بسم الله الرحمن الرحیم

راهنمای جامع آزمون نفوذگر اخلاقی

مترجمان:

رضا نوری
سعید رحیمی
نوید باباخانی

انتشارات انستیتو ایزایران

گروه صنایع امنیت فاوا صاایران

- سرشناسه :گریوز، کیمبرلی، ۱۹۷۴- م. Graves, kimberly
- عنوان و نام پدیدآور : راهنمای جامع آزمون نفوذگر اخلاقی/ کیمبرلی گریوز؛ مترجمان: رضا نوری سعید رحیمی، نوید باباخانی
- مشخصات نشر : تهران: انستیتو ایزایران،۱۳۸۹.
- مشخصات ظاهری : ۲۷۲ص.
- شابک: ۵۲۰۰۰ ریال : ۹۷۸-۹۶۴-۲۰۱-۰۲۲-۶
- وضعیت فهرست نویسی : فیپا
- یادداشت عنوان اصلی :CEH: official certified ethical hacker review guide-2007
- موضوع : داده پردازی- -کارمندان- -گواهی نامه
- موضوع : کامپیوترها- -ایمنی اطلاعات- - آزمون ها- -راهنمای مطالعه
- موضوع : هکرها- -آزمون ها- -راهنمای مطالعه
- موضوع: شبکه های کامپیوتری- - آزمون ها- -راهنمای مطالعه
- شناسه افزوده : نوری، رضا، ۱۳۵۶ - ، مترجم
- شناسه افزوده : رحیمی،سعید، ۱۳۶۲- ، مترجم
- شناسه افزوده : باباخانی، نوید،۱۳۶۵- ، مترجم
- شناسه افزوده : انستیتو ایزایران
- رده بندی کنگره : ۱۳۸۹ ۲ ر/ ۲ QA ۷۶
- رده بندی دیویی : ۰۰۵/۸
- شماره کتابشناسی ملی : ۱۹۶۰۵۶۶

انتشارات انستیتو ایزایران

گروه صنایع امنیت فاوا صاایران

- **نام کتاب:** .....راهنمای جامع آزمون نفوذگر اخلاقی
- **نویسنده:** .....کیمبرلی گریوز
- **مترجمان:** .....رضا نوری،سعید رحیمی،نوید باباخانی
- **نوبت چاپ:** ..... اول- بهار ۸۹
- **شمارگان:** ..... ۲۰۰۰ جلد
- **قیمت:** ..... ۵۲۰۰ تومان
- **شابک:** ۹۷۸-۹۶٤-۲۰۱-۰۲۲-٦
- **طراح جلد:** ..... محسن محمد صادقی
- **ناظر چاپ:** ..... حسین نادری

ناشر از همکاری **گروه صنایع امنیت فاواصاایران** در چاپ این کتاب به منظور توسعه فناوری اطلاعات و ارتباطات در کشور قدردانی می کند.

تهران، میرداماد، خیابان شهید حصاری، شماره ۳۶
تلفن: ۷۸-۲۲۲۵٤ نمابر: ۲۲۲۲۵۲۶۵
books@isiran-net.com

پیشگفتار

امروزه در عصری بسر می‌بریم که از آن به عصر اطلاعات یاد می‌شود و در سرتاسر دنیا داده‌ها و اطلاعات از ارزش خاصی برخوردار است و در کنار استفاده‌های فردی، این سازمان‌ها و مؤلفه‌های یک کشور هستند که بیشترین استفاده را از منابع اطلاعاتی می‌برند و استفاده درست از اطلاعات، از نیازهای مبرم سازمان‌ها در جهت پیشبرد اهداف خود است. در عین حال سرقت اطلاعات که برای آن هزینه و وقت صرف شده یکی از خطرات بالقوه شبکه‌های رایانه‌ای به شمار می‌آید.

به هر حال امروزه امنیت ملی و اقتدار سیاسی و اقتصادی به طرز پیچیده‌ای به امنیت اطلاعات گره خورده است و نه تنها دولت‌ها، بلکه تک تک افراد را نیز تهدید می‌کند. با این تفاسیر، تدوین و اجرای تدابیر امنیتی برای هر فرد یا سازمان امری اجتناب ناپذیر بوده و می‌تواند با احتمال بسیار خوبی جلوی مخاطرات عمدی یا غیرعمدی را بگیرد و یا آنها را به حداقل برساند.

