

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



راهنمای جامع آزمون نفوذگر اخلاقی

مترجمان:

رضانوری

سعید رحیمی

نوید باباخانی



گروه صنایع امنیت فضا و مخابرات



انتشارات انستیتو ایز ایران

- سرشناسه: گریوز، کیمبرلی، ۱۹۷۴- Graves, kimberly
- عنوان و نام پدیدآور: راهنمای جامع آزمون نفوذگر اخلاقی/ کیمبرلی گریوز؛ مترجمان: رضا نوری
- سمید رحیمی، نوید باباخانی
- مشخصات نشر: تهران: انستیتو ایزایران، ۱۳۸۹.
- مشخصات ظاهری: ۲۷۲ص
- شابک: ۵۲۰۰۰-۰۲۲۰۶-۲۰۱-۹۶۴-۹۷۸
- وضعیت فهرست نویسی: فیا
- یادداشت عنوان اصلی: CEH: official certified ethical hacker review guide-2007
- موضوع: داده پردازي - 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، سمید، ۱۳۲۴ - مترجم
- شناسه افزوده: باباخانی، نوید، ۱۳۶۵ - مترجم
- شناسه افزوده: انستیتو ایزایران
- رده بندی کنگره: ۱۳۸۹ / ۲ / ۷۶۱ / ۳ QA
- رده بندی دیویی: ۰۰۵۸
- شماره کتابشناسی ملی: ۱۹۶۰۵۶۶



گروه صنایع امنیت فاوا صا ایران



انشارات انستیتو ایزایران

- ◀ 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: ۹۷۸-۹۶۴-۲۰۱-۰۲۲-۶
- ◀ طراح جلد: محسن محمد صادقی
- ◀ ناظر چاپ: حسین نادری

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

کلیه حقوق قانونی و شرعی برای ناشر محفوظ است.
تکثیر تمام یا قسمتی از این اثر بصورت حرفه‌ای و چاپ مجدد، چاپ افست، پلی کپی فتوکپی و انواع دیگر چاپ ممنوع است. نقل مطالب به صورت معمول در مقاله های تحقیقاتی با ذکر نام کامل ناشر و کتاب آزاد است.

تهران، میرداماد، خیابان شبید حصاری، شماره ۳۶

تلفن: ۲۲۲۵۴-۷۸ 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 صایران

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 ببریم.

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 تجمع این دو، مجموعه‌ای تحت عنوان گروه صنایع امنیت فناوری اطلاعات و ارتباطات (صافاوا) به عنوان ششمین مجموعه وابسته به صایران 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 صایران 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.....	۱۹
فصل اول: آشنایی با نفوذ اخلاقی، اخلاق و قوانین	۲۳
شناسایی عبارات مرتبط با نفوذ اخلاقی	۲۴
شناسایی انواع مختلف تکنولوژی‌های نفوذ.....	۲۵
شناسایی مراحل مختلف نفوذ اخلاقی و فهرست بندی ۵ مرحله نفوذ اخلاقی.....	۲۷
مرحله‌ی اول: شناسایی	۲۷
مرحله‌ی دوم: پویش (scan).....	۲۸
مرحله‌ی سوم: حصول دسترسی	۲۸
مرحله‌ی چهارم: حفظ دسترسی	۲۹
مرحله‌ی پنجم: رد گم کردن	۲۹
هکتیویسم چیست؟.....	۲۹
فهرست‌بندی انواع مختلف طبقات نفوذگرها	۳۰
نفوذگرهای اخلاقی و crackerها - آنها چه کسانی هستند؟	۳۱
نفوذگرهای اخلاقی چه کار می‌کنند؟	۳۲
اهدافی که مهاجمان قصد رسیدن به آن را دارند	۳۲
مثبت امنیت، کارایی و سهولت استفاده	۳۳
تعریف مهارت‌های مورد نیاز برای تبدیل شدن به یک نفوذگر اخلاقی	۳۴

