

آشنایی با مدارک و آزمون های بین المللی امنیت Certified Ethical Hacker (CEH)

مدیریت آموزش شرکت کاریار ارقام

فهرست

- ۱- مقدمه: ۳
- ۲-تعداد امتحانات : یک آزمون در مجموع ۴
- ۳-نمونه مدرک CEH ۴
- ۴-میزان درآمد دارندگان مدارک بین المللی امنیت اطلاعات در سال ۲۰۰۹ ۵
- ۵-مزایای دستیابی به مدرک: CEH ۵
- ۶-مسیر دوره های امنیت شبکه ۶
- ۷-آزمون CEH: ۷

۱- مقدمه:

آزمون و مدرک بین المللی CEH مخفف Certified Ethical Hacker متعلق به EC-Council یا International Council of Electronic Commerce Consultants می باشد، این شرکت یک هیات بین المللی از مشاوران تجارت الکترونیکی است که به منظور تامین / پشتیبانی تجارت الکترونیکی انفرادی و سازمانی به صورت حرفه ای ایجاد شده است. این سازمان که در نیویورک آمریکا قرار دارد شامل گستره وسیعی از اعضا در سراسر دنیا می باشد. تاسیس این سازمان با استناد به این واقعیت صورت گرفته است که دنیای فن آوری اطلاعات به سوی تجارت الکترونیک در حال حرکت می باشد و لذا مدارک و دوره های EC-Council نیز بر اساس ترکیب تجارت و آموزش تکنیکال و ایجاد بستر مناسب جهت دستیابی به یک کسب و کار موفق بنا نهاده شده است. این مدارک بر اساس ابعاد انکار ناپذیر e-business از جمله open standards, scalability, availability, security و ایجاد گردیده و این سازمان نماینده شرکتهای بزرگی از جمله Microsoft، IBM، Xerox، SONY، Motorola، Quantum، Cisco و Verizon می باشد.

در حقیقت EC-Council در دنیای صنعت صدای جهانی متخصصین تجارت الکترونیک بوده و در این راستا گام بر می دارد. یکی از معروفترین و کاربردی ترین مدارک این سازمان مدرک CEH یا مدرک تخصصی هکریهای قانونمند می باشد. مدرک CEH در حیطه امنیت اطلاعات و ارتباطات از اعتبار بین المللی بالایی برخوردار است و به نوعی می توان آن را یک مدرک بی طرفانه در نظر گرفت که میزان توانایی فرد در خنثی کردن یک حمله از سوی یک هکر یا کدهای مخرب را بر اساس رهنمودهای قانونی می سنجد و مبنای مفهومی و عملی بسیار مفیدی در حیطه امنیت به شمار می رود. رتبه مدرک فوق در مجموع عدد ۹ از ۱۰ می باشد که رتبه بسیار بالایی در بین دیگر مدارک بین المللی IT به شمار می رود. این مدرک برای متخصصین امنیت اطلاعات با تجربه، سوابق و مدارک قبلی مرتبط مناسب است و دارنده مدرک CEH یک متخصص حرفه ای و ماهر است که درک بالایی در خصوص ضعفها و نقاط آسیب پذیر در سیستم ها را دارا بوده و همواره در راستای آشکار نمودن و در نهایت رفع آنها اقدام می نماید. وی با استفاده از تخصص خود را نفوذ به سیستم ها، نخست اقدام به هک نمودن آنها کرده و پس از مشخص شدن بخش های آسیب پذیر، با ارایه راهکارهای عملی مناسب نسبت به رفع آنها اقدام خواهد نمود. عملیات هک در ایالات متحده و بیشتر کشورهای جهان یک جرم محسوب می گردد، لذا کاربرد تکنیک های آموخته شده در دوره های آماده سازی برای کسب این مدرک باید تنها با درخواست سازمان یا مالک موسسه ای که سیستم آن هک شده است انجام شود. همچنین این مدرک بر روی تکنیکها و تکنولوژیهای هک از دیدگاه دفاعی تکیه می نماید. تکنیکهای Hacking شامل راهها و روشهایی می باشد که طی آن برنامه ها به نحوی طراحی می گردند که کارهایی فراتر از آنچه از آنها انتظار می رود را در جهت سیاستها و پروسه های امنیتی، انجام دهند. این دوره افراد را با Check List های امنیتی آشنا نموده و توانایی بررسی سیستم امنیتی موجود، ابزار شناسایی نقاط ضعف سیستم و بالاتر از همه کلیه متودولوژیهای تعیین وضعیت امنیت یک سازمان توسط تستهای نفوذ را به افراد اعطا می نماید. انجام Hack در آمریکا و اکثر کشورهای جهان جرم محسوب می گردد اما انجام تستهای هک که توسط متخصصین و هکریهای قانونمند و طبق درخواست سازمانها صورت می گیرد کاملاً قانونی بوده و جهت تشخیص نقاط ضعف سیستمها انجام می گیرد.

