راهنمای کاربردی مدارک بین‌المللی لینوکس

RHCSS و LPIC-3 (303 Security)

(مدیریت و پیکربندی امنیت در لینوکس)

مؤلف:

مهندس سید حسین رجاء

ناشر:

کانون نشر علوم

سرشناسه: رجاء، سیدحسین، ۱۳۶۲ -
عنوان و نام پدیدآور: راهنمای کاربردی مدارک بین‌المللی RHCSS و LPIC-3 (303security)
(مدیریت و پیکربندی امنیت در لینوکس)/ مولف سیدحسین رجاء.
مشخصات نشر: تهران: انتشارات آترا: کانون نشر علوم، ۱۳۹۵.
مشخصات ظاهری: ۳۸۴ص.: مصور، جدول، نمودار.
شابک: ۹۷۸۶۰۰۶۴۲۵۳۰۶
وضعیت فهرست‌نویسی: فیپا
یادداشت کتابنامه: ص. ۳۷۸-۳۸۴.
موضوع: سیستم‌عامل لینوکس -- آزمون‌ها
موضوع: سیستم‌های [illegible] کامپیوتری)
رده‌بندی کنگره: ۱۳۹۵ ۷ ۶۷ [illegible]س/QA ۷۶/۷۶
رده‌بندی دیویی: ۵/۴۳۲
شماره کتابشناسی ملی: ۴۱۰۹۳۴

نام کتاب: راهنمای کاربردی مدارک بین‌المللی لینوکس LPIC-3 (303 Security) و RHCSS
ناشر: انتشارات آترا
ناشر همکار: کانون نشرعلوم
مولف: سید حسین رجاء
صفحه‌آرا: فاطمه آدیگوزل‌پور اردبیلی
طرح جلد: زهرا سلطان‌آبادی
چاپ اول: بهار ۱۳۹۵
تیراژ: ۱۰۰۰
چاپ و صحافی: کانون نشرعلوم
قیمت: ۳۴۰۰۰ تومان
شابک: ۹۷۸۶۰۰۶۴۲۵۳۰۶

مراکز پخش:
نشر و پخش آترا: میدان انقلاب، خیابان جمالزاده جنوبی، کوچه شهید آقاصبوری پلاک ۱۳
تلفن: ۶۶۹۲۲۰۸۲
پخش علوم: خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد۱
تلفن: ۶۶۴۹۴۹۱۱-۶۶۹۶۱۵۶۸

سخن ناشر

به نام خداوند بخشنده و مهربان

گستره دانش بشری در برابر علم بی‌پایان و نامتناهی حضرت حق (جلّ جلاله) بسیار ناچیز است؛ همچنان که می‌فرماید: «و ما عطا نکردیم به شما علم را جز اندکی» شاهدی است بر ضعف معرفت انسان نسبت به حکمت صَمَدانی. با این حال چه نیکو سفارش فرموده است خاتم انبیاء، حضرت محمد مصطفی (ص) که «بجویید علم را اگر چه به سرزمین چین». این توصیه، تمامی پیروان راستین دین حنیف اسلام را به فراگیری و اکتساب علوم و فنون مختلف در همه زمان‌ها و همه مکان‌ها فرا می‌خواند.

تلاش کانون نشر علوم، همواره معطوف به تولید آثار شایسته و بایسته در زمینه فنی و مهندسی بوده است؛ اگرچه که در این راه مشکلات و دشواری‌های فراوانی حادث شده و خواهد شد. این امر تا حدّی بسیار، تابعی از ماهیت رشته‌های فنی و مهندسی و معارف مربوط به آنهاست؛ چرا که این رشته‌ها به‌سرعت و بی‌وقفه در حال نو به نو شدن می‌باشند. این امر رسالت کانون نشر علوم را در نشر آثار مربوطه، اعم از تألیف یا ترجمه، خطیر کرده و می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از قافله علوم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجاهت علمی مورد خور شأن مخاطبین اندیشمند و فاضل نیز باشد. امید است که خداوند منّان در این مهم مساعدت و یاری نماید.

پایان سخن اینکه، کانون نشر علوم دست یاری و همّت تمامی مؤلفین و مترجمین علاقه‌مند در زمینه علوم فنی و مهندسی را به‌گرمی می‌فشارد و تمامی ایشان را خاضعانه و صمیمانه به همکاری فرا می‌خواند. همچنین این مجموعه از تمامی مخاطبین استدعا دارد که با نظرات صائب و راهگشای خود، در بهبود شکلی و محتوایی آثار منتشر شده مساعدت فرمایند؛ و صد البته که تمامی کاستی‌ها از این رهگذر تنها و تنها متوجه این مجموعه بوده و هست.

