

امنیت پست الکترونیکی

www.ketab.ir

سید حسین رجاء

انتشارات پندار پارس

سرشناسه : رجاء، سیدحسین، ۱۳۶۲ -
 عنوان و نام پدیدآور : امنیت پست الکترونیکی / حسین رجاء.
 مشخصات نشر : تهران : پندار پارس : مائلی، ۱۳۹۰.
 مشخصات ظاهری : ۱۶۰ ص. : مصوره، نمودار.
 شابک : ۹۷۸-۶۰۰-۶۵۲۹-۰۰۰-۴ : ۴۵۰۰۰ ریال
 وضعیت فهرست نویسی : فیا
 موضوع : پست الکترونیکی -- پیش‌بینی‌های امنیتی
 موضوع : پست الکترونیکی
 رده بندی کنگره : TK۵۱۰۵۷۳/۱۳۹۰۷۳ : ۱۳۹۰۷۳/۱۳۹۰
 رده بندی دیویی : ۶۹۲/۸۴
 شماره کتابشناسی ملی : ۲۵۹۶۴۲۷

انتشارات پندار پارس

دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوچه رشتنچی، شماره ۱۱، واحد ۱۶
 تلفن: ۷۷۵۷۲۳۳۵ - تلفکس: ۶۶۶۲۹۵۷۸ همراه: ۹۱۲۲۴۵۲۳۴۸
 www.pendarepars.com
 info@pendarepars.com



نام کتاب : امنیت پست الکترونیکی

ناشر : انتشارات پندار پارس ناشر همکار: مائلی

تالیف : سید حسین رجاء

چاپ نخست : زمستان ۹۰

شمارگان : ۱۰۰۰ نسخه

طرح جلد : محمد اسماعیلی هدی

لینوگرافی، چاپ، صحافی : ترام‌سنج، فرشویه، خیام

قیمت : ۴۵۰۰ تومان شابک : ۹۷۸-۶۰۰-۶۵۲۹-۰۰۰-۴

تذکره گونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد

به نام خداوند جان و خرد

پیش‌گفتار

فن‌آوری پست الکترونیکی، با توجه به استفاده روز افزون از آن در عصر اطلاعات، به یکی از ملزومات زندگی بشر، برای مکاتبات و مراسلات بین افراد، تبدیل شده است. با توجه به این مسئله، نکته قابل اهمیت در مورد پست الکترونیکی این است که سرور و سرویس پست الکترونیکی و پیام‌ها و مکاتبات رد و بدل شده بین افراد، دارای امنیت قابل قبولی باشد تا افراد با اطمینان خاطر از این فن‌آوری، استفاده کنند.

ابتدا به بررسی نحوه عملکرد سیستم پست الکترونیکی و معرفی پروتکل‌های آن می‌پردازیم. با بررسی صورت گرفته مشخص شد که برای ارزیابی مخاطرات سیستم پست الکترونیکی، روش خاصی ارائه نشده است.

با بررسی روش‌های ارزیابی سایر سیستم‌ها و نقاط ضعف و قوت آنها، از روش آقای کانوری که روشی برای ارزیابی در حیطه امنیت شبکه می‌باشد، برای ارزیابی مخاطرات پست الکترونیکی استفاده می‌کنیم. با ارائه جداول خاص و استفاده از فرمول کانوری، به بررسی مخاطرات می‌پردازیم که معیار کار ما برای ارزیابی مخاطرات می‌باشد. پس از آن، به معرفی و بحث بر روی مخاطرات موجود در سرور و سرویس پست الکترونیکی می‌پردازیم.

سپس به مکانیزم‌های امن کردن مخاطرات سرور و سرویس پست الکترونیکی می‌پردازیم. میزان کاهش مخاطره را با به‌کارگیری مکانیزم‌ها و راهکارهای موجود، به صورت مطالعه موردی و به وسیله آزمایش‌هایی بدست می‌آوریم. در نهایت و در فصل نتیجه‌گیری، پست الکترونیکی را از لحاظ امنیت و نوع سازمان، دسته‌بندی کرده و مکانیزم‌های ایمن‌سازی آن را ارائه می‌دهیم.

مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان رشته نرم افزار، متخصصین لینوکس و تمامی افراد علاقه‌مند به حوزه پست الکترونیکی می‌باشند.