مدرک CEH با استفاده از روش معکوس سایر دوره ها، روشهای دفاعی را عمیقاً با استفاده از حمله به سیستمها مورد بررسی قرار می دهد. این مدرک یکی از معتبرترین مدارک بین المللی در جامعه Security می باشد.

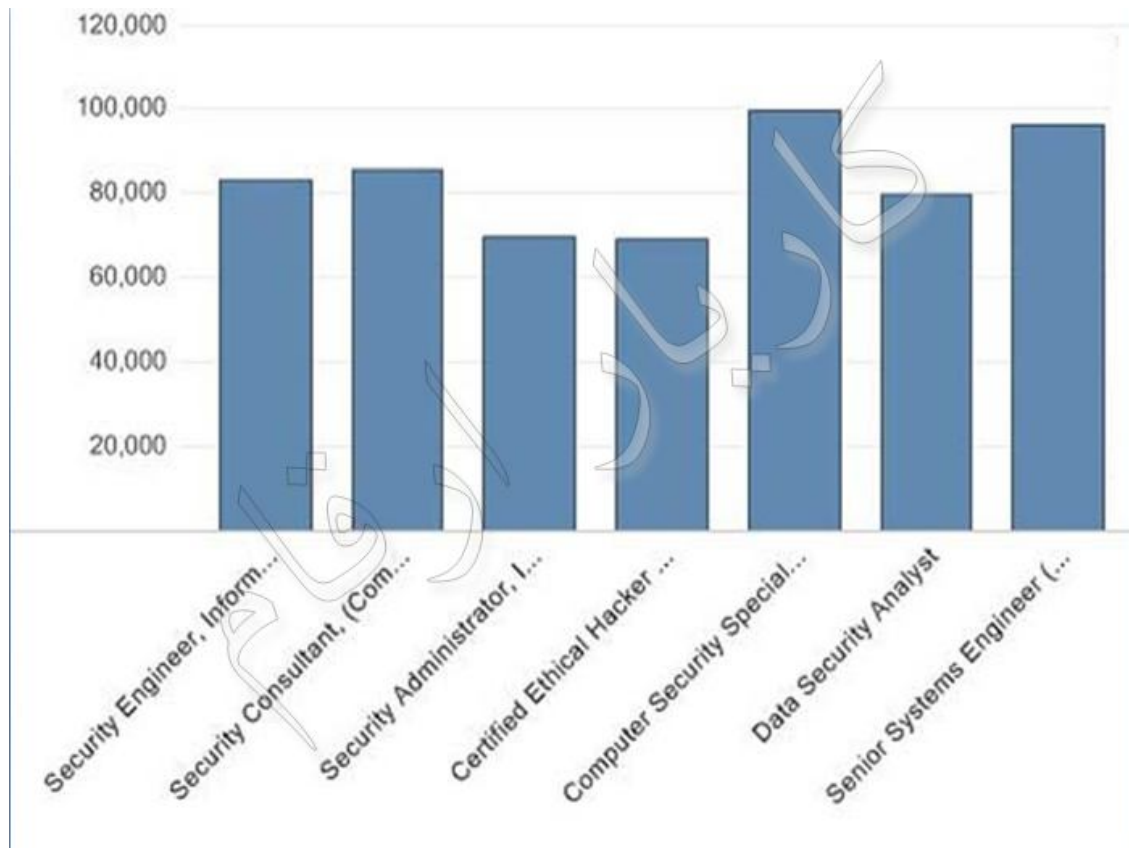
۲- تعداد امتحانات : یک آزمون در مجموع