۳۵.....	پژوهش آسیب پذیری چیست؟
۳۵.....	شرح روش‌های هدایت نفوذگرهای اخلاقی
۳۶.....	ساخت یک برنامه‌ی ارزیابی امنیت
۳۶.....	انواع نفوذهای اخلاقی
۳۷.....	انواع آزمون‌ها
۳۷.....	گزارش نفوذ اخلاقی
۳۸.....	شناخت جوانب قانونی نفوذ
۳۸.....	شناخت قانون فدرال 18 U.S.C. 1029, 1030 ایالات متحده
۳۹.....	موارد حایز اهمیت در امتحان
۴۱.....	سؤالات
۴۳.....	پاسخ سؤالات
۴۵.....	فصل دوم: ردگیری و مهندسی اجتماعی
۴۶.....	ردگیری
۴۶.....	تعریف واژه ردگیری
۴۸.....	شرح روش‌های جمع‌آوری اطلاعات
۴۹.....	شرح اطلاعات رقابتی
۴۹.....	شناخت صورت برداری DNS
۵۱.....	آشنایی با جستجوی Whois و ARIN
۵۶.....	شناسایی انواع مختلف رکوردهای DNS
۵۷.....	شناخت چگونگی استفاده از traceroute، در فرایند ردگیری
۵۸.....	شناخت چگونگی ردیابی ایمیل
۵۹.....	شناخت چگونگی کار عنکبوت‌های وب
۵۹.....	موارد حایز اهمیت در امتحان
۶۰.....	مهندسی اجتماعی
۶۱.....	مهندسی اجتماعی چیست؟
۶۳.....	رایج‌ترین انواع حملات چیست؟
۶۴.....	آشنایی با تهاجم از طریق عناصر داخلی
۶۵.....	آشنایی با استفاده غیر مجاز از اطلاعات شناسایی افراد

۶۵.....	شرح حملات تخلیه.....
۶۵.....	شناخت کلاهبرداری‌های آنلاین.....
۶۶.....	شناخت مبهم سازی URL.....
۶۷.....	مقابله با مهندسی اجتماعی.....
۶۸.....	موارد حایز اهمیت در امتحان.....
۷۰.....	سؤالات.....
۷۳.....	پاسخ سؤالات.....
۷۵.....	فصل سوم: پویش و صورت برداری.....
۷۶.....	پویش.....
۷۶.....	تعریف عبارات پویش پورت، پویش شبکه و پویش آسیب پذیری‌ها.....
۷۷.....	شناخت روش CEH برای پویش.....
۷۸.....	شناخت روش‌های Ping Sweep.....
۸۰.....	شناخت سویچ‌های دستوری Nmap.....
۸۳.....	شناخت پویش SYN، XMAS، NULL، IDLE و FIN.....
۸۴.....	انواع پرچم‌های برقراری ارتباط در TCP.....
۸۶.....	شناخت تکنیک‌های شماره گیری جنگی.....
۸۷.....	شناخت روش‌های Banner Grabbing و ردگیری سیستم عامل.....
۸۸.....	شناخت چگونگی استفاده از سرورهای پراکسی در حملات.....
۸۹.....	شناخت چگونگی عملکرد ناشناس کننده‌ها (Anonymizer).....
۸۹.....	شناخت روش‌های تونل سازی HTTP.....
۹۰.....	درک تکنیک‌های جعل IP.....
۹۰.....	موارد حایز اهمیت در امتحان.....
۹۱.....	صورت برداری.....
۹۲.....	صورت برداری چیست؟.....
۹۳.....	نشست تهی (Null session) به چه معناست؟.....
۹۴.....	صورت برداری از طریق SNMP چیست؟.....
۹۶.....	انتقال DNS Zone در ویندوز ۲۰۰۰.....
۹۷.....	مراحل انجام یک صورت برداری چیست؟.....

