

۱۰۰۰ - ۱۰۷

امن سازی سیستم عامل های مایکروسافت ویندوز ۷ و اندروید

مؤلفین:

دکتر بابک صادقیان

گوهر شکوری گرگانی

www.ketab.ir

سرشناسه

: صادقیان، بابک، ۱۳۴۰-

عنوان و نام پدیدآور

: امن‌سازی سیستم‌عامل‌های مایکروسافت ویندوز ۷ و اندروید

: مولفین بابک صادقیان، گوهر شکوری گرکانی

مشخصات نشر

: تهران: انتشارات ناقوس، ۱۳۹۴.

مشخصات ظاهری

: ۱۷۸ ص: مصور، جدول.

شابک

: ۹۷۸-۹۶۴-۳۷۷-۷۹۲-۰ : بها: ۱۵۰,۰۰۰ ریال به همراه DVD

وضعیت فهرست‌نویسی: فیپا

: کتابنامه: ص ۱۶۷-۱۷۰.

یادداشت

: ویندوز مایکروسافت-اقدامات تأمینی

موضوع

: اندروید (منبع الکترونیکی)-تدابیر ایمنی

موضوع

: سیستم‌های عامل (کامپیوتر)-تدابیر ایمنی

موضوع

: شکوری گرکانی، گوهر، ۱۳۶۵-

شناسه ازدود

: ۱۳۹۴ ص ۲۲/س ۹۴/۷۶/۷۶ QAV6

رده دی‌ک‌کره

: ۰۰۵/۸

رده بنیادیویی

شماره کتابشناختی: ۳۹۲۶۳۶۰



NAGHOOS
PUBLICATION

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناقوس

چاپ اول

: امن‌سازی سیستم‌عامل‌های مایکروسافت ویندوز ۷ و اندروید

نام کتاب

: انتشارات ناقوس

ناشر

: بابک صادقیان، گوهر شکوری گرکانی

تألیف

: ۱۳۹۴

چاپ اول

: ۲۰۰ جلد

تیراژ

: نارنجستان

چاپ و صحافی

: صدف پورعبدی

سرپرست صفحه‌آرا

: ۱۵۰,۰۰۰ ریال

قیمت با DVD همراه

: ۹۷۸-۹۶۴-۳۷۷-۷۹۲-۰

شابک

: 978-964-377-792-0

ISBN

S.M.S : ۳۰۰۰۴۵۲۳۲۳

کد حقوق برای سرمایه‌گذار محفوظ
است. تمامی یا قسمتی از این اثر
به صورت چاپی یا چاپ مجدد،
چاپ صوتی، پلی‌کپی، فتوکپی و انواع
دیگر چاپ ممنوع است و بیکرد قانونی
دارد.

مرکز پخش: انتشارات ناقوس

۱- میدان انقلاب، خیابان کارگر جنوبی، خیابان ۱۲ فروردین- بین وحیدنظری و روانمهر- بن‌بست حقیقت- پلاک ۴

تلفن و فاکس: ۶۳۳۲۵ (۲۰ خط)

۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۳۰۵۰۸۳

۳- کتابفروشی گلریزان: ضلع جنوب‌شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

فهرست مطالب

۹	پیشگفتار
۱۱	مقدمه مؤلف
۱۳	بخش اول
۱۳	امن سازی مایکروسافت ویندوز ۷
۱۵	فصل اول
۱۵	معرفی مایکروسافت ویندوز ۷
۱۶	۱-۱ ویژگی های امنیتی ویندوز ۷
۱۶	۱-۱-۱ مرورگر
۱۷	۲-۱-۱ ویژگی Apple
۱۷	۳-۱-۱ الحاقیه های امنیتی
۱۷	۴-۱-۱ ویژگی BitLocker To Go
۱۸	۵-۱-۱ بهبود کنترل حساب کاربری
۱۸	۶-۱-۱ دسترسی مستقیم
۱۸	۷-۱-۱ بیومتریک و کارت هوشمند
۱۹	۸-۱-۱ خط مشی های مختلف در فایروال ویندوز
۱۹	۲-۱ ویژگی های امنیتی حفظ شده از ویندوز ویستا
۱۹	۱-۲-۱ حفاظت از سرریز بافر
۱۹	۲-۲-۱ حداقل امتیاز
۱۹	۳-۲-۱ حفاظت در برابر بدافزارها
۱۹	۴-۲-۱ حفاظت هسته
۲۰	۵-۲-۱ سرویس BitLocker
۲۱	فصل دوم
۲۱	امن سازی مقدماتی
۲۱	۱-۲ تنظیمات قبل از نصب: تنظیمات BIOS
۲۱	۱-۱-۲ تنظیم کلمه عبور برای BIOS
۲۲	۲-۱-۲ توالی بوت
۲۳	۲-۲ نکات امنیتی در نصب ویندوز ۷
۲۳	۱-۲-۲ پارتیشن بندی دیسک سخت