کد آزمون: 312-50: Ethical Hacking and Countermeasures v4

۳- نمونه مدرک CEH



۴- میزان درآمد دارندگان مدارک بین المللی امنیت اطلاعات در سال ۲۰۰۹



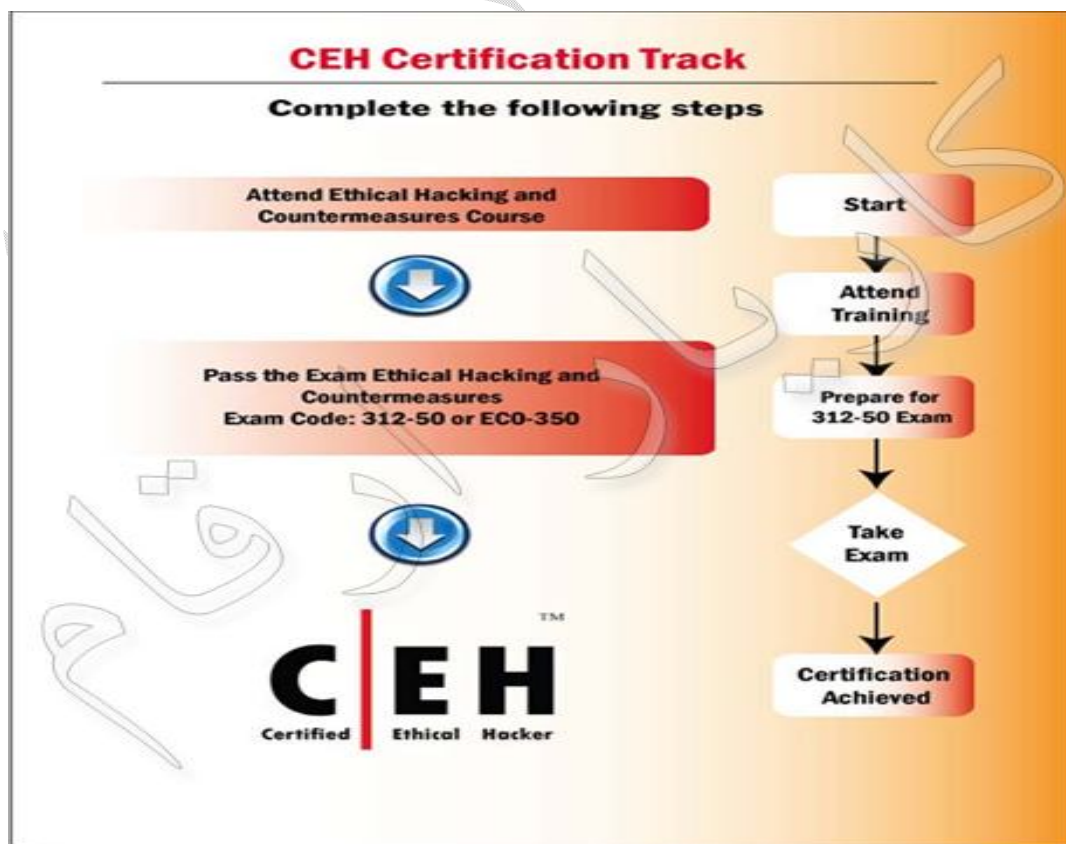
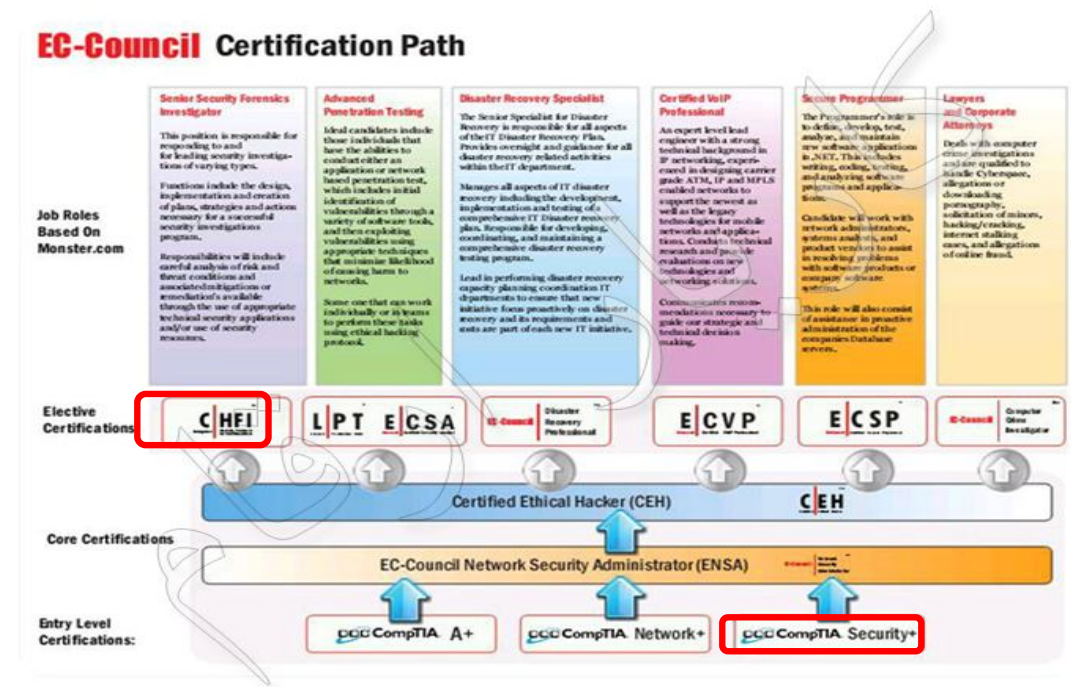
۵- مزایای دستیابی به مدرک: CEH

