Certified Ethical Hacker Instructor-Led Training

Demand for Certified Ethical Hacker has increased exponentially in last few years. Most of the data are on digital platform now and hence the need for its security is a must.

Ethical hacking course prepares you to be the security defender and protects the confidential data from cyber-attacks and unwanted disruptions.

The need of certified professionals in the IT industry is rising day by day where the professionals are supposed to protect the data, network and transactions of informations.

About this training

- **Study Material:-** 24*7 Lab Access, Live lectures of Training, Streaming Recorded Videos, Online Lab Workbook, and Remote Virtual Lab access.
- **Duration:- 1 month**

What you will learn?

- Techniques of Network Scanning
- Techniques of Network Scanning countermeasures
- Laws and standards of Information security
- Covering footprinting through the website, social media, search engine
- Footprinting tools
- Enumeration techniques. For instance, NetBIOS, SNMP, NTP, NFS, SMTP, DNS, VoIP.
- System hacking. Its methodology, steganography, and steganalysis attacks.
- Methodologies of web server attacks and a comprehensive attack to refrain them.
- SQL injection attacks and tools to detect them.
- Hacking tools, methodologies, encryption and security of wireless.
- Mobile platform security. Including its tools and guidelines.
- Sniffing techniques and defending.
- Social engineering techniques and identifying theft.
- Attack techniques of Dos and DDoS.
- Session Hijack- application and network. Its concepts and tools.
- Firewall, IDS, IPS concepts, solutions and evading tools.
- Cloud computing and security. Methods of threats and attacking.
- Penetration testing and roadmap.
- Threats and defence of IoT and OT platforms.
- Cryptography and PKI, its attacks and tools.

Certification

CEH 312-50 (ECC EXAM) & 312-50 (VUE)

About Instructor

The course will be conducted by the professional and verified instructor of UniNets. His 14+ years of experience will make the course to go on a systematic pattern where all the topics will be covered from the scratch. He has worked with big companies as professional employee and now working as professional trainer. The candidates will be able to get the essence of his both side experiences.

Course Content

- Network and Communication Technologies
    - Networking technologies - instance, hardware & infrastructure
    - Web technologies - instance, web 2.0 &skype
    - Systems technologies - Communication protocols
    - Telecommunication technologies
    - Mobile technologies
    - Wireless terminologies
    - Cloud computing
    - Cloud deployment models
- Information Security Threats and Attack Vectors
    - Malware - Trojan, virus, backdoor, worms
    - Malware operations
    - Information security threats and attack vectors
    - Attacks on a system - DoS, DDoS, wireless threats, web server and web application attacks, SQL injection, session hijacking
    - Botnet - Cloud computing threats and attacks
    - Mobile platform attack vectors
    - Cryptography attacks
- Information Security Technologies
    - Information security elements
    - Information security management - IA, Defense-in-Depth, incident management
    - Security trends
    - Hacking and ethical hacking
    - Vulnerability assessment and penetration testing
    - Cryptography
    - Encryption algorithms
    - Wireless encryption
    - Bring Your Own Device (BYOD)
    - Backups and archiving (instance, local, network)
    - IDS, firewalls, and honeypots
- Information Security Assessment and Analysis
    - Data analysis
    - Systems analysis
    - Risk assessments
    - Vulnerability assessment and penetration testing
    - Technical assessment methods
    - Network sniffing
    - Malware analysis
- Information Security Assessment Process
    - Footprinting

