فهرست

فصل اول مقدمه ۱

۱-۱ طرح مسئله ۱

۱-۲ اهداف ٤

۱-۳ پرسش‌ها و فرضیات ٤

۱-٤ تحقیقات مرتبط ٦

۱-٥ ساختار کتاب ۸

فصل دوم مفاهیم پایه ۱۱

۲-۱ اصول پست الکترونیکی ۱۱

۲-۱-۱ سیستم‌های پست الکترونیکی لینوکسی ۱۱

MDA ۱۲

فیلترگذاری خودکار پست الکترونیکی ۱۳

پاسخگویی خودکار پست الکترونیکی ۱٤

مقداردهی اولیه برنامه توسط پست الکترونیکی ۱٥

MTA ۱٥

MUA ۱۷

محل ذخیره پیام‌ها ۱۷

چگونگی نمایش پیام‌ها ۱۷

۲-۱-۲ پروتکل‌های پست الکترونیکی ۱۸

پروتکل‌های MTA ۱۸

پروتکل SMTP ۱۸

پروتکل ESMTP ۱۹

پروتکل‌های MUA ۱۹
پروتکل POP ۱۹
۲-۲ پروتکل SMTP ۲۱
۲-۲-۱ دستورات کلاینتی SMTP ۲۱
۲-۲-۲ پاسخ‌های سرور ۲۳
۲-۳ پروتکل‌های POP و IMAP ۲٤
۲-٤ MIME ۲٥
۲-٤-۱ برنامه Uuencode ۲٦
۲-٤-۲ MIME و داده‌های باینری ۲٦
۲-٤-۳ فیلدهای سرآیند MIME ۲٦
فیلد Content-Transfer-Encoding ۲۷
فیلد Content-Type ۲۸
Multipart Content-Type ۲۹
۲-٥ دسته بندی حملات ۲۹
۲-٦ نتایج حمله ۳۰
فصل سوم مخاطرات ۳۳
۳-۱ ارزیابی مخاطرات سیستم‌های پست الکترونیکی ۳۳
۳-۱-۱ احتمال کلی و تأثیر ۳٥
۳-۱-۲ روش‌های دیگر ۳٥
۳-۱-۳ روش کانوری ۳٦
۳-۱-٤ عناصر جدول ارائه شده ۳۷
۳-۲ مخاطرات سرور پست الکترونیکی ۳۹
۳-۲-۱ مخاطرات سرورهای خانواده یونیکس ۳۹

حملات شبکه ای.....۳۹
دسترسی شبکه ای ۳۹
۳-۲-۲ مخاطرات بسته‌های پست الکترونیکی Sendmail، Qmail و Postfix ۴۱
بسته پست الکترونیکی Sendmail.....۴۱
بسته پست الکترونیکی Qmail.....۴۲
بسته پست الکترونیکی Postfix ۴۵
برنامه‌های اصلی postfix.....۴۵
صف‌های پیام postfix.....۴۷
برنامه‌های کاربردی postfix.....۴۷
برنامه‌های پیکربندی postfix ۴۸
جداول lookup در postfix ۴۸
مخاطرات موجود در بسته‌های پست الکترونیکی sendmail، qmail و postfix.....۴۹
نداشتن مجوز مناسب فایل ۴۹
کاربری با سطح دسترسی بالا ۴۹
۳-۲-۳ Open Relays ۵۰
۳-۲-۴ Spam.....۵۲
۳-۲-۵ ویروس‌ها.....۵۴
۳-۳ مخاطرات سرویس پست الکترونیکی ۵۵
۳-۳-۱ سوء استفاده از برخی دستورات و کاوش گری.....۵۵
۳-۳-۲ سوء استفاده از سرآیندهای پست الکترونیکی ۶۰
فیلد سرآیند TO ۶۱
۳-۳-۳ مخاطره نا امن بودن محتوای پیام‌ها ۶۴
۳-۳-۴ نا امن بودن سرورهای POP3 و IMAP ۶۵

٣-٣-٥ نا امن بودن Webmail ٦٦
٣-٤ جدول و نمودار کلی ٦٧
فصل چهارم راهکارهای ایمن سازی ۶۹
٤-١ ایمن سازی سرور پست الکترونیکی ٦٩
٤-١-١ ایمن سازی سرورهای خانواده یونیکس ٧٠
مانیتورینگ فایل‌های Log ٧٠
جلوگیری از حملات شبکه ای ٧١
بلوکه کردن دسترسی شبکه ای به سرور ٧١
استفاده کردن از سیستم‌های IDS یا IPS ٧٢
محاسبه میزان کاهش مخاطره ٧٣
٤-١-٢ ایمن سازی بسته پست الکترونیکی Sendmail ٧٥
مجوزهای فایل ٧٥
کاربران sendmail ٧٥
٤-١-٣ Qmail و امنیت ٧٦
محاسبه میزان کاهش مخاطره ٧٧
٤-١-٤ postfix و امنیت ٧٨
٤-١-٥ اجتناب از open relay ٧٨
پیکربندی رله گزینشی ٧٩
پیکربندی رله گزینشی در Sendmail ٧٩
پیکربندی رله گزینشی در Qmail ٨٠
استفاده از برنامه tcpwrapper ٨١
پیکربندی tcpwrapper ٨١
پیکربندی tcpserver ٨٢