۲۵.....	۲-۲-۲ نوع سیستم فایل.....
۲۷.....	فصل سوم.....
۲۷.....	حساب ها و گروه های کاربری.....
۲۷.....	۱-۳ حساب های کاربری.....
۲۸.....	۱-۱-۳ تنظیمات مقدماتی.....
۳۱.....	۲-۱-۳ خط مشی بستن حساب.....
۳۴.....	۳-۱-۳ کنترل حساب های کاربری (UAC).....
۴۳.....	۴-۱-۳ خط مشی های کلمه عبور.....
۴۸.....	۵-۳ امنیت ورود تعاملی به سیستم.....
۵۲.....	۳-۲ گروه های کاربری.....
۵۳.....	۱-۲-۳ حذف گروه های کاربری غیر ضروری.....
۵۵.....	فصل چهارم.....
۵۵.....	به روز رسانی.....
۵۵.....	۱-۴ به روز رسانی خودک.....
۵۶.....	۲-۴ نصب به روز رسانی ها با آخرین.....
۵۹.....	فصل پنجم.....
۵۹.....	سرویس های غیر ضروری.....
۵۹.....	۱-۵ تنظیمات سرویس های سیستمی.....
۶۱.....	۲-۵ معرفی سرویس های سیستمی در ویندوز ۷.....
۶۱.....	۱-۲-۵ سرویس Application Management.....
۶۲.....	۲-۲-۵ سرویس BitLocker Drive Encryption.....
۶۲.....	۳-۲-۵ سرویس Distributed Transaction Coordinator.....
۶۲.....	۴-۲-۵ سرویس Netlogon.....
۶۲.....	۵-۲-۵ سرویس Network Access Protection Agent.....
۶۳.....	۶-۲-۵ سرویس Network Media Player Network Sharing.....
۶۳.....	۷-۲-۵ سرویس Parental Controls.....
۶۳.....	۸-۲-۵ سرویس Remote Desktop Configuration.....
۶۳.....	۹-۲-۵ سرویس Remote Procedure Call.....
۶۴.....	۱۰-۲-۵ سرویس Remote Registry.....
۶۴.....	۱۱-۲-۵ سرویس Smart Card.....
۶۴.....	۱۲-۲-۵ سرویس Smart Card Removal Policy.....

۶۴.....	Storage سرویس ۱۳-۲-۵
۶۵.....	TCP/IP NetBIOS Helper سرویس ۱۴-۲-۵
۶۵.....	Windows Search سرویس ۱۵-۲-۵
۶۵.....	SNMP Trap سرویس ۱۶-۲-۵
۶۵.....	Workstation سرویس ۱۷-۲-۵

فصل ششم ۶۷

۶۷.....	دستگاه‌های غیرضروری
۶۷.....	۱-۶ حذف درایور یک دستگاه
۶۸.....	۱-۱-۶ حذف درایورهای دستگاه‌های قابل انتقال
۶۹.....	۲-۱-۶ حذف درایور چاپگر

فصل هفتم ۷۱

۷۱.....	دسترسی محلی
۷۱.....	۱-۷ سیستم فایل
۷۱.....	۱-۱-۷ تبدیل سیستم فایل
۷۲.....	۲-۱-۷ رمزکردن سیستم فایل
۷۳.....	۲-۷ پیکربندی مجوزهای دسترسی
۷۳.....	۱-۲-۷ اعطای مجوزهای دسترسی
۷۴.....	۲-۲-۷ ویرایش مجوزهای دسترسی
۷۵.....	۳-۲-۷ تغییر مالکیت یک فایل
۷۶.....	۴-۲-۷ فایل‌های سیستمی
۷۶.....	۵-۲-۷ فایل‌های ثبت رویداد
۷۷.....	۶-۲-۷ نرم‌افزارها و برنامه‌های نصب‌شده
۷۸.....	۷-۲-۷ فایل‌های داده کاربر

فصل هشتم ۷۹

۷۹.....	تنظیمات امنیتی شبکه
۷۹.....	۱-۸ پورت‌های غیرضروری
۸۱.....	۲-۸ اتصال از راه دور
۸۴.....	۳-۸ به اشتراک‌گذاری