در جهت پیشبرد این تدابیر و اهداف امنیتی، تربیت افراد متعهد و کارآزموده در زمینه امنیت و نفوذ به سیستم‌ها (که اصطلاحاً نفوذگران اخلاقی نامیده می‌شوند) بسیار مفید خواهد بود. آزمون نفوذگر اخلاقی گواهی شده (Certified Ethical Hacker) توسط انجمن بین المللی مشاوران تجارت الکترونیک (EC-Council) ایجاد شده تا ابزار صنعتی گواهی دهنده‌ای برای تعیین صلاحیت متخصصان امنیت باشد. گواهینامه CEH، به کسانی اعطا می‌شود که به آن سطح از دانش و مهارت‌های عیب‌یابی لازم در جهت فراهم کردن پشتیبانی در زمینه امنیت شبکه و کامپیوترها رسیده باشند.

آزمون نفوذگر اخلاقی به صورت دوره‌ای به روز رسانی می‌شود تا گواهی‌های اعطا شده برای نرم افزار و سخت افزارهای جدید نیز کاربردی باشد. این امر بسیار ضروری است زیرا یک نفوذگر اخلاقی باید قادر باشد با جدیدترین تجهیزات کار کند.

کتابی که پیش روی شماست، به عنوان راهنمایی مختصر و قابل حمل طراحی شده که می‌تواند در کنار مطالعات کامل‌تر، به عنوان ابزار آزمایشگاهی و نیز برای کسانی که می‌خواهند اطلاعات خود را قبل از آزمون تقویت کنند مفید واقع شود. هدف نویسنده در این کتاب این نیست که به تمام سؤالات شما پاسخ دهد بلکه در این کتاب سعی شده که شما را با مسائل و موضوعاتی که برای آزمون باید در آنها خبره باشید، آشنا کند.

رئیس گروه صنایع امنیت فاوا صاایران

بهمن آصفی

اگر دشمن خودتان را بشناسید، لازم نیست از صدها جنگ بترسید و اگر خودتان را می‌شناسید و دشمن را نمی‌شناسید، برای هر پیروزی که حاصل می‌کنید شکستی را متحمل خواهید شد. اگر نه خود را می‌شناسید و نه دشمن را، در هر جنگ و کارزاری از پای در خواهید آمد.

برای دفاع مؤثر می‌بایست کلیه ابزارها و روال‌های مورد استفاده دشمن را بشناسیم. با این شناخت نه تنها بهتر می‌توانیم نیازهای دفاعی خود را بشناسیم بلکه تکنیک‌های دفاعی بهتری را نیز می‌توانیم بکار بریم.

لذا در این کتاب، روش‌های هک و ارزیابی سیستم‌های رایانه‌ای مطرح شده است و برای کسانی که تصمیم به ایجاد امنیت در شبکه‌های رایانه‌ای دارند می‌تواند بسیار مفید واقع شود تا با شناخت ضعف‌های امنیتی و تکنیک‌های نفوذ، شبکه امن‌تری را ایجاد و با ارزیابی مداوم آن، این امنیت را حفظ نمایند.

امید است ترجمه این کتاب که حاصل تلاش جمعی از متخصصین حوزه امنیت فناوری اطلاعات می‌باشد کمکی در جهت بالا بردن سطح معلومات امنیتی و ایجاد امنیت در شبکه‌های رایانه‌ای کشور عزیزمان باشد.

دکتر مرتضی براری

عضو هیئت علمی دانشگاه مالک اشتر

معرفی گروه صافاوا

در بهار ۱۳۸۶ به دنبال انتزاع دو مجموعه صنعت امنیت مخابرات از شرکت صنایع مخابرات با بیش از ۲۰ سال سابقه طراحی و تولید انواع رمز کننده‌های صوت و دیتا در حوزه امنیت مخابرات و مراکز امنیت نرم افزار و سخت افزار از شرکت ایزایران با سابقه ۵ ساله در تأمین و ارائه خدمات امن سازی بومی نرم افزارها و سخت افزارها و امنیت شبکه‌های رایانه‌ای در حوزه امنیت فناوری اطلاعات و تجمیع این دو، مجموعه‌ای تحت عنوان گروه صنایع امنیت فناوری اطلاعات و ارتباطات (صافاوا) به عنوان ششمین مجموعه وابسته به صاایران ایجاد گردید.

این الحاق موجب رشد هر دو صنعت، ادغام و تقویت متمرکز برخی امور و مأموریت‌های موازی و نیز بهره‌مندی متقابل از توانمندی‌های یکدیگر و نهایتاً ارتقای جایگاه و مأموریت امنیت در بین شرکت‌های صاایران را فراهم ساخته است.

محصولات و خدمات این گروه در پنج حوزه تکنولوژی امنیت ارتباطات، امنیت فناوری اطلاعات، رمزنگاری، کنترل امنیت و ارزیابی سامانه‌های نرم افزاری به متقاضیان عرضه می‌گردد.

