

[FORGOTTEN] CISCO DIVD Academy Ethical Hacker

Learn the art of offensive security to uncover cyber threats and vulnerabilities before the cybercriminals do.

SCHEDULE

Aug 27, 2023 - Aug 30, 2024

Languages

English

Instructor

Victor Gevers

[https://skillsforall.com/launch?id=80c156bc-84a4-47c9-a233-](https://skillsforall.com/launch?id=80c156bc-84a4-47c9-a233-5eafe7bdde82&tab=curriculum&view=a2f2eff1-791f-5595-8680-4a3b27778d2e)

[5eafe7bdde82&tab=curriculum&view=a2f2eff1-791f-5595-8680-4a3b27778d2e](https://skillsforall.com/launch?id=80c156bc-84a4-47c9-a233-5eafe7bdde82&tab=curriculum&view=a2f2eff1-791f-5595-8680-4a3b27778d2e)

- [overview](#)
- [Welcome to the Ethical Hacker Course](#)
- [1.0.1-1.0.2 Why Should I Take This Module and what will i learn?](#)
- [1.1.1 Overview](#)
- [1.1.3 Lab - Researching PenTesting Careers](#)
- [1.1.4 Threat Actors](#)

overview

i started ripping this course on August 30th of 2023

so some things may be a bit different if you take the course

<https://skillsforall.com/course/ethical-hacker?courseLang=en-US>

learn the art of offensive security to uncover cyber threats and vulnerabilities before the cybercriminals do.

SCHEDULE: Aug 27, 2023 - Aug 30, 2024

Language: English

Instructor: Victor Gevers

Estimated amount of time required to complete: 70 Hours

difficulty: Intermediate

Number of labs: 34

pacing: Self-Paced

Instructor



Victor Gevers

- [Overview](#)
- [Curriculum](#)
- [Resources](#)

The digital landscape is evolving at an unprecedented rate and cyber threats lurk around every corner. Cybersecurity resilience in the modern world cannot be just an add on - it's a necessity. Offensive security professionals like ethical hackers and penetration testers can help proactively discover unknown threats and address them before the cybercriminals do.

This course is designed to prepare you with an Ethical Hacker skillset and give you a solid understanding of offensive security. You will become proficient in the art of scoping, executing, and

reporting on vulnerability assessments, while recommending mitigation strategies. Follow an engaging gamified narrative throughout the course and get lots of practice with hands-on labs inspired by real-world scenarios.

After completing this course, continue your cybersecurity career in offensive security as an ethical hacker or penetration tester. Or use this course to strengthen your defensive security knowledge. By understanding the mindset of threat actors, you will be able to more effectively implement security controls and monitor, analyze, and respond to current security threats.

Prerequisites:

[Junior Cybersecurity Analyst Career Path](#), or equivalent entry-level cybersecurity knowledge
Basic programming knowledge

what you will learn.

Course Introduction

Course Introduction

[Welcome to the Ethical Hacker Course](#)

[The Fictional Companies in the Ethical Hacker Course](#)

[What Will I Learn in This Course?](#)

[Ethical Hacking Statement](#)

badge not found or type unknown

Module 1: Introduction to Ethical Hacking and Penetration Testing

1.0. Introduction

[1.0.1 Why Should I Take This Module?](#)

[1.0.2 What Will I Learn in This Module?](#)

1.1. Understanding Ethical Hacking and Penetration Testing

[1.1.1 Overview](#)

[1.1.2 Why Do We Need to Do Penetration Testing?](#)

[1.1.3 Lab - Researching PenTesting Careers](#)

[1.1.4 Threat Actors](#)

1.2. Exploring Penetration Testing Methodologies

[1.2.1 Overview](#)

[1.2.2 Why Do We Need to Follow a Methodology for Penetration Testing?](#)

[1.2.3 Environmental Considerations](#)

[1.2.4 Practice - Types of Penetration Tests](#)

[1.2.5 Surveying Different Standards and Methodologies](#)

[1.2.6 Lab - Compare Pentesting Methodologies](#)

1.3. Building Your Own Lab

[1.3.1 Overview](#)

[1.3.2 Requirements and Guidelines for Penetration Testing Labs](#)

[1.3.3 What Tools Should You Use in Your Lab?](#)

[1.3.4 Practice - Requirements and Guidelines for Penetration Testing Labs](#)

[1.3.5 What If You Break Something?](#)

[1.3.6 Lab - Deploy a Pre-Built Kali Linux Virtual Machine \(VM\)](#)

[1.3.7 Lab - Investigate Kali Linux](#)

1.4. Summary

[1.4.1 What Did I Learn in this Module?](#)