فصل نهم ۸۷

۸۷.....	آنتی‌ویروس
---------	------------

۸۷.....	۱-۹ پوشش برای اکتشاف ویروس ها
۸۸.....	۲-۹ به روز رسانی آنتی ویروس
۸۸.....	۳-۹ معرفی چند آنتی ویروس
۹۱.....	فصل دهم
۹۱.....	پشتیبان گیری و بازگردانی
۹۱.....	۱-۱۰ پشتیبان گیری
۹۲.....	۱-۱-۱۰ نکات قبل از پشتیبان گیری
۹۲.....	۲-۱-۱۰ ایجاد نسخه پشتیبان
۹۴.....	۳-۱-۱۰ نگهداری نسخه پشتیبان
۹۵.....	۴-۱-۱۰ بازگردانی
۹۵.....	۱-۲-۱۰ ابزارهای فایل ها و فولدرها
۹۷.....	فصل یازدهم
۹۷.....	رویدادننگاری
۹۸.....	۱-۱۱ تنظیمات کلی رویدادها
۹۸.....	۱-۱-۱۱ حداکثر اندازه فایل های رویدادننگاری
۹۹.....	۲-۱-۱۱ دسترسی به فایل های رویدادها
۱۰۰.....	۳-۱-۱۱ حفظ رویدادهای قدیمی
۱۰۱.....	۴-۱-۱۱ پشتیبان گیری از فایل های رویدادننگاری
۱۰۲.....	۲-۱۱ خط مشی های رویدادننگاری
۱۰۳.....	۱-۲-۱۱ ورود به حساب کاربری
۱۰۳.....	۲-۲-۱۱ مدیریت حساب های کاربری
۱۰۴.....	۳-۲-۱۱ دسترسی به سرویس دایرکتوری
۱۰۴.....	۴-۲-۱۱ Audit logon events
۱۰۴.....	۵-۲-۱۱ دسترسی به اشیاء
۱۰۵.....	۶-۲-۱۱ تغییر خط مشی ها
۱۰۵.....	۷-۲-۱۱ Audit privilege use
۱۰۵.....	۸-۲-۱۱ Audit process tracking
۱۰۶.....	۹-۲-۱۱ رویدادهای سیستمی
۱۰۷.....	فصل دوازدهم
۱۰۷.....	فایروال
۱۰۷.....	۱-۱۲ تنظیمات کلی فایروال ویندوز

۱۰۸.....	۲-۱۲ تنظیمات پروفایل‌های فایروال
۱۱۰.....	۱-۲-۱۲ پروفایل دامنه
۱۱۴.....	۲-۲-۱۲ پروفایل خصوصی
۱۱۸.....	۳-۲-۱۲ پروفایل عمومی
۱۲۲.....	۳-۱۲ فایروال‌های خارجی
۱۲۵.....	فصل سیزدهم
۱۲۵.....	امن‌سازی سرویس‌ها
۱۲۵.....	۱-۱۲ پروتکل telnet
۱۲۵.....	۱-۱-۱۲ نصب سرویس telnet
۱۲۶.....	۲-۱-۱۲ فعال‌سازی تصدیق اصالت NTLM
۱۲۷.....	۲-۱۲ پروتکل انتقال فایل FTP
۱۲۸.....	۱-۲-۱۲ تصدیق اصالت کاربران FTP
۱۲۹.....	۲-۲-۱۲ رویدادنکاری
۱۲۹.....	۳-۲-۱۲ تنظیمات SSL
۱۳۱.....	فصل چهاردهم
۱۳۱.....	ابزارهای امنیتی
۱۳۱.....	۱-۱۴ تحلیل‌گر امنیتی MBSA
۱۳۴.....	۲-۱۴ ابزار SCM
۱۳۷.....	بخش دوم
۱۳۷.....	امن‌سازی اندروید
۱۳۹.....	فصل اول
۱۳۹.....	معرفی اندروید
۱۴۱.....	فصل دوم
۱۴۱.....	تنظیمات امنیتی سیستم
۱۴۱.....	۱-۲ به‌روزرسانی سفت‌افزار
۱۴۲.....	۲-۲ امنیت ورود به سیستم
۱۴۶.....	۳-۲ رمز کردن
۱۴۸.....	۴-۲ تنظیم زمان قفل شدن صفحه نمایش
۱۵۰.....	۵-۲ صرف‌نظر از اتصال خودکار به شبکه‌های بی‌سیم

