شاگرد قانون‌مند کلاس هکرها!

چگونه با دریافت CEH هکر کلاه‌سفید شویم؟

رخنه‌ها و آسیب‌پذیری‌های امنیتی هیچ‌گاه به انتهای خط نخواهند رسید. آسیب‌پذیری‌هایی که روزبه‌روز رنگ و بوی عجیب‌تری به خود می‌گیرند و شرکت‌ها را مجبور می‌کنند برای محافظت از زیرساخت‌ها، بانک‌های اطلاعاتی و به‌ویژه شبکه‌های ارتباطاتی کارشناسان زبده و حرفه‌ای را استخدام کنند. برای یافتن شغل مورد علاقه‌تان در دنیای امنیت به چیزی فراتر از مهارت‌ها فردی نیاز دارید. شاید در به‌کارگیری ابزارهای امنیتی و نصب بسته‌های پیچیده امنیتی سطح بالایی از دانش و تخصص را داشته باشید. بااین‌حال، بیشتر شرکت‌ها ترجیح می‌دهند افرادی را استخدام کنند که مباحث امنیتی را به شکل استاندارد و منطبق با دوره‌های بین‌المللی فراگرفته باشند. CEH، یکی از محبوب‌ترین دوره‌های آموزشی در حوزه امنیت است که بیشتر آموزشگاه‌های داخل کشور آن را آموزش می‌دهند. اما این دوره چیست و چه مباحثی را آموزش می‌دهد؟

مقدمه‌ای بر آزمون CEH

دوره هکر قانونمند **CEH** (سرنام Certified Ethical Hacker) با هدف آزمایش و تایید سطح آمادگی یک متقاضی برای انجام ارزیابی‌های امنیتی طراحی‌شده است. این آزمون از سوی شورای بین‌المللی گروه مشاوران تجارت الکترونیکی (EC-Council) طراحی، نگهداری و مدیریت‌شده و بیشتر برای افرادی که در اوایل حرفه کاری خود در زمینه امنیت اطلاعات قرار دارند، مناسب است. در حالت ایده‌آل افرادی که در زمینه امنیت یا آموزش مباحث امنیتی دست‌کم دو سال تجربه دارند باید به فکر شرکت در این آزمون باشند. در این آزمون متقاضی باید به پرسش‌ها و تست‌هایی که بیشتر به مباحث زیربنایی و جزییات شبکه‌ها و سامانه‌های کامپیوتری یک سازمان با رویکرد امنیتی مرتبط هستند، پاسخ دهد. اما یک هکر قانونمند کیست؟ فردی است که آسیب‌پذیری و نواقص امنیتی زیرساخت‌های یک سازمان بزرگ یا کوچک را پیش از آن‌که رخنه‌ها از سوی هکرها شناسایی‌شده و استفاده شود، شناسایی کرده و راهکاری برای برطرف کردن آسیب‌پذیری‌ها ارائه می‌کند. **CEH** دوره‌ای است که تمرکز آن روی امنیت شبکه قرار دارد. در این دوره مدیران امنیتی، مدیران شبکه، حسابرسان امنیتی و سایر کارشناسان فناوری اطلاعات سطح مهارت‌های خود را در حوزه امنیت افزایش می‌دهند. در این دوره متقاضیان دریافت **مدرک CEH** باید به 125 سوالی که در هفت بخش قرار گرفته و در ادامه با آن‌ها آشنا خواهید شد، پاسخ دهند.