این کتاب با توجه به مطالعات علمی و تجربه فنی نگارنده در سرورهای پست الکترونیکی Qmail، Exim، Sendmail، Postfix و Exchange Server تألیف شده است. بدیهی است که مطالب این کتاب، خالی از اشکال نمی‌باشد و نظرات خوانندگان، ما را در بهبود سطح علمی و فنی کتاب، یاری خواهد کرد؛ لذا از خوانندگان محترم درخواست می‌شود هرگونه پیشنهاد و انتقادی در جهت بهبود و اصلاح محتویات کتاب را به آدرس الکترونیکی hosseinraja@dspri.com ارسال نمایند.

در نهایت بر خود لازم می‌دانم از موسسه تحقیقاتی داده‌سنجی پیشرفته، جناب مهندس مقدسی و جناب مهندس سید محمد رجاء، که اینجانب را در مراحل مختلف تألیف این کتاب یاری رسانده‌اند، کمال تشکر را داشته باشم.

سید حسین رجاء

پاییز ۱۳۹۰

www.ketab.ir

فهرست

فصل اول مقدمه.....	۱
۱-۱ طرح مسئله.....	۱
۲-۱ اهداف.....	۴
۳-۱ پرسش‌ها و فرضیات.....	۴
۴-۱ تحقیقات مرتبط.....	۶
۵-۱ ساختار کتاب.....	۸
فصل دوم مفاهیم پایه.....	۱۱
۱-۲ اصول پست الکترونیکی.....	۱۱
۱-۲-۱ سیستم‌های پست الکترونیکی اینوکسی.....	۱۱
MDA.....	۱۲
فیلترگذاری خودکار پست الکترونیکی.....	۱۳
پاسخگویی خودکار پست الکترونیکی.....	۱۴
مقاردهی اولیه برنامه توسط پست الکترونیکی.....	۱۵
MTA.....	۱۵
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

۱۹.....	پروتکل‌های MUA
۱۹.....	پروتکل POP
۲۱.....	۲-۲ پروتکل SMTP
۲۱.....	۱-۲-۲ دستورات کلاینتی SMTP
۲۳.....	۲-۲-۲ پاسخ‌های سرور
۲۴.....	۲-۲ پروتکل‌های POP و IMAP
۲۵.....	۴-۲ MIME
۲۶.....	۱-۴-۲ برنامه Uuencode
۲۶.....	۲-۴-۲ MIME و داده‌های باینری
۲۶.....	۳-۴-۲ فیلدهای سرآیند MIME
۲۷.....	فیلد Content-Transfer-Encoding
۲۸.....	فیلد Content-Type
۲۹.....	Multipart Content-Type
۲۹.....	۵-۲ دسته بندی حملات
۳۰.....	۶-۲ نتایج حمله
۳۳.....	فصل سوم مخاطرات
۳۳.....	۱-۳ ارزیابی مخاطرات سیستم‌های پست الکترونیکی
۳۵.....	۱-۱-۳ احتمال کلی و تأثیر
۳۵.....	۲-۱-۳ روش‌های دیگر
۳۶.....	۳-۱-۳ روش کانوری
۳۷.....	۴-۱-۳ عناصر جدول ارائه شده
۳۹.....	۲-۳ مخاطرات سرور پست الکترونیکی
۳۹.....	۱-۲-۳ مخاطرات سرورهای خانواده یونیکس

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

۶۶.....	۵-۳-۲ Webmail نا امن بودن
۶۷.....	۴-۳ جدول و نمودار کلی
۶۹.....	فصل چهارم راهکارهای ایمن سازی
۶۹.....	۱-۴ ایمن سازی سرور پست الکترونیکی
۷۰.....	۱-۱-۴ ایمن سازی سرورهای خانواده یونیکس
۷۰.....	مانیتورینگ فایل های Log
۷۱.....	جلوگیری از حملات شبکه ای
۷۱.....	بلوکه کردن دسترسی شبکه ای به سرور
۷۲.....	استفاده کردن از سیستم های IDS یا IPS
۷۳.....	محاسبه میزان کاهش مخاطره
۷۵.....	۲-۱-۴ ایمن سازی بسته پست الکترونیکی Sendmail
۷۵.....	مجوزهای فایل
۷۵.....	کاربران sendmail
۷۶.....	۳-۱-۴ Qmail و امنیت
۷۷.....	محاسبه میزان کاهش مخاطره
۷۸.....	۴-۱-۴ postfix و امنیت
۷۸.....	۵-۱-۴ اجتناب از open relay
۷۹.....	پیکربندی رله گزینشی
۷۹.....	پیکربندی رله گزینشی در Sendmail
۸۰.....	پیکربندی رله گزینشی در Qmail
۸۱.....	استفاده از برنامه tcpwrapper
۸۱.....	پیکربندی tcpwrapper
۸۲.....	پیکربندی tcpserver