۶-۲	غیرفعال کردن «اطلاع رسانی شبکه»	۱۵۲
۷-۲	خاموش کردن بی سیم	۱۵۳
۸-۲	خاموش کردن بلوتوث	۱۵۴
۹-۲	غیرفعال کردن سرویس های مکان یابی	۱۵۵
۱۰-۲	فعال کردن حالت پرواز	۱۵۶
۱۱-۲	پاک کردن داده ها	۱۵۷
۱۲-۲	گذاشتن کلمه عبور برای سیم کارت	۱۵۹
۱۳-۲	غیر قابل رؤیت کردن کلمه عبور	۱۶۱
۱۴-۲	غیرفعال کردن ویژگی های مربوط به توسعه	۱۶۱
۱۵-۲	عدم نصب برنامه های کاربردی از منابع ناشناخته	۱۶۲
۱۶۵	فصل سوم	
۱۶۵	تنظیمات امنیت مرورگر اینترنت	
۱-۳	غیرفعال کردن جواکریپت	۱۶۵
۲-۳	غیرفعال کردن حالت اسکریپت	۱۶۶
۳-۳	پاک کردن تاریخچه	۱۶۷
۴-۳	فعال کردن بررسی های امنیتی SSL برای وبسایت ها	۱۶۸
۵-۳	عدم پذیرش کوکی ها	۱۶۹
۶-۳	پاک کردن داده های کوکی ها	۱۷۰
۷-۳	عدم به یاد سپاری داده های مربوط به فرم های اینترنتی	۱۷۱
۸-۳	پاک کردن داده های فرم های اینترنتی	۱۷۲
۹-۳	غیرفعال کردن مکان یابی	۱۷۲
۱۰-۳	پاک کردن داده های مکان یابی	۱۷۳
۱۱-۳	عدم به یاد سپاری کلمات عبور	۱۷۵
۱۲-۳	پاک کردن کلمات عبور وارد شده در مرورگر اینترنت	۱۷۶
۱۷۷	مراجع	

پیشگفتار

در مباحث مربوط به مهندسی کامپیوتر اصطلاح Hardening برای فرآیند مستحکم کردن یک سیستم با کاهش سطح آسیب‌پذیری آن به کار می‌رود. اگر ترجمه لغوی این اصطلاح را در نظر بگیریم بایستی آنرا به سخت‌سازی یا مستحکم‌سازی ترجمه کرد، ولی در میان افراد فنی کامپیوتری در ایران این اصطلاح معمولاً با عبارت «امن سازی» معادل‌سازی می‌گردد. از آنجاکه این کتاب برای افراد فنی نوشته می‌شود، ما نیز در این کتاب از اصطلاح امن‌سازی استفاده می‌کنیم. اما سطح آسیب‌پذیری یک محیط نرم‌افزاری یا Surface of Vulnerability یا سطح آسیب‌پذیری به مجموع نقاط مختلفی که یک کاربر غیرمجاز می‌تواند سعی در ورود داده و/یا استخراج داده از آن محیط مورد نظر کند، گفته می‌شود.

نمونه‌هایی از چنین نقاطی: فیلدها، واسط‌ها، پروتکل‌ها و سرویس‌های ورود کاربر است. مسلماً هر چه قدر یک سیستم کارهای بیشتری انجام دهد سطح آسیب‌پذیری بزرگتری دارد؛ از طرفی یک سیستم تک‌عملکردی محکم‌تر از یک سیستم چندعملکردی است. از این رو، یک رویکرد برای بهبود امنیت اطلاعات، کاستن سطح آسیب‌پذیری یک سیستم با نرم‌افزار است. استراتژی‌های اصلی برای کاهش سطح آسیب‌پذیری عبارتند از: کاستن از مقدار کار در حال اجرا و حذف نرم‌افزارهای غیر ضروری، کاستن از نقاط ورود در دسترس کاربرانی که اعتمادی به آن‌ها نیست و نام‌های کاربری غیر ضروری، و حذف سرویس‌هایی که نسبتاً متقاضی ندارند.

شیوه‌های مختلفی برای مستحکم‌سازی سیستم وجود دارد. این اقدامات ممکن است شامل به‌کارگیری وصله‌های نرم‌افزاری (یا patch)، بستن پورت‌های شبکه‌ای باز، و راه‌اندازی سیستم‌های تشخیص نفوذ، فایروال، و سیستم‌های جلوگیری از نفوذ باشد. همچنین، ابزارها و برنامه‌های نوشته‌شده‌ای وجود دارند که خصوصیات غیر لازم را در فایل پیکربندی غیرفعال کرده یا اقدامات پیشگیرانه مختلف دیگری را انجام می‌دهند. به هر حال توجه به این نکته ضروری است که اگرچه کاستن سطح آسیب‌پذیری به جلوگیری از شکست امنیتی کمک می‌کند، ولی میزان صدمات و خسارتی را که یک مهاجم -که آسیب‌پذیری را پیدا کرده است- وارد می‌کند کاهش نمی‌دهد.