[1.4.2 Reflection Questions](#)

[1.4.3 Quiz - Introduction to Ethical Hacking and Penetration Testing](#)

badge not found or type unknown

Module 2: Planning and Scoping a Penetration Testing Assessment

2.0. Introduction

[2.0.1 Why Should I Take This Module?](#)

[2.0.2 What Will I Learn in This Module?](#)

2.1. Comparing and Contrasting Governance, Risk, and Compliance Concepts

[2.1.1 Overview](#)

[2.1.2 Regulatory Compliance Considerations](#)

[2.1.3 Local Restrictions](#)

[2.1.4 Practice - Regulations](#)

[2.1.5 Legal Concepts](#)

[2.1.6 Contracts](#)

[2.1.7 Disclaimers](#)

[2.1.8 Practice - Legal Concepts](#)

[2.1.9 Lab - Compliance Requirements and Local Restrictions](#)

2.2. Explaining the Importance of Scoping and Organizational or Customer Requirements

[2.2.1 Overview](#)

[2.2.2 Rules of Engagement](#)

[2.2.3 Practice - Rules of Engagement](#)

[2.2.4 Target List and In-Scope Assets](#)

[2.2.5 Practice - Target List and In-Scope Assets](#)

[2.2.6 Validating the Scope of Engagement](#)

[2.2.7 Strategy: Unknown vs. Known Environment Testing](#)

[2.2.8 Practice - Strategy: Unknown vs. Known Environment Testing](#)

[2.2.9 Lab - Pre-Engagement Scope and Planning](#)

[2.2.10 Lab - Create a Pentesting Agreement](#)

2.3. Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity

[2.3.1 Overview](#)

[2.3.2 Practice - Demonstrate an Ethical Hacking Mindset](#)

[2.3.3 Lab - Personal Code of Conduct](#)

2.4. Summary

[2.4.1 What Did I Learn in this Module?](#)

[2.4.2 Reflection Questions](#)

[2.4.3 Quiz - Planning and Scoping a Penetration Testing Assessment](#)

badge not found or type unknown

Module 3: Information Gathering and Vulnerability Scanning

3.0. Introduction

[3.0.1 Why Should I Take This Module?](#)

[3.0.2 What Will I Learn in This Module?](#)

3.1. Performing Passive Reconnaissance

[3.1.1 Overview](#)

[3.1.2 Active Reconnaissance vs. Passive Reconnaissance](#)

[3.1.3 Practice - Active Reconnaissance vs. Passive Reconnaissance](#)

[3.1.4 Lab - Using OSINT Tools](#)

[3.1.5 DNS Lookups](#)

[3.1.6 Practice - DNS Lookups](#)

[3.1.7 Identification of Technical and Administrative Contacts](#)

[3.1.8 Practice - Identification of Technical and Administrative Contracts](#)

[3.1.9 Lab - DNS Lookups](#)

[3.1.10 Cloud vs. Self-Hosted Applications and Related Subdomains](#)

[3.1.11 Social Media Scraping](#)

[3.1.12 Lab - Employee Intelligence Gathering](#)

[3.1.13 Cryptographic Flaws](#)

[3.1.14 Lab - Finding Information from SSL Certificates](#)

[3.1.15 Company Reputation and Security Posture](#)

[3.1.16 Practice - File Metadata](#)

[3.1.17 Practice - Web Archiving, Caching, and Public Code Repositories](#)

[3.1.18 Lab - Finding Out About the Organization](#)

[3.1.19 Lab - Advanced Searches](#)

[3.1.20 Open-Source Intelligence \(OSINT\) Gathering](#)

[3.1.21 Lab - Shodan Searches](#)

3.2. Performing Active Reconnaissance

[3.2.1 Overview](#)

[3.2.2 Nmap Scan Types](#)

[3.2.3 Practice - Nmap Scan Types](#)

[3.2.4 Types of Enumeration](#)

[3.2.5 Practice - Exploring Enumeration via Packet Crafting with Scapy](#)

[3.2.6 Lab - Enumeration with Nmap](#)

[3.2.7 Packet Inspection and Eavesdropping](#)

[3.2.8 Practice - Packet Inspection and Eavesdropping](#)

[3.2.9 Lab - Packet Crafting with Scapy](#)

[3.2.10 Lab - Network Sniffing with Wireshark](#)

3.3. Understanding the Art of Performing Vulnerability Scans

[3.3.1 Overview](#)

[3.3.2 How a Typical Automated Vulnerability Scanner Works](#)

[3.3.3 Practice - How a Typical Automated Vulnerability Scanner Works](#)

[3.3.4 Types of Vulnerability Scans](#)