سید محمدحسین منوّری
کانون نشر علوم

مقدمه مؤلف

دوره آموزشی LPIC 3 بالاترین دوره آموزشی در مدارک LPIC است. دوره LPIC-3(303 Security) در سطح Senior طبقه‌بندی می‌گردد با گرایش امنیت و سومین سطح در جمع دوره‌های حرفه‌ای لینوکس LPI می‌باشد. سرفصل‌های این دوره به صورت تخصصی بر روی موضوع امنیت تمرکز دارند.

عناوین آزمون ۳۰۳ به اختصار شامل موارد زیر است:

۱- رمزنگاری:

۱-۱- رمزنگاری با استفاده از Openssl.

۱-۱-۱- تولید certificate و Key.

۱-۱-۲- تست‌های SSL/TLS بر روی سرویس‌دهنده و سرویس‌گیرنده.

۱-۲-آشنایی با SSL, Openssl, X509, CRL, RSA و DSA.

۱-۳- رمزنگاری با GPG.

۱-۳-۱- مدیریت و تنظیمات GPG.

۱-۴- رمزنگاری فایل سیستم‌ها.

۱-۴-۱- آشنایی با LUKS dm-crypt, cryptmount و cryptsetup.

۲- کنترل سطوح دسترسی:

۲-۱- تنظیمات مربوط به سیستم PAM و nsswitch.

۲-۲- بررسی لیست‌های دسترسی و کلاس‌های مربوطه.

۲-۳- آشنایی با SELinux، تنظیم و کنترل و به‌کارگیری آن از طریق خط فرمان.

۲-۳- آشنایی با SMACK و AppArmor.

۳- امنیت سرویس‌ها:

۳-۱- ایمن‌سازی BIND/DNS.

۳-۱-۱- بررسی محیط chroot.

۳-۱-۲- آشنایی با TSIG.

۳-۱-۳- کار با لیست‌های دسترسی در BIND و آشنایی با named-checkconf.

۳-۲- ایمن‌سازی سرویس Mail.

۳-۲-۱- تنظیمات postfix و sendmail.

۳-۲-۲- بررسی محیط chroot.

۳-۲-۳- به‌کارگیری سیستم ایمیل بر روی TLS.

۳-۳- ایمن‌سازی Apache/HTTP/HTTPS.

۳-۳-۱- تنظیم وب سرور.

۳-۳-۲- به‌کارگیری SSL، htaccess، Basic Authentication، htpasswd و AllowOverride.

۳-۴- ایمن‌سازی سرویس ftp.

۳-۴-۱- تنظیمات Pure-ftpd و vsftpd.

۳-۴-۲- ارسال اطلاعات ftp بر روی SSL/TLS.

۳-۴-۳- ایمن‌سازی OpenSSH.

۳-۴-۳-۱- بررسی دستورات و پیکربندی OpenSSH.

۳-۴-۳-۲- به‌کارگیری ssh-keygen و ssh-agent.

۳-۵- ایمن‌سازی NFSV4.

۳-۵-۱- بررسی ویژگی‌های امنیتی ارتقا یافته در NFSV4 و مکانیسم‌های امنیتی آن.

۳-۶- گرفتن لاگ از سیستم با Syslog.

۴- امنیت شبکه:

۴-۱- تشخیص نفوذ.

۴-۱-۱- تنظیم و به‌کارگیری snort و Tripwire.

۴-۲- ابزارهای اسکن امنیت شبکه.

۴-۲-۱- بررسی ابزارهای nmap, wireshark, tshark, nessus و ...

۴-۳- بررسی ابزارهای مانیتورینگ شبکه از جمله ntop، ...

۴-۴- پیکربندی netfilter/iptables.

۴-۵- پیکربندی OpenVpn.

سعی شده است اکثر عناوین ذکر شده در بالا که کاربردی هستند، در این کتاب پوشش داده شوند.

