مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 1: Introduction To Ethical Hacking	• 1 Elements of Security • 2 Cyber Kill Chain • 3 MITRE ATT&CK Framework • 3.1 Activity - Researching the MITRE ATTACK Framework • 4 Hacking • 5 Ethical Hacking • 6 Information Assurance • 7 Risk Management • 8 Incident Management • 9 Information Security Laws and Standards • 10 Introduction to Ethical Hacking Review
Module 2: Footprinting and Reconnaissance	• 1 Footprinting Concepts • 2 OSINT Tools • 2.1 Activity - Conduct OSINT with OSR Framework • 2.2 Activity - OSINT with theHarvester • 2.3 Activity - Add API Keys to theHarvester • 2.4 Activity - Extract Document Metadata with FOCA • 2.5 Activity - Extract Document Metadata with FOCA • 3 Advanced Google Search • 3.1 Activity - Google Hacking • 4 Whois Footprinting • 4.1 Activity - Conducting Whois Research • 5 DNS Footprinting • 5.1 Activity - Query DNS with NSLOOKUP • 6 Website Footprinting • 6.1 Activity - Fingerprint a Webserver with ID Serve • 6.2 Activity - Extract Data from Websites • 6.3 Activity - Mirror a Website with HTTrack • 7 Email Footprinting • 7.1 Activity - Trace a Suspicious Email • 8 Network Footprinting • 9 Social Network Footprinting • 10 Footprinting and Reconnaissance Countermeasures • 11 Footprinting and Reconnaissance Review

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 3: Scanning Networks	• 1 Scanning Concepts • 2 Discovery Scans • 2.1 Activity - ICMP ECHO and ARP Pings • 2.2 Activity - Host Discovery with Angry IP Scanner • 3 Port Scans • 3.1 Activity - Port Scan with Angry IP Scanner • 4 Other Scan Types • 5 Scanning Tools • 5.1 Activity - Hping3 Packet Crafting • 5.2 Activity - Fingerprinting with Zenmap • 6 NMAP • 6.1 Activity - Nmap Basic Scans • 6.2 Activity - Host Discovery with Nmap • 6.3 - Activity - Nmap Version Detection • 6.4 Activity - Nmap Idle (Zombie) Scan • 6.5 Activity - Nmap FTP Bounce Scan • 6.6 - Activity - NMAP Scripts • 7 Firewall and IDS Evasion • 7.1 Activity - Nmap Advanced Scans • 8 Proxies • 9 Scanning Countermeasures • 10 Scanning Networks Review
Module 4: Enumeration	• 1 Enumeration Overview • 2 SMB_NetBIOS_Enumeration • 2.1 Activity - Enumerate NetBIOS Information with Hyena • 3 File Transfer Enumeration • 4 WMI Enumeration • 4.1 - Activity - Enumerating WMI with Hyena • 5 SNMP Enumeration • 5.1 Activity - Enumerate WMI, SNMP and Other Information Using SoftPerfect • 6 LDAP Enumeration • 7 DNS Enumeration

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 4: Enumeration	• 8 SMTP Enumeration • 8.1 Activity - Enumerate Email Users with SMTP • 9 Remote Connection Enumeration • 10 Website Enumeration • 10.1 Activity - Enumerate a Website with DirBuster • 11 Other Enumeration Types • 12 Enumeration Countermeasures and Review
Module 5: Vulnerability Analysis	• 1 Vulnerability Scanning • 1.1 Vulnerability Scanning with OpenVAS • 2 Vulnerability Assessment • 3 Vulnerability Analysis Review
Module 6: System Hacking	• 1 System Hacking Concepts • 2 Common OS Exploits • 3 Buffer Overflows • 3.1 Activity - Performing a Buffer Overflow • 4 System Hacking Tools and Frameworks • 4.1 Activity - Hack a Linux Target from Start to Finish • 5 Metasploit • 5.1 Activity - Get Started with Metasploit • 6 Meterpreter • 7 Keylogging and Spyware • 7.1 Activity - Keylogging with Meterpreter • 8 Netcat • 8.1 Activity - Using Netcat • 9 Hacking Windows • 9.1 Activity - Hacking Windows with Eternal Blue • 10 Hacking Linux • 11 Password Attacks • 11.1 Activity - Pass the Hash • 11.2 Activity - Password Spraying • 12 Password Cracking Tools