- امکان استفاده از لوگوی CEH
- موقعیت شغلی و استخدامی بهتر با توجه به تخصص و دانش مورد تأیید EC-Council
- دریافت حقوق بیشتر
- دستیابی به بخش ویژه سایت EC-Council جهت دارندگان مدارک

جهت آغاز مباحث CEH برخورداری از دانش کافی شبکه و اطلاع از مبانی امنیت مخصوصاً Security+ شبکه مفید می باشد.

۶- مسیر دوره های امنیت شبکه

در نمودارهای زیر دانش تقریبی لازم جهت ورود به هریک از دوره های امنیت شبکه مشخص گردیده است.



۷- آزمون CEH :

کد آزمونهای این مدرک EC0 ۳۵۰- و ۳۱۲-۵۰ است و ۲۲ هدف اصلی زیر را پوشش می دهد.

۱. مسایل قانونی و اخلاقی Ethics and Legal Issues
۲. Footprinting
۳. Scanning
۴. لیست کردن/صورت ریز Enumeration
۵. هک سیستم System Hacking
۶. Trojans and Bacheloor
۷. Sniffers
۸. Denial of Service
۹. Social Engineering
۱۰. Session Hijacking
۱۱. هک کردن وب سرورها Hacking Web Servers
۱۲. آسیب پذیری های کاربرد وب Web Application Vulnerabilities
۱۳. تکنیک های بدست آوردن رمز عبور Web Based Password Cracking Techniques
۱۴. هک کردن شبکه های بی سیم SQL Injection
۱۵. Viruses and Worms
۱۶. هک کردن شبکه های Novell
۱۷. هک کردن شبکه های Linux
۱۸. IDS / IPS
۱۹. Honey Pots
۲۰. Buffer Overflow
۲۱. رمز نویسی / کد نویسی Cryptography
۲۲. روش شناسی / اسلوب شناسی / متدولوژی آزمون نفوذ Penetration Testing Methodologies

سوالهای این آزمون که تنها آزمون لازم برای دستیابی به مدرک CEH است، به صورت چند گزینه ای است و شامل ۱۲۵ سوال می باشد و ۳ ساعت زمان پاسخگویی به امتحان دهندگان داده می شود. حد نصاب نمره قبولی ۷۰٪ از کل نمره بوده و به یکی از سه روش زیر برگزار می گردد. مراکز آزمون VUE ، مراکز آزمون Prometric و یا Web Based at Prometric Prime .