Ethical Hacker

Scope and Sequence

Version 1.0

Contents

Introduction

The digital landscape is evolving at an unprecedented rate with unknown threats lurking around every corner. Cybersecurity resilience in the modern world cannot be just an addon - it's a necessity.
Organizations must build cybersecurity resilience, and offensive security professionals like Ethical Hackers and Penetration Testers can help proactively discover unknown threats and address them before cybercriminals do.

Target Audience

This course is designed to prepare learners with the Ethical Hacker skillset. Learners will become proficient in the art of scoping, executing, and reporting on vulnerability assessments, while recommending mitigation strategies. By using an engaging gamified narrative throughout the course, with real-world inspired hands-on practice labs, learners develop essential workforce readiness skills to lay a solid foundation in offensive security.

After completing this course, learners can enter cybersecurity careers, either on the offensive security side as ethical hackers or penetration testers, or on the defensive security side by understanding the mindset and tactics of threat actors, while implementing security controls and monitoring, analyzing, and responding to current security threats.

Prerequisites

Learners are expected to have the following skills:

- Entry-level cybersecurity knowledge:
  CCST Cybersecurity certification or Cybersecurity Essentials (version 3.0) or Junior Cybersecurity Analyst Career Path, or equivalent
- Basic programming knowledge

Additional experience with networking, firewalls, Linux, and programming is a plus.

Certification Alignment

There are no target certifications for this course. After successfully completing this course, students receive a Cisco validated digital badge.

Course Description

In this course, learners develop ethical hacking and penetration testing skills that build a foundation for success in the cybersecurity industry. With the support of video and rich interactive media, participants learn, apply, and practice ethical hacking skills in meaningful ways through a series of realistic hands-on lab experiences.

The course also includes many opportunities for learners to practice what they are learning as they are learning it. Learning by doing is the most powerful way to build new skills and knowledge.

The Ethical Hacker course includes the following features:

- 34 labs support the independent acquisition of knowledge and ethical hacking skills.
- 86 practice activities provide opportunities for self-assessment and identification of learning deficits.
- 10 modules of content cover important topics that enable students to face ethical hacking challenges.
- Assessments include 10-chapter exams, a final exam, and a skills-based assessment.
- Multimedia learning tools, including videos, interactive practice activities and realistic lab experiences address a variety of learning styles and help stimulate learning and promote increased knowledge retention.

Equipment Requirements

Hands-on labs require computers capable of running virtualization software (VirtualBox or UTM) with at least 4GB of RAM and 20GB of free disk space. Other learning experiences require focused internet-based research and the completion of lab documents.

Software:

- Oracle Virtual Box or UTM
- Lab virtual machine OVA file

Course Outline

The Ethical Hacker course introduces important concepts in cybersecurity and ethical hacking. This includes labs in which students use ethical hacking tools against simulated targets. By the end of the course, students have learned how to use ethical hacking tools to find, assess, and exploit vulnerabilities in a range of simulated targets that mimic real-world scenarios.

Listed below are the current set of modules and their associated competencies for this course offering. Each module is an integrated unit of learning that consists of content, activities, labs, and assessments that target a specific set of competencies. The size of the module will depend on the depth of knowledge and skill needed to master the competency.

Table 1: Module Title and Objective

Module Title/Topic Title	Objective
Module 1: Introduction to Ethical Hacking and Penetration Testing	Explain the importance of methodological ethical hacking and penetration testing.
1.1 Understanding Ethical Hacking and Penetration Testing	Explain the importance of ethical hacking and penetration testing.
1.2 Exploring Penetration Testing Methodologies	Explain different penetration testing methodologies and frameworks.