۹۷.....	موارد حایز اهمیت در امتحان
۹۹.....	سؤالات
۱۰۲.....	پاسخ سؤالات
۱۰۵.....	فصل چهارم: نفوذ به سیستم
۱۰۶.....	درک تکنیک‌های شکستن کلمه عبور
۱۰۸.....	شناخت درهم سازی LanManager
۱۰۸.....	شکستن کلمات عبور ویندوز ۲۰۰۰
۱۰۹.....	هدایت SMB Logon به سمت مهاجم
۱۰۹.....	هدایت SMB
۱۱۰.....	حملات SMB Relay MITM و راه‌های مقابله با آن
۱۱۱.....	حمله‌ی منع سرویس از طریق NetBIOS
۱۱۲.....	راه‌های مقابله با شکستن کلمه‌ی عبور
۱۱۳.....	شناسایی انواع مختلف کلمات عبور
۱۱۴.....	حملات آن‌لاین غیرفعال
۱۱۵.....	حملات آن‌لاین فعال
۱۱۷.....	حملات آفلاین
۱۱۸.....	حملات غیر الکترونیکی
۱۱۹.....	شناخت Keyloggerها و فناوری‌های دیگر جاسوسی
۱۲۰.....	یادگیری افزایش اختیارات
۱۲۱.....	اجرای نرم افزارها
۱۲۱.....	سرریز کردن حافظه
۱۲۲.....	شناسایی Rootkitها
۱۲۳.....	استقرار Rootkitها روی ویندوز ۲۰۰۰ و XP
۱۲۳.....	پشته پروتکلی TCP/IP با Rootkit جاسازی شده
۱۲۳.....	راه‌های مقابله با Rootkit
۱۲۴.....	یادگیری چگونگی مخفی کردن فایل‌ها
۱۲۵.....	Stream کردن فایل‌های NTFS
۱۲۵.....	راه‌های مقابله با استریم NTFS

۱۲۶.....	شناخت فناوری‌های استیگنوگرافی.....
۱۲۷.....	یادگیری چگونگی پاک کردن ردپا و از بین بردن شواهد.....
۱۲۷.....	غیرفعال کردن بازرسی.....
۱۲۸.....	پاک کردن ثبت وقایع.....
۱۲۸.....	موارد حایز اهمیت در امتحان.....
۱۳۰.....	سؤالات.....
۱۳۲.....	پاسخ سؤالات.....
۱۳۳.....	فصل پنجم: تروجان‌ها، درهای پشتی، ویروس‌ها و کرم‌ها.....
۱۳۴.....	تروجان‌ها و درهای پشتی.....
۱۳۵.....	تروجان چیست؟.....
۱۳۶.....	کانال Overt و Covert به چه معنی می‌باشد؟.....
۱۳۷.....	لیست انواع مختلف تروجان‌ها.....
۱۳۷.....	تروجان‌های اتصال معکوس چگونه کار می‌کنند؟.....
۱۴۰.....	شناخت چگونگی کار تروجان Netcat.....
۱۴۰.....	نشانه‌های یک حمله‌ی تروجان چیست؟.....
۱۴۱.....	“Wrapping” (بسته بندی) به چه معنی است؟.....
۱۴۱.....	کیت‌های ساخت تروجان و تولیدکنندگان تروجان.....
۱۴۲.....	تکنیک‌های مقابله با تروجان‌ها و جلوگیری از آنها.....
۱۴۲.....	روش‌های گریز از تروجان‌ها.....
۱۴۳.....	بررسی سیستم فایل‌ها، هدف فرعی مقابله با تروجان.....
۱۴۴.....	ویروس‌ها و کرم‌ها.....
۱۴۴.....	شناخت تفاوت بین ویروس و کرم.....
۱۴۵.....	شناخت انواع ویروس‌ها.....
۱۴۶.....	شناخت تکنیک‌های گریز از آنتی‌ویروس.....
۱۴۶.....	شناخت روش‌های کشف ویروس.....
۱۴۷.....	موارد حایز اهمیت در امتحان.....
۱۴۸.....	سؤالات.....
۱۵۲.....	پاسخ سؤالات.....

