Introduction to Ethical Hacking

Learning Objectives: Learn the basics of maintaining Information Security and measures taken to become an EC Council certified ethical hacker.

Topics

- Introduction to Ethical Hacking and Its Importance
- Understanding the Various Phases of Ethical Hacking Methodology
- Ethics and Legal Considerations in Ethical Hacking

Footprinting and Reconnaissance

Learning Objectives: Understand the fundamentals of Footprinting and Reconnaissance.

Topics

- Gathering Information About Targets and Their Networks
- Techniques for Footprinting, Such as DNS Queries, Social Engineering, and WHOIS Lookups
- Tools and Methodologies for Reconnaissance

Scanning Networks

Learning Objective: Understand in detail the factors involved in developing a skill of Scanning Networks.

Topics

- Understanding Different Scanning Techniques and Their Purposes
- Active and Passive Scanning Methods
- Conducting Network Scans Using Tools Like Nmap, Nessus, and Wireshark

Enumeration

Learning Objectives: Learn the fundamentals of enumeration and why it is important in the process of becoming a certified Ethical Hacker.

Topics

- Techniques for Gathering Information About Network Resources, Such as Usernames, Shares, and Services
- Enumerating Network Protocols and Their Vulnerabilities
- Enumeration Tools and Methodologies

Vulnerability Analysis

Learning Objectives: Learn the procedure to check all the vulnerabilities in the systems, computers and other ecosystem tools.

Topics

- Identifying and Analyzing System Vulnerabilities
- Vulnerability Scanning Tools and Techniques
- Common Vulnerabilities and Exposures (CVE) Databases

System Hacking

Learning Objectives: Learn everything about the compromise of computer systems and software to access the target computer and misuse sensitive information.

Topics

- Techniques For Gaining Unauthorized Access to Systems
- Exploiting System Vulnerabilities, Weak Configurations, and Misconfigurations
- Password Cracking, Privilege Escalation, and Backdoor Creation

Malware Threats

Learning Objectives: Learn and understand how malware threat actors use to infect systems and networks and gain access to sensitive information.

Topics

- Understanding Various Types of Malware (Viruses, Worms, Trojans, Ransomware, Etc.)
- Analyzing and Reverse-engineering Malware Samples
- Detection and Mitigation Strategies for Malware Attacks

Sniffing

Learning Objectives: Learn the process of monitoring and capturing all data packets passing through a network

Topics

- Understanding Network Sniffing Techniques and Protocols
- Tools and Countermeasures for Sniffing Detection and Prevention
- Analyzing Captured Network Traffic

Social Engineering

Learning Objectives: Learn how to detect weaknesses to address your various kinds of security related issues.

Topics

- Psychological Manipulation Techniques Used for Social Engineering Attacks
- Pretexting, Phishing, Baiting, and Other Social Engineering Methods
- Mitigation Strategies and Awareness for Social Engineering Attacks

Denial-of-Service (DoS) Attacks

Learning Objectives: Understand how an attack against a computer or network reduces, restricts, or prevents accessibility of its system resources to authorized users.

Topics

- Understanding Dos and Distributed Dos (DDoS) Attacks
- Techniques And Tools for Conducting Dos Attacks
- Mitigation Strategies and Countermeasures

Session Hijacking

Learning Objectives: Understand how to take over an active TCP/IP communication session without the user's permission.

Topics

- Understanding Session Hijacking Techniques and Their Implications
- Man-in-the-middle (MitM) Attacks, Asension Hijacking Tools, and Countermeasures
- Protecting Session Integrity and Confidentiality

Evading IDS, Firewalls, and Honeypots

Learning Objectives: Understand the basics and fundamentals of Evading IDS, Firewalls, and Honeypots.

Topics

- Techniques for Evading Intrusion Detection Systems (IDS), Firewalls, and Honeypots
- Firewall and IDS Evasion Tools and Methods
- Identifying and Countering Honeypots

Hacking Web Applications

Learning Objectives: Learn the basics and introduction to hacking webapps and the dos and don'ts of ethical web application hacking.

Topics

- Web Application Vulnerabilities and Their Exploitation
- Injection Attacks, Cross-site Scripting (XSS), and Other Web Application Attacks
- Web Application Security Best Practices

SQL Injection

Learning Objectives: Learn about SQL injection - an attack where the hacker makes use of unvalidated user input to enter arbitrary data or SQL commands

Topics

- Understanding SQL Injection Attacks and Their Impact
- Techniques for Exploiting SQL Vulnerabilities
- Mitigating SQL Injection Attacks

Wireless Network Hacking

Learning Objectives: Learn the fundamentals of hacking wireless networks and the applications of ethical wireless network hacking.

Topics

- Wireless Network Vulnerabilities and Weaknesses
- Wi-Fi Hacking Techniques, Tools, and Countermeasures
- Securing Wireless Networks

Mobile Platform Hacking

Learning Objectives: Learn the fundamentals of hacking mobile platforms and the applications of ethical mobile platform hacking.

