

به نام ایزد بکنا

راهنمای جامع آزمون

CEH v10

Ric Messier

ترجمه: مهران تاجبخش

انتشارات پندار پارس

www.ketab.ir

سرشناسه	مسیر، ریک
عنوان و نام پدیدآور	Messier, Ric
مشخصات نشر	راهنمای جامع آزمون Ric Messier/CEH v10 : ترجمه مهران تاجبخش.
مشخصات ظاهری	تهران : پندار پارس ۱۳۹۹.
شابک	۵۷۰ ص.
وضعیت فهرست نویسی	978-600-820187-8
یادداشت	فیا
عنوان گسترده	Ceh v10 Certified ethical hacker Study, 2019
موضوع	راهنمای جامع آزمون سی ای ایچ وی ده.
موضوع	کامپیوترها -- امنیت اطلاعات -- آزمون‌ها -- راهنمای مطالعه
موضوع	Computer security -- Examinations -- Study guides
موضوع	آزمایش نفوذ (ایمن سازی 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 ی‌سه	۹۷۶Q۸
رده بندی دیویر	۸۰۷۶/۰۰۵
شماره کتابشناسی ملل	۶۱ ۶۴۵

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگر جنوبی، وی ران، شماره ۱۴، واحد ۱۶

www.pendarepars.com

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۴۵۲۱۱۸ - ۹۱



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 : ۹۷۸-۶۰۰-۸۲۰۱-۸۷-۸

* هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

فهرست

۵.....	فصل نخست: هکر قانونمند
۶.....	مروری بر اخلاق
۷.....	واژگان رنگ‌ها
۸.....	مروری بر هک اخلاقی
۹.....	متدولوژی هک اخلاقی
۹.....	یادداشت برداری و بازآفرینی
۱۰.....	اختصاص شمارش
۱۱.....	دسترسی یافتن
۱۲.....	حفظ دسترسی
۱۲.....	مخفی کردن و اهدا
۱۳.....	خلاصه
۱۵.....	فصل دوم: مبانی شبکه
۱۶.....	مدل‌های ارتباطی
۱۷.....	پروتکل‌ها
۱۸.....	مدل OSI
۲۰.....	معماری TCP/IP
۲۱.....	توپولوژی‌ها
۲۲.....	شبکه خطی (Bus)
۲۲.....	شبکه ستاره‌ای (Star)
۲۳.....	شبکه حلقه‌ای (Ring)
۲۴.....	شبکه مش (Mesh)
۲۵.....	شبکه مرکب (Hybrid)
۲۶.....	شبکه فیزیکی (Physical networking)
۲۶.....	آدرس دهی (Addressing)
۲۷.....	مک آدرس‌ها (MAC addresses)
۲۷.....	سوئیچینگ (Switching)
۲۸.....	IP
۲۹.....	عنوان‌ها (Headers)

۳۰	IP headers
۳۱	مقایسه Octet و Byte
۳۲	آدرس دهی (Addressing)
۳۳	زیر شبکه ها (Subnets)
۳۵	TCP
۳۹	UDP
۴۰	پروتکل ICMP
۴۱	معماری های شبکه
۴۱	رایج شبکه
۴۲	اسازی شبکه (Isolation)
۴۳	دسترسی به داده ها
۴۴	پردازش داده ها
۴۵	سرویس دهنده فضای ذخیره سازی (Storage as a Service)
۴۶	سرویس دهنده سخت افزار (Infrastructure as a Service)
۴۷	سرویس دهنده بستر نرم افزاری (Platform as a Service)
۴۹	سرویس دهنده نرم افزار (Software as a Service)
۴۹	اینترنت اشیا (Internet of Things)
۴۹	خلاصه
۵۲	سوالات مرور فصل
۵۵	فصل سوم: مبانی امنیت
۵۶	مثلث امنیت
۵۷	محرمانگی
۵۸	مشمولیت
۶۰	دسترسی
۶۱	شش ضلعی پارکرین
۶۲	ریسک
۶۴	سیاست ها، استانداردها و دستورالعمل ها
۶۴	سیاست های امنیتی
۶۶	استانداردهای امنیت

۶۶	استانداردهای امنیت
۶۶	دستورالعمل‌ها
۶۷	راهنما
۶۷	فناوری‌های امنیتی
۶۸	فایروال‌ها
۷۳	سیستم‌های تشخیص نفوذ
۷۶	سیستم‌های پیشگیری از نفوذ
۷۸	مدیریت رخدادهای امنیت اطلاعات
۷۹	آمادگی شدن
۷۹	دفاع در مقیاس
۸۱	دفاع در سطح
۸۲	ثبت لاگ
۸۴	ممیزی
۸۶	خلاصه
۹۱	فصل چهارم: جمع‌آوری اطلاعات و بازآفرینی
۹۲	منابع اطلاعات آزاد
۹۳	سازمان‌ها
۱۰۱	افراد
۱۰۴	شبکه‌های اجتماعی
۱۱۳	فعالیت
۱۱۴	سایت‌های کاریابی
۱۱۴	سرور DNS
۱۱۶	جستجوی نام دامنه (Name lookups)
۱۲۲	بازآفرینی غیرفعال
۱۲۵	اطلاعات وبسایت
۱۳۰	جمع‌آوری اطلاعات فناوری
۱۳۰	هک کردن با گوگل
۱۳۲	اینترنت اشیا (IoT)

