

مرجع امنیت در شبکه‌های کامپیوتری بر اساس سرفصل‌های Security +

مؤلف: علی محمدیون



NAGHOOS
PUBLICATION

سرشناسه : محمدیون اتی کندی، علی، ۱۳۶۴
 عنوان و نام پدیدآور : مرجع امنیت در شبکه‌های کامپیوتری براساس سرفصل‌های + Security
 مؤلف علی محمدیون اتی کندی
 مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۳
 مشخصات ظاهری : ۵۱۸ ص: مصور، جدول
 شابک : ۹۷۸-۹۶۴-۳۷۷-۷۱۲-۸
 بهای ۳۰۰۰۰۰ ریال
 وضعیت فهرست‌نویسی : فیا
 موضوع : شبکه‌های کامپیوتری-تدابیر ایمنی
 موضوع : پایگاه‌های اطلاعاتی-امنیت
 موضوع : کامپیوترها-ایمنی اطلاعات
 رده بندی کنگره : TK5۱۰۵/۵۹/م۳ م۴ ۱۳۹۳
 رده بندی دیویی : ۰۰۵/۸
 شماره کتابشناسی ملی : ۳۶۱۴۴۲۰



برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناقوس

نام کتاب : مرجع امنیت در شبکه‌های کامپیوتری براساس سرفصل‌های + Security

چاپ اول

ناشر : انتشارات ناقوس

«در نوبت چاپ اول از دستگاه چاپ
 دیجیتال استفاده شده است»

مؤلف : علی محمدیون

S.M.S : ۳۰۰۰۴۵۲۳۲۳

چاپ اول : ۱۳۹۳

تیراژ : ۲۰۰ جلد

لینوگرافی : نارنجستان

چاپ و صحافی : نارنجستان

صفحه‌آرا : صدف پورعیدی

قیمت : ۳۰۰۰۰۰ ریال

شابک : ۹۷۸-۹۶۴-۳۷۷-۷۱۲-۸

ISBN : 978-964-377-712-8

کلیه حقوق برای ناشر محفوظ است.
 تکثیر تمامی یا قسمتی از این اثر به
 صورت هروقتی یا چاپ مجدد، چاپ
 نیست، بله‌قی، فتوکپی و انواع دیگر
 چاپ ممنوع است و بیکر به باورنی دارد

مراکز پخش:

۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگر جنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲

تلفن و فاکس: ۶۶۴۰۸۵۲۰ - ۶۶۴۰۱۷۹۸ - ۶۶۴۱۷۰۷۲ - ۶۶۴۶۶۷۹۳

۲- کتابفروشی الیاس: خیابان انقلاب، نبش فروردین تلفن: ۶۶۴۰۵۰۸۴

فهرست مطالب

۱۲۸	اشتباهات متداول مدیران سازمان‌ها	۱۱	فصل اول: شبکه‌بندی عمومی و مفاهیم امنیتی
۱۲۳	فصل سوم: کدگذاری و پروتکل‌های رمزنگاری	۱۱	شمای کلی
۱۳۳		۱۶	شناسایی تهدیدها
۱۳۲	مفهوم کدگذاری	۲۸	نقاط نفوذ
۱۳۲	سرویس رمزنگاری	۲۸	دفاع از حملات و تهدیدها
۱۳۴	پروتکل رمزنگاری		لزوم پیاده‌سازی استاندارد مدیریت امنیت
۱۳۴	الگوریتم رمزنگاری	۲۵	اطلاعات در سازمان‌ها
۱۴۲	تجزیه و تحلیل رمز		فصل دوم: لایه‌های TCP/IP و نقاط نفوذ (نقاط آسیب‌پذیر) آنها
۱۴۵	معرفی پروتکل‌های رمزنگاری	۴۷	
۱۴۸	روش‌های رمزگذاری	۴۸	دیباجه و تاریخ شکل‌گیری TCP/IP
۱۵۰	امضای دیجیتال	۴۹	مدل تحت شبکه TCP/IP
۱۵۱	حملات متداول و راه‌حل‌های ممکن	۴۹	حملات رایج روی لایه‌های TCP/IP
۱۵۲	سناریوهای متداول در فاش شدن رمزها	۵۲	لایه‌های شبکه‌های حاکم بی‌سیم
۱۵۳	چگونه یک رمز امن را انتخاب کنید:		پروتکل‌های مرتبط با نامه الکترونیک (E-mail)
۱۵۴	پروتکل‌های انتقال امن	۵۳	
۱۵۶	خطرها، حملات و ملزومات امنیتی	۵۵	Packet sniffing
۱۵۸	وسایل ذخیره‌سازی	۵۹	حملات تپ‌ی یا Null Session Attacks
۱۶۰	تکنولوژی SAN	۶۶	کنترل دسترسی
۱۶۰	NAS	۷۰	کنترل امنیت اطلاعات
۱۶۶	RADIUS	۷۲	فیلترینگ بسته‌های اطلاعاتی TCP/IP
۱۶۷	روش کار سرور RADIUS Access-Request	۷۳	پورت‌های شناخته‌شده
۱۶۸	وظیفه AH	۸۴	پورت‌های ثبت‌شده
۱۶۸	پروتکل امنیتی SSL	۱۲۱	مقایسه مدل‌های مرجع OSI و TCP/IP
۱۷۱	پروتکل امنیتی TLS	۱۲۵	اشتباهات متداول مدیران سیستم