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 6: System Hacking	• 13 Windows Password Cracking • 13.1 Activity - Cracking Windows Passwords • 13.2 Activity - Cracking Password Hashes with Hashcat • 14 Linux Password Cracking • 15 Other Methods for Obtaining Passwords • 16 Network Service Attacks • 16.1 Activity - Brute Forcing a Network Service with Medusa • 17 Post Exploitation • 18 Pivoting • 18.1 Activity - Pivoting Setup • 19 Maintaining Access • 19.1 Activity - Persistence • 20 Hiding Data • 20.1 Activity - Hiding Data Using Least Significant Bit Steganography • 21 Covering Tracks • 21.1 Activity - Clearing Tracks in Windows • 21.2 Activity - View and Clear Audit Policies with Auditpol • 22 System Hacking Countermeasures • 23 System Hacking Review
Module 7: Malware Threats	• 1 Malware Overview • 2 Viruses • 3 Trojans • 3.1 Activity - Deploying a RAT • 4 Rootkits • 5 Other Malware • 6 Advanced Persistent Threat • 7 Malware Makers • 7.1 Activity - Creating a Malware Dropper and Handler • 8 Malware Detection • 9 Malware Analysis • 9.1 Activity - Performing a Static Code Review • 9.2 Activity - Analyzing the SolarWinds Orion Hack • 10 Malware Countermeasures • 11 Malware Threats Review

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 8: Sniffing	• 1 Network Sniffing • 2 Sniffing Tools • 2.1 Activity- Sniffing HTTP with Wireshark • 2.2 Activity - Capturing Files from SMB • 3 ARP and MAC Attacks • 3.1 Activity - Performing an MITM Attack with Ettercap • 4 Name Resolution Attacks • 4.1 Activity - Spoofing Responses with Responder • 5 Other Layer 2 Attacks • 6 Sniffing Countermeasures • 7 Sniffing Review
Module 9: Social Engineering	• 1 Social Engineering Concepts • 2 Social Engineering Techniques • 2.1 Activity - Deploying a Baited USB Stick • 2.2 Activity - Using an O.MG Lightning Cable • 3 Social Engineering Tools • 3.1 Activity - Phishing for Credentials • 4 Social Media, Identity Theft, Insider Threats • 5 Social Engineering Countermeasures • 6 Social Engineering Review
Module 10: Denial-of-Service	• 1 DoS-DDoS Concepts • 2 Volumetric Attacks • 3 Fragmentation Attacks • 4 State Exhaustion Attacks • 5 Application Layer Attacks • 5.1 Activity - Performing a LOIC Attack • 5.2 Activity - Performing a HOIC Attack • 5.3 Activity - Conducting a Slowloris Attack • 6 Other Attacks • 7 DoS Tools • 8 DoS Countermeasures • 9 DoS Review

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 11: Session Hijacking	• 1 Session Hijacking • 2 Compromising a Session Token • 3 XSS • 4 CSRF • 5 Other Web Hijacking Attacks • 6 Network-Level Session Hijacking • 6.1 Activity - Hijack a Telnet Session • 7 Session Hijacking Tools • 8 Session Hijacking Countermeasures • 9 Session Hijacking Review
Module 12: Evading IDS, Firewalls, and Honeypots	• 1 Types of IDS • 2 Snort • 3 System Logs • 4 IDS Considerations • 5 IDS Evasion • 5.1 Activity - Fly Below IDS Radar • 6 Firewalls • 7 Packet Filtering Rules • 8 Firewall Deployments • 9 Split DNS • 10 Firewall Product Types • 11 Firewall Evasion • 11.1 Activity - Use Social Engineering to Bypass a Windows Firewall • 11.2 Activity - Busting the DOM for WAF Evasion • 12 Honeypots • 13 Honeypot Detection and Evasion • 13.1 Activity - Test and Analyze a Honey Pot • 14 Evading IDS, Firewalls, and Honeypots Review

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 13: Hacking Web Servers	• 13.1 Web Server Operations • 13.2 Hacking Web Servers • 13.3 Common Web Server Attacks • 13.3.1 Activity - Defacing a Website • 13.4 Web Server Attack Tools • 13.5 Hacking Web Servers Countermeasures • 13.6 Hacking Web Servers Review
Module 14: Hacking Web Applications	• 1 Web Application Concepts • 2 Attacking Web Apps • 3 A01 Broken Access Control • 4 A02 Cryptographic Failures • 5 A03 Injection • 5.1 Activity - Command Injection • 6 A04 Insecure Design • 7 A05 Security Misconfiguration • 8 A06 Vulnerable and Outdated Components • 9 A07 Identification and Authentication Failures • 10 A08 Software and Data integrity Failures • 11 A09 Security Logging and Monitoring Failures • 12 A10 Server-Side Request Forgery • 13 XSS Attacks • 13.1 Activity - XSS Walkthrough • 13.2 Activity - Inject a Malicious iFrame with XXS • 14 CSRF • 15 Parameter Tampering • 15.1 Activity - Parameter Tampering with Burp • 16 Clickjacking • 17 SQL Injection • 18 Insecure Deserialization Attacks • 19 IDOR • 19.1 Activity - Hacking with IDOR • 20 Directory Traversal • 21 Session Management Attacks

