

راهنمای کاربردی مدارک بین‌المللی لینوکس
RHCSS و LPIC-3(303 Security)

(مدیریت و پیکربندی امنیت در لینوکس)



مؤلف: مهندس سید حسین رجاء

فهرست مطالب

پیشگفتار.....	۱۵
فصل صفر.....	۲۱
معرفی مدارک LPI.....	۲۱
لینوکس پایه.....	۲۱
مدرك 1 LPIC.....	۲۳
عناوین آزمون ۱۰۱.....	۲۴
عناوین آزمون ۱۰۲.....	۲۶
مدرك 2 LPIC.....	۲۷
عناوین آزمون ۲۰۱.....	۲۸
عناوین آزمون ۲۰۲.....	۲۹
مدرك 3 LPIC.....	۳۰
عناوین آزمون ۳۰۰.....	۳۲
عناوین آزمون ۳۰۱.....	۳۳
عناوین آزمون ۳۰۳.....	۳۴
عناوین آزمون ۳۰۵.....	۳۶
فصل اول.....	۴۱
کنترل دسترسی.....	۴۱
آیا متن باز از نظر امنیتی مناسب است؟.....	۴۱
چرا بستن کد منبع، باعث توقف حملات نمی‌شود؟.....	۴۳

چرا پنهان نگه داشتن نقاط آسیب پذیر، باعث دور شدن آن‌ها از برنامه نمی‌شود؟.....	۴۶
OSS/FS چگونه در برابر اسب‌های تروجان مقابله می‌کند؟.....	۴۷
توصیه‌ها.....	۴۸
مجوزها.....	۵۰
مجوز دهی نمادی.....	۵۲
دستور chmod برای تغییر مجوزها.....	۵۴
Umask چیست و نحوه تنظیم آن.....	۵۶
دستور chown.....	۵۹
SUID چیست و نحوه تنظیم آن.....	۶۱
SGID چیست و نحوه تنظیم آن.....	۶۷
اجرای دستورات با مجوز دیگر کاربران.....	۶۹
واگذاری وظایف به کاربران با sudo.....	۷۲
Pluggable authentication module یا PAM چیست؟.....	۷۷
فایل‌های پیکربندی PAM.....	۷۸
مثال اول از تنظیم PAM.....	۸۳
مثال دوم از پیکربندی PAM.....	۸۶
اعمال سیاست‌های گذرواژه.....	۸۸
جلوگیری از استفاده مجدد گذرواژه توسط کاربر.....	۹۰
تعیین حداقل طول گذرواژه.....	۹۱
اعمال پیچیدگی در زمان ایجاد یا تغییر گذرواژه.....	۹۱
تنظیم تاریخ انقضای گذرواژه.....	۹۲
مجبور کردن کاربران لینوکسی به تعویض گذرواژه‌های خود.....	۹۳
فهرست گزینه‌های دستور chage.....	۹۴
چگونگی تنظیم گذرواژه و غیرفعال کردن کاربران.....	۹۸
کنترل بر روی لاگین های ssh ناموفق با pam_tally2.....	۱۰۰
reset کردن گذرواژه root.....	۱۰۴
کسب اطلاعات در مورد کاربران وارد شده به سیستم.....	۱۰۶

