

امنیت فضای سایبر

(مدیریت سامانه‌ها، برگزاری آزمون و بررسی رخنه‌ها)

توماس جی. موبرای

مترجمین

حجت‌اله قدیری

علی میرزایی

تابستان ۱۳۹۴

سرشناسه	موبری، تامس ج.، ۱۹۵۶ - م.
عنوان و نام پدیدآور	امنیت فضای سایبر : مدیریت سامانه‌ها . برگزاری آزمون ، و بررسی رخنه‌ها / توماس جی . موبرای ؛ مترجم حجت‌اله قدیری ، علی میرزایی .
مشخصات نشر	دانشکده علوم و فنون فارابی، ۱۳۹۳.
مشخصات ظاهری	۵۳۰ ص : مصور ، جدول ، نمودار.
شابک	۹۷۸-۶۰۰-۷۳۷۶-۱۶-۴ :
قیمت	۲۵۰۰۰۰ ریال :
وضعیت فهرست‌نویسی : فیبا	
عنوان اصلی	Cybersecurity : managing systems, conducting testing, and investigating intrusions :
موضوع	فضای مجازی -- تدابیر ایمنی
موضوع	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	کامپیوترها -- ایمنی اطلاعات
موضوع	جرایم کامپیوتری -- پیشگیری
شناسه افزوده	میرزایی، علی، ۱۳۵۷ - مترجم
شناسه افزوده	قدیری، حجت‌اله، ۱۳۴۶ - مترجم
شناسه افزوده	دانشکده علوم و فنون فارابی
رده‌بندی کنگره	۱۳۹۳ / الف ۷ م ۹ / HMA۵۱
رده‌بندی دیوپی	۳۰۲ / ۴۸۳۳ :
شماره کتابشناسی ملی :	۳۶۵۵۶۷۱



نام کتاب: امنیت فضای سایبر : مدیریت سامانه‌ها ، برگزاری آزمون ، و بررسی رخنه‌ها

ترجمه: حجت‌اله قدیری، علی میرزایی

ویراستار ادبی: حسین زارع‌شاهی

مدیر مسئول: علی افصلی

صفحه آرا: نادیا بیشه

طرح جلد: حسین باقری

قیمت: ۲۵۰۰۰۰ ریال

تاریخ انتشار: تابستان ۱۳۹۴

شمارگان: ۱۰۰۰ جلد

نوبت چاپ: اول تابستان ۱۳۹۴

درباره نویسنده

دکتر توماس جی. موبرای^۱، دارنده جایزه طلای "جی پن سنز"^۲، معمار ارشد امنیتی دانشگاه ایالتی اوهایو^۳ است. علاوه بر این او:

■ متخصص تایید شده معماری زکمن^۴

■ معمار متخصص و دارای تاییدیه موسسه FEAC

■ متخصص تایید شده HIMSS در زمینه محافظت سلامت اطلاعات سیستم های مدیریتی

■ آزمونگر رسمی در نفوذ به شبکه، سایبر تولزمیت^۵ و مدیر آزمایشگاه سایبر^۶

■ بنیانگذار نورث راپ جرومن /تسک^۷ و انجمن پدافند جنگ سایبر

■ آزمونگر تایید شده نفوذ به شبکه (GPEN) توسط برگه های طلایی محققان می باشد.

وی در نگارش دو کتاب زیر همکاری نموده است:

ضدالگوها: بازسازی نرم افزارها، معماری ها و پروژه ها در بحران
John Wiley & Sons, ISBN ۱۹۹۸)، و دوره آموزشی معماری نرم افزار

^۱ Mowbray

^۲ Certified Network Penetration Tester

^۳ نام موسسه ای در زمینه امنیت

^۴ Ohio State University

^۵ Zachman

^۶ Toolsmith

^۷ Cyber Lab Manager

^۸ Northrup Grumman/tasc

(۹-۱۴۱۲۲۷-۱۳-۰۰-۹۷۸ Prentice Hall, ۲۰۰۳). او همچنین سردبیر مجله معماری

اینترپرایز است. شما می‌توانید با دکتر موبرای در سایت اجتماعی لینکداین^۱ ارتباط برقرار کنید.

www.ketab.ir

^۱ LinkedIn

فهرست

این کتاب چه چیزی را پوشش می‌دهد	۱۹
این کتاب چگونه ساختاربندی شده است؟	۱۹
این کتاب چگونه بوجود آمده است؟	۲۱
آنچه شما برای استفاده از این کتاب نیاز دارید:	۲۲
فصل اول: خلاصه اجرایی	۲۹
چرا با ضدالگوها شروع کنیم؟	۳۰
ساختار امنیتی	۳۲
ضدالگو: تشخیص بدافزار مبتنی بر امضاء در مقابل تهدیدات چنگانه	۳۳
راه‌حل بازنگری شده: تشخیص بدافزارها مبتنی بر اعتبار، رفتار و تخریب	۳۴
ضد الگو: صدور گواهینامه سندمحور و مجوزهای رسمی	۳۶
ضدالگو: گسترش استانداردهای IA بدون منافع ثابت شده	۳۷
ضد الگو: گواهینامه‌های امنیت سیاست محور، تهدید را نشان نمی‌دهند	۴۰
راه حل بازیابی شده: خط مشی آموزش امنیت	۴۱
خلاصه	۴۷
تکالیف	۴۸
فصل دوم: مشکلات: ضد الگوهای سایبر	۴۹
مفاهیم ضدالگوها	۵۰
عوامل در ضد الگوهای سایبری	۵۱