۲۷۱	معایب رایانش ابری	۱۷۳	PGP و S/MIME
۲۷۱	پردازش ابری	۱۷۳	OpenPGP
۲۷۳	فصل پنجم: شناسایی حملات در شبکه	۱۷۵	فصل چهارم: زیرساخت شبکه
۲۷۳	شناسایی حملات	۱۷۵	زیرساخت شبکه
	انواع حملات در شبکه‌های کامپیوتری	۱۷۵	مدل OSI
۲۷۳		۱۷۶	خصوصیات مدل OSI
۲۷۴	وظایف یک سرویس‌دهنده	۱۸۱	ارتباطات اتصال‌گرا
۲۷۵	سرویس‌های حیاتی و مورد نیاز	۱۸۲	Windowing
	مشخص نمودن پروتکل‌های مورد نیاز	۱۸۳	اعلام وصول
۲۷۶		۱۸۴	بسته‌های داده
	مزایای غیرفعال نمودن پروتکل‌ها و	۱۸۹	هاب‌ها در لایه Physical
۲۷۷	سرویس‌های غیرضروری	۱۹۱	شناخت استانداردها
	حمله‌های فعال آنلاین (Active Online Attacks)	۱۹۲	Net BIOS
۲۷۹		۱۹۴	سرویس‌ها
۲۸۰	حملات آفلاین	۱۹۷	پروتکل TCP/IP
۲۹۱	استراتژی طراحی شبکه	۱۹۸	معرفی پروتکل TCP/IP
۲۹۲	TCP/IP گزینه‌ای عمومی	۱۹۹	لایه‌های پروتکل TCP/IP
۲۹۲	سیستم عامل Net Ware	۲۰۲	اهداف طراحی TCP/IP
۲۹۴	مستندسازی	۲۰۳	نمایش اطلاعات پورت‌ها
۲۹۶	تست شبکه	۲۰۵	IPv6
۲۹۹	گزارشی از چند حمله مهم	۲۰۶	امنیت پروتکل IPv6
۳۰۰	علائم هک شدن	۲۰۹	پروتکل‌های IPSec
۳۰۱	آسیب‌پذیری CSRF	۲۱۰	پروتکل ESP
۳۰۲	افزایش امنیت روی تجهیزات سیسکو	۲۱۳	نحوه عملکرد داخلی پروتکل SSL
۳۰۳	سرورها	۲۱۴	کارت شبکه
۳۰۴	ابزارهای ذخیره‌سازی	۲۲۲	آشنایی با سویچ شبکه
۳۰۴	قابلیت‌های یک سرور	۲۲۴	انتخاب رمز عبور
۳۰۶	اتصالات شبکه‌ای	۲۲۶	امنیت رمز عبور
۳۰۷	مدیریت و سرویس‌پذیری		استفاده از پروتکل نقطه به نقطه (-) Using Point to
	تروجان DNSChanger مرسوم به Zlob	۲۳۰	(Point Protocol)
۳۰۹		۲۳۹	مبانی شبکه‌های بی‌سیم
۳۱۳	فصل ششم: امنیت شبکه	۲۵۰	مشکلات استفاده از شبکه‌های وایرلس
	پیاده‌سازی و نگهداری شبکه‌های کامپیوتری به	۲۵۰	تقسیم‌بندی سیستم‌های وایرلس
۳۱۳	صورت ایمن		اقدامات امنیتی به هنگام اتصال به شبکه‌های
	اما موارد مربوط پیاده‌سازی امنیت در	۲۵۱	Wireless
۳۱۴	سیستم‌ها که عبارتند از:	۲۶۷	رایانش ابری
		۲۶۹	ساختار رایانش ابری