فرآیند Hardening بخشی از مدیریت حوادث امنیتی کامپیوتر (Computer Security Incident Management) است، که تیم‌های پاسخ به حوادث امنیتی کامپیوتر یا CSIRT (Computer Security Incident Response Team) ها به آن می‌پردازند.

کتاب حاصل نتیجه بخشی از مطالعاتی است که در مرکز پژوهشی آپای دانشگاه صنعتی امیرکبیر طی قراردادی که به منظور حمایت از مطالعات این حوزه توسط ستاد ICT معاونت علمی و فناوری ریاست جمهوری در سال ۱۳۹۱ منعقد گردید صورت گرفته است. در بخشی از این مطالعات قرار بود که بسته آموزشی برای امن‌سازی دو سیستم عامل تهیه گردد. فرصت پیش آمده بهانه‌ای شد تا امن‌سازی چهار سیستم عامل متداول Windows 7, Windows Server 2008, Ubuntu Server و Android مورد مطالعه قرار گیرد و بسته آموزشی برای امن‌سازی آنها تهیه گردد. بدین منظور، ابتدا اطلاعات

لازم با استفاده از منابع در دسترس اینترنتی مطابق سرفصل تهیه شده جمع‌آوری گردید و سپس اطلاعات جمع‌آوری شده روی سیستم‌های واقعی امتحان شد. پس از آن، مطالب نوشته شده تکمیل و مورد بازبینی قرار گرفتند. تهیه اسلاید، تهیه تصاویر آموزشی، تنظیم مطالب برای قرائت، صدابرداری، صداگذاری روی اسلایدها و تهیه ویدئوی آموزشی مراحل مختلفی بودند که تیم مطالعاتی برای تهیه بسته آموزشی طی کرد. عزیزانی که در این فعالیت همکاری کردند شامل جناب دکتر رضا سپهری، خانم مهندس فرشته جعفری، خانم مهندس مهشید نوابی و خانم مهندس پروانه آقاجانی بودند که به صورت پاره‌وقت به بررسی‌های مربوطه و فعالیت‌های مربوط به تهیه بسته آموزشی پرداختند. اگر چه مناعت این عزیزان مانع از آن شد تا نام آنها بر روی جلد کتاب ظاهر گردد، در اینجا بر خود لازم می‌دانیم از تمامی این عزیزان که حداکثر تلاش خود را برای تهیه کاری ارزنده انجام دادند سپاسگزاری و قدردانی نماییم. همچنین، بر خود لازم می‌دانیم از جناب آقای دکتر محامدپور ریاست وقت ستاد ICT مذکور، جناب آقای مهندس جعفری و جناب آقای مهندس سجادی که قرارداد حمایتی با توجهات آنان به ثمر نشست تشکر و قدردانی نماییم.

www.ketab.ir

مقدمه مؤلف

امن‌سازی^۱ سیستم‌های کامپیوتری به معنای کاهش آسیب‌پذیری‌های این سیستم‌ها با هدف به حداقل رساندن ریسک‌های امنیتی است. به‌صورت کلی، امن‌سازی سیستم‌های کامپیوتری در چهار سطح زیر انجام می‌پذیرد:

- امن‌سازی فیزیکی
- امن‌سازی سیستم‌عامل
- امن‌سازی شبکه
- امن‌سازی برنامه‌های کاربردی

موضوع اصلی این کتاب، امن‌سازی سیستم‌عامل است که می‌تواند شامل موارد مختلفی مانند تغییر تنظیمات پیش‌فرض سیستم‌عامل، حذف سرویس‌ها و نرم‌افزارهای غیرضروری، حذف حساب‌ها و گروه‌های کاربری غیرضروری، رمزنگاری داده‌ها، رویدادننگاری، انجام بازرسی، نصب آنتی‌ویروس، نصب و تنظیم فایروال، به‌روزرسانی سیستم‌عامل و برنامه‌های نصب‌شده بر روی آن، و مواردی از این قبیل باشد.

این کتاب شامل خط‌مشی‌ها، سناریوها و دستورالعمل‌هایی جهت ایجاد امن‌سازی مایکروسافت ویندوز ۷ و سیستم‌عامل اندروید است. توصیف و دستورالعمل‌های مطرح‌شده در این کتاب تا حدی اطمینان می‌دهد که کامپیوترهای استفاده‌کننده از این سیستم‌عامل در برابر تهدیدات رایج امنیتی ایمن هستند.