فهرست مطالب / ۵

۱۱۴	مانیتور کردن فعالیت‌های کاربران
۱۲۳	جلوگیری از تغییر یا ویرایش فایل و دایرکتوری
۱۳۳	بررسی صحت توسط md5sum
۱۳۴	کار با SELinux یا Security Enhanced Linux
۱۳۷	MAC یا Security Mandatory Access Control
۱۵۳	RBAC یا Security Role Based Access Control
۱۵۶	MLS یا Multi Level Security
۱۵۷	MCS یا Multi Category Security
۱۵۹	وضعیت‌های SELinux و LOG ها
۱۷۰	پارامترهای SELinux
۱۸۷	تغییر Context یا Labling
۱۹۱	کپی کردن و SELinux
۱۹۳	Type Enforcement یا TE
۱۹۳	کار با MCS
۲۰۱	فصل دوم
۲۰۱	امنیت برنامه‌ها
۲۰۱	راهکارهایی برای ایمن‌سازی سیستم‌عامل (OS Hardening)
۲۱۴	دستور Isuf
۲۱۸	استفاده از دستور Isuf
۲۳۲	تنظیم vsftpd به صورت Anonymous
۲۳۳	تنظیم فایروال برای ftp
۲۳۴	دسترسی به ftp
۲۳۷	تنظیم دسترسی فقط خواندنی برای کاربران
۲۳۹	فایل /etc/vsftpd/ftpusers
۲۳۹	کنترل دسترسی‌ها در آپاچی
۲۴۴	تنظیم فایروال (iptables) در سرویس‌دهنده NFS
۲۴۶	HTTPS و آپاچی

۲۶۰ امنیت Mail Server
۲۶۰ پیکربندی DomainKeys و DKIM
۲۶۸ رله کردن
۲۶۸ Open relay
۲۷۰ رله گزینشی
۲۷۱ استفاده از برنامه tcpwrapper
۲۷۲ پیکربندی tcpwrapper
۲۷۳ استفاده از برنامه tcpserver
۲۷۳ پیکربندی tcpserver
۲۷۴ اجتناب کردن از open relay ها
۲۷۴ پیدا کردن میزبان ایمیل از راه دور
۲۷۵ فایل smtpoutes برای ایمیل های خروجی
۲۷۵ رله کردن به SMART HOST
۲۷۶ SMTP Auth
۲۷۶ استفاده از SASL
۲۷۷ SASL چیست؟
۲۷۷ SASL چگونه عمل می کند؟
۲۷۹ مکانیسم های تأیید هویت SASL
۲۷۹ استفاده از SASL درون SMTP
۲۸۱ نصب و استفاده از SMTP AUTH
۲۸۹ نصب Courier Auth
۲۹۳ Courier POP3 SSL
۲۹۳ نصب و استفاده از Courier POP3 SSL
۲۹۹ Courier IMAP SSL
۳۰۴ ایمن کردن SMTP
۳۰۴ SMTP همراه با SSL یا TLS
۳۱۲ استفاده از SSL در SquirrelMail
۳۱۵ نصب و پیکربندی OpenSSH

فهرست مطالب / ۷

دسترسی به ماشین‌های راه دور.....	۳۱۷
کپی ssh گونه فایل‌ها.....	۳۱۹
امنیت بیشتر روی ssh.....	۳۲۰
چگونه دسترسی کاربری را به OpenSSH محدود یا قطع کنیم؟.....	۳۲۱
دسترسی‌های مبتنی بر کاربر/گروه.....	۳۲۱
عدم دسترسی‌های مبتنی بر کاربر/گروه.....	۳۲۲
کنترل دسترسی به سرویس‌ها.....	۳۲۳
مثال‌ها.....	۳۲۴
استفاده از ssh بدون نیاز به کلمه عبور.....	۳۲۵
تونل گذاری SSH.....	۳۲۷
پیکربندی برنامه‌های کاربردی جهت استفاده از پراکسی.....	۳۳۱
امنیت در NFS.....	۳۳۲
نصب و پیکربندی (AIDE Advanced Intrusion Detection)	
.....(Environment)	۳۳۳
Bastille Linux برای سخت کردن سیستم (Hardening).....	۳۴۰
نصب و راه‌اندازی squid.....	۳۴۴
مزایای proxy server.....	۳۴۴
نصب و پیکربندی Squid در توزیع‌های لینوکسی.....	۳۴۷
پارامترهای مهم squid.....	۳۴۸
راه‌اندازی squid.....	۳۵۱
استفاده از قابلیت Proxy و Caching.....	۳۵۱
تحلیل LOG های squid با استفاده از Sarg.....	۳۶۵
تعریف قوانین و سیاست‌های squid.....	۳۷۴
بلاک کردن سایت‌ها برای برخی از کاربران.....	۳۷۵
بلاک کردن بارگذاری فایل‌ها با پسوندشان توسط squid.....	۳۷۸
محدود کردن Web Connection های همزمان از یک کلاینت توسط	
.....squid	۳۸۱
بلاک کردن پورت خاص توسط squid.....	۳۸۳

