به‌نام ایزد یکتا

راهنمای جامع آزمون

CEH v10

Ric Messier

ترجمه: مهران تاجبخش

انتشارات پندار پارس

سرشناسه	:	مسیر، ریک Messier, Ric
عنوان و نام پدیدآور	:	راهنمای جامع آزمون Ric Messier/CEH v10 : ترجمه مهران تاجبخش.
مشخصات نشر	:	تهران : پندار پارس ، ۱۳۹۹.
مشخصات ظاهری	:	۵۷۰ : ص.
شابک	:	978-600-820187-8
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	عنوان اصلی: Ceh v10 Certified ethical hacker Study ,2019
عنوان گسترده	:	راهنمای جامع آزمون سی ای اچ وی ده.
موضوع	:	کامپیوترها — ایمنی اطلاعات — آزمون‌ها — راهنمای مطالعه
موضوع	:	Computer security -- Examinations -- Study guides
موضوع	:	آزمایش نفوذ (ایمن‌سازی کامپیوتر) — آزمون‌ها — راهنمای مطالعه
موضوع	:	Penetration testing (Computer security) -- Examinations -- Study guides
موضوع	:	هکرها — آزمون‌ها — راهنمای مطالعه
موضوع	:	Hackers -- Examinations -- Study guides
شناسه افزوده	:	تاجبخش، مهران، ۱۳۴۷ - مترجم
رده بندی کنگره	:	۹/۷۶QA
رده بندی دیویی	:	۸۰۷۶/۰۰۵
شماره کتابشناسی ملی	:	۶۱ ۶۴۵

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، روی روستم، شماره ۱۴، واحد ۱۶

www.pendarepars.com

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸همراه: ۰۹ ۴۵۲۱۲۸

نام کتاب	:	راهنمای جامع آزمون CEH v10
ناشر	:	انتشارات پندار پارس
تالیف	:	ریک ماسیر
ترجمه	:	مهران تاجبخش
چاپ نخست	:	بهار ۹۹
شمارگان	:	۵۰۰ نسخه
طرح جلد	:	رامین شکرالهی
چاپ، صحافی	:	روز
قیمت	:	۱۲۰۰۰۰ تومان

شابک : ۸-۸۷-۸۲۰۱-۶۰۰-۹۷۸

فهرست

پیش‌گفتار

آیا در فکر کسب گواهینامه هکر اخلاقی (CEH)هستید؟ بدون توجه به اینکه چه تخصص‌هایی در تست امنیت دارید- هک اخلاقی، تست نفوذ، عضویت در تیم قرمز و یا برآورد نرم‌افزارها- به دنبال کسب مهارت و دانش لازم در گواهینامه هکر اخلاقی هستید. استفاده از تکنیک‌های موجود در تست امنیت و هک اخلاقی باعث شده است تا سازمان‌ها شناخت بهتری درباره حملات و تهدیدهای بالقوه موجود داشته شوند. با توجه به اینکه امروزه حملات سازماندهی شده است، برای تشخیص و مقابله با آنها نیاز داریم تا از تکنیک‌ها و روش‌های مختلفی استفاده کنیم.

بدون در نظر گرفتن مخاطب این کتاب، باید در نظر داشته باشیم که بین ۸۰ تا ۹۰ درصد حملات امروزی مبتنی بر حملات مهندسی اجتماعی است. امروزه با توجه به استفاده از فناوری‌های دفاع در عمق و ایمن‌سازی ارتباط‌های خارجی شبکه سازمان، استفاده از روش‌های قدیمی مبتنی بر آسیب‌پذیری‌های تکنیکی موجود در تجهیزات و نرم افزارهای شبکه‌های سازمان، کارآیی ندارند. در حال حاضر تمرکز حملات بر روی استفاده از آسیب‌پذیری‌های موجود در داخل سازمان است و به همین دلیل است که دیستریبوتورهای رومیزی داخل سازمان، هدف حمله و دستکاری قرار می‌گیرند.

این کتاب برای کمک به منظور فرگیری دانش و مهارت مورد نظر برای کسب گواهینامه هکر اخلاقی نوشته شده است. البته باید در نظر داشته باشید که علی رغم ارائه مطالب کامل و جامع در مورد مفاهیم و فناوری‌های موجود در این حوزه، کسب تجربه‌های عملی و کاربردی در بکارگیری آنها نقش بسیار مهمی ایفا می‌کند.