[3.3.5 Practice - Types of Vulnerability Scans](#)

[3.3.6 Lab - Vulnerability Scanning with Kali Tools](#)

[3.3.7 Challenges to Consider When Running a Vulnerability Scan](#)

3.4. Understanding How to Analyze Vulnerability Scan Results

[3.4.1 Overview](#)

[3.4.2 Sources for Further Investigation of Vulnerabilities](#)

[3.4.3 Lab - Investigate Vulnerability Information Sources](#)

[3.4.4 How to Deal with a Vulnerability](#)

3.5. Summary

[3.5.1 What Did I Learn in this Module?](#)

[3.5.2 Reflection Questions](#)

[3.5.3 Quiz - Information Gathering and Vulnerability Scanning](#)

badge not found or type unknown

Module 4: Social Engineering Attacks

4.0. Introduction

[4.0.1 Why Should I Take This Module?](#)

[4.0.2 What Will I Learn in This Module?](#)

4.1. Pretexting for an Approach and Impersonation

[4.1.1 Overview](#)

[4.1.2 Practice - Pretexting and Impersonation](#)

4.2. Social Engineering Attacks

[4.2.1 Overview](#)

[4.2.2 Email Phishing](#)

[4.2.3 Vishing](#)

[4.2.4 Short Message Service \(SMS\) Phishing](#)

[4.2.5 Universal Serial Bus \(USB\) Drop Key](#)

[4.2.6 Watering Hole Attacks](#)

[4.2.7 Practice - Pivot Attack](#)

[4.2.8 Practice - Social Engineering Attacks](#)

4.3. Physical Attacks

[4.3.1 Overview](#)

[4.3.2 Tailgating](#)

[4.3.3 Dumpster Diving](#)

[4.3.4 Shoulder Surfing](#)

[4.3.5 Badge Cloning](#)

[4.3.6 Practice - Physical Attacks](#)

4.4. Social Engineering Tools

[4.4.1 Overview](#)

[4.4.2 Social-Engineer Toolkit \(SET\)](#)

[4.4.3 Browser Exploitation Framework \(BeEF\)](#)

[4.4.4 Practice - Browser Exploitation Framework](#)

[4.4.5 Call Spoofing Tools](#)

[4.4.6 Practice - Call Spoofing Tools](#)

[4.4.7 Lab - Explore the Social Engineer Toolkit \(SET\)](#)

[4.4.8 Lab - Using the Browser Exploitation Framework \(BeEF\)](#)

4.5. Methods of Influence

[4.5.1 Overview](#)

[4.5.2 Practice - Methods of Influence](#)

4.6. Summary

[4.6.1 What Did I Learn in this Module?](#)

[4.6.2 Reflection Questions](#)

[4.6.3 Quiz - Social Engineering Attacks](#)

badge not found or type unknown

Module 5: Exploiting Wired and Wireless Networks

5.0. Introduction

[5.0.1 Why Should I Take This Module?](#)

[5.0.2 What Will I Learn in This Module?](#)

[5.1. Exploiting Network-Based Vulnerabilities](#)

[5.1.1 Overview](#)

[5.1.2 Windows Name Resolution and SMB Attacks](#)

[5.1.3 Practice - Windows Name Resolution and SMB Attacks](#)

[5.1.4 Lab - Scanning for SMB Vulnerabilities with enum4linux](#)

[5.1.5 DNS Cache Poisoning](#)

[5.1.6 Practice - DNS Cache Poisoning](#)

[5.1.7 SNMP Exploits](#)

[5.1.8 SMTP Exploits](#)

[5.1.9 Practice - SMTP Commands](#)

[5.1.10 FTP Exploits](#)

[5.1.11 Pass-the-Hash Attacks](#)

[5.1.12 Kerberos and LDAP-Based Attacks](#)

[5.1.13 Kerberoasting](#)

[5.1.14 On-Path Attacks](#)

[5.1.15 Practice - Kerberos, LDAP, and On-Path Attacks](#)

[5.1.16 Lab - On-Path Attacks with Ettercap](#)

[5.1.17 Route Manipulation Attacks](#)

[5.1.18 DoS and DDoS Attacks](#)

[5.1.19 Practice - DoS and DDoS Attacks](#)

[5.1.20 Network Access Control \(NAC\) Bypass](#)

[5.1.21 VLAN Hopping](#)

[5.1.22 Practice - NAC Bypass and VLAN Hopping](#)

[5.1.23 DHCP Starvation Attacks and Rogue DHCP Servers](#)

[5.1.24 Practice - DHCP Starvation and Rogue DHCP Servers](#)

[5.2. Exploiting Wireless Vulnerabilities](#)