هک اخلاقی چیست؟

هک اخلاقی عبارتی است که نشان می‌دهد قصد شما از نفوذ به سامانه‌های اطلاعاتی فعالیت‌های مجرمانه یا خرابکاری نیست. در دنیای امنیت واژه هکر با فعالیت‌های مخرب سایبری عجین شده، اما چگونه می‌توانیم رفتار فردی که مکانیزم‌های دفاعی سیستم‌های اطلاعاتی را شکسته و به آن‌ها واردشده است، اخلاق‌مدار توصیف کنیم؟ اصطلاح هکر اخلاقی توصیف‌کننده فردی است که از مهارت‌های مشابه با هکرهای کلاه‌سیاه استفاده می‌کند، با این تفاوت که او به دنبال کسب سودی مشترک است. به عبارت دقیق‌تر، این فرد با شناسایی آسیب‌پذیری‌های درون

زیرساخت‌های یک سازمان و اطلاع دادن به آن‌ها در مورد این آسیب‌پذیری‌ها به دنبال کسب منفعت است، درحالی‌که یک هکر کلاه‌سیاه آسیب‌پذیری‌ها را شناسایی کرده و بدون اطلاع سازمان به استخراج اطلاعات پرداخته یا آسیب‌هایی را به زیرساخت‌ها وارد می‌کند. هکرهای اخلاق‌مدار (کلاه‌سفید)، امنیت سیستم‌های متعلق به کارفرمایان یا مشتریان خود را آزمایش می‌کنند تا بتوانند تمهیدات امنیتی قدرتمندی را پیاده‌سازی کنند.
همانند بسیاری از تخصص‌های فنی، یک برنامه صدور گواهینامه برای انجام این اقدامات در نظر گرفته‌شده است تا هکرهای اخلاقی بتوانند سطح دانش‌پایه و مهارت‌های خود را نشان دهند. **دوره CEH** با این هدف تدوین‌شده است. شرکت‌هایی که به دنبال استخدام کارکنان یا مشاوران برای انجام آزمون‌های نفوذ هستند، بیشتر به سراغ افرادی می‌روند که **گواهینامه CEH** را کسب کرده‌اند. این مدرک نشان می‌دهد، افراد در زمینه ارزیابی مسائل امنیتی سطح خوبی از دانش را داشته و مهم‌تر از آن به لحاظ اخلاقی و فنی شایستگی خود را به اثبات رسانده‌اند.

چرا باید یک هکر اخلاق مدار باشیم؟

این پرسشی است که اغلب افراد آن را مطرح می‌کنند. پاسخ روشن است. بازار کار هکرهای کلاه‌سفید پر رونق است. تقاضا برای متخصصان امنیت اطلاعات روبه فزونی نهاده و افرادی که سطح متوسطی از دانش و تجربه را دارند، به‌راحتی دستمزدهای بالا دریافت می‌کنند. TechTarget، در سال 2014 نظرسنجی را با محوریت حقوق و دستمزدی که کارشناسان امنیت اطلاعات دریافت می‌کنند، ترتیب داد. نتایج این نظرسنجی نشان داد، این افراد به‌طور میانگین 112،372 دلار دستمزد دریافت می‌کنند. کسب مدرک CEH یک راه عالی برای افرادی است که قصد دارند به شکل جدی به دنیای امنیت وارد شوند.

مطلب پیشنهادی

تمرکز بر نقاط ضعف کاربران و زیرساخت‌ها
متداول‌ترین روش‌های هکرها برای پیاده‌سازی حملات