    - Scanning - Port scanning, vulnerability scanning, proxy chaining, IP spoofing, banner grabbing, network discovery.
    - Enumeration
    - System hacking - password cracking, executing applications, privilege escalation, hiding files, covering tracks
- Information Security Controls
    - Systems security controls
    - Application/file server
    - IDS
    - Firewalls
    - Cryptography
    - Disk Encryption
    - Network security
    - Physical security
    - Threat modeling
    - Biometrics
    - Wireless access technology - networking, RFID, Bluetooth
    - Trusted networks
    - Privacy/confidentiality (with regard to engagement)
- Information Security Attack Detection
    - Security policy implications
    - Vulnerability detection
    - IP Spoofing detection
    - Verification procedures - false positive/negative validation
    - Social engineering (human factors manipulation)
    - Vulnerability scanning
    - Malware detection
    - Sniffer detection
    - DoS and DDoS detection
    - Detect and block rogue AP
    - Evading IDS - evasion, fragmentation
    - Evading Firewall - firewalking, tunneling
    - Honeypot detection
    - Steganalysis
- Information Security Attack Prevention
    - Defend against web server attacks
    - Patch management
    - Encoding schemes for web application
    - Defend against web application attacks
    - Defend against SQL injection attacks
    - Defend against wireless and Bluetooth attacks
    - Mobile platforms security
    - Mobile Device Management (MDM)
    - BYOD Security
    - Cloud computing security
- Information Security Systems
    - Network/host based intrusion
    - Boundary protection appliances
    - Access control mechanisms - smart cards
    - Cryptography techniques - IPSec, SSL, PGP
    - Domain name system (DNS)
    - Network topologies
    - Subnetting

    - Routers / modems / switches
    - Security models
    - Database structures
- Information Security Programs
    - Operating environments - Linux, Windows, Mac
    - Anti-malware systems and programs - anti-keylogger, anti-spyware, anti-rootkit, anti-trojan, anti-virus
    - Wireless IPS deployment
    - Programming languages - C++, Java, C#, C
    - Scripting languages - PHP, Javascript
- Information Security Tools
    - Network/wireless sniffers - Wireshark, Airsnort
    - Port scanning tools - Nmap, Hping
    - Vulnerability scanner - Nessus, Qualys, Retina
    - Vulnerability management and protection systems - Founds tone, Ecora
    - Log analysis tools - Exploitation tools
    - Footprinting tools - Maltego, FOCA, Recon-ng
    - Network discovery tools - Network Topology Mapper
    - Enumeration tools - SuperScan, Hyena, NetScanTools Pro
    - Steganography detection tools - Malware detection tools
    - DoS/DDoS protection tools - Patch management tool (MBSA)
    - Web Server security tools
    - Web application security tools (eg: Acunetix WVS)
    - Web application firewall (eg: dotDefender)
    - SQL injection detection tools - IBM Security AppScan
    - Wireless and Bluetooth security tools
    - Information Security Tools
    - Android, iOS, Windows Phone OS, and BlackBerry device security tools
    - MDM Solutions
    - Mobile Protection Tools
    - Intrusion Detection Tools - Snort
    - Hardware and software firewalls - Comodo Firewall
    - Honeypot tools - KFSenser
    - IDS/Firewall evasion tools - Traffic IQ Professional
    - Packet fragment generators
    - Honeypot Detection Tools
    - Cloud security tools - Core CloudInspect
    - Cryptography tools - Advanced Encryption Package
    - Cryptography toolkit - OpenSSL
    - Disk encryption tools
    - Cryptanalysis tool - CrypTool
- Information Security Procedures
    - Cryptography
    - Public key infrastructure (PKI)
    - Digital signature and Pretty Good Privacy (PGP)
    - Security Architecture (SA)
    - Service oriented architecture
    - Information security incident
    - N-tier application design
    - TCP/IP networking (instance, network routing)
    - Security testing methodology
- Information Security Assessment Methodologies
    - Web server attack methodology

    - Web application hacking methodology
    - SQL injection methodology and evasion techniques
    - SQL injection evasion techniques
    - Wireless and Bluetooth hacking methodology
    - Mobile platform (Android, iOS, Windows Phone OS, and BlackBerry) hacking methodology
    - Mobile Rooting and Jailbreaking
- Information Security Policies/Laws/Acts
    - Security policies
    - Compliance regulations (instance, PCI-DSS, SOX)
- Ethics of Information Security
    - Professional code of conduct
    - Appropriateness of hacking

Note: ***Most of the course topics are covered with hands-on lab exercises and others are theoretical

Thank You

Visit us

https://www.uninets.com/