Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی
و برگزارکننده دوره های آموزشی

Designed by
طراحی شده توسط
کاریار ارقام
Carrier Digit

دوره جامع امنیت؛ دفاع + نفوذ

CEH v9 & CAST 614 Advanced Network Defense

مدت(ساعت): ۵۰ | **پیش نیاز:** CCNA | **اعتباردهنده:** EC-Council

کاریار ارقام نماینده رسمی شرکت بین المللی EC-Council در ایران

معرفی دوره :

این دوره ، تلفیقی از دو دوره پر طرفدار EC-Council به نامهای **CEH v9** و **CAST 614 Advanced Network Defense** میباشد که در تدوین آن تا جای ممکن مفاهیم کاربردی و عملی آموزش داده میشود. لازم به ذکر است این دوره اولین سری از دوره های ترکیبی است که به صورت هم زمان به مفاهیم **حمله و دفاع** پرداخته میشودو دانشجویان علاوه بر اینکه با روشهای نفوذ آشنا میگردند ، راهکارهای دفاعی رانیز فرامیگیرند . متخصصان کارکرد های فایروال ها مانند TMG را در آن به صورت کلی فرا میگیرند و با مفاهیم کاربردی مهمی همچون IPSec به صورت عملیاتی آشنا میشوند. آشنایی با تکنیک های نوین تست نفوذ پذیری ، آشنایی عملی با ایمن سازی سرورها ، آشنایی باحملات مرسوم وب با استفاده از آخرین نکات آموزشی همراه با کار عملی یکی دیگر از نکات برجسته این دوره آموزشی میباشد.

مخاطبان دوره :

- متخصصین امنیت
- مدیران شبکه
- متخصصان تست نفوذ
- مشاورین امنیت

اهداف دوره :

- آشنایی با تئوری حملات
- آشنایی عملی با حملات پر کاردبر به صورت POC
- آشنایی عملی با ایمن سازی سرورها
- آشنایی با کارکرد های اولیه فایروال TMG
- آشنایی با حملات مرسوم WEB

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از لابراتوارسخت افزاری ونرم افزاری مجهز
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی
- امکان برگزاری آزمون بین المللی جهت دریافت مدرک بین المللی برای دوره CEH وجود دارد.
- طراحی شده توسط تیم اساتید کاریار ارقام

« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاریار ارقام است »
لطفا در باز نشر این مستند نام پدیدآورنده لحاظ گردد.

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲

Course Outline :	محتوای دوره:

CEH v9 + CAST 614 Advanced Network Defense

Module 01: Introduction to Ethical Hacking
Information Security Overview
- Essential Terminology
- Elements of Information Security
- The Security, Functionality, and Usability Triangle

Information Security Threats and Attack Vectors
- Top Information Security Attack Vectors
- Information Security Threat Categories
- Types of Attacks on a System
- Operating System Attacks
- Misconfiguration Attacks
- Application-Level Attacks
- Examples of Application-Level Attacks
- Shrink Wrap Code Attacks

Hacking Concepts, Types, and Phases
- What is Hacking
- Who is a Hacker?
- Hacker Classes
- Hacking Phases
- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Module 02: Footprinting and Reconnaissance
What is Footprinting?
- What is Footprinting?
- Footprinting Methodology
- Footprinting through Search Engines
- Finding Company's Public and Restricted Websites
- Determining the Operating System
- People Search Online Services
- People Search Online Services
- Footprinting through Job Sites

Footprinting using Advanced Google Hacking Techniques
- Google Advance Search Operators
- Finding Resources Using Google Advance Operator
- Information Gathering Using Google Advanced Search

Footprinting through Social Networking Sites
Mirroring Entire Website
Website Mirroring Tools
Extract Website Information
Monitoring Web Updates Using Website Watcher
WHOIS Footprinting
WHOIS Lookup
DNS Footprinting
Extracting DNS Information
Footprinting through Social Engineering
- Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
- Maltego

LAB: Information Gathering

Module 03: Scanning Networks
- Overview of Network Scanning
- TCP Communication Flags
- Scanning Techniques
- Check for Live Systems
- Check for Open Ports
- Banner Grabbing
- Scan for Vulnerability

LAB: Vulnerability Scan & Open Port and Service Detection

Module 04: System Hacking
- Cracking Passwords
- Escalating Privileges
- Covering Tracks
- Antivirus-Bypass (Advance Backdoor Creation)
- Exploitation
- Scan for Vulnerability
- Key Logging

LAB: Attack to System, Privilege Escalation and Custom Backdoor Creation

« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاریار ارقام است »
لطفا در باز نشر این مستند نام پدیدآورنده لحاظ گردد.

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس :۸۸۰۶۵۲۲۲

Course Outline :	محتوای دوره:
Module 05: Web Hacking • Webserver Concepts • Web App Threats • SQL Injection • Cross-Site-Scripting (XSS) • Authentication Bypass • Scan for Vulnerability • Parameter Tampering **LAB: Attack Web Server (SQLi, XSS, Authentication Bypass)** **Module 06:** Firewalls & Configuration and Advance Filtering • Firewall • Firewall Architecture	• Demilitarized Zone (DMZ) • Types of Firewall • Packet Filtering Firewall • Circuit-Level Gateway Firewall • Application-Level Firewall • Stateful Multilayer Inspection Firewall **LAB: Firewall Configuration (Access Rules, WEB Server Publishing)** **Module 07:** Hardening Windows Server • NAP (DHCP) • IPSec • Security Compliance Manager (SCM) • CA • IIS Security **LAB: Configuration (SSL Configuration, NAP, IPSec)**

Accredited by CARRIER DIGIT Computer Software LLC
« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاریار ارقام است »
لطفا در باز نشر این مستند نام پدیدآورنده لحاظ گردد.
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس :۸۸۰۶۵۲۲۲