چگونه مدرک CEH را دریافت کنیم؟

برنامه CEH را گروهی متشکل از کارشناسان امنیت اطلاعات سازمان EC-Council اداره می‌کنند و یک گواهینامه سطح مقدماتی است که هدف از برگزاری آن ارزیابی سطح افرادی است که در حوزه امنیت اطلاعات تجربه کمی دارند. البته افرادی که هیچ‌گونه تجربه و پس‌زمینه قبلی در زمینه امنیت اطلاعات ندارند می‌توانند در این دوره ثبت‌نام کنند. برای دریافت این مدرک یا شرکت در آزمون CEH راهکارهای مختلفی پیش روی‌تان قرار دارد. می‌توانید به شکل شخصی، آنلاین یا حضور در مراکز معتبر آموزش‌های لازم را فرابگیرید. هرچند حضور در کلاس‌های آموزشی به شما تضمین می‌دهد که مباحث را به شکل درستی فرا خواهید گرفت. اگر ترجیح می‌دهید، در هیچ‌یک از برنامه‌های آموزش رسمی CEH شرکت نکنید، باید با نحوه ثبت‌نام و واریز وجه آشنایی داشته باشید که با توجه به دشواری‌هایی که وجود دارد، پیشنهاد نمی‌کنم، از این راه به فکر دریافت مدرک فوق باشید. باید به 125 سوال چند گزینه‌ای در مدت زمان 4 ساعت پاسخ دهید که به‌طور متوسط برای هر سوال کمی کمتر از دو دقیقه فرصت دارید که پاسخ دهید. برای موفقیت در این آزمون باید حداقل به 88 سؤال به‌درستی پاسخ دهید. به‌عبارت‌دیگر، به 70 درصد از سوالات به‌درستی پاسخ دهید. مدت اعتبار مدرک CEH سه سال است و پس از پایان این زمان باید اعتبار مدرک خود را برای یک بازه زمانی سه ساله دیگر تمدید کنید.

آزمون CEH شامل چه مباحثی است؟

آزمون CEH بر مبنای یک طرح هفت بخشی تدوین‌شده که هر بخش سوالات خاص خود را دارد. این هفت بخش به شرح زیر هستند:
حوزه 1: 21.79%) Background)
حوزه 2: 12.73%) Analysis/Assessment)
حوزه 3: 23.73%) Security)
حوزه 4: 28.91%) Tools/Systems/Programs)
حوزه 5: 8.77%) Procedures/Methodology)

حوزه 6: Regulation/Policy (1.90%)
حوزه 7: Ethics (2.17%)
همان‌گونه که مشاهده می‌کنید، باید بیشتر وقت خود را صرف حوزه‌های 1،3 و 5 کنید. توجه داشته باشید، اگر مقداری از زمان خود را صرف مطالعه خط‌مشی‌ها و مقررات یا بخش اخلاق کنید، کار بیهوده‌ای انجام نداده‌اید.

آشنایی با 7 بخش آزمون CEH

همان‌گونه که اشاره شد، سوالات آزمون CEH به هفت دامنه/بخش مختلف تقسیم شده‌اند. هر دامنه با حداقل دو و حداکثر 36 سوال شما را ارزیابی می‌کنند. خلاصه سوالات مطرح‌شده در هر یک از بخش‌های این آزمون به شرح زیر است:

دامنه 1: پس‌زمینه (Background)

نخستین حوزه آزمون CEH برای ارزیابی دانش عمومی متقاضیان در زمینه امنیت اطلاعات طراحی‌شده است. 27 سوال به این بخش از آزمون اختصاص داده‌شده و خود این دامنه به سه زیر دامنه به شرح زیر تقسیم‌شده است:
فناوری‌های شبکه و ارتباطات (10 سوال)
تهدیدات امنیتی اطلاعات و بردارهای حمله (9 سوال)
فناوری‌های امنیت اطلاعات (8 سوال)
درحالی‌که اطلاعات کمی درباره سبک و سیاق سوال‌های این دامنه ارائه‌شده است، بااین‌حال، در نگارش قبلی اطلاعات جامع‌تری درباره سوال‌های هر یک از زیرحوزه‌ها به شرح زیر ارائه‌شده بود:
فناوری‌های شبکه (سخت‌افزار، زیرساخت‌ها و...)
فناوری‌های وب (وب 2.0، اسکایپ و...)
فناوری‌های سیستم
پروتکل‌های ارتباطی
عملیات انجام شده از سوی بدافزارها
فناوری‌های همراه (گوشی‌های هوشمند)
فناوری‌های مخابراتی
پشتیبان‌گیری و آرشیو کردن (محلی، شبکه و ...)
سوال‌های این دامنه بیشتر به مباحثی اختصاص دارند که یک هکر کلاه‌سفید باید اطلاعاتی در مورد آن‌ها داشته باشد.