۵۳..... قالب‌های ضد الگوی سایبری

۵۷..... کاتالوگ ضد الگوهای امنیتی سایبری

۸۲..... خلاصه

۸۴..... تکالیف

۸۵..... فصل سوم: امنیت موسسات با استفاده از جدول زکمن

۸۵..... معماری زکمن چیست و چرا به آن نیاز داریم؟

۸۶..... موسسات پیچیده و در حال تغییر هستند

۸۷..... چارچوب زکمن برای معماری سازمانی

۸۹..... نمونه‌های اولیه (اصلی) در برابر نمونه‌های ترکیبی

۹۰..... جدول زکمن چگونه به امنیت سایبری کمک می‌کند؟

۹۲..... هر شخصی مشخصات خودش را داراست

۹۲..... معدن طلا در ردیف دوم قرار دارد

۹۳..... چارچوب هایی برای ردیف ۳

۹۴..... الگوهای حل مساله معماری

۱۱۷..... خلاصه

۱۱۹..... تکالیف

۱۲۱..... فصل چهارم: مدیریت شبکه برای متخصصان امنیتی

۱۲۳..... مدیریت شبکه و حساب‌های مدیریتی

۱۲۶..... نصب سخت‌افزار

۱۳۰..... بازسازی مجدد سیستم عامل‌ها

خواندن و کپی کردن CD ها و DVD ها	۱۳۵
نصب محافظ سیستم / ضد بدافزار	۱۳۸
تنظیم کردن شبکه ها	۱۴۵
نصب برنامه های کاربردی و آرشیو بندی	۱۵۲
شخصی سازی کنترل ها و تنظیمات سیستم های مدیریتی	۱۵۶
مدیریت اتصال دور	۱۵۸
مدیریت دسترسی های مدیریتی کاربران	۱۶۰
مدیریت سرویس	۱۶۳
تنظیم دیسک ها	۱۶۷
انتقال اطلاعات بین سیستم ها و شبکه ها	۱۶۹
تبدیل فایل های متنی بین سیستم عامل ها	۱۷۱
ساخت دیسک های پشتیبان	۱۷۲
فرمت کردن دیسک ها	۱۷۳
پیکربندی دیوارهای آتش	۱۷۵
تبدیل و جابجایی ماشین های مجازی	۱۷۹
دانش های ثانویه مدیریت شبکه	۱۸۳
خلاصه	۱۸۴
تکالیف	۱۸۶
فصل پنجم: شخصی سازی بک ترک و ابزارهای امنیتی	۱۸۷

۱۸۸	ایجاد و اجرا کردن فایل‌های فشرده بک ترک
۱۹۰	سفارشی کردن بک ترک توسط ماشین مجازی
۱۹۱	بروزرسانی و ارتقاء بک ترک و ابزارهای تست نفوذ
۱۹۲	اضافه کردن ویندوز به بک ترک به وسیله VMware
۲۰۰	چالش‌های انجام عملیات لایسنس برای مدیران شبکه
۲۰۲	خلاصه
۲۰۴	تکالیف
۲۰۵	فصل ششم: تحلیل پروتکل و برنامه‌نویسی شبکه
۲۰۶	نظریه و تکنیک ایجاد شبکه
۲۰۸	پروتکل‌های پرکاربرد شبکه
۲۲۰	برنامه‌نویسی شبکه: Bash
۲۲۹	برنامه‌نویسی شبکه: رابط خط فرمان ویندوز
۲۳۴	برنامه‌نویسی پایتون، جستجوی سریع شبکه
۲۳۹	خلاصه
۲۴۱	تکالیف
۲۴۳	فصل هفتم: شناسایی، ارزیابی آسیب پذیری و تست سایبری
۲۴۴	روش‌های ارزیابی امنیت سایبری
۲۴۹	آشنایی با روش تست امنیت سایبری
۲۸۴	خلاصه فصل
۲۸۶	تکالیف