Topics

- Mobile Device Vulnerabilities and Security Risks
- Techniques for Exploiting Mobile Platforms and Applications
- Mobile Device Security Best Practices

IoT (Internet of Things) Hacking

Learning Objectives: Get a deep understanding of what IoT hacking is and how to apply various tools mitigate threats.

Topics

- IoT Security Challenges and Vulnerabilities
- Hacking IoT Devices, Protocols, and Applications
- IoT Security Considerations and Best Practices

Cloud Computing

Learning Objectives: Learn the basics and fundamentals of Cloud computing and cloud security.

Topics

- Cloud Computing Security Risks and Challenges
- Assessing and Securing Cloud Infrastructure and Services
- Cloud Security Best Practices

Cryptography

Learning Objectives: Learn the art of converting text into another form for secret transmission and reception.

Topics

- Basics of Cryptography and its Importance in Security
- Cryptographic Algorithms, Protocols, and their Vulnerabilities
- Implementing Secure Cryptographic Practices

Penetration Testing

Learning Objectives: Learn about penetration testing and how to identify vulnerabilities.

Topics

- Introduction to Penetration Testing and its Methodologies
- Planning, Conducting, and Reporting on Penetration Tests
- Tools and Frameworks for Penetration Testing

Complementary Courses Worth US$ 6000

1) Becoming a Cyber Security Professional - A Beginner's Career Guide [On-Demand Course]
Master the fundamentals of cybersecurity, explore diverse job roles, and gain comprehensive knowledge to kickstart your career in this high-demand field. Acquire the essential skills, certifications, and practical expertise needed to become a true cybersecurity expert. Uncover top job search sites and networking strategies to secure a rewarding career and excel in the cybersecurity industry.

- Course Duration: **2 Hours**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

2) Cyber Security for Absolute Beginners - 2022 Edition - Part 01 [On-Demand Course]

Master the art of cyber security and safeguard systems from relentless cyberattacks. Explore the world of hackers, their methods, and the tools to combat them. Gain comprehensive knowledge to become a skilled cyber security professional and defend against evolving digital threats.

- Course Duration: **3 Hours 23 Minutes**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

3) Cyber Security for Absolute Beginners - 2022 Edition - Part 02 [On-Demand Course]

Gain a strong foundation in cyber security, focusing on networking, privacy, and malware defense. Master TCP/IP, and DNS, and safeguard online privacy. Learn advanced techniques like VPNs, Tor, anti-malware tools, backups, encryption, and social engineering defense to become a skilled cybersecurity professional.

- Course Duration: **6 Hours**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

4) Practical Cyber Hacking Skills for Beginners [On-Demand]

Master the art of cybersecurity, protecting computers and networks from digital threats. From Kali Linux to phishing techniques, gain hands-on skills in network security and scanning tools. Become an expert in incident response and data protection, forging a successful career in the ever-evolving world of cybersecurity.

- Course Duration: **8 Hours 20 Minutes**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

5) Web Hacker's Toolbox - Tools Used by Successful Hackers [On-Demand]

Master the essential toolbox of ethical hackers and penetration testers. Learn to use Sqlmap for automated SQL injection, Google Hacking for web app security, and Burp Suite Intruder for fuzzing. Exploit race conditions with OWASP ZAP and elevate your penetration testing skills for real-world projects.

- Course Duration: **3 Hours**
- Author: **Dawid Czagan**, Founder and CEO at Silesia Security Lab, and Trainer

6) Web Hacking Expert – Full-Stack Exploitation Mastery [On-Demand]

Dive into full-stack exploitation to master modern web attacks. Learn to bypass Content Security Policy (CSP), hack through PDFs, images, and links, and steal secrets from AngularJS applications. Learn to exploit race conditions and discover powerful attacks like HTTP parameter pollution, subdomain takeover, and clickjacking.

- Course Duration: **4 Hours 46 Minutes**
- Author: **Dawid Czagan**, Founder and CEO at Silesia Security Lab, and Trainer

7) Linux Crash Course for Beginners – 2023 [On-Demand]

Master Linux's system administration, understand its open-source nature and navigate the file system with essential commands. Gain fundamental Linux command line skills and grasp the inner workings of this powerful operating system.

- Course Duration: **5 Hours 47 Minutes**

- Author: **Imran Afzal**, Systems Engineer, Entrepreneur, Instructor, and Public Speaker

8) Certified Ethical Hacker (CEH) v12 312-50 Exam Guide [e-Book]

Master the art of ethical hacking with this comprehensive cybersecurity book. Gain insights into InfoSec, attack vectors, and emerging technologies. Prepare for the CEH v11 certification exam and become a certified cybersecurity professional.

- No. of Pages: **664**
- Author: **Dale Meredith**, EC-Council Certified Ethical Hacker/Instructor, and a Microsoft Certified Trainer