دامنه 2 :تجزیه‌وتحلیل/ارزیابی (Analysis/Assessment)

بخش/ دامنه دوم **آزمون CEH** روی انواع مختلفی از مکانیسم‌های تحلیل و ارزیابی متمرکز است و انتظار می‌رود یک هکر کلاه‌سفید بتواند این تحلیل‌ها را به‌درستی انجام دهد. در این حوزه در مجموع 16 پرسش مطرح‌شده که به دو زیر دامنه تقسیم‌شده است:
1. ارزیابی و تحلیل امنیت اطلاعات (8 سوال)
2. فرآیند ارزیابی امنیت اطلاعات (8 سوال)
همان‌گونه که نام زیردامنه نشان می‌دهد، این بخش از آزمون جنبه‌های ادراکی و شناختی را ارزیابی می‌کند. به عبارت دیگر، پرسش‌های این بخش مجموعه مهارت‌های عمومی و ادراکی متقاضیان را ارزیابی کرده و به چالش می‌کشد. در این حوزه شورای EC چهار عنوان زیر را در نظر گرفته است:
1. تحلیل داده‌ها
2. تجزیه‌وتحلیل سیستم
3. ارزیابی ریسک
4. روش‌های ارزیابی فنی
این بخش از آزمون بیشتر سعی دارد میزان شناخت و سطح ارزیابی‌های سطح بالای شما را در مواجه‌شدن با مسائل امنیتی بررسی کند.

مطلب پیشنهادی

برای مقابله با تهدید اصول آن را یاد بگیرید
10 تکنیک پایه هک که می‌تواند شما را از حمله هکرها مصون نگه دارد

دامنه 3: امنیت

امنیت یکی از سه حوزه بزرگ و مهم **آزمون CEH** است که 30 سوال برای آن در نظر گرفته‌شده است. سوالات مطرح‌شده در این بخش میزان شناخت‌تان از تمامی جنبه‌های مدیریت حوادث امنیتی، از جمله پیشگیری، تشخیص و دفاع پیشگیرانه در برابر حملات را ارزیابی می‌کنند. سه زیر دامنه این بخش به شرح زیر هستند:
1. کنترل امنیت اطلاعات (15 سوال)
2. تشخیص حملات امنیتی (9 سوال)
3. پیشگیری از حمله به داده‌ها (بانک‌های اطلاعاتی) (6 سوال)
سوال‌های این بخش از آزمون، موضوعات و مباحث مختلفی را ارزیابی کرده و در نتیجه به سطح بالایی از دانش و تجربه برای پاسخ‌گویی به این سوالات نیاز است. هدف از سوالات مطرح‌شده در این بخش ارزیابی سطح دانش‌تان در به‌کارگیری ابزارهای امنیتی است. ابزارهایی که برای پیشگیری یا شناسایی حملات از آن‌ها استفاده می‌شود.
به‌عنوان یک متقاضی شرکت‌کننده در این آزمون باید با نحوه پیکربندی و اجرایی کردن این ابزارها آشنایی داشته باشید. موضوعاتی که سازمان EC به‌صراحت در طرح امتحان قبلی خود به آن‌ها اشاره‌کرده بود، به شرح زیر هستند:
- کنترل‌های امنیتی سیستم
- فایل سرور/ برنامه
- فایروال
- رمزنگاری
- امنیت شبکه
- امنیت فیزیکی
- مدل‌سازی تهدیدات
- روش‌های تائید (اعتبار سنجی مثبت / منفی کاذب)
- مهندسی اجتماعی (دستکاری عوامل انسانی)
- اسکنرهای آسیب‌پذیر
- پیامدهای اتخاذ خط‌مشی‌های امنیتی
- حریم خصوصی / محرمانه بودن (با توجه به مشارکت)
- زیستی (بیومتریک)
- فناوری‌های دسترسی بی‌سیم (شبکه، RFID، بلوتوث و غیره)
- شبکه‌های قابل اعتماد
- آسیب‌پذیری
همان‌گونه که مشاهده می‌کنید این بخش از آزمون مباحث مختلفی را پوشش می‌دهد و به بیشتر موضوعات تنها با یک یا دو سوال اشاره‌شده است. بسیاری از این موضوعات (مانند مهندسی اجتماعی و روش‌های تأیید) برای اطلاع از این موضوع که درک درستی از مفاهیم اساسی به دست آورده‌اید، مطرح شده‌اند. اما برای پاسخ‌گویی به پرسش‌های دیگر (مانند فایل
سرور/برنامه) به دانش بیشتری نیاز دارید.