[5.2.1 Overview](#)

[5.2.2 Rogue Access Points](#)

[5.2.3 Evil Twin Attacks](#)

[5.2.4 Disassociation \(or Deauthentication\) Attacks](#)

[5.2.5 Preferred Network List Attacks](#)

[5.2.6 Wireless Signal Jamming and Interference](#)

[5.2.7 War Driving](#)

[5.2.8 Initialization Vector \(IV\) Attacks and Unsecured Wireless Protocols](#)

[5.2.9 KARMA Attacks](#)

[5.2.10 Fragmentation Attacks](#)

[5.2.11 Practice - IV, Unsecured Wireless, KARMA, and Fragmentation Attacks](#)

[5.2.12 Credential Harvesting](#)

[5.2.13 Bluejacking and Bluesnarfing](#)

[5.2.14 Bluetooth Low Energy \(BLE\) Attacks](#)

[5.2.15 Radio-Frequency Identification \(RFID\) Attacks](#)

[5.2.16 Password Spraying](#)

[5.2.17 Exploit Chaining](#)

[5.2.18 Practice - Wireless Attacks](#)

5.3. Summary

[5.3.1 What Did I Learn in this Module?](#)

[5.3.2 Reflection Questions](#)

[5.3.3 Quiz - Exploiting Wired and Wireless Networks](#)

badge not found or type unknown

Module 6: Exploiting Application-Based Vulnerabilities

6.0. Introduction

[6.0.1 Why Should I Take This Module?](#)

[6.0.2 What Will I Learn in This Module?](#)

6.1. Overview of Web Application-Based Attacks for Security Professionals and the OWASP Top 10

[6.1.1 Overview](#)

[6.1.2 The HTTP Protocol](#)

[6.1.3 Practice - The HTTP Protocol](#)

[6.1.4 Web Sessions](#)

[6.1.5 Practice - Web Sessions](#)

[6.1.6 OWASP Top 10](#)

[6.1.7 Lab - Website Vulnerability Scanning](#)

[6.1.8 Lab - Using the GVM Vulnerability Scanner](#)

6.2. How to Build Your Own Web Application Lab

[6.2.1 Overview](#)

6.3. Understanding Business Logic Flaws

[6.3.1 Overview](#)

[6.3.2 Practice - Business Logic Flaws](#)

6.4. Understanding Injection-Based Vulnerabilities

[6.4.1 Overview](#)

[6.4.2 SQL Injection Vulnerabilities](#)

[6.4.3 Practice - SQL Injection Attacks](#)

[6.4.4 Command Injection Vulnerabilities](#)

[6.4.5 Practice - Command Injection Vulnerabilities](#)

[6.4.6 Lightweight Directory Access Protocol \(LDAP\) Injection Vulnerabilities](#)

[6.4.7 Lab - Injection Attacks](#)

6.5. Exploiting Authentication-Based Vulnerabilities

[6.5.1 Overview](#)

[6.5.2 Session Hijacking](#)

[6.5.3 Practice - Session Hijacking](#)

[6.5.4 Redirect Attacks](#)

[6.5.5 Default Credentials](#)

[6.5.6 Kerberos Vulnerabilities](#)

[6.5.7 Practice - Kerberos Vulnerabilities](#)

[6.5.8 Lab - Using Password Tools](#)

6.6. Exploiting Authorization-Based Vulnerabilities

[6.6.1 Overview](#)

[6.6.2 Parameter Pollution](#)

[6.6.3 Practice - Parameter Pollution](#)

[6.6.4 Insecure Direct Object Reference Vulnerabilities](#)

[6.6.5 Practice - Insecure Direct Object Reference Vulnerabilities](#)

6.7. Understanding Cross-Site Scripting (XSS) Vulnerabilities

[6.7.1 Overview](#)

[6.7.2 Reflected XSS Attacks](#)

[6.7.3 Practice - Reflected XSS Attacks](#)

[6.7.4 Stored XSS Attacks](#)

[6.7.5 Practice - Stored XSS Attacks](#)

[6.7.6 XSS Evasion Techniques](#)

[6.7.7 XSS Mitigations](#)

[6.7.8 Lab - Cross Site Scripting](#)

6.8. Understanding Cross-Site Request Forgery (CSRF/XSRF) and Server-Side Request Forgery Attacks

[6.8.1 Overview](#)

[6.8.2 Practice - CSRF/XSRF Attacks](#)

6.9. Understanding Clickjacking

[6.9.1 Overview](#)

6.10. Exploiting Security Misconfigurations

[6.10.1 Overview](#)

[6.10.2 Exploiting Directory Traversal Vulnerabilities](#)