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 14: Hacking Web Applications	• 22 Response Splitting • 23 Overflow Attacks • 24 XXE Attacks • 25 Web App DoS • 26 Soap Attacks • 27 AJAX Attacks • 28 Web API Hacking • 29 Webhooks and Web Shells • 30 Web App Hacking Tools • 31 Hacking Web Applications Countermeasures • 32 Hacking Web Applications Review
Module 15: SQL Injection	• 1 SQL Injection Overview • 2 Basic SQL Injection • 3 Finding Vulnerable Websites • 4 Error-based SQL Injection • 5 Union SQL Injection • 5.1 Activity - Testing SQLi on a Live Website - Part 1 • 5.2 Activity - Testing SQLi on a Live Website - Part 2 • 6 Blind SQL Injection • 7 SQL Injection Tools • 7.1 Activity - SQL Injection Using SQLmap • 8 Evading Detection • 9 Analyzing SQL Injection • 10 SQL Injection Countermeasures • 11 SQL Injection Review
Module 16: Hacking Wireless Networks	• 1 Wireless Concepts • 2 Wireless Security Standards • 3 WI-FI Discovery Tools • 4 Common Wi-Fi Attacks • 5 Wi-Fi Password Cracking • 6 WEP Cracking • 6.1 Activity - Cracking WEP

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 16: Hacking Wireless Networks	• 7 WPA,WPA2,WPA3 Cracking • 7.1 Activity - WPA KRACK Attack • 8 WPS Cracking • 9 Bluetooth Hacking • 10 Other Wireless Hacking • 10.1 Activity - Cloning an RFID badge • 10.2 Activity - Hacking with a Flipper Zero • 11 Wireless Security Tools • 12 Wireless Hacking Countermeasures • 13 Hacking Wireless Networks Review
Module 17: Hacking Mobile Platforms	• 1 Mobile Device Overview • 2 Mobile Device Attacks • 3 Android Vulnerabilities • 4 Rooting Android • 5 Android Exploits • 5.1 Activity - Hacking Android • 5.2 Activity - Using a Mobile Device in a DDoS Campaign • 6 Android-based Hacking Tools • 7 Reverse Engineering an Android App • 8 Securing Android • 9 iOS Overview • 10 Jailbreaking iOS • 11 iOS Exploits • 12 iOS-based Hacking Tools • 13 Reverse Engineering an iOS App • 14 Securing iOS • 15 Mobile Device Management • 16 Hacking Mobile Platforms Countermeasures • 17 Hacking Mobile Platforms Review
Module 18: IoT AND OT Hacking	• 1 IoT Overview • 2 IoT Infrastructure • 3 IoT Vulnerabilities and Threats • 3.1 Activity - Searching for Vulnerable IoT Devices

مسارتك
masartech

Name of Course	Certified Ethical Hacker (CEH) v12
Lessons	**Outline**
Module 18: IoT AND OT Hacking	• 4 IoT Hacking Methodology and Tools • 5 IoT Hacking Countermeasures • 6 OT Concepts • 7 IT-OT Convergence • 8 OT Components • 9 OT Vulnerabilities • 10 OT Attack Methodology and Tools • 11 OT Hacking Countermeasures • 12 IoT and OT Hacking Review
Module 19: Cloud Computing	• 1 Cloud Computing Concepts • 2 Cloud Types • 3 Cloud Benefits and Considerations • 4 Cloud Risks and Vulnerabilities • 5 Cloud Threats and Countermeasures • 5.1 Activity - Hacking S3 Buckets • 6 Cloud Security Tools And Best Practices • 7 Cloud Computing Review
Module 20: Cryptography	• 1 Cryptography Concepts • 2 Symmetric Encryption • 2.1 Activity - Symmetric Encryption • 3 Asymmetric Encryption • 3.1 Activity - Asymmetric Encryption • 4 Public Key Exchange • 5 PKI • 5.1 Activity - Generating and Using an Asymmetric Key Pair • 6 Digital Signatures • 7 Hashing • 7.1 Activity - Calculating Hashes • 8 Common Cryptography Use Cases • 9 Cryptography Tools • 10 Cryptography Attacks • 11 Cryptography Review • 12 Course Conclusion