1.3 Building Your Own Lab	Configure a virtual machine for your penetration testing learning experience.
Module 2: Planning and Scoping a Penetration Testing Assessment	Create penetration testing preliminary documents.
2.1 Comparing and Contrasting Governance, Risk, and Compliance Concepts	Explain the role of governance, risk, compliance, and environmental factors in planning penetration testing.
2.2 Explaining the Importance of Scoping and Organizational or Customer Requirements	Create a penetration test scope and plan document that addresses organizational requirements for penetration testing services.
2.3 Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity	Create your personal code of conduct to provide professionalism and integrity in your ethical hacking practice.
Module 3: Information Gathering and Vulnerability Scanning	Perform information gathering and vulnerability scanning activities.
3.1 Performing Passive Reconnaissance	Perform passive reconnaissance activities.
3.2 Performing Active Reconnaissance	Perform active reconnaissance activities.
3.3 Understanding the Art of Performing Vulnerability Scans	Perform vulnerability scans.
3.4 Understanding How to Analyze Vulnerability Scan Results	Analyze the results of reconnaissance exercises.
Module 4: Social Engineering Attacks	Explain how social engineering attacks succeed.
4.1 Pretexting for an Approach and Impersonation	Explain how pretexting is used in social engineering attacks.
4.2 Social Engineering Attacks	Explain different types of social engineering attacks.
4.3 Physical Attacks	Explain different types of physical attacks.
4.4 Social Engineering Tools	Explain how social engineering attack tools facilitate attacks.
4.5 Methods of Influence	Explain how social engineering attacks enlist user participation.
Module 5: Exploiting Wired and Wireless Networks	Explain how to exploit wired and wireless network vulnerabilities.
5.1 Exploiting Network-Based Vulnerabilities	Explain how to exploit network-based vulnerabilities.
5.2 Exploiting Wireless Vulnerabilities	Explain how to exploit wireless vulnerabilities.
Module 6: Exploiting Application-Based Vulnerabilities	Explain how to exploit application-based vulnerabilities.
6.1 Overview of Web Application-Based Attacks for Security Professionals and the OWASP Top 10	Explain common web application attacks.
6.2 How to Build Your Own Web Application Lab	Describe common web application testing tools.
6.3 Understanding Business Logic Flaws	Explain how business logic flows enable attackers to exploit web applications.
6.4 Understanding Injection-Based Vulnerabilities	Use tools to conduct injection attacks.
6.5 Exploiting Authentication-Based Vulnerabilities	Use tools to exploit authentication-based vulnerabilities.
6.6 Exploiting Authorization-Based Vulnerabilities	Explain how authorization-based vulnerabilities are exploited.
6.7 Understanding Cross-Site Scripting (XSS) Vulnerabilities	Explain cross-site scripting vulnerabilities.

6.8 Understanding Cross-Site Request Forgery (CSRF/XSRF) and Server-Side Request Forgery Attacks	Explain cross-site request forgery (CSRF/XSRF) and server-side request forgery attacks.
6.9 Understanding Clickjacking	Explain clickjacking.
6.11 Exploiting File Inclusion Vulnerabilities	Explain how file inclusion vulnerabilities are exploited.
6.12 Exploiting Insecure Code Practices	Explain how to exploit insecure code.
Module 7: Cloud, Mobile, and IoT Security	Explain how to exploit cloud, mobile, and IoT security vulnerabilities.
7.1 Researching Attack Vectors and Performing Attacks on Cloud Technologies	Explain how to attack cloud technologies.
7.2 Explaining Common Attacks and Vulnerabilities Against Specialized Systems	Explain common attacks against specialized systems.
Module 8: Performing Post-Exploitation Techniques	Explain how to perform post-exploitation activities.
8.1 Creating a Foothold and Maintaining Persistence After Compromising a System	Explain how to create a foothold and maintain persistence after compromising a system.
8.2 Understanding How to Perform Lateral Movement, Detection Avoidance, and Enumeration	Explain how to perform lateral movement, detection avoidance, and enumeration.
Module 9: Reporting and Communication	Create a penetration testing report.
9.1 Comparing and Contrasting Important Components of Written Reports	Describe the major components of a written pentest report.
9.2 Analyzing the Findings and Recommending the Appropriate Remediation Within a Report	Recommend appropriate remediation based on the findings of a pentesting campaign.
9.3 Explaining the Importance of Communication During the Penetration Testing Process	Explain the components necessary for communications during the pentest process.
9.4 Explaining Post-Report Delivery Activities	Explain necessary processes to complete the pentesting engagement.
Module 10: Tools and Code Analysis	Classify pentesting tools by use case.
10.1 Understanding the Basic Concepts of Scripting and Software Development	Analyze code for pentesting use.
10.2 Understanding the Different Use Cases of Penetration Testing Tools and Analyzing Exploit Code	Classify pentesting tools by their primary use cases.