فصل هشتم: تست نفوذ.....	۲۸۷
اشکال حملات سایبری.....	۲۸۸
نفوذ شبکه.....	۲۹۱
ابزارهای تجاری تست نفوذ.....	۲۹۵
استفاده از Netcat برای ایجاد ارتباط و انتقال داده‌ها و کدهای پاییری.....	۲۹۷
استفاده از Netcat برای ایجاد تقویت کننده‌ها و چارت‌ها.....	۲۹۹
کاربرد SQL Injection و تکنیک‌های CROSS-SITE جهت حمله به نرم‌افزارهای تحت وب و پایگاه داده.....	۳۰۳
جمع‌آوری هویت کاربران با استفاده از جزئی‌نگری و بدست آوردن هش.....	۳۰۷
کرک کردن کلمات عبور.....	۳۱۰
به دست آوردن دسترسی.....	۳۱۴
فازهای مخرب نهایی.....	۳۱۴
خلاصه.....	۳۲۰
تکالیف.....	۳۲۳
فصل نهم: محافظت از شبکه‌های سایبری با استفاده از تحلیل پیشرفته گزارشات.....	۳۲۵
مقدمه‌ای درباره دفاع از شبکه‌های سایبری.....	۳۲۶
روش‌ها و ابزار کلی برای تحقیقات سایبری.....	۳۲۸
استراتژی متداوم تحقیق سایبری.....	۳۳۱
خلاصه‌ای از فرآیند تحقیقات سایبری.....	۳۳۴
پایش شبکه.....	۳۳۶

۳۴۳	 تحلیل گزارشات متنی
۳۵۰	 تجزیه و تحلیل گزارشات باسنری
۳۵۷	 بررسی گزارشات سایبری
۳۵۷	 حذف تهدیدات سایبری
۳۶۳	 کشف نفوذ در ویندوز
۳۶۴	 خلاصه فصل
۳۶۵	 تکالیف
۳۶۷	 فصل دهم: امنیت فضای سایبر برای کاربران، رسانه‌های عمومی و دنیای مجازی
۳۶۸	 انجام جستجوهای گوگلی
۳۶۹	 محافظت از لپ‌تاپ‌ها، رایانه‌های شخصی و دستگاه‌های تلفن همراه
۳۷۲	 بروز ماندن با ضدبدافزارها و روزرسانی نرم‌افزارها
۳۷۳	 مدیریت کلمه عبور
۳۷۵	 محافظت در برابر نرم‌افزارهای مخرب محرک
۳۷۷	 درامان ماندن از خطرات ایمیل
۳۷۹	 بانکداری و خرید آنلاین ایمن
۳۸۱	 درک مفهوم بدافزارهای مخرب و باجگیران
۳۸۲	 آیا دستگاه شما مورد حمله قرار گرفته است؟
۳۸۳	 مراقب رسانه‌های اجتماعی باشید
۳۸۴	 ایمن ماندن در دنیای مجازی
۳۸۸	 خلاصه

۳۹۰	تکالیف
۳۹۱	فصل یازدهم: ملزومات امنیت سایبری در مشاغل کوچک
۳۹۲	نصب محافظ‌های ضد بدافزار
۳۹۳	بروز کردن سیستم عامل‌ها
۳۹۴	بروزرسانی برنامه‌های کاربردی
۳۹۵	تغییر کلمات عبور پیش فرض
۳۹۶	آموزش کاربران نهایی
۳۹۶	مدیریت سیستم مؤسسات کوچک
۳۹۸	اساس امنیت بی‌سیم برای مشاغل کوچک
۳۹۹	نکاتی برای کاربران اپل مکینتاش
۴۰۱	خلاصه
۴۰۲	تکالیف
۴۰۳	فصل دوازدهم: امنیت سایبری مؤسسات بزرگ: مراکز داده و ابرها
۴۰۴	کنترل بحران امنیتی
۴۲۹	امنیت ابری
۴۳۸	خلاصه
۴۳۹	تکالیف
۴۴۱	فصل سیزدهم: اطلاعات بهداشت و درمان و امنیت فناوری اطلاعات
۴۴۲	HIPAA

۴۴۳	ارزیابی خطرات بهداشت و درمان
۴۴۴	مدیریت رکوردهای سلامت
۴۴۵	فناوری اطلاعات حوزه سلامت و روند قضایی آن
۴۴۶	از دست دادن داده‌ها
۴۴۷	مدیریت گزارشات در سازمان‌های بهداشت و درمان
۴۴۸	احراز هویت و کنترل دسترسی
۴۵۱	خلاصه
۴۵۲	تکالیف
۴۵۳	فصل چهاردهم: جنگ سایبر: یک معماری برای بازدارندگی
۴۵۴	مقدمه‌ای بر بازدارندگی سایبری
۴۵۸	روش شناسی و مفروضات
۴۶۱	چالش‌های بازدارندگی سایبری
۴۶۴	فرض‌های حقوقی و بیمانی
۴۶۷	استراتژی بازدارندگی سایبری
۴۷۳	مدل مرجع
۴۷۵	معماری راه‌حل
۴۸۲	شبیه‌سازی ساخت‌یافته
۴۹۶	خلاصه
۴۹۸	تکالیف
۴۹۹	فصل آخر: واژه‌نامه
۵۱۷	کتاب‌شناسی