در SSH ( PasswordLess ).....	۳۵۶
Authentication.....	۳۵۶
Access Control در Apache.....	۳۶۱
کنترل دسترسی توسط میزبان.....	۳۶۱
کنترل دسترسی با متغیرهای دلخواه.....	۳۶۲
کنترل دسترسی با mod_rewrite.....	۳۶۳
ماژول آپاچی mod_access_compat.....	۳۶۴
Allow Directive.....	۳۶۵
Deny Directive.....	۳۶۸
Order Directive.....	۳۶۹

۳۷۲	.....Satisfy Directive
۳۷۴	.....<Limit> Directive
۳۷۵	.....<LimitExcept> Directive
۳۷۶	.....مثال‌های کاربردی از Access Control در Apache
۴۰۵	.....Apache در Authentication و Authorization
۴۰۵	.....ماژول‌ها و Directive‌های مرتبط
۴۰۶	.....معرفی
۴۰۷	.....پیش‌نیازها
۴۰۸	.....محافظت از دایرکتوری درون وب سرور توسط رمز عبور
۴۱۱	.....اجازه دادن به بیش از یک نفر برای دسترسی
۴۱۲	.....جایگزین‌هایی برای ذخیره‌سازی رمز
۴۱۳	.....استفاده از ارائه‌دهندگان متعدد
	.....استفاده از ارائه‌دهندگان مجوز (authorization providers) برای کنترل
۴۱۵	.....دسترسی
۴۱۷	.....مثال کاربردی از Authentication و Authorization در Apache
۴۲۷	.....ایجاد گواهینامه‌ها و کلیدهای Self-Signed SSL برای Apache
۴۲۷	.....فعال کردن HTTPS برای Apache
۴۲۷	.....ایجاد گواهینامه SSL برای Apache
۴۴۵	.....امنیت ایمیل سرور
۴۴۵	.....پیکربندی DomainKeys و DKIM
۴۷۲	.....ممانعت از Open Relay و پیکربندی Selective Relay
۴۷۵	.....پیکربندی SMTP Auth
۵۰۲	.....پیکربندی Courier Auth، Courier IMAP و Coureir POP
۵۱۸	.....پیکربندی Courier POP3 SSL
۵۴۹	.....پیکربندی Courier IMAP SSL
	.....پیکربندی SMTPSD یا ایمن کردن SMTP (SMTP همراه با TLS / SSL)
۵۶۲	.....
۵۹۳	.....استفاده از SSL در SquirrelMail

۵۹۶.....	مقابله با ویروس در سرور ایمیل.....
۶۴۲.....	مقابله با Spam در سرور ایمیل.....
۶۷۳.....	نصب و پیکربندی MailsScanner.....
۶۸۹.....	نصب و پیکربندی maildrop.....
۷۰۸.....	ایمن‌سازی NFS.....
۷۰۸.....	دسترسی میزبان.....
۷۰۸.....	استفاده از NFSv2 یا NFSv3.....
۷۰۹.....	استفاده از NFSv4.....
۷۱۰.....	مجوزهای فایل.....
۷۱۱.....	پیکربندی Firewal برای NFS.....
۷۱۷.....	مدهای امنیتی در سرویس Samba.....
۷۳۱.....	چرا باید از پروکسی استفاده نماییم؟.....
۷۳۲.....	مزایای پروکسی معمولی (Regular Proxy).....
۷۳۲.....	مزایای پروکسی معکوس (Reverse Proxy).....
۷۳۲.....	اسکوئید (Squid).....
۷۳۳.....	نصب و پیکربندی Squid.....
۷۴۶.....	پیکربندی squid proxy به عنوان فیلتر وب.....
۷۴۶.....	محدود کردن دسترسی به وبسایت‌های خاص.....
۷۵۰.....	محدود کردن دسترسی به کلمات کلیدی خاص.....
۷۵۴.....	محدود کردن دسترسی به آدرس‌های IP خاص.....
۷۵۹.....	محدود کردن دسترسی به آدرس‌های IP خاص.....
۷۶۰.....	تغییر شماره پورت پروکسی Squid.....
۷۶۰.....	محدود کردن حجم دانلود توسط Squid.....
۷۶۱.....	پیکربندی Squid به عنوان Transparent Proxy.....
<b>۷۶۵.....</b>	<b>فصل سوم.....</b>
<b>۷۶۵.....</b>	<b>امنیت شبکه‌های لینوکس.....</b>
۷۶۵.....	فایروال در لینوکس.....