فهرست مطالب

مقدمه

آزمون نفوذگر اخلاقی گواهی شده (Certified Ethical Hacker) توسط انجمن بین المللی مشاوران تجارت الکترونیک (EC-Council) ایجاد شده تا ابزار صنعتی گواهی دهنده‌ای برای تعیین صلاحیت متخصصان امنیت باشد. گواهینامه CEH، به کسانی اعطا می‌شود که به آن سطح از دانش و مهارت‌های عیب‌یابی لازم در جهت فراهم کردن پشتیبانی در زمینه امنیت شبکه و کامپیوترها رسیده باشند.

آزمون CEH بصورت دوره‌ای به روز رسانی می‌شود تا گواهی‌های اعطا شده برای نرم افزار و سخت افزارهای جدید نیز کاربردی باشد. این امر بسیار ضروری است زیرا یک نفوذگر اخلاقی باید قادر باشد با جدیدترین تجهیزات کار کند. جدیدترین تغییرات در اهداف CEH، در سال ۲۰۰۶ تصویب شده‌اند که در این کتاب نیز انعکاس یافته‌اند.

گواهی CEH چیست؟

گواهی CEH ایجاد شده تا یک گواهی گسترده در جهت ارزیابی شایستگی افراد مختلف باشد. این گواهی برای متصدیان امنیت، بازرسان شبکه، متخصصان امنیت شبکه، مدیران سیستم و هر کسی که به طور روزانه با امنیت شبکه سروکار دارد، طراحی شده است.

هدف نفوذگران اخلاقی کمک به سازمان‌هاست تا معیارهای انحصاری خود را در مقابل نفوذهای بدخواهانه بکار بگیرند. این نفوذگران برای انجام کار خود، به شبکه این سازمان‌ها حمله می‌کنند البته با داشتن حد و مرز قانونی. فلسفه این کار از این جمله معروف ناشی شده که "اگر می‌خواهی یک دزد را دستگیر کنی، همانند یک دزد فکر کن". همانطور که تکنولوژی پیشرفت می‌کند، سازمان‌ها به این تکنولوژی وابسته‌تر می‌شوند و در این بین منابع اطلاعاتی به مؤلفه‌های بحرانی بقای سازمان تبدیل شده‌اند.

شما برای گرفتن گواهی CEH کافیست که تنها یک آزمون را با موفقیت بگذرانید، اما بدست آوردن این گواهی به این معنی نیست که شما می‌توانید به سازمان‌ها خدمات ارائه کنید بلکه این اولین گام است. پس از کسب گواهی CEH، شما قادر خواهید بود که تجارب بیشتری کسب کنید و متعاقباً دانش و گواهی‌های پیچیده‌تر و کاربردی‌تری را کسب کنید.

چه کسانی باید از این کتاب استفاده کنند؟

راهنمای جامع آزمون نفوذگر اخلاقی، به عنوان راهنمایی مختصر و قابل حمل طراحی شده که

می‌تواند در کنار مطالعات کامل‌تر، به عنوان ابزار آزمایشگاهی و نیز برای کسانی که می‌خواهند اطلاعات خود را قبل از آزمون تقویت کنند مفید واقع شود. هدف ما در این کتاب این نیست که به تمام سوالات شما پاسخ دهیم بلکه در این کتاب سعی شده که شما را با مسائل و موضوعاتی که برای آزمون باید در آنها خبره باشید آشنا کنیم.

اگر می‌خواهید که تبدیل به یک نفوذگر اخلاقی شوید این کتاب دقیقاً همان چیزی است که نیاز دارید، اما اگر تنها می‌خواهید که آزمون را پشت سر بگذارید بدون اینکه دانش کافی در مورد نفوذگری اخلاقی بدانید این راهنما برای شما مفید نخواهد بود. این کتاب برای کسانی نوشته شده که می‌خواهند مهارت‌ها و دانش لازم برای گذراندن آزمون را کسب کنند و سپس این دانش را در دنیای واقعی به کار بگیرند.

اهداف آزمون CEH

در آغاز هر فصل این کتاب، موضوعات و اهداف آزمون CEH (که در وب‌سایت EC-Council بدان‌ها اشاره شده است) بطور کامل آورده شده‌اند. در اینجا این اهداف را بطور خلاصه ذکر می‌کنیم:

اخلاق و قانونمداری
ردگیری
پویش
صورت برداری
نفوذ به سیستم
تروجان‌ها و درهای پشتی
اسنیفرها
منع سرویس
مهندسی اجتماعی
ربودن نشست
نفوذ به سرورهای وب
آسیب پذیری‌های نرم افزارهای تحت وب
روش‌های مبتنی بر وب برای شکستن کلمه عبور
تزریق SQL
نفوذ بی‌سیم
ویروس‌ها و کرم‌ها

امنیت فیزیکی
نفوذ به لینوکس
گریز از IDS، Honeypot و فایروال
سرریز کردن حافظه
رمزنگاری
شیوه‌های تست نفوذ