مقدمه:

ایـن دوره بر روی تکنیـک ها و تکنولـوژی های هک از دیدگـاه حمله تکیه می کنـد. ایـن دوره افراد را با چک لیست های امنیتی آشنا نموده و توانایـی بررسی سیستـم امنیتـی موجود ، ابزار شنـاسایی نقـاط ضعف سیستـم و بالاتـر از همه متودولـوژی های تعییـن وضعیت امنیـت یک سازمـان توسط تست هـای نفوذ را به افراد اعطا می نمایـد. در دوره CEH روش های دفاعـی عمیقـاً با استفـاده از حمله به سیستم ها ، مورد بررسی قرار خواهد گرفت.

مزایا:

در طی این دوره دانشجو با اکثر تکنیک ها و ابزار های نفوذ وهک آشنا میشود در نتیجه درک بهتری از تهدیدات امنیتی در شبکه داخلی و اینترنت پیدا کرده و بهتر میتواند با خطرات امنیتی مقابله کند.

همچنین در پایان دوره یک سناریوی کامل برای انجام عملیات تست نفوذ و هک تعریف و پیاده سازی میشود.

در اتمام دوره دانشجو قادر به :

شناسایی تهدیدات امنیتی موجود در فضای سایبری و شبکه داخلی

استفاده از تکنیک های جلوگیری از حملات سایبری

ارزیابی سطح امنیت تجهیزات Active در شبکه

خواهد بود.

پیشنیاز:

آشنایی با مفاهیم شبکه های کامپیوتری و TCP/IP

آشنایی مختصر با سیستم عامل Linux

مخاطبان دوره:

مدیران و کارشناسان فعال در حوزه شبکه و امنیت

مدت دوره :

۶۰ ساعت

سرفصل ها:

مقدمه و آشنایی با هک و هکر قانونمند

آشنایی کامل با مفهیم و مراحل Reconnaissance , Footprinting , Social Engineering

آشنایی با سیستم عامل Backtrack R3

معرفی ابزار های موجود در Backtrack R3

آشنایی کامل با مراحل Scanning

آشنایی با ابزارها و تکنیکهای Social Engineering

آشنایی کامل با مراحل System Hacking(Password Cracking, Escalating Privileges)

آشنایی با مراحل Password Cracking و Cryptography

ساخت و مخفی سازی Trojans, Backdoors, Viruses

ساخت و استفاده از Backdoor برای Client Hacking

آشنایی با مفاهیم Sniff و مراحل انجام Sniffing

بدست آوردن کلمات عبور و اطلاعات کاربران در شبکه LAN با استفاده از تکنیک های Sniff و Spoof

دور زدن Firewall ها با تکنیک Source Ip Spoofing

آشنایی با روش های بدست آوردن Account ایمیل ها و شبکه های اجتماعی

آشنایی با تکنیک ها و ابزار های Brute Force

آشنایی با حملات و تکنیک های DOS , DDOS

آشنایی با طراحی Fake Page

آشنایی کامل با Wireless Hacking(WEP/WPA/WPA2)

آشنایی با ابزار قدرتمند Metasploit در سیستم عامل BT5r3

آشنایی با Exploit و مراحل انجام Exploit Attack

آشنایی با مراحل تشخیص IDP ها و استفاده از HoneyPot .

آشنایی کامل با حملات SQL Injection و هک کردن Website های asp , php بدون استفاده از ابزارهای کمکی.

آشنایی با روش های امن کردن شبکه LAN در برابر حملات:

VLAN Trunking Protocol (VTP) spoofing

Spanning Tree Protocol (STP) poisoning

Control Plan flooding

Traffic interception

MAC spoofing

IP spoofing

CAM table flooding

DHCP spoofing

ARP spoofing

Unauthorized network access

Management session spoofing

Link flooding (IP Spoofing, DOS, Traffic Flooding)

آشنایی با کدنویسی امن برای جلوگیری از حملات SQL Injection

آشنایی با تکنیک های جلوگیری از حملات Brute Force

آشنایی با طراحی و پیاده سازی سیاست های امنیتی در سطوح مختلف

آشنایی با اقدامات مفید بعد از بروز حملات سایبری.

آشنایی با پیکربندی های امنیتی در تجهیزات شبکه Switch , Router , Firewall

آشنایی با ابزار های مفید برای ثبت وقایع امنیتی در شبکه.

اهمیت تجزیه و تحلیل امنیتی

Advance Googling

تجزه و تحلیل بسته های TCP/IP

تکنیک های پیشرفته Sniffing

تست های پیشرفته Wireless

طراحی DMZ

تجزیه و تحلیل Snort

تجزیه و تحلیل Log

تجزیه و تحلیل Exploit ها

متودولوژی های Penetration

حقوق کاربران و مشتریان

جمع آوری اطلاعات

تست نفوذ خارجی

تست نفوذ داخلی

تست نفوذ Router و Switch

تست نفوذ نرم افزار ها

تست نفوذ فیزیکی

تست نفوذ Data Base

شناسایی Virus و Trojan

تهیه گزارش از عملیات تست نفوذ

تجزیه و تحلیل گزارشات تست نفوذ