فصل ششم: استیفرها	۱۵۵
شناخت پروتکل‌های در معرض Sniffing	۱۵۶
شناخت Sniffing فعال و غیرفعال	۱۵۷
شناخت سمی سازی ARP	۱۵۸
شناخت ضبط با ابزار Ethereal و فیلترهای نمایش در آن	۱۵۹
شناخت سیل MAC	۱۶۰
شناخت تکنیک‌های جعل DNS	۱۶۰
شرح راه‌های مقابله با Sniffing	۱۶۳
موارد حایز اهمیت در امتحان	۱۶۴
سؤالات	۱۶۵
پاسخ سؤالات	۱۶۷
فصل هفتم: منع سرویس و ربودن نشست	۱۶۹
منع سرویس	۱۷۰
شناخت انواع حملات DoS	۱۷۰
شناخت چگونگی کار حمله‌ی DDoS	۱۷۲
شناخت چگونگی کار BOTها/BOTNETها	۱۷۴
حمله‌ی Smurf چیست؟	۱۷۵
سیل SYN چیست؟	۱۷۵
شرح راه‌های مقابله با DoS/DDoS	۱۷۵
ربودن نشست	۱۷۷
شناخت جعل در مقایسه با ربودن	۱۷۷
فهرست بندی انواع روش‌های ربودن نشست	۱۷۷
شناخت پیش بینی sequence-number	۱۷۹
مراحل انجام ربودن نشست چیست؟	۱۸۰
شرح چگونگی جلوگیری از ربودن نشست	۱۸۲
موارد حایز اهمیت در امتحان	۱۸۳
سؤالات	۱۸۵
پاسخ سؤالات	۱۸۹

فصل هشتم: نفوذ به سرورهای وب، آسیب پذیری های نرم افزارهای تحت وب و روش های شکستن	
مبتنی بر وب کلمه عبور	۱۹۱
نفوذ کردن به سرورهای وب	۱۹۲
فهرست انواع آسیب پذیری های سرور وب	۱۹۲
شناخت حملات علیه سرورهای وب	۱۹۳
شناخت exploit های IIS Unicode	۱۹۴
شناخت روش های مدیریت patch	۱۹۴
تشریح روش های مقاوم سازی سرور وب	۱۹۵
آسیب پذیری های نرم افزاری تحت وب	۱۹۶
دانستن اینکه نرم افزارهای تحت وب چگونه کار می کنند	۱۹۶
اهداف نفوذ کردن به نرم افزارهای تحت وب	۱۹۶
آنا تومی یک حمله	۱۹۷
تهدیدات نرم افزارهای تحت وب	۱۹۷
شناخت هک گوگلی	۱۹۹
شناخت راه های مقابله با نفوذ به نرم افزارهای تحت وب	۱۹۹
شکستن مبتنی بر وب کلمات عبور	۱۹۹
لیست انواع احراز هویت	۲۰۰
پسورد شکن چیست؟	۲۰۰
پسورد شکن چگونه کار می کند؟	۲۰۰
شناخت حملات کلمه عبور: طبقه بندی	۲۰۱
شناخت راه های مقابله با شکستن کلمات عبور	۲۰۱
موارد حایز اهمیت در امتحان	۲۰۱
سؤالات	۲۰۳
پاسخ سؤالات	۲۰۵
فصل نهم: تزریق SQL و سرریز کردن حافظه	۲۰۷
تزریق SQL	۲۰۸
تزریق SQL چیست؟	۲۰۸
شناخت مراحل انجام تزریق SQL	۲۰۸