۷۶۶	.....Iptables چیست؟
۷۶۷	.....Iptables نصب بسته
۷۶۷	.....iptables مدیریت سرور
۷۶۸	.....iptables پردازش بسته در
۷۶۹	.....پردازش برای بسته‌های هدایت شده توسط فایروال
۷۷۴	.....مقاصد و جهش‌ها (Targets And Jumps)
۷۷۷	.....Iptables عملیات سوئیچ‌های مهم
۷۷۸	.....Iptables جدول معیارهای رایج مطابقت در
۷۷۹	.....UDP و TCP جدول شرایط مطابقت مشترک
۷۸۱	.....ICMP (Ping) جدول شرایط مطابقت مشترک
۷۸۲	.....جدول شرایط مطابقت اضافه
۷۸۴	.....استفاده از زنجیره‌های تعریف شده توسط کاربر
۷۸۶	.....iptables ذخیره و بازگرداندن اسکریپت
۷۸۹	.....بازیابی از یک اسکریپت از دست رفته
۷۹۱	.....iptables بارگذاری ماژول‌های هسته مورد نیاز توسط
۷۹۳	.....iptables نمونه اسکریپت
۷۹۳	.....دفاع ابتدایی از سیستم عامل
۷۹۶	.....iptables مقدار دهی اولیه به صورت پیشرفته
۸۰۰	.....DNS اجازه دسترسی به فایروال شما
۸۰۱	.....SSH و WWW اجازه دسترسی به فایروال شما
۸۰۲	.....اجازه دسترسی دادن به فایروال برای دسترسی به اینترنت
۸۰۳	.....اجازه دسترسی به شبکه خانگی خود برای دسترسی به فایروال
۸۰۴	.....Masquerading (NAT چند به یک)
۸۰۸	.....NAT از نوع Port Forwarding (DHCP DSL)
۸۱۳	.....NAT استاتیک
۸۱۹	.....iptables عیب‌یابی
۸۱۹	.....LOG های فایروال بررسی
۸۲۲	.....iptables شروع نمی‌شود!

۸۲۳	مدیریت و پیکربندی سیستم حسابرسی لینوکس (Auditing).....
۸۲۴	پیش نیازها.....
۸۲۴	بررسی نصب Audit.....
۸۲۵	پیکربندی Audit.....
۸۳۲	جستجو در Log های Audit رویدادها.....
۸۳۲	ایجاد گزارش های Audit.....
۸۳۶	تجزیه و تحلیل یک فرآیند با استفاده از atrace.....
۸۳۸	Port Scanner قدرتمند nmap.....
۸۳۹	مثال هایی از nmap.....
۸۸۰	کارت راهنمای nmap.....
۸۸۰	مشخصات هدف.....
۸۸۰	کشف میزبان.....
۸۸۱	تکنیک های اسکن.....
۸۸۲	مشخصات پورت و ترتیب اسکن.....
۸۸۳	تشخیص نسخه سرویس.....
۸۸۳	اسکن نوع اسکریپت.....
۸۸۴	تشخیص OS.....
۸۸۵	زمان بندی و کارایی.....
۸۸۶	Evasion و Spoofing فایروال IDS.....
۸۸۷	گزینه های خروجی Nmap.....
۸۸۸	سایر گزینه های Nmap.....
۸۸۹	پیکربندی iptables برای ممانعت از حملات Nmap.....
۸۹۹	Packet Capturing و تحلیل آن توسط دستور tcpdump.....
۹۵۹	<b>مراجع و منابع.....</b>