هکر قانونمند جلد اول

Certified Ethical Hacker

سرشناسه	: حدادیان، امین، ۱۳۷۱ -
عنوان و نام پدیدآور	: هکر قانونمند مبتنی بر EC-Council Certified Ethical Hacker v8.0 / امین حدادیان.
مشخصات نشر	: اصفهان: نخبگان شریف، ۱۳۹۴
مشخصات ظاهری	: ۲ج.:مصور(رنگی)، جدول(رنگی)، نمودار(رنگی) .
شابک	: ج.۱: ۲-۰-۹۶۱۲۸-۶۰۰-۹۷۸؛ ج.۲: ۹-۱-۹۶۱۲۸-۶۰۰-۹۷۸
وضعیت فهرست نویسی	: فیپا
موضوع	: آزمایش نفوذ (ایمن‌سازی کامپیوتر)
موضوع	: کامپیوترها -- کنترل دسترسی
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: هکرها
رده بندی کنگره	: ۱۳۹۴ ۳ح۹ک/QA۷۶/۹
رده بندی دیویی	: ۸/۵۰۰
شماره کتابشناسی ملی	: ۳۹۲۰۶۷۸

انتشارات نخبگان شریف

عنوان اثر: هکر قانونمند جلد اول

مولف : امین حدادیان

نوبت چاپ : اول

سال نشر: ۱۳۹٤

شمارگان : ۲۰۰۰ جلد

صفحه آرا : امین حدادیان

مسئول چاپ و نشر : مهندس محمدهادی احمدی

قیمت : ۲۵۰۰۰ تومان

شابک : ۲ -۰- ۹۶۱۲۸ -۶۰۰-۹۷۸ **ISBN: 978-600-96128-0-2**

شابک دوره: ۸-۸-۹۶۱۲۸-۶۰۰-۹۷۸

اصفهان - خیابان میر - جنب پل هوایی - مجتمع تجاری پگاه - واحد شماره ۱۱

۰۳۱-۳۶۶۲۲۶۹۰ ۰۳۱-۳۶۶۲۲۴۹۹

۰۹۱۳ ۳۰ ۳۰۱۴۱ www.bamabashidlotfan.ir

ahmadi.mohamadhadi61@gmail.com

@ negin141

فهرست مطالب

سخنی با خوانندگان

امروزه کمتر کسی را می‌توان یافت که اطلاعاتی برای ازدست رفتن نداشته باشد. همه ما در معرض ازدست رفتن اطلاعاتی هستیم که ممکن است به‌دست آوردن آنها دیگر امکان‌پذیر نباشد. از سوی دیگر نوع دیگری از دزدی و ناامنی در محیط‌های کاری رواج یافته است که ریشه در گسترش فناوری اطلاعات و ارتباطات و آسیب‌های همراه آن دارد. آن ناامنی، اطلاعاتی است که در گذشته‌های دور بارزترین مصداق آن دانستن جای کلید گاو صندوق بزرگانی بود که گنجینه‌های نهفته در آن داشتند، اما امروز همه افراد گنجینه‌های گرانبهایی در اختیار دارند و معمولاً امکان دسترسی به آنها ازسوی افراد مختلف امکان‌پذیر است.

حوزه‌ای که این بعد از زندگی را تحت پوشش قرار می‌دهد، امنیت فناوری اطلاعات است. بدون شک مهم‌ترین مقوله در امنیت فناوری اطلاعات آگاهی است، در صورتی‌که همه ما از جوانب مختلف امنیت اطلاعات و یا ناامنی‌های اطلاعاتی آگاه باشیم، کمتر دچار ضرر و زیان می‌شویم. دردناک‌ترین بُعد ناامنی اطلاعات زمانی است که اطلاعات دزدیده شده تنها اطلاعات فردی و شخصی نیست، بلکه مربوط به گروهی از افراد یک سازمان و حتی یک کشور است که امکان خرابکاری با مقیاس بزرگتر را فراهم می‌کند.

ساده‌ترین و موثرترین راه برای دستیابی به آگاهی، آموزش است. بنابراین آموزش امنیت اطلاعات یکی از مهم‌ترین مباحثی است که باید در سطح فردی، سازمانی و ملی به آن پرداخته شود.

امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات است که باهدف تضمین استمرار فعالیت‌های کاری به حداقل رساندن ریسک‌های کاری و به حداکثر رساندن بازدهی سرمایه‌گذاری‌ها و فرصت‌ها صورت می‌گیرد که طبق این دیدگاه امنیت اطلاعات تاثیر مثبتی بر روند سازمان دارد. از منظری دیگر امنیت فناوری اطلاعات کنترلی برای تضمین تداوم حفاظت از دارایی‌های سازمان از آسیب یا ازدست دادن معنا شده است. به عبارت دیگر امنیت اطلاعات حفاظت از اطلاعات و به حداقل رساندن خطر افشای آن در بخش‌های غیر مجاز اشاره دارد که مستلزم نوعی از ابزارها برای جلوگیری ازسرقت، حمله، جنایت و جاسوسی و خرابکاری است. امنیت اطلاعات توجه تمامی‌سازمان‌ها را در سراسر دنیا به خود جلب کرده است. با توجه به این‌که اقتصاد و کسب و کار مدرن برای بقا بطور کامل به فناوری اطلاعات وابسته‌اند، نیاز به حفاظت از اطلاعات ازقبل بیش‌تر می‌شود.

از آن‌جا که تقریبا همه جنبه‌های زندگی ما به وسیله ابزارها، رویه‌ها و تکنولوژی تحت کنترل قرار گرفته‌اند این موارد اهمیتی فزاینده یافته که اثرات گسترده فناوری الکترونیک نقاط ضعف و آجزای محرّمانه را نیز درک کرده است.

هر سازمان برای رسیدن به سطح قابل قبولی از امنیت بایستی تمام عوامل مؤثر در امنیت رادر نظر بگیرد و لازم به ذکر است که عدم توجه متناسب به تمام عوامل در بیش‌تر مواقع سایر تمهیدات امنیتی را بی اثر می‌کند.

منبع اصلی این کتاب، مجموعه کتب آموزشی CEH V8.0 است که که از سوی شرکت EC-Council به عنوان مرجع اصلی برای آزمون‌های بین المللی معرفی شده است. لذا این کتاب برای کسانی که تمایل دارند در آزمون بین المللی ۵۰-۳۱۲ شرکت EC-Council شرکت کنند مناسب خواهد بود. همچنین این کتاب برای خود خوانی(Self Study) مناسب است اما توصیه می‌شود در کنار کلاس‌های آموزشی از آن استفاده گردد.

از آنجایی که پیشنیاز دوره CEH، تسلط بر مبانی شبکه و نیز مبانی امنیت شبکه است، در تألیف این کتاب نیز فرض بر آن گرفته شده است که شما خواننده گرامی‌دوره‌های Network+ و Security+ شرکت EC-Council و یا دوره‌های معادل آنها در شرکت Cisco را گذرانده اید. به دلیل تخصصی بودن مطالب، در نگارش این کتاب تلاش شده است تا از ادبیاتی ساده، روان و قابل فهم استفاده شود. از آنجایی که برگرداندن بسیاری از اصطلاحات و مفاهیم انگلیسیِ هک و امنیت به معادلِ آنها در فارسی، معنا و مفهوم آنها را دچار دگرگونی می ساخت، در اغلب موارد اصطلاحات انگلیسی به جای معادل (برگردان) فارسی آنها استفاده شده است. لذا خواننده این کتاب می‌بایست حتماً دوره Security+ را گذرانده باشد و یا به درک قابل قبولی از مفاهیم شبکه، امنیت و هک رسیده باشد. همچنین به دلیل فهم ساده‌تر برخی مطالب از طریق شکل‌ها، تلاش شده تا آنها را بصورت مصور توضیح داده و از آوردن توضیحات اضافی خودداری شود.

قابل ذکر است کلیه مطالب این کتاب صرفاً جنبه آموزشی دارد و مسئولیت هرگونه سوء استفاده از ابزارهای معرفی شده در آن، بر عهده شخص استفاده کننده می‌باشد.

بی‌صبرانه منتظر دریافت نظرات، پیشنهادات و انتقادات شما عزیزان هستم. درصورت یافتن هرگونه مشکل نگارشی و یا علمی لطفاً اینجانب را در جریان بگذارید.

e-mail:info@DES.co.ir
Web-site:www.DES.co.ir
Cyber Security & Protection Services

مهندس توفیق