

هکر قانونمند

(CEH v9)

تست به همراه پاسخ تشریحی

مطابق با آخرین سرفصل آزمون بین‌المللی

ec-council – CEH v9

محتوی کارت قرعه‌کشی و عضویت

در باشگاه خوانندگان پندار پارس

تألیف: ریموند بلاکمن

برگردان: مهندس مهران تاجبخش

انتشارات پندار پارس

فهرست

فصل نخست: تست‌های آمادگی آزمون ۱.....	۹
فصل دوم: تست‌های آمادگی آزمون ۲.....	۴۳
فصل سوم: تست‌های تمرینی ۳.....	۷۵
فصل چهارم: تست‌های تمرینی ۴.....	۱۰۵
فصل پنجم: تست‌های تمرینی ۵.....	۱۳۷

پاسخ‌نامه‌ها

پاسخ‌نامه: تست‌های آمادگی آزمون ۱.....	۱۷۱
پاسخ‌نامه: تست‌های آمادگی آزمون ۲.....	۱۸۳
پاسخ‌نامه: تست‌های آمادگی آزمون ۳.....	۱۹۵
پاسخ‌نامه: تست‌های آمادگی آزمون ۴.....	۲۰۷
پاسخ‌نامه: تست‌های آمادگی آزمون ۵.....	۲۲۱

پیش گفتار

ظهور و توسعه فناوری‌های نوین در حوزه فناوری اطلاعات و شبکه‌های کامپیوتری و قابلیت‌های موجود در آنها باعث شده است که استفاده از این فناوری‌ها در سازمان‌ها و موسسات مختلف اعم از دولتی و خصوصی و مالی و تجاری و بانک‌ها و ... روز به روز بیشتر شود؛ تا جایی که امروزه واحدهای فناوری اطلاعات به عنوان یکی از بخش‌های غیر قابل تفکیک در سازمان و موسسات مختلف تبدیل شده است. استفاده و به کارگیری هر فناوری جدید، افزون بر نکات مثبت، با نقاط ضعف و آسیب‌پذیری‌هایی نیز همراه است.

مهم‌ترین نقاط ضعف آسیب‌پذیری‌هایی که در حوزه فناوری اطلاعات، راهبران و کاربران آنها را تهدید می‌کند را می‌توان به دو بخش انسانی و غیر انسانی تقسیم کرد. در بخش انسانی، عدم آموزش کافی و سهل انگاری و همچنین مظاهر کاربردی را می‌توان برشمرد و در بخش تهدیدهای غیر انسانی، نقاط ضعف و آسیب‌پذیری‌های ناشی از تصمیم و وابستگی نامناسب و همچنین شناسایی آسیب‌پذیری‌های جدید در آن را می‌توان نام برد.

با توجه به اینکه شناسایی و دسترس‌سازی آسیب‌پذیری‌ها و نقاط ضعف موجود به همراه بررسی و کشف نقاط ضعف و آسیب‌پذیری‌های جدید در سیستم‌های سخت‌افزاری و نرم‌افزاری مورد استفاده، و ارائه راهکارهای رفع و کاهش آنها نقش بسیار زیاد و مثری در امن‌سازی حوزه فناوری اطلاعات در سازمان و موسسات ایفا می‌کند، بنابراین نیاز به متخصصان تست نفوذ و هکر قانونمند که در این حوزه آموزش‌های تخصصی و مدونی را گذرانده‌اند، لازم و ضروری می‌باشد.

بدون تردید شناخته‌شده‌ترین، به‌روزترین و معتبرترین دوره آموزش در حوزه تست نفوذ و هکر قانونمند، دوره (Certified Ethical Hacking) CEH می‌باشد که پس از رخداد ۱۱ سپتامبر ۲۰۰۱ در مرکز تجارت جهانی نیویورک، به طور جدی‌تر و سازمان یافته‌تر و در سطح وسیع‌تر توسط موسسه EC-Council مورد توجه قرار گرفت.

هم اینک بیش از ۱۵۰/۰۰۰ نفر در سراسر دنیا این دوره تخصصی در حوزه تست نفوذ و هکر قانونمند را گذرانده و موفق به دریافت مدرک بین‌المللی آن شده‌اند.

با توجه به ظهور و پیدایش تهدیدها و آسیب‌پذیری‌های مختلف به همراه ارائه فناوری‌های نوین در حوزه‌های سخت‌افزاری و نرم‌افزاری و کاربردهای آنها، لازم است که متخصصان حوزه تست نفوذ و هکر قانونمند، پی‌درپی خود را به‌روز نگه دارند تا بتوانند با این چالش‌ها در حوزه فناوری اطلاعات به بهترین شکل ممکن برخورد نمایند. در همین راستا موسسه EC-Council به طور منظم و دست‌کم یک بار در سال اقدام به به‌روزرسانی محتوا و برنامه آموزشی دوره CEH خود می‌نماید. هم اکنون این دوره آموزشی با آخرین برنامه و سرفصل و محتوای ارائه شده با عنوان CEHV9 مورد استفاده قرار می‌گیرد.