۱۳۴	خلاصه
۱۳۶	سوالات مرور مطالب فصل
۱۴۱	فصل پنجم: اسکن شبکه
۱۴۱	نکته اخلاقی
۱۴۳	Ping Sweeps
۱۴۳	استفاده از fping
۱۴۵	استفاده از ابزار MegaPing
۱۴۶	اسکن پورت‌ها
۱۴۷	Nmap
۱۶۱	masscan
۱۶۳	MegaPing
۱۶۵	اسکن آسیب پذیری
۱۶۷	OpenVAS
۱۷۳	اجرای اسکن آسیب پذیری
۱۷۹	Nessus
۱۸۵	ایجاد و پردازش بسته‌ها
۱۸۶	hping
۱۸۸	packETH
۱۹۰	fragroute
۱۹۲	تکنیک‌های گول زدن
۱۹۴	خلاصه
۱۹۶	سوالات مرور فصل
۲۰۱	فصل ششم: برآورد و سرشماری
۲۰۲	برآورد سرویس‌ها
۲۰۶	فراخوانی روال‌های راه دور
۲۰۶	SunRPC
۲۰۹	Remote Method Invocation
۲۱۲	Server Message Block
۲۱۳	ابزارهای داخلی

۲۱۶	اسکرپت‌های nmap
۲۱۸	Metasploit
۲۲۰	سایر ابزارها
۲۲۳	پروتکل SNMP
۲۲۵	پروتکل SMTP
۲۲۸	جمع‌آوری اطلاعات مبتنی بر وب
۲۳۴	خلاصه
۲۳۶	سوالات مرور فصل
۲۴۱	فصل هفتم: نفوذ به سیستم
۲۴۲	جستجوی کسپلوی
۲۴۶	آماده‌سازی سیستم
۲۴۷	ماژول‌های Metasploit
۲۵۰	Exploit-DB
۲۵۲	جمع‌آوری رمزهای عبور
۲۵۵	رمزگشای رمزعبور
۲۵۶	John the Ripper
۲۵۸	Rainbow جداول
۲۶۰	آسیب‌پذیری سمت کاربر
۲۶۲	مراحل پس از اکسپلویت
۲۶۳	ارتقای سطح دسترسی
۲۶۸	چرخش
۲۷۱	ماندگاری
۲۷۴	مخفی کردن شواهد
۲۸۱	خلاصه
۲۸۳	سوالات مرور فصل
۲۸۷	فصل هشتم: بدافزار
۲۸۸	انواع بدافزار
۲۸۸	ویروس

۲۹۰	کرم
۲۹۱	تروجان
۲۹۱	بات نت
۲۹۲	باچ افزار
۲۹۳	دراپر
۲۹۴	آنالیز بدافزار
۲۹۵	آنالیز استاتیک
۳۰۴	آنالیز دینامیک
۳۱۲	ایچ بدافزار
۳۱۳	نگارن بدافزار
۳۱۶	استفاده از Metasploit
۳۲۰	ساختار بد افزارها
۳۲۲	راه حل های ضد ریسک
۳۲۳	خلاصه
۳۲۵	سوالات مرور فصل
۳۲۹	فصل نهم: استیفرها
۳۳۰	نسخه برداری بسته ترافیکی
۳۳۱	tcpdump
۳۳۶	tshark
۳۳۸	Wireshark
۳۴۲	Berkeley Packet Filter (BPF)
۳۴۴	انعکاس/هم پوشانی پورت
۳۴۵	آنالیز بسته ترافیکی
۳۵۰	حملات گول زدن
۳۵۰	حمله گول زدن با پروتکل ARP
۳۵۴	حمله گول زدن DNS
۳۵۷	sslstrip
۳۵۸	خلاصه
۳۶۱	سوالات مرور فصل