[6.10.3 Practice - Directory Transversal](#)

[6.10.4 Cookie Manipulation Attacks](#)

6.11. Exploiting File Inclusion Vulnerabilities

[6.11.1 Overview](#)

[6.11.2 Local File Inclusion Vulnerabilities](#)

[6.11.3 Remote File Inclusion Vulnerabilities](#)

6.12. Exploiting Insecure Code Practices

[6.12.1 Overview](#)

[6.12.2 Comments in Source Code](#)

[6.12.3 Lack of Error Handling and Overly Verbose Error Handling](#)

[6.12.4 Practice - Insecure Code](#)

[6.12.5 Hard-Coded Credentials](#)

[6.12.6 Race Conditions](#)

[6.12.7 Unprotected APIs](#)

[6.12.8 Practice - Unprotected APIs](#)

[6.12.9 Hidden Elements](#)

[6.12.10 Lack of Code Signing](#)

[6.12.11 Additional Web Application Hacking Tools](#)

[6.12.12 Practice - Web Hacking Tools](#)

[6.12.13 Lab - Use the OWASP Web Security Testing Guide](#)

6.13. Summary

[6.13.1 What Did I Learn in this Module?](#)

[6.13.2 Reflection Questions](#)

[6.13.3 Quiz - Performing Post-Exploitation Techniques](#)

badge not found or type unknown

Module 7: Cloud, Mobile, and IoT Security

7.0. Introduction

[7.0.1 Why Should I Take This Module?](#)

[7.0.2 What Will I Learn in This Module?](#)

7.1. Researching Attack Vectors and Performing Attacks on Cloud Technologies

[7.1.1 Overview](#)

[7.1.2 Practice - Types of Cloud Services](#)

[7.1.3 Credential Harvesting](#)

[7.1.4 Practice - Credential Harvesting](#)

[7.1.5 Privilege Escalation](#)

[7.1.6 Account Takeover](#)

[7.1.7 Metadata Service Attacks](#)

[7.1.8 Attacks Against Misconfigured Cloud Assets](#)

[7.1.9 Resource Exhaustion and DoS Attacks](#)

[7.1.10 Cloud Malware Injection Attacks](#)

[7.1.11 Side-Channel Attacks](#)

[7.1.12 Practice - Cloud Attack Types](#)

[7.1.13 Tools and Software Development Kits \(SDKs\)](#)

7.2. Explaining Common Attacks and Vulnerabilities Against Specialized Systems

[7.2.1 Overview](#)

[7.2.2 Attacking Mobile Devices](#)

[7.2.3 Practice - Mobile Device Vulnerabilities](#)

[7.2.4 Practice - Attacking Mobile Devices](#)

[7.2.5 Attacking Internet of Things \(IoT\) Devices](#)

[7.2.6 Analyzing IoT Protocols](#)

[7.2.7 Practice - Analyzing IoT Protocols](#)

[7.2.8 IoT Security Special Considerations](#)

[7.2.9 Common IoT Vulnerabilities](#)

[7.2.10 Practice - Common IoT Vulnerabilities](#)

[7.2.11 Data Storage System Vulnerabilities](#)

[7.2.12 Management Interface Vulnerabilities](#)

[7.2.13 Practice - Management Interface Vulnerabilities](#)

[7.2.14 Exploiting Virtual Machines](#)

[7.2.15 Vulnerabilities Related to Containerized Workloads](#)

[7.2.16 Practice - Vulnerabilities Related to Containerized Workloads](#)

7.3. Summary

[7.3.1 What Did I Learn in this Module?](#)

[7.3.2 Reflection Questions](#)

[7.3.3 Quiz - Cloud, Mobile, and IoT Security](#)

badge not found or type unknown

Module 8: Performing Post-Exploitation Techniques

8.0. Introduction

[8.0.1 Why Should I Take This Module?](#)

[8.0.2 What Will I Learn in This Module?](#)

8.1. Creating a Foothold and Maintaining Persistence After Compromising a System

[8.1.1 Overview](#)

[8.1.2 Reverse and Bind Shells](#)

[8.1.3 Practice - Reverse and Bind Shells](#)

[8.1.4 Command and Control \(C2\) Utilities](#)

[8.1.5 Practice - Types of C2 Utilities](#)

[8.1.6 Scheduled Jobs and Tasks](#)

[8.1.7 Custom Daemons, Processes, and Additional Backdoors](#)

[8.1.8 New Users](#)

8.2. Understanding How to Perform Lateral Movement, Detection Avoidance, and Enumeration

[8.2.1 Overview](#)

[8.2.2 Post-Exploitation Scanning](#)