۸۳.....	اجتناب کردن از open relay ها
۸۳.....	محاسبه میزان کاهش مخاطره
۸۵.....	۶-۱-۴ بلوکه کردن Spam ها
۸۶.....	ممانعت کردن از قبول پیام‌ها از میزبان‌های spam مشهور
۸۶.....	ایجاد لیست خودتان از میزبان‌های spam
۸۷.....	استفاده از ارائه دهنده لیست میزبان‌های spam
۸۷.....	اعتبار سنجی اطلاعات جلسه smtp
۸۸.....	فیلتر کردن پست الکترونیکی‌های spam
۸۸.....	پیاده سازی بلوکه کردن spam روی Qmail
۸۸.....	ایجاد لیست خودتان از میزبان‌های spam
۸۹.....	استفاده از سرور MAPS RSS
۸۹.....	استفاده از فیلتر کردن پیام‌ها
۹۱.....	محاسبه میزان کاهش مخاطره
۹۲.....	۷-۱-۴ فیلتر کردن ویروس‌ها
۹۳.....	فیلتر کردن ویروس بر اساس عبارات شناخته شده
۹۴.....	پویش کردن ویروس‌ها
۹۵.....	پیاده سازی فیلترینگ ویروس
۹۶.....	پیاده سازی پویش کردن ویروس
۹۷.....	محاسبه میزان کاهش مخاطره
۹۷.....	۲-۴ ایمن سازی سرویس پست الکترونیکی
۹۸.....	۱-۲-۴ استفاده از فایروال‌های پست الکترونیکی
۹۸.....	غیر فعال کردن برخی دستورات [2]
۹۹.....	ردیابی سرآیندها

۹۹.....	فیلد سرآیند Received
۱۰۱.....	فیلد سرآیند Message-Id
۱۰۱.....	فایروال‌های پست الکترونیکی
۱۰۲.....	درون فایروال شبکه
۱۰۲.....	درون DMZ
۱۰۳.....	به عنوان یک سرور پست الکترونیکی داخلی
۱۰۴.....	محاسبه میزان کاهش مخاطره
۱۰۵.....	۳-۲-۴ استفاده از SASL
۱۰۶.....	SASL چیست؟
۱۰۶.....	SASL چگونه عمل می‌کند؟
۱۰۷.....	مکانیزم‌های تایید هویت SASL
۱۰۷.....	استفاده از SASL درون SMTP
۱۰۹.....	محاسبه میزان کاهش مخاطره
۱۱۰.....	۴-۲-۴ S-MIME
۱۱۰.....	S-MIME Multipart SubType
۱۱۱.....	S-MIME Application SubType
۱۱۲.....	MIME به همراه PGP
۱۱۲.....	محاسبه میزان کاهش مخاطره
۱۱۳.....	۵-۲-۴ امن کردن سرورهای POP3 و IMAP
۱۱۴.....	پروتکل‌های خانواده SSL
۱۱۴.....	پروتکل SSL
۱۱۵.....	پروتکل Record SSL
۱۱۶.....	پروتکل دست دمی SSL

۱۱۷.....	پروتکل تغییر مشخصات رمز SSL
۱۱۸.....	پروتکل هشدار دهنده SSL
۱۱۹.....	پروتکل TLS
۱۲۰.....	بسته OpenSSL
۱۲۳.....	محاسبه میزان کاهش مخاطره
۱۲۴.....	۶-۲-۴ امن کردن سرورهای Webmail
۱۲۴.....	امن کردن سرور MySQL
۱۲۴.....	امن کردن سرور Apache
۱۲۵.....	محاسبه میزان کاهش مخاطره
۱۲۶.....	۳-۴ جدول و نمودار کلی
۱۲۹.....	فصل پنجم نتیجه‌گیری و پیشنهادات
۱۲۹.....	۱-۵ نتیجه‌گیری
۱۳۲.....	۱-۱-۵ پست الکترونیکی‌های با امنیت متوسط برای سازمان‌های اجرایی
۱۳۳.....	۲-۱-۵ پست الکترونیکی‌های با امنیت بالا برای سازمان‌های ملی
۱۳۵.....	۳-۱-۵ پست الکترونیکی با امنیت بالا به همراه محرمانگی، برای سازمان‌های حساس
۱۳۹.....	فصل ششم مراجع و منابع