۲۰۹.....	شناخت آسیب پذیری‌های سرور SQL
۲۱۰.....	شرح راه‌های مقابله با تزریق SQL
۲۱۰.....	حمله سرریز کردن حافظه (Buffer Overflow)
۲۱۰.....	شناسایی انواع حملات سرریز کردن حافظه و روش‌های شناسایی
۲۱۱.....	نگاه کلی به حمله سرریز کردن حافظه از نوع مبتنی بر پشته
۲۱۱.....	نگاه کلی به تکنیک‌های mutation سرریز کردن حافظه
۲۱۲.....	موارد حایز اهمیت در امتحان
۲۱۳.....	سؤالات
۲۱۵.....	پاسخ سؤالات
۲۱۷.....	فصل دهم: نفوذ بی سیم
۲۱۸.....	نگاه کلی به مکانیزم‌های احراز هویت WEP و WPA و تکنیک‌های crack کردن
۲۲۱.....	نگاه کلی به اسنifferهای بی سیم و پیدا کردن SSIDها و جعل MAC
۲۲۱.....	شناخت Access Point های ولگرد
۲۲۲.....	شناخت تکنیک‌های نفوذ بی سیم
۲۲۲.....	تشریح روش‌های امن سازی شبکه‌های بی سیم
۲۲۳.....	موارد حایز اهمیت در امتحان
۲۲۴.....	سؤالات
۲۲۶.....	پاسخ سؤالات
۲۲۷.....	فصل یازدهم: امنیت فیزیکی
۲۲۸.....	وقایع نفوذ به امنیت فیزیکی
۲۲۹.....	شناخت امنیت فیزیکی
۲۳۰.....	برای امنیت فیزیکی چه چیزی مورد نیاز است؟
۲۳۰.....	برای امنیت فیزیکی روی چه کسانی می‌توان حساب کرد؟
۲۳۰.....	عوامل اثرگذار بر امنیت فیزیکی
۲۳۱.....	موارد حایز اهمیت در امتحان
۲۳۲.....	سؤالات
۲۳۴.....	پاسخ سؤالات

۲۳۵.....	فصل دوازدهم: نفوذ به لینوکس
۲۳۶.....	مبانی لینوکس
۲۳۷.....	شناخت چگونگی کامپایل کرنل لینوکس
۲۳۸.....	شناخت دستورات کامپایل GCC
۲۳۹.....	یادگیری چگونگی راهاندازی مازول های کرنل لینوکس
۲۳۹.....	شناخت روش های استحکام بخشی به لینوکس
۲۴۰.....	موارد حایز اهمیت در امتحان
۲۴۲.....	سؤالات
۲۴۴.....	پاسخ سؤالات
۲۴۵.....	فصل سیزدهم: گریز از HoneyPot, IDS و فایروال
۲۴۶.....	لیست انواع سیستم های کشف اختلالگری و تکنیک های گریز
۲۴۸.....	لیست تکنیک های گریز از انواع فایروال و honeypot
۲۵۰.....	موارد حایز اهمیت در امتحان
۲۵۱.....	سؤالات
۲۵۳.....	پاسخ سؤالات
۲۵۵.....	فصل چهاردهم: رمزنگاری
۲۵۶.....	نگاه کلی به رمزنگاری و تکنیک های آن
۲۵۷.....	شرح چگونگی ساخت کلیدهای عمومی و خصوصی
۲۵۷.....	نگاه کلی به الگوریتم های RC5, RC4, SHA, MD5 و Blowfish
۲۵۸.....	موارد حایز اهمیت در امتحان
۲۶۰.....	سؤالات
۲۶۱.....	پاسخ سؤالات
۲۶۳.....	فصل پانزدهم: شیوه های تست نفوذ
۲۶۴.....	تعریف سنجش امنیت
۲۶۴.....	نگاه کلی به شیوه های تست نفوذ
۲۶۵.....	لیست مراحل تست نفوذ
۲۶۷.....	نگاه کلی به چارچوب حقوقی تست نفوذ

۲۶۷.....	لیست ابزارهای اتوماتیک تست نفوذ.....
۲۶۸.....	نگاه کلی به خروجی‌های تست نفوذ.....
۲۶۹.....	موارد حایز اهمیت در امتحان.....
۲۷۰.....	سؤالات.....
۲۷۲.....	پاسخ سؤالات.....

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 خیره 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 Honeypot IDS و فایروال

سرریز کردن حافظه

رمزنگاری

شیوه‌های تست نفوذ