[8.2.3 Legitimate Utilities and Living-off-the-Land](#)

[8.2.4 Practice - Post Exploitation](#)

[8.2.5 Post-Exploitation Privilege Escalation](#)

[8.2.6 Practice - Post Exploitation Privilege Escalation](#)

[8.2.7 How to Cover Your Tracks](#)

[8.2.8 Practice - Steganography](#)

8.3. Summary

[8.3.1 What Did I Learn in this Module?](#)

[8.3.2 Reflection Questions](#)

[8.3.3 Quiz - Performing Post-Exploitation Techniques](#)

badge not found or type unknown

Module 9: Reporting and Communication

9.0. Introduction

[9.0.1 Why Should I Take This Module?](#)

[9.0.2 What Will I Learn in This Module?](#)

9.1. Comparing and Contrasting Important Components of Written Reports

[9.1.1 Overview](#)

[9.1.2 Report Contents](#)

[9.1.3 Practice - Penetration Reporting](#)

[9.1.4 Storage Time for Report and Secure Distribution](#)

[9.1.5 Practice - Control and Distribution of Reports](#)

[9.1.6 Note Taking](#)

[9.1.7 Common Themes/Root Causes](#)

[9.1.8 Practice - Common Themes/Root Causes](#)

[9.1.9 Lab - Explore PenTest Reports](#)

9.2. Analyzing the Findings and Recommending the Appropriate Remediation Within a Report

[9.2.1 Overview](#)

[9.2.2 Technical Controls](#)

[9.2.3 Administrative Controls](#)

[9.2.4 Operational Controls](#)

[9.2.5 Physical Controls](#)

[9.2.6 Practice - Recommended Controls](#)

[9.2.7 Lab - Recommend Remediation Based on Findings](#)

9.3. Explaining the Importance of Communication During the Penetration Testing Process

[9.3.1 Overview](#)

[9.3.2 Communication Triggers](#)

[9.3.3 Practice - Communication Triggers](#)

[9.3.4 Reasons for Communication](#)

[9.3.5 Goal Reprioritization and Presentation of Findings](#)

9.4. Explaining Post-Report Delivery Activities

[9.4.1 Overview](#)

[9.4.2 Post-Engagement Cleanup](#)

[9.4.3 Additional Post-Report Delivery Activities](#)

[9.4.4 Practice - Post Report Delivery](#)

9.5. Summary

[9.5.1 What Did I Learn in this Module?](#)

[9.5.2 Reflection Questions](#)

[9.5.3 Quiz - Reporting and Communication](#)

badge not found or type unknown

Module 10: Tools and Code Analysis

10.0. Introduction

[10.0.1 Why Should I Take This Module?](#)

[10.0.2 What Will I Learn in This Module?](#)

10.1. Understanding the Basic Concepts of Scripting and Software Development

[10.1.1 Overview](#)

[10.1.2 Logic Constructs](#)

[10.1.3 Practice - Logic Constructs](#)

[10.1.4 Data Structures](#)

[10.1.5 Practice - Data Structures](#)

[10.1.6 Libraries](#)

[10.1.7 Procedures](#)

[10.1.8 Functions](#)

[10.1.9 Classes](#)

[10.1.10 Analysis of Scripts and Code Samples for Use in Penetration Testing](#)

[10.1.11 Practice - Scripting](#)

[10.1.12 The Bash Shell](#)

[10.1.13 Resources to Learn Python](#)

[10.1.14 Resources to Learn Ruby](#)

[10.1.15 Resources to Learn PowerShell](#)

[10.1.16 Resources to Learn Perl](#)

[10.1.17 Resources to Learn JavaScript](#)

[10.1.18 Practice - Programming Languages](#)

[10.1.19 Lab - Analyze Exploit Code](#)

[10.1.20 Lab - Analyze Automation Code](#)

10.2. Understanding the Different Use Cases of Penetration Testing Tools and Analyzing Exploit Code

[10.2.1 Overview](#)

[10.2.2 Penetration Testing - Focused Linux Distributions](#)

[10.2.3 Common Tools for Reconnaissance and Enumeration](#)

[10.2.4 Practice - Common Tools for Reconnaissance and Enumeration](#)

[10.2.5 Common Tools for Vulnerability Scanning](#)

[10.2.6 Practice - Common Tools for Vulnerability Scanning](#)

[10.2.7 Common Tools for Credential Attacks](#)

[10.2.8 Practice - Common Tools for Credential Attacks](#)

[10.2.9 Common Tools for Persistence](#)

[10.2.10 Practice - Common Tools for Persistence](#)

[10.2.11 Common Tools for Evasion](#)

[10.2.12 Practice - Common Tools for Evasion](#)