ارائه مطالب در حوزه هک و تست نفوذ بدون در نظر گرفتن موارد اخلاقی و قانونی امکان‌پذیر نیست، به همین دلیل است که در بخش های مختلفی از کتاب به این موارد اشاره شده است. شناخت این موارد و بکارگیری آنها باعث حفاظت از خود و افرادی که برای آنها کار می‌کنیم، خواهد شد. نسخه خیلی کوتاه و مختصر از جنبه‌های اخلاقی و قانونی هک و تست نفوذ این است که هیچگاه باعث خرابی و اختلال در سیستم کارفرما نشویم.

در پایان هر فصل مجموعه‌ای از سوالات ارائه شده است. این سوالات برای مرور مطالب ارائه شده در هر فصل است. سوالات به صورت چند گزینه‌ای ارائه شده و در همان قالب سوالات آزمون CEH است. خواندن دقیق مطالب هر فصل و پاسخ به سوالات در پایان هر فصل و کسب مهارت و تجربه عملی در مورد آنها می‌تواند باعث کسب موفقیت شما در آزمون CEH شود.

CEH چیست؟

گواهینامه هکر اخلاقی (Certified Ethical Hacker) به منزله تائید دانش و مهارت کافی دارنده آن برای اجرای پروژه‌های مختلف در حوزه هک اخلاقی و تست نفوذ می‌باشد.

CEH گواهینامه‌ای است که دارنده آن توانایی تشخیص آسیب‌پذیری‌ها و موارد امنیتی موجود و ارائه راهکارهایی برای از بین بردن و یا کاهش آنها را دارد. استفاده از هکر اخلاقی (CEH) یکی از راه‌هایی است که سازمان‌ها می‌توانند خود را در مقابل حملات محافظت کنند، زیرا هکر اخلاقی قادر است تا راه‌های حمله بالقوه موجود را پیش از مهاجم تشخیص دهد. با این هدف، یک هکر اخلاقی دقیقا همان مسیری را که یک مهاجم دنبال می‌کند طی می‌کند. اسکن آسیب‌پذیری‌های شبکه با استفاده از ابزارهای تست خودکار آسیب‌پذیری، به تنهایی کافی نیست. زیرا این ابزارها در برخی موارد دارای تشخیص‌های نادرست می‌باشند و علاوه بر آن قادر به شناسایی بسیاری از آسیب‌پذیری‌های موجود نمی‌باشند.

از آنجایی که سازمان‌ها نیاز به شناسایی نقاط آسیب‌پذیر در شبکه دارند، باید افرادی را برای این کار به‌کار گیرند، البته باید در نظر داشته باشیم که شناسایی آسیب‌پذیری‌های سازمان، کار بسیار پیچیده و دشواری است. استفاده از اسکنرها برای شروع مناسب هستند، اما شناسایی نقاط نفوذ و آسیب‌پذیری در شبکه‌هایی با ساختارهای پیچیده، نیازمند جمع‌آوری اطلاعات جزئی‌تر و نیز استفاده از راه‌کارهای نوآورانه و خلاق است. به همین دلیل است که سازمان‌ها ناگزیر از استفاده از هکرهای اخلاقی می‌باشند.

آزمون CEH به دو دلیل طراحی شده است. در این آزمون نه تنها دانش فنی عمیق متقاضی آن مورد سنجش قرار می‌گیرد، بلکه رعایت نکات و موارد اخلاقی و قانونی در روند استفاده از آنها نیز همواره مد نظر می‌باشد. سازمان‌ها با بکارگیری افرادی که دارای گواهینامه CEH می‌باشند، مطمئن می‌شوند که آنها علاوه بر داشتن دانش و توانایی لازم برای تست نفوذ و شناسایی آسیب‌پذیری‌های موجود در شبکه و فناوری‌های مورد استفاده سازمان، هیچگاه کاری که منجر به بروز اختلال و خرابی در سیستم‌ها و روندهای سازمان خود را انجام نمی‌دهند.

هدف کتاب

برای اینکه خواننده کتاب بتواند خود را برای گذراندن آزمون CEHv10 آماده کند، در این کتاب موضوعات زیر مطابق با آخرین سرفصل‌های ارائه شده برای آزمون CEHv10 ارائه شده است:

- مقدمه‌ای بر هک اخلاقی
- جمع‌آوری و یادداشت‌برداری
- اسکن شبکه
- سرشماری و برآورد
- آنالیز آسیب‌پذیری
- هک سیستم
- تهدیدهای بدافزار
- اسنیفرها
- مهندسی اجتماعی