۳۸۶Squid Tag های مهم
۳۹۸squid Traffic Shaping توسط
۴۳۲Squid Proxy Authentication
۴۳۹فصل سوم
۴۳۹امنیت شبکه
۴۳۹ping: جواب ندادن به
۴۳۹MAC آدرس جعل کردن
۴۴۱hosts بلاک کردن یک سایت با فایل
۴۴۱(iptables) فایروال
۴۴۳فعال و غیرفعال کردن فایروال
۴۴۴Trusted سرویس‌های
۴۴۴(Other Ports) دیگر پورت‌ها
۴۴۵Trusted Interfaces
۴۴۵masquerading
۴۴۵Port forwarding
۴۴۶ICMP Filter
۴۴۶پیکربندی
۴۴۸filter زنجیره‌های جدول
۴۴۸nat زنجیره‌های جدول
۴۴۸mangle زنجیره‌های جدول
۴۴۹شکل کلی
۴۵۰سوئیچ‌ها
۴۶۰ذخیره و بازگردانی Rule های iptables در لینوکس
۴۶۳(Stateful Packet Filtering) تصفیه مبتنی بر حالت
۴۶۵redirect کردن
۴۶۶iptables مثال‌هایی از
۴۷۱ICMP بستن پروتکل

فهرست مطالب / ۹

اجازه دادن به WWW و SSH برای دسترسی به فایروال	۴۷۴
اجازه دادن به فایروال برای دسترسی به اینترنت	۴۷۵
بررسی LOG های فایروال	۴۷۶
inactive بودن فایروال	۴۷۸
مثالی جامع برای حالت stateful firewall	۴۷۹
دفاع ابتدایی از سیستم‌عامل توسط sysctl.conf	۴۸۴
پیگیری تغییرات بر روی فایل‌ها توسط Audit	۴۸۷
اسکن آدرس‌های IP در شبکه با nmap	۴۹۴
جلوگیری از اسکن توسط nmap توسط iptables	۵۰۳
جلوگیری از حملات رایجی که تعداد connection زیاد تولید می‌کنند	
	۵۰۹
جلوگیری از حملاتی که رشته‌های خاصی در payload خود دارند	۵۱۰
آنالیز Packet ها با استفاده از دستور tcpdump	۵۱۳
پیدا کردن حفره‌های امنیتی توسط Nessus	۵۳۳
آشنایی با NAT و پیکربندی آن	۵۴۷
گونه‌های پیاده‌سازی NAT	۵۵۱
Source NAT یا SNAT	۵۵۱
Destination NAT یا DNAT	۵۵۴
NAPT یا PAT	۵۵۶
پیاده‌سازی NAT	۵۵۷

فصل چهارم.....۵۶۷

امنیت و رمزنگاری.....	۵۶۷
رمزنگاری.....	۵۶۷
رمزنگاری، پنهان نگاری، کدگذاری.....	۵۶۸
اصول شش‌گانه کرش‌هف.....	۵۶۹
رمزنگاری پیشرفته.....	۵۷۰
عناصر مهم رمزنگاری.....	۵۷۱