دامنه 4: ابزارها، سامانه‌ها، برنامه‌ها

دانش‌پژوهان علاقه‌مند به شرکت در **آزمون CEH** به این نکته توجه داشته باشند که **آزمون CEH** برای ارزیابی سطح توانمندی حرفه‌ای شما در نظر گرفته‌شده است. در نتیجه برای پاسخ‌گویی درست به سوالات نباید تنها به حفظ جزوات آموزشی و کتاب‌ها بسنده کنید. دامنه 4 یکی دیگر از بخش‌های این آزمون است که 36 سوال برای آن در نظر گرفته‌شده و تمرکزش بر دانش شما از سامانه‌های رایج، برنامه‌ها و ابزارهایی که یک هکر کلاه‌سفید برای انجام

کار خود از آن‌ها استفاده می‌کند، تاکید دارد.
این بخش به سه زیر دامنه تقسیم‌شده است:
1. سیستم‌های امنیت اطلاعات (7 سوال)
2. برنامه‌های امنیت اطلاعات (5 سوال)
3. ابزارهای امنیت اطلاعات (24 سوال)
این بخش از آزمون ترکیبی از مطالب نظری و عملی است. شورای EC تلاش کرده تا دانش متقاضی را در مورد ابزارهایی که برای اهداف مختلف مورد استفاده قرار می‌گیرند، از جمله موارد زیر آزمایش کند:
1. نفوذ مبتنی بر شبکه / میزبان
2. شنود بی‌سیم/شبکه (Wireshark، AirSnort و ...)
3. مکانیزم‌های کنترل دسترسی (کارت‌های هوشمند و مشابه)
4. تکنیک‌های رمزنگاری ((IPsec، SSL، PGP
5. زبان‌های برنامه‌نویسی ((C ++، Java، C #، C
6. زبان‌های اسکریپت‌نویسی ((PHP، JavaScript
7. لوازم به کار گرفته‌شده در ارتباط با حفاظت مرزی
8. توپولوژی شبکه
9. زیرشبکه
10. پویش پورت‌ها ((Nmap
11. سامانه نام دامنه ((DNS
12. روترها / مودم‌ها / سوئیچ‌ها
13. اسکنرهای آسیب‌پذیر (Nessus، Retina و ...)
14. سیستم‌های مدیریت آسیب‌پذیری و حفاظت (مانند Foundstone و (Ecora
15. محیط‌های عامل (ویندوز، لینوکس، مک)
16. سیستم‌های ضدویروس و برنامه‌ها
17. ابزارهای تحلیل گزارش‌ها
18. مدل‌های امنیتی
19. ابزارهایی که برای بهره‌برداری از اکسپولیت‌ها استفاده می‌شود
20. ساختارهای بانک اطلاعاتی عناوین یاد شده به‌خوبی گواه این موضوع هستند که برای پاسخ‌گویی به پرسش‌های این بخش باید به‌درستی با ابزارهای این حوزه آشنا بوده و به شکل عملی با آن‌ها کار کرده باشید. پرسش‌های این بخش از شناسایی کارآمدترین ابزارها برای انجام یک کار خاص تا خواندن خروجی یا فرمت‌بندی ورودی برای یک ابزار را شامل می‌شوند. برای پاسخ‌گویی درست به سوالات این بخش تجربه عملی کار با رایج‌ترین ابزارهای امنیت اطلاعات ضروری است. سعی کنید نحوه کار با ابزارهای Nmap، Metasploit، John the Ripper، THC Hydra، OWASP Zed، Wireshark، Aircrack-ng، Maltego، Cain and Abel و Nikto Website Vulnerability Scanner را به‌خوبی یاد بگیرید.