۳۶۰	روش‌های انتشار	۳۱۵	افزونه‌ها (Service Pack)
۳۶۱	نشانه‌های یک سیستم آلوده	۳۱۵	دیوار آتش (Fire Wall)
۳۶۱	راهنمای پاک‌سازی بدافزار با نصب ابزار	۳۱۷	موقعیت قرارگیری و محل نصب
۳۶۱	راهنمای حذف دستی بدافزار	۳۱۷	فایروال‌های لایه‌ای
۳۶۱	پاک‌سازی رجیستری‌های زیر به حالت پیش‌فرض	۳۱۷	نکاتی در رابطه با استفاده از فایروال
۳۶۱	ابزارها	۳۱۹	کلیاتی از پروتکل TCP/IP
۳۶۲	ابزارهای متمرکز بر سیستم	۳۲۰	کار فایروال (دیوار آتش)
۳۶۲	آنالیز نرم‌افزاری	۳۲۲	انواع فایروال‌ها
۳۶۲	راهنمایی محیط	۳۲۵	خصوصیات مهم یک فایروال
هشت نکته مهم درباره امنیت در شبکه اینترنت		۳۲۶	انواع زون (Zone) های امنیتی
۳۶۵		۳۲۷	سیاست وجودی DMZ
۳۶۷	افزایش امنیت در رایانه‌های شخصی	۳۲۸	ایجاد زون‌های امنیتی
۳۶۷	۱. اتصال به شبکه امن	۳۲۸	نواحی (Zone) های امنیتی مهم
۳۶۷	۲. فعال‌سازی فایروال و پیکربندی آن	۳۲۹	طراحی مناطق امنیتی
۳. نصب و استفاده از آنتی‌ویروس و		۳۳۲	امنیت شبکه IPS و IDS
۳۶۸	آنتی‌اسپم	۳۳۳	Honey pot
۳۶۸	۴. حذف برنامه‌های غیرضروری	۳۳۸	راهمحل‌های امنیت شبکه
۵. غیرفعال کردن سرویس‌های غیرضروری		۳۳۹	مانیتورینگ و مدیریت امنیت اطلاعات
۳۶۸	۶. تغییر ویژگی‌های پیش‌فرض غیرضروری	۳۴۵	پیاده‌سازی امنیت در شبکه سیار یا بی‌سیم
۳۶۹	۷. انجام کارها با توجه به اصل حداقل حق دسترسی	۳۴۵	مانیتورینگ
۳۶۹	۸. امن کردن مرورگر وب	۳۴۹	منابع موجود روی دستگاه‌ها
۳۷۰	۹. تولید رمز عبور قوی	۳۴۹	نحوه انجام عملیات مانیتورینگ
۳۷۱	رمزگذاری اطلاعات	۳۵۱	پنج ابزار اساسی مرکز عملیات شبکه
نصب نرم‌افزارهای شناسایی عوامل نفوذی را		۳۵۴	سرویس‌های NOC
۳۷۱	فراموش نکنید.	۳۵۵	فصل هفتم: امنیت سیستم‌ها
به دور رایانه خود دیوار آتش (فایروال)		۳۵۵	مقدمه
۳۷۱	بکشید.	۳۵۶	بدافزار (Malware)
حذف برنامه‌های دسترسی از راه دور.		۳۵۷	حذف کردن بدافزارها
از امنیت شبکه‌های رایانه‌ای اطمینان حاصل		۳۵۸	انواع بدافزارها
۳۷۱	کنید.	۳۵۸	ویروس
یک برنامه ضدسرزنامه بلادرنگ نصب کنید		۳۵۸	کرم
۳۷۲		۳۵۹	اسب تروا
غیرفعال‌سازی Image Previews در Outlook		۳۵۹	در پشتی
۳۷۲		۳۵۹	نرم‌افزارهای جاسوسی
		۳۵۹	روتکیت (Root Kit)
		۳۶۰	ابزار نفوذ
		۳۶۰	تبلیغات ناخواسته