اجتناب کردن از open relayها ۸۳
محاسبه میزان کاهش مخاطره ۸۳
٤-۱-٦ بلوکه کردن Spamها ۸۵
ممانعت کردن از قبول پیام‌ها از میزبان‌های spam مشهور ۸٦
ایجاد لیست خودتان از میزبان‌های spam ۸٦
استفاده از ارائه دهنده لیست میزبان‌های spam ۸۷
اعتبار سنجی اطلاعات جلسه smtp ۸۷
فیلتر کردن پست الکترونیکی‌های spam ۸۸
پیاده سازی بلوکه کردن spam روی Qmail ۸۸
ایجاد لیست خودتان از میزبان‌های spam ۸۸
استفاده از سرور MAPS RSS ۸۹
استفاده از فیلتر کردن پیام‌ها ۸۹
محاسبه میزان کاهش مخاطره ۹۱
٤-۱-۷ فیلتر کردن ویروس‌ها ۹۳
فیلتر کردن ویروس بر اساس عبارات شناخته شده ۹۳
پویش کردن ویروس‌ها ۹٤
پیاده سازی فیلترینگ ویروس ۹۵
پیاده سازی پویش کردن ویروس ۹٦
محاسبه میزان کاهش مخاطره ۹۷
٤-۲ ایمن سازی سرویس پست الکترونیکی ۹۷
٤-۲-۱ استفاده از فایروال‌های پست الکترونیکی ۹۸
غیر فعال کردن برخی دستورات[2] ۹۸
ردیابی سرآیندها ۹۹

فیلد سرآیند Received ۹۹
فیلد سرآیند Message-Id ۱۰۱
فایروال‌های پست الکترونیکی ۱۰۱
درون فایروال شبکه ۱۰۲
درون DMZ ۱۰۲
به عنوان یک سرور پست الکترونیکی داخلی ۱۰۳
محاسبه میزان کاهش مخاطره ۱۰۴
٤-۲-۳ استفاده از SASL ۱۰۵
SASL چیست؟ ۱۰۶
SASL چگونه عمل می‌کند؟ ۱۰۶
مکانیزم‌های تایید هویت SASL ۱۰۷
استفاده از SASL درون SMTP ۱۰۷
محاسبه میزان کاهش مخاطره ۱۰۹
٤-۲-٤ S-MIME ۱۱۰
S-MIME Multipart SubType ۱۱۰
S-MIME Application SubType ۱۱۱
MIME به همراه PGP ۱۱۲
محاسبه میزان کاهش مخاطره ۱۱۳
٤-۲-۵ امن کردن سرورهای POP3 و IMAP ۱۱۳
پروتکل‌های خانواده SSL ۱۱٤
پروتکل SSL ۱۱٤
پروتکل Record SSL ۱۱۵
پروتکل دست دهی SSL ۱۱٦

پروتکل تغییر مشخصات رمز SSL ۱۱۷
پروتکل هشدار دهنده SSL ۱۱۸
پروتکل TLS ۱۱۹
بسته OpenSSL ۱۲۰
محاسبه میزان کاهش مخاطره ۱۲۳
٤-۲-٦ امن کردن سرورهای Webmail ۱۲٤
امن کردن سرور MySql ۱۲٤
امن کردن سرور Apache ۱۲٤
محاسبه میزان کاهش مخاطره ۱۲۵
٤-۳ جدول و نمودار کلی ۱۲٦
فصل پنجم نتیجه‌گیری و پیشنهادات ۱۲۹
۵-۱ نتیجه گیری ۱۲۹
۵-۱-۱ پست الکترونیکی‌های با امنیت متوسط برای سازمان‌های اجرایی ۱۳۲
۵-۱-۲ پست الکترونیکی‌های با امنیت بالا برای سازمان‌های ملی ۱۳۳
۵-۱-۳ پست الکترونیکی با امنیت بالا به همراه محرمانگی، برای سازمان‌های حساس .. ۱۳۵
فصل ششم مراجع و منابع ۱۳۹