دامنه 5: روال‌ها/ متدولوژی

برای این بخش 11 سوال درباره روال‌ها و متدولوژی‌های مرسوم امنیت اطلاعات در نظر گرفته‌شده است. این بخش به دو زیر دامنه به شرح زیر تقسیم‌شده است:
1. روال‌های امنیت اطلاعات (5 سوال)
2. روش‌های ارزیابی امنیت اطلاعات (6 سوال)
برای پیاده‌سازی یک راهکار امنیتی و مقابله با بردارهای حمله یک هکر کلاه‌سفید باید درک درستی از مباحث یادشده داشته باشید. این بخش از آزمون دانش در زمینه طراحی و معماری زیربنایی انواع مختلف سامانه‌ها را در رابطه با موضوعات رمزنگاری، زیرساخت کلید عمومی (PKI)، معماری امنیت (SA)، معماری سرویس‌گرا (SOA)، رخداد امنیتی اطلاعات، طراحی برنامه چند لایه (N-Layer)، شبکه‌های مبتنی بر IP / TCP (مسیریابی شبکه) و روش تست امنیتی ارزیابی می‌کند. سوالات مطرح شده در این بخش بیشتر از مباحث فناوری اطلاعات و توسعه نرم‌افزار اقتباس شده‌اند. افرادی که درباره مباحث توسعه نرم‌افزار یا فناوری اطلاعات پیش‌زمینه‌ای دارند در پاسخ‌گویی به سوالات این بخش نباید با مشکل خاصی روبه‌رو شوند.

دامنه 6: خط‌مشی/ مقررات

این بخش یکی از کوچک‌ترین بخش‌های **آزمون CEH** است و تنها دو سوال دارد. به‌عنوان یک هکر کلاه‌سفید باید به‌درستی بدانید هنگام رویارویی با سیاست‌ها و خط‌مشی‌های حاکمیتی درون‌سازمانی و قوانین وضع‌شده از سوی نهادهای قانونی چه رفتار حرفه‌ای از خود نشان دهید. این بخش از آزمون دانش برخی از مقررات مهم امنیت اطلاعات و خط‌مشی‌های حاکمیتی اعمال‌شده را ارزیابی می‌کند.

دامنه 7: اخلاق‌مداری

بخش نهایی **آزمون CEH** پیرامون مباحث اخلاقی است. پرسش‌های این بخش به این موضوع اختصاص دارند که آیا متقاضی می‌داند چگونه از مهارت‌هایی که آموخته به شکل درست استفاده کند؟ در این بخش از آزمون، باید به سه پرسش درباره مباحث اخلاقی پاسخ داده و دانش خود را در مواجه‌شدن با موقعیت‌های خاص ارزیابی کنید. دقت کنید، این بخش از آزمون در ظاهر بی‌اهمیت است، اما یکی از مهم‌ترین بخش‌هایی است که ممکن است شانس را شما برای موفقیت در آزمون با چالش جدی روبه‌رو کند.

منبع:

resources
gocertify
resources
thebalancecareers

تاریخ انتشار:
09 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/15458/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A8%D8%A7-%D8%AF%D8%B1%DB%8C%D8%A7%D9%81%D8%AA-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87%E2%80%8C%D8%B3%D9%81%DB%8C%D8%AF-%D8%B4%D9%88%DB%8C%D9%85%D8%9F