۴۲۰	معرفی مرکز عملیات امنیت شبکه (SOC)	۳۷۲	بر روی لینک‌ها و فایل‌های ضمیمه‌شده
۴۳۱	فصل هشتم: امنیت در وب	۳۷۲	نامه‌های الکترونیکی کلیک نکنید.
۴۳۱	حمله web application	۳۷۳	حملات روی رمزهای عبور
۴۴۳	ویژگی‌های یک WAF خوب	۳۷۳	اهمیت یک رمز عبور
۴۴۵	واسط مدیریتی	۳۷۳	انتخاب یک رمز عبور خوب
۴۵۱	روشها و لزوم امنیت برنامه‌های وب	۳۷۴	حفاظت از رمزهای عبور
۴۵۱	امنیت برنامه‌های وب و برداشت‌های اولیه	۳۷۵	آشنایی با مکانیسم حملات Brute Forcing
۴۵۲	نقاط آسیب‌پذیر (vulnerability)	۳۷۵	حمله Dictionary
۴۵۴	تهاجم (attack)	۳۷۶	حمله Dictionary Harvest
۴۵۴	ایمن‌سازی شبکه، host و برنامه	۳۷۶	حمله Brute Force
۴۵۵	تهدیدات	۳۷۷	ممیزی شناور یا ثابت
۴۵۶	اصول امنیت برنامه‌های وب	۳۷۷	بازیابی کلمه عبور
۴۵۷	امنیت برنامه‌های وب و برداشت‌های اولیه	۳۷۷	موارد قابل بازیابی
۴۵۸	ایمن‌سازی شبکه، host و برنامه	۳۷۸	شتابدهی با GPU های Nvidia
۴۶۰	نقاط آسیب‌پذیر	۳۸۰	حمله دورگه
۴۶۰	حملات	۳۸۱	کلمات عبور امن
۴۶۱	نقاط آسیب‌پذیر	۳۸۱	محدودیت اساسی
۴۶۱	حملات		معرفی نرم‌افزارهای تولید رمز عبور قوی و مطمئن
۴۶۲	نقاط آسیب‌پذیر	۳۸۲	۱. نرم‌افزار Sticky Password
۴۶۲	حملات	۳۸۲	۲. نرم‌افزار Password Depot Professional
۴۶۲	نقاط آسیب‌پذیر	۳۸۳	۳. نرم‌افزار Random Password Generator
۴۶۳	حملات	۳۸۳	برخی از ویژگی‌های کلیدی این برنامه
۴۶۳	نقاط آسیب‌پذیر	۳۸۴	۴. نرم‌افزار Password 1.0.9.337:
۴۶۳	حملات	۳۸۶	سیستم‌عامل ویندوز
۴۶۴	نقاط آسیب‌پذیر	۳۸۶	استفاده از سیستم‌عامل متن باز لینوکس
۴۶۴	حملات	۳۸۹	چگونه یک سیستم‌عامل را انتخاب نماییم
۴۶۴	نقاط آسیب‌پذیر	۳۹۰	فناوری‌های امنیت اطلاعات واکنشی
۴۶۴	ضعف امنیت فیزیکی	۳۹۹	محل‌های امن برای تجهیزات
۴۶۵	حملات	۳۹۹	انتخاب لایه کانال ارتباطی امن
۴۶۵	نقاط آسیب‌پذیر		نگاهی به طراحی اتاق سرور (Data Center)
۴۶۵	حملات	۴۰۳	استاندارد
۴۶۶	نقاط آسیب‌پذیر		کابل‌کشی شبکه کامپیوتری طبق استاندارد
۴۶۶	حملات	۴۱۱	TIA EIA-568-B
۴۶۶	نقاط آسیب‌پذیر	۴۱۲	نگهداری سرورها
۴۶۷	حملات	۴۱۵	طراحی امن شبکه
۴۶۷	نخستین ایمیل	۴۱۵	امنیت VPN
۴۷۱	هفت نکته مهم امنیت ایمیل که باید بدانید		

۵۱۰	نقش امنیت در تداوم کسب و کار	۴۷۴	سرویس ایمیل (Mail Server)
۵۱۱	نسخه پشتیبان و بازگردانی اطلاعات	۴۷۸	مجازی سازی چیست؟
۵۱۱	پشتیبان گیری آنلاین		شرح خدمات مجازی سازی سرورها و
۵۱۲	پشتیبان گیری محلی	۴۹۱	کلاسترینگ بانک اطلاعاتی
۵۱۲	پشتیبان گیری مبتنی بر شبکه	۴۹۲	Hyper-V در Windows server 2012
۵۱۳	آشنایی با اصل بکاپ گیری و Tape Drive ها	۵۰۲	رایانش ابری
۵۱۵	نمونه سوالات به زبان اصلی		فصل نهم: سیاست های امنیتی و تداوم امنیت در
		۵۰۹	کسب و کار
		۵۰۹	سیاست های امنیتی