۳۶۷	فصل دهم: مهندسی اجتماعی
۳۶۸	مهندسی اجتماعی
۳۷۰	بهانه
۳۷۲	FYI
۳۷۲	روش‌های مهندسی اجتماعی
۳۷۳	مهندسی اجتماعی فیزیکی
۳۷۳	سترسی به نشان
۳۷۵	دام 'سانی
۳۷۵	بیومتریک
۳۷۶	تماس 'فنی
۳۷۷	طعمه‌گذار
۳۷۸	حملات فیشینگ
۳۸۱	حملات وب‌سایت
۳۸۲	کی‌برداری
۳۸۴	حملات گول زدن
۳۸۵	مهندس اجتماعی از طریق شبکه بی‌سیم
۳۸۹	خودکارسازی حمله مهندسی اجتماعی
۳۹۲	خلاصه
۳۹۴	سوالات مرور فصل
۳۹۹	فصل یازدهم: امنیت بی‌سیم
۴۰۰	Wi-Fi
۴۰۱	انواع شبکه‌های بی‌سیم
۴۰۴	تأیید هویت در شبکه‌های بی‌سیم
۴۰۵	رم‌نگاری در شبکه بی‌سیم
۴۱۱	حملات در شبکه بی‌سیم
۴۲۱	بلوتوث
۴۲۲	اسکن بلوتوث
۴۲۳	Bluejacking

۴۲۴.....	Bluesnarfing
۴۲۴.....	Bluebugging
۴۲۴.....	تجهیزات همراه
۴۲۸.....	خلاصه
۴۳۰.....	سوالات مرور فصل
۴۳۵.....	فصل دوازدهم: حمله و دفاع
۴۳۶.....	حملات نرم افزارهای تحت وب
۴۳۷.....	پردازش داده‌های خارجی XML
۴۳۹.....	Cross-Site Scripting (XSS)
۴۴۱.....	تست SQL
۴۴۴.....	تزریق داده در
۴۴۵.....	حملات اخذ اطلاعات سرور
۴۴۶.....	حملات پهنای
۴۴۹.....	حملات کندکننده
۴۵۱.....	روش‌های سنتی حمله
۴۵۱.....	نفوذ از طریق نرم افزار
۴۵۲.....	سرریزی بافر
۴۵۵.....	مقدارگذاری حافظه هیپ
۴۵۵.....	انتقال جانبی
۴۵۷.....	دفاع در عمق/دفاع در سطح
۴۵۹.....	معماری تدافعی شبکه
۴۶۱.....	خلاصه
۴۶۳.....	سوالات مرور فصل
۴۶۷.....	فصل سیزدهم: رمزنگاری
۴۶۸.....	مبانی رمزنگاری
۴۶۸.....	رمز جاگذاری
۴۷۱.....	Diffie-Hellman
۴۷۳.....	رمزنگاری کلید متقارن
۴۷۳.....	Data Encryption Standard (DES)

۴۷۴	 Advanced Encryption Standard (AES)
۴۷۵	 رمزنگاری کلید نامتقارن
۴۷۶	 سیستم‌های رمزنگاری ترکیبی
۴۷۷	 عدم انکار
۴۷۸	 رمزنگاری منحنی بیضوی
۴۷۹	 صادر کننده گواهینامه و مدیریت کلید
۴۷۹	 صادر کننده گواهینامه (CA)
۴۸۲	 تابع سر قابل اعتماد
۴۸۴	 گواهینامه‌های خودامضا
۴۸۶	 رمزنگاری هش
۴۸۷	 پروتکل‌های PGP و S/MIME
۴۸۹	 خلاصه
۴۹۲	 سوالات مرور فصل
۴۹۵	 فصل چهاردهم: طراحی و معماری امنیت
۴۹۶	 طبقه‌بندی داده
۴۹۷	 مدل‌های امنیت
۴۹۷	 ماشین حالت
۴۹۸	 Biba
۴۹۹	 Bell-LaPadula
۵۰۰	 مدل مشمولیت کلارک-ویلسون
۵۰۱	 معماری نرم‌افزار
۵۰۲	 معماری لایه‌ای نرم‌افزار
۵۰۴	 معماری مبتنی بر سرویس
۵۰۷	 نرم‌افزارهای مبتنی بر فضای ابری
۵۰۹	 نکات مربوط به بانک اطلاعات
۵۱۲	 معماری امنیت
۵۱۹	 سوالات مرور فصل
۵۲۳	 پیوست ۱: پاسخ تشریحی پرسش‌های مرور پایان فصل‌ها

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 تکنیک موجود در تجهیزات و نرم افزارهای شبکه‌های سازمان، کارایی ندارند. در حال حاضر تمرکز حملات بر روی استفاده از آسیب‌پذیری‌های موجود در داخل سازمان است و به همین دلیل است که سیستم‌های 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 علی‌رغم 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 یاد اخلاقی و قانونی امکان‌پذیر نیست، به همین دلیل است که در بخش‌های مختلفی از کتاب به این موارد اشاره شده است. شناخت این موارد و بکارگیری آنها باعث حفاظت از خود و افراد که با 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 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 تایید 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 دقیقاً 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 به کار 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 به کارگیری 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 شود را انجام نمی‌دهند.

هدف کتاب

برای اینکه خواننده کتاب بتواند خود را برای گذراندن آزمون CEH v10 آماده کند، در این کتاب موضوعات زیر مطابق با آخرین سرفصل‌های ارائه شده برای آزمون CEH v10 ارائه شده است:

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