[10.2.13 Exploitation Frameworks](#)

[10.2.14 Practice - Exploitation Frameworks](#)

[10.2.15 Common Decompilation, Disassembly, and Debugging Tools](#)

[10.2.16 Practice - Common Decompilation, Disassembly, and Debugging Tools](#)

[10.2.17 Common Tools for Forensics](#)

[10.2.18 Practice - Common Tools for Forensics](#)

[10.2.19 Common Tools for Software Assurance](#)

[10.2.20 Practice - Common Tools for Software Assurance](#)

[10.2.21 Wireless Tools](#)

[10.2.22 Practice - Wireless Tools](#)

[10.2.23 Steganography Tools](#)

[10.2.24 Practice - Steganography Tools](#)

[10.2.25 Cloud Tools](#)

[10.2.26 Practice - Cloud Tools](#)

10.3. Summary

[10.3.1 What Did I Learn in this Module?](#)

[10.3.2 Reflection Questions](#)

[10.3.3 Quiz - Tools and Code Analysis](#)

Final Capstone Activity

Final Capstone Activity

[Objectives](#)

[Required Resources](#)

badge not found or type unknown

Ethical Hacker: Course Final Exam

Course Final Exam

End of Course Survey

Resources

No Resources Found.

Welcome to the Ethical Hacker Course

i started ripping this course on August 30th of 2023
so some things may be a bit different if you take the course

<https://skillsforall.com/course/ethical-hacker?courseLang=en-US>

The Fictional Companies in the Ethical Hacker Course

Throughout the content of the course, you follow an engaging gamified narrative and get lots of practice with hands-on labs inspired by real-world scenarios. On this journey, you will be guided by your virtual mentor “Alex” at our fictional offensive security company, **Protego Security Solutions**. Within your role as a junior penetration tester at Protego, you will learn all the penetration testing phases of a client engagement. **Pixel Paradise**, a video game company, is the fictional company that will serve as your client during the course.

Below are informational flyers for each fictional company.

Complete Your Employer: Protego Security Solutions

Your Employer: Protego Security Solutions

(id copy and paste with formatting but this is just so hard with all the details so ill just do a picture

The Fictional Companies in the Ethical Hacker Course

Throughout the content of the course, you follow an engaging gamified narrative and get lots of practice with hands-on labs inspired by real-world scenarios. On this journey, you will be guided by your virtual mentor “Alex” at our fictional offensive security company, **Protego Security Solutions**. Within your role as a junior penetration tester at Protego, you will learn all the penetration testing phases of a client engagement. **Pixel Paradise**, a video game company, is the fictional company that will serve as your client during the course.

Below are informational flyers for each fictional company.

Your Employer: Protego Security Solutions



Offering the best in penetration testing and security assessment services.

Founded

2009 in San Francisco, CA by a group of cybersecurity professionals who had previously worked for the U.S. Department of Defense. Privately owned.

Employees

75 including a dedicated team of ethical hackers and cybersecurity analysts

Revenue

\$37 Million annually

Services

Security assessments, cybersecurity risk assessment, disaster recovery planning, user training and testing

Offices

Headquarters in San Francisco, CA. Branch offices in London and Singapore.

Protego Security Solutions employs a team of highly-skilled and certified cybersecurity professionals. In addition to penetration testing, we provide made-to-order cybersecurity training to our clients. Because of this focus on training and learning, we hire promising entry-level candidates who work and grow professionally in our supportive mentored environment.

Our Mission

At Protego Security Solutions (PSS), we are committed to helping our clients secure their networks, systems, and applications against cyber threats. Every business has a right to be secure. Our teams of ethical hackers and security experts are dedicated to identifying vulnerabilities, mitigating risks, and providing comprehensive solutions to protect our clients' digital assets.

Our Services

- Penetration Testing
- Vulnerability Assessment
- Network Security Testing
- Website Security Testing
- Mobile Application Security Testing
- Social Engineering Testing
- Cybersecurity Consulting
- User Security Training

Protego Personnel Certifications

- Infosec Institute Certified Penetration Tester (CPT)
- CompTIA PenTest+
- Certified Information Security Managers (CISM)
- Certified Information Systems Security Professionals (CISSP)
- Certified Ethical Hacker (CEH)
- Certified Expert Penetration Tester (CEPT)
- Global Information Assurance Certification (GIAC) Penetration Tester (GPEN)
- And many others

Accreditations

- PCI Qualified Security Assessor ("QSA")
- HITRUST CSF
- Council of Registered Ethical Security Testers (CREST)
- ISO 27001
- CHECK Service Provider

About Us

At Protego, we believe in each other. We value the contributions of all employees and create a people-first culture of inclusion. We are proud to engage with our Bay Area community, and we are committed to continued growth and leadership in the gaming industry.