در برنامه آموزشی این دوره بیش از ۲۷۰ نوع روش حمله و نفوذ مورد بررسی قرار می‌گیرد و افزون بر آن در مجموعه آموزشی ارائه شده برای این دوره، بیش از ۱۴۰ کار عملی در قالب فعالیت‌های آزمایشگاهی بر گرفته

شده از سناریوهای واقعی با معرفی ۲۲۰۰ ابزار مختلف و به کارگیری بخشی از آنها به صورت عملی پیش‌بینی شده است.

با آزمون بین‌المللی CEHv9 بیشتر آشنا شویم

سرفصل و محتوای آموزشی و همچنین شرایط و قالب برگزاری آزمون بین‌المللی آن توسط موسسه EC-Council آمریکا به طور سالانه اعلام می‌گردد. البته در معرفی این دوره آموزشی به صراحت اعلام شده است که محتوا و سرفصل آموزشی و شرایط برگزاری آزمون می‌تواند بدون اطلاع قبلی در هر زمانی توسط موسسه EC-Council به‌روزرسانی شود و تغییر کند. این آزمون بین‌المللی دارای کد 312-50 است. این آزمون از ۱۲۵ پرسش چند گزینه‌ای تشکیل شده است و زمان برگزاری آزمون ۴ ساعت بوده و برای کسب موفقیت در آزمون، داوطلب باید دست‌کم ۷۰ درصد امتیاز در نظر گرفته شده برای آزمون را کسب کند. این آزمون توسط موسسات ECCEXAM / VUE برگزار می‌شود.

موضوع‌های تشکیل‌دهنده این دوره آموزشی، ۲۰ عنوان به شرح زیر می‌باشند:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Network
- Enumeration
- System Hacking
- Malware Threats
- Evading IDS, Firewalls and Honeypots
- Sniffing
- Social Engineering
- Denial of Services
- Session Hijacking
- Hacking Web servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- Cloud Computing
- Cryptography

محتوای موضوعی آزمون بین‌المللی CEHV9

- حوزه بررسی و برآورد تهدید و آسیب‌پذیری‌ها: ۱۶ درصد
- حوزه امنیت: ۲۶ درصد
- حوزه ابزارها / سیستم‌ها / نرم‌افزارها: ۳۲ درصد
- حوزه روش‌ها و متدها: ۲۲ درصد
- حوزه قوانین و آیین‌نامه‌ها: ۴ درصد

چه مطالعاتی را در این کتاب خواهید آموخت

در این کتاب مطالب در ۵ فصل ارائه شده است، بیش از ۶۰۰ پرسش چند گزینه‌ای برگرفته شده از آخرین تغییرات و به‌روزرسانی‌ها، شما را آماده می‌کند که در آزمون بین‌المللی CEHV9 شرکت کنید.

تلاش شده است تا پرسش‌ها، تمرین‌های طراحی و ارائه شوند که تا حد زیادی به آزمون واقعی دوره بین‌المللی EC-Council CEH شباهت داشته باشد.

در پایان کتاب به تفکیک هر فصل، کتاب پاسخ‌نامه به انضمام پاسخ تشریحی آنها نیز ارائه شده است.

گفتمنی است که استفاده از این کتاب به عنوان تنها منبع آموزشی برای آماده‌سازی آزمون بین‌المللی CEH کافی نیست و بهترین کاربرد این کتاب در تست‌های ارزیابی میزان فراگیری دانش و همچنین آشنایی با نمونه سوالات آزمون بین‌المللی می‌باشد.

این کتاب برای چه کسانی است

با توجه به اینکه آشنایی با روش‌های گردآوری اطلاعات و شناسایی نقاط ضعف و آسیب‌پذیری‌ها و همچنین ابزارها و فناوری‌هایی که برای نفوذ استفاده می‌شوند، برای همه متخصصان امنیت و تست نفوذ و ادله الکترونیک لازم و ضروری می‌باشد، بنابراین مطالعه این کتاب به همه این گروه‌ها توصیه می‌گردد. هرچند، این کتاب می‌تواند برای همه کسانی که در حوزه امنیت فضای مجازی و تست نفوذ فعالیت می‌کنند و یا خود را برای آزمون بین‌المللی CEH آماده می‌کنند نیز مفید باشد.

درباره مترجم

با بیش از ۲۶ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه در حدود ۱۰ سال است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و فضای مجازی و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت داشته و دارای چندین مدرک بین‌المللی در حوزه شبکه، امنیت شبکه و تست نفوذ است که عبارتند از:

Network+, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW security Professional, ISO27001 Lead Auditor.

در صورت نیاز به برقراری ارتباط با مترجم می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

مهران تاجبخش

زمستان ۹۵

www.ketab.ir