۵۷۲	تعاریف مهم رمزنگاری
۵۷۲	سرویس رمزنگاری
۵۷۴	پروتکل رمزنگاری
۵۷۴	الگوریتم رمزنگاری
۵۷۶	رمزنگاری کلید متقارن
۵۷۷	رمزنگاری کلید نامتقارن یا کلید عمومی
۵۷۸	مقایسه رمزنگاری کلید متقارن و کلید نامتقارن
۵۷۹	مفاهیم زیرساخت کلید عمومی
۵۷۹	زوج کلیدهای چندتایی
۵۸۱	زیرساخت کلید عمومی
۵۸۱	بررسی اجمالی
۵۸۲	روش‌های تأیید گواهی
۵۸۲	مراکز صدور گواهی
۵۸۳	گواهی‌های موقت و شناسایی یگانه
۵۸۳	وب (شبکه) اعتماد
۵۸۵	زیرساخت کلید عمومی ساده
۵۸۵	تاریخچه
۵۸۷	مثال‌های کاربردی
۵۸۹	کشف رمز کلید
۵۹۰	بازیابی و آماده‌سازی در برابر حوادث
۵۹۰	آگاه ساختن طرف اعتماد کننده
۵۹۰	آماده‌سازی
۵۹۱	بازیابی
۵۹۲	مدیریت گواهی مستقل
۵۹۲	پشتیبانی از عدم انکار
۵۹۳	گواهی دیجیتال
۵۹۳	انواع مختلف گواهی
۵۹۴	انواع کلاس‌های گواهی دیجیتال

فهرست مطالب / ۱۱

۵۹۵	معناشناسی و ساختار گواهی
۵۹۸	ساختارهای دیگر گواهی
۵۹۸	SPKI
۵۹۹	PGP
۶۰۰	SET
۶۰۰	گواهی‌های اختیاری
۶۰۰	مدیریت گواهی
۶۰۱	صدور گواهی (Issuing Certificate)
۶۰۱	ابطال گواهی (Revoking Certificates)
	انتشار یک لیست از گواهی‌های باطل شده (Publishing a Certificate)
۶۰۲	(Revocation List)
	وارد و صادر کردن گواهی (Importing and Exporting Certificates)
۶۰۲	
۶۰۳	پروتکل RSA
۶۰۷	پروتکل تبادل کلید دیفی-هلمن
۶۰۸	تاریخچه
۶۰۹	جزئیات پروتکل دیفی-هلمن
۶۱۱	مثال عددی
۶۱۲	امنیت پروتکل دیفی-هلمن
۶۱۳	مشکل شناسایی دو طرف در پروتکل دیفی-هلمن
۶۱۳	الگوریتم امضای دیجیتالی (DSA)
۶۱۴	تولید کلید
۶۱۴	انتخاب پارامترهای الگوریتم
۶۱۵	تخصیص کلید به کاربر
۶۱۵	الگوریتم تولید امضا
۶۱۶	درستی الگوریتم تصدیق امضا
۶۱۶	حساسیت
۶۱۶	امنیت لایه انتقال

۶۱۸	تعریف
۶۲۰	تاریخچه
۶۲۰	برنامه‌نویسی امن
۶۲۰	SSL ۱,۰ ، ۲,۰ ، ۳,۰
۶۲۱	TLS 1.0
۶۲۱	TLS 1.1
۶۲۱	TLS 1.2
۶۲۱	برنامه‌های کاربردی
۶۲۲	وبسایت‌ها
۶۲۲	تبادل کلید
۶۲۲	SSL
۶۲۳	پروتکل رکورد در SSL
۶۲۴	پروتکل تغییر مشخصات رمز در SSL
۶۲۴	پروتکل هشدار در SSL
۶۲۴	پروتکل دست دادن در SSL
۶۲۵	امنیت
۶۲۶	OpenSSL
۶۲۷	استاندارد X.509
۶۲۷	ساختار گواهی
۶۲۹	فیلد Extension
۶۳۰	پسوند فایل‌های گواهی‌های X.509
۶۳۰	نمونه گواهی
۶۳۴	کار با GPG
۶۳۹	مراجع و منابع