مخاطبین اصلی کتاب، متخصصین لینوکس، مدیران شبکه، متخصصین حوزه نرم‌افزارهای متن باز، برنامه نویسان، متقاضیان و شرکت‌کنندگان در آزمون‌های LPIC-1، LPIC-2، RHCA، RHCE و به‌خصوص LPIC-3 (303 Security) و RHCSS، دانشجویان رشته نرم‌افزار و فناوری اطلاعات، کارشناسان امنیت و تمامی افراد علاقه‌مند به حوزه لینوکس و مباحث پیرامونی آن می‌باشند.

سید حسین رجاء کارشناس ارشد فناوری اطلاعات (IT) می‌باشد که حدوداً ۱۶ سال فعالیت در زمینه‌های مختلف IT، من جمله برنامه‌نویسی، شبکه، امنیت شبکه، پایگاه داده، مجازی سازی، سیسکو، لینوکس، ویندوز، ایمیل سرور، تدریس و تألیف را تجربه کرده است. از جمله مدارک علمی ایشان می‌توان به CCIE R&S، CCIE Service Provider و LPIC-3(301,302,303,305) اشاره کرد.

قابل ذکر است، کتاب‌های زیر در زمینه مدارک LPIC از اینجانب تاکنون منتشر شده است:

- راهنمای جامع مدرک بین‌المللی Linux LPIC-3(305 Mail and Messaging)، مؤلف سید حسین رجاء، انتشارات آترا و 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

همچنین، علاوه بر موارد ذکر شده در بالا، کتاب‌های زیر در زمینه لینوکس و سرویس‌های آن از اینجانب تاکنون منتشر شده است:

- راهنمای جامع لینوکس (ورود دو جلدی)، مؤلف سید حسین رجاء، انتشارات آترا و کانون نشر علوم، ۱۳۹۴
- برنامه‌نویسی پوسته در لینوکس توسط Bash، مؤلف سید حسین رجاء، انتشارات آترا و کانون نشر علوم، ۱۳۹۵
- Qmail(راه‌اندازی، پیکربندی و مدیریت)، مؤلف سید حسین رجاء، انتشارات افق دور و ریواس، ۱۳۹۳
- امنیت پست الکترونیکی، مؤلف سید حسین رجاء، انتشارات پندار پارس، ۱۳۹۰

کتاب حاضر با توجه به مطالعات علمی و سال‌ها تجربه فنی نگارنده در زمینه لینوکس، امنیت 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 کتب 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.

بر خود لازم می‌دانم از تمام کسانی که در تولید و تألیف این کتاب به اینجانب یاری رساندند بخصوص جناب مهندس سید محمد حسین منوری مدیر محترم انتشارات کانون نشر علوم، سرکار خانم سلطان آبادی، سرکار خانم اردبیلی و سرکار خانم آمنه سادات بهشتی کمال تشکر را داشته باشم.

در نهایت این کتاب را در وهله اول، به ساحت مقدس چهارده معصوم علیهم‌السلام و در وهله دوم، به پدر و مادرم، همسرم نرگس سادات و فرزندم زهرا سادات تقدیم می‌نمایم.

سید حسین رجاء- بهار ۱۳۹۵

فهرست مطالب

مقدمه مؤلف ۵

فصل صفر: معرفی مدارک LPI ۱۵

لینوکس پایه ۱۶

عناوین آزمون ۱۰۱ ..... ۱۸

مدرک LPIC 1 ..... ۱۸

عناوین آزمون ۱۰۲ ..... ۱۹

مدرک LPIC 2 ..... ۲۰

عناوین آزمون ۲۰۱ ..... ۲۱

عناوین آزمون ۲۰۲ ..... ۲۲

مدرک LPIC 3 ..... ۲۳

عناوین آزمون ۳۰۰ ..... ۲۴

عناوین آزمون ۳۰۱ ..... ۲۵

عناوین آزمون ۳۰۳ ..... ۲۶

عناوین آزمون ۳۰۵ ..... ۲۷

فصل اول: کنترل دسترسی ۳۱

آیا متن باز از نظر امنیتی مناسب است؟ ۳۲

چرا بستن کد منبع، باعث توقف حملات نمی‌شود؟ ۳۳

چرا پنهان نگه‌داشتن نقاط آسیب‌پذیر، باعث دور شدن آن‌ها از ... نمی‌شود؟ ۳۵

OSS/FS چگونه در برابر اسب‌های تروجان مقابله می‌کند؟ ۳۵

توصیه‌ها ۳۶

مجوزها ۳۷

مجوز دهی نمادی ۳۸

دستور chmod برای تغییر مجوزها ۳۹

Umask چیست و نحوه تنظیم آن ۴۰

دستور chown ۴۲

SUID چیست و نحوه تنظیم آن ۴۴

SGID چیست و نحوه تنظیم آن ۴۶

اجرای دستورات با مجوز دیگر کاربران ۴۷

واگذاری وظایف به کاربران با sudo ۴۹

Pluggable authentication module یا PAM چیست؟ ۵۳

فایل‌های پیکربندی PAM ۵۳

مثال اول از تنظیم PAM ۵۶

مثال دوم از پیکربندی PAM ۵۷

اعمال سیاست‌های گذرواژه ۵۸

جلوگیری از استفاده مجدد گذرواژه توسط کاربر ۵۹

تعیین حداقل طول گذرواژه ۶۰

اعمال پیچیدگی در زمان ایجاد یا تغییر گذرواژه ۶۰
تنظیم تاریخ انقضای گذرواژه ۶۰
مجبور کردن کاربران لینوکسی به تعویض گذرواژه‌های خود ۶۱
فهرست گزینه‌های دستور chage ۶۲
چگونگی تنظیم گذرواژه و غیرفعال کردن کاربران ۶۴
کنترل بر روی لاگین‌های ssh ناموفق با pam_tally2 ۶۵
reset کردن گذرواژه root ۶۷
کسب اطلاعات در مورد کاربران وارد شده به سیستم ۶۸
مانیتور کردن فعالیت‌های کاربران ۷۳
جلوگیری از تغییر یا ویرایش فایل و دایرکتوری ۷۷
بررسی صحت توسط md5sum ۸۰
کار با SELinux یا Security Enhanced Linux ۸۰
MAC یا Mandatory Access Control Security ۸۱
RBAC یا Role Based Access Control Security ۸۸
MLS یا Multi Level Security ۹۰
MCS یا Multi Category Security ۹۰
وضعیت‌های SELinux و LOGها ۹۲
پارامترهای SELinux ۹۸
تغییر Context یا Labling ۱۰۶
کپی کردن و SELinux ۱۰۸
TE یا Type Enforcement ۱۰۹
کار با MCS ۱۰۹

فصل دوم: امنیت برنامه‌ها ۱۱۳

راهکارهایی برای ایمن‌سازی سیستم‌عامل (OS Hardening) ۱۱۴
دستور lsof ۱۲۲
استفاده از دستور lsof ۱۲۵
تنظیم vsftpd به‌صورت Anonymous ۱۳۲
تنظیم فایروال برای ftp ۱۳۲
دسترسی به ftp ۱۳۳
تنظیم دسترسی فقط خواندنی برای کاربران ۱۳۵
فایل /etc/vsftpd/ftpusers ۱۳۶
کنترل دسترسی‌ها در آپاچی ۱۳۷
تنظیم فایروال (iptables) در سرویس‌دهنده NFS ۱۴۰
HTTPS و آپاچی ۱۴۱
پیکربندی DomainKeys و DKIM ۱۵۱
امنیت Mail Server ۱۵۱
Open relay ۱۵۵

رله کردن ۱۵۵
رله گزینشی ۱۵۶
استفاده از برنامه tcpwrapper ۱۵۷
پیکربندی tcpwrapper ۱۵۷
استفاده از برنامه tcpserver ۱۵۸
پیکربندی tcpserver ۱۵۸
اجتناب کلی از open relayها ۱۵۸
پیدا کردن میزبان ایمیل از راه دور ۱۵۹
فایل mtproutes برای میل‌های خروجی ۱۵۹
رله کردن به SMART HOST ۱۵۹
استفاده از SASL ۱۶۰
SMTP Auth ۱۶۰
SASL چیست؟ ۱۶۰
SASL چگونه عمل می‌کند؟ ۱۶۰
مکانیسم‌های تأیید هویت SASL ۱۶۱
استفاده از SASL درون SMTP ۱۶۱
نصب و استفاده از SMTP AUTH ۱۶۲
نصب Courier Auth ۱۶۷
Courier POP3 SSL ۱۶۹
نصب و استفاده از Courier POP3 SSL ۱۶۹
Courier IMAP SSL ۱۷۴
ایمن کردن SMTP ۱۷۶
SMTP همراه با SSL یا TLS ۱۷۶
استفاده از SSL در SquirrelMail ۱۸۱
نصب و پیکربندی OpenSSH ۱۸۳
دسترسی به ماشین‌های راه دور ۱۸۴
کپی ssh گونه فایل‌ها ۱۸۵
امنیت بیشتر روی ssh ۱۸۵
چگونه دسترسی کاربری را به OpenSSH محدود یا قطع کنیم؟ ۱۸۶
دسترسی‌های مبتنی بر کاربر/گروه ۱۸۶
مثال‌ها ۱۸۷
عدم دسترسی‌های مبتنی بر کاربر/ گروه ۱۸۷
کنترل دسترسی به سرویس‌ها ۱۸۷
استفاده از ssh بدون نیاز به کلمه عبور ۱۸۸
تونل گذاری SSH ۱۸۹
پیکربندی برنامه‌های کاربردی جهت استفاده از پراکسی ۱۹۲
امنیت در NFS ۱۹۲
نصب و پیکربندی AIDE (Advanced Intrusion Detection Environment) ۱۹۳

Bastille Linux برای سخت کردن سیستم (Hardening) ۱۹۸
نصب و راه‌اندازی squid ۲۰۰
مزایای proxy server ۲۰۱
نصب و پیکربندی Squid در توزیع‌های لینوکسی ۲۰۲
پارامترهای مهم squid ۲۰۳
راه‌اندازی squid ۲۰۴
استفاده از قابلیت Proxy و Caching ۲۰۵
تحلیل LOGهای squid با استفاده از Sarg ۲۱۴
تعریف قوانین و لیست‌های squid ۲۲۱
بلاک کردن سایت‌ها برای برخی از کاربران ۲۲۲
بلاک کردن بارگذاری فایل‌ها با پسوند توسط squid ۲۲۴
محدود کردن Web Connection های همزمان از یک کلاینت توسط squid ۲۲۶
بلاک کردن پورت خاص توسط squid ۲۲۷
Tagهای مهم Squid ۲۲۸
Traffic Shaping توسط squid ۲۳۵
Squid Proxy Authentication ۲۵۶

فصل سوم: امنیت شبکه ۲۶۱
امنیت: جواب ندادن به ping ۲۶۲
جعل کردن آدرس MAC ۲۶۲
بلاک کردن یک سایت با فایل hosts ۲۶۳
فایروال (iptables) ۲۶۳
فعال و غیرفعال کردن فایروال ۲۶۴
سرویس‌های Trusted ۲۶۵
دیگر پورت‌ها (Other Ports) ۲۶۵
Trusted Interfaces ۲۶۵
masquerading ۲۶۵
Port forwarding ۲۶۶
ICMP Filter ۲۶۶
پیکربندی ۲۶۶
زنجیره‌های جدول filter ۲۶۷
زنجیره‌های جدول nat ۲۶۷
زنجیره‌های جدول mangle ۲۶۷
شکل کلی ۲۶۸
سوئیچ‌ها ۲۶۹
ذخیره و بازگردانی Ruleهای iptables در لینوکس ۲۷۴
تصفیه مبتنی بر حالت (Stateful Packet Filtering) ۲۷۶
redirect کردن ۲۷۷

مثال‌هایی از iptables ۲۷۷
بستن پروتکل ICMP ۲۸۰
اجازه دادن به WWW و SSH برای دسترسی به فایروال ۲۸۱
اجازه دادن به فایروال برای دسترسی به اینترنت ۲۸۲
بررسی LOGهای فایروال ۲۸۳
ina ive بودن فایروال ۲۸۴
برای حالت stateful firewall ۲۸۴
دفاع ابتدایی از سیستم‌عامل توسط sysctl.conf ۲۸۷
پیگیری تغییرات فایل‌ها توسط Audit ۲۸۸
اسکن آدرس‌های IP در شبکه با nmap ۲۹۲
جلوگیری از اسکن توسط nmap توسط iptables ۲۹۷
جلوگیری از حملات DoS که تعداد connection زیاد تولید می‌کنند ۲۹۹
جلوگیری از حملاتی که رشته‌های خاصی در payload خود دارند ۳۰۰
آنالیز Packetها با استفاده از دستور tcpdump ۳۰۱
پیدا کردن حفره‌های امنیتی توسط Nessus ۳۱۲
آشنایی با NAT و پیکربندی آن ۳۲۵
گونه‌های پیاده‌سازی NAT ۳۲۷
SNAT یا Source NAT ۳۲۷
DNAT یا Destination NAT ۳۲۹
PAT یا NAPT ۳۳۰
پیاده‌سازی NAT ۳۳۰

فصل چهارم: امنیت و رمزنگاری ۳۳۷

رمزنگاری ۳۳۸
رمزنگاری، پنهان نگاری، کدگذاری ۳۳۸
اصول شش‌گانه کرشهف ۳۳۹
رمزنگاری پیشرفته ۳۴۰
عناصر مهم رمزنگاری ۳۴۰
تعاریف مهم رمزنگاری ۳۴۱
سرویس رمزنگاری ۳۴۱
پروتکل رمزنگاری ۳۴۱
الگوریتم رمزنگاری ۳۴۲
رمزنگاری کلید متقارن ۳۴۳
رمزنگاری کلید نامتقارن یا کلید عمومی ۳۴۳
مقایسه رمزنگاری کلید متقارن و کلید نامتقارن ۳۴۴
مفاهیم زیرساخت کلید عمومی ۳۴۴
زوج کلیدهای چندتایی ۳۴۵
زیرساخت کلید عمومی ۳۴۵

بررسی اجمالی ۳۴۶
روش‌های تأیید گواهی ۳۴۶
مراکز صدور گواهی ۳۴۶
گواهی‌های موقت و شناسایی یگانه ۳۴۷
وب (شبکه) اعتماد ۳۴۷
زیرساخت کلید عمومی ساده ۳۴۸
تاریخچه ۳۴۸
مثال‌های کاربردی ۳۴۹
آگاه ساختن طرف اعتماد کننده ۳۵۰
کشف رمز کلید ۳۵۰
بازیابی و آماده‌سازی در هر حوادث ۳۵۰
آماده‌سازی ۳۵۰
بازیابی ۳۵۱
مدیریت گواهی مستقل ۳۵۱
پشتیبانی از عدم انکار ۳۵۱
انواع مختلف گواهی ۳۵۲
انواع کلاس‌های گواهی دیجیتال ۳۵۲
گواهی دیجیتال ۳۵۲
معناشناسی و ساختار گواهی ۳۵۳
ساختارهای دیگر گواهی ۳۵۴
SPKI ۳۵۴
PGP ۳۵۵
SET ۳۵۵
گواهی‌های اختیاری ۳۵۵
مدیریت گواهی ۳۵۶
صدور گواهی (Issuing Certificate) ۳۵۶
ابطال گواهی (Revoking Certificates) ۳۵۶
انتشار یک لیست از گواهی‌های باطل شده (Publishing a Certificate Revokation List) ۳۵۶
وارد و صادر کردن گواهی (Importing and Exporting Certificates) ۳۵۷
پروتکل RSA ۳۵۷
پروتکل تبادل کلید دیفی-هلمن ۳۶۰
تاریخچه ۳۶۰
جزئیات پروتکل دیفی- هلمن ۳۶۰
مثال عددی ۳۶۲
امنیت پروتکل دیفی-هلمن ۳۶۲
مشکل شناسایی دو طرف در پروتکل دیفی-هلمن ۳۶۲
انتخاب پارامترهای الگوریتم ۳۶۳
الگوریتم امضای دیجیتال (DSA) ۳۶۳

تولید کلید ۳۶۳
الگوریتم تولید امضا ۳۶۴
درستی الگوریتم تصدیق امضا ۳۶۴
تخصیص کلید به کاربر ۳۶۴
حساسیت ۳۶۴
امنیت لایه انتقال ۳۶۵
تاریخچه ۳۶۶
برنامه‌نویسی امن ۳۶۷
SSL 1.0، 2.0، 3.0 ۳۶۷
TLS 1.0 ۳۶۷
TLS 1.1 ۳۶۷
TLS 1.2 ۳۶۷
تاریخچه ۳۶۷
برنامه‌های کاربردی ۳۶۸
وب‌سایت‌ها ۳۶۸
تبادل کلید ۳۶۸
SSL ۳۶۸
پروتکل رکورد در SSL ۳۶۹
پروتکل تغییر مشخصات رمز در SSL ۳۶۹
پروتکل هشدار در SSL ۳۶۹
پروتکل دست دادن در SSL ۳۶۹
OpenSSL ۳۷۰
امنیت ۳۷۰
استاندارد X.509 ۳۷۱
ساختار گواهی ۳۷۱
فیلد Extension ۳۷۲
پسوند فایل‌های گواهی‌های X.509 ۳۷۲
نمونه گواهی ۳۷۲
کار با GPG ۳۷۴

مراجع و منابع ۳۷۷