What Will I Learn in This Course?

The digital landscape is evolving at an unprecedented rate and cyber threats lurk around every corner. Cybersecurity resilience in the modern world cannot be just an add on - it's a necessity.

Offensive security professionals like ethical hackers and penetration testers can help proactively discover unknown threats and address them before the cybercriminals do.

This course is designed to prepare you with an Ethical Hacker skillset and give you a solid understanding of offensive security. You will become proficient in the art of scoping, executing, and reporting on vulnerability assessments, while recommending mitigation strategies.

After completing this course, continue your cybersecurity career in offensive security (red team) as an ethical hacker or penetration tester. Or use this course to strengthen your defensive security (blue team) knowledge. By understanding the mindset of threat actors, you will be able to more effectively implement security controls and monitor, analyze, and respond to current security threats.

Module Title	Module Objective
Introduction to Ethical Hacking and Penetration Testing	Explain the importance of methodological ethical hacking and penetration testing.
Planning and Scoping a Penetration Testing Assessment	Create penetration testing preliminary documents.
Information Gathering and Vulnerability Scanning	Perform information gathering and vulnerability scanning activities.
Social Engineering Attacks	Explain how social engineering attacks succeed.
Exploiting Wired and Wireless Networks	Explain how to exploit wired and wireless network vulnerabilities.
Exploiting Application-Based Vulnerabilities	Explain how to exploit application-based vulnerabilities.
Cloud, Mobile, and IoT Security	Explain how to exploit cloud, mobile, and IoT security vulnerabilities.
Performing Post-Exploitation Techniques	Explain how to perform post-exploitation activities.
Reporting and Communication	Create a penetration testing report.
Tools and Code Analysis	Classify pentesting tools by use case.

Ethical Hacking Statement

This is a multiple choice question. Once you have selected an option, select the submit button below

In this course, you will explore and apply various tools and techniques within a controlled, "sandboxed" Ethical Hacker Kali Linux virtual machine environment to simulate cyber-attacks and discover, assess, and exploit built-in vulnerabilities. It is crucial to acknowledge that the hands-on labs are meant solely for educational purposes, aiming to equip you with the skills to identify and safeguard against real-world threats. The vulnerabilities and weaknesses demonstrated here must be used responsibly and ethically, exclusively within this designated "sandboxed" environment.

Engaging with these tools, techniques, or resources beyond the provided "sandboxed" virtual environment or outside your authorized scope may lead to violations of local laws and regulations. We strongly emphasize the **importance** of seeking clarification from your administrator or instructor before attempting any experimentation.

It is imperative to comprehend that **unauthorized access to data, computer systems, and networks is illegal** in numerous jurisdictions, **regardless of intentions or motivations**. We emphasize the significance of using your newfound knowledge responsibly and ensuring compliance with all applicable laws and regulations.

By accepting this "Ethical Hacker Statement," you acknowledge the critical importance of utilizing the skills acquired in this course for ethical and lawful purposes only, and you commit to upholding the principles of responsible cybersecurity practices. Remember, with great power comes great responsibility.

Your Acknowledgment

Do you acknowledge and accept your responsibility, as the user of this course, to be cognizant of and compliant with local laws, regulations, and ethical use?

☐

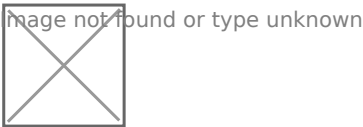
Yes, I accept my responsibility as specified in the **Ethical Hacking Statement**.

☐

No, I do not accept my responsibility as specified in the **Ethical Hacking Statement**.

1.0.1-1.0.2 Why Should I Take This Module and what will i learn?

1.0.1 Why Should I Take This Module?



Protego Security Solutions Task

Welcome to Protego! My name is Alex. I will be your mentor for your first 90 days here. Our recruiter was very impressed with your enthusiasm and desire to enter the cybersecurity profession.

We'll be working together to get you ready for your role as an entry-level penetration tester. We'll be talking about ways that you can prepare for participating in our customer engagements and I have a number of activities for you to complete that will quickly enhance your skills.

We will talk about some important big ideas in penetration testing and then get your practice lab environment up and running.

I know you will enjoy working at Protego, and I look forward to working with you as you grow in your career with us.

Before we jump into how to perform penetration testing, you first need to understand some core concepts about the "art of hacking" that will help you understand the other concepts discussed throughout this course. For example, you need to understand the difference between *ethical hacking* and *unethical hacking*. The tools and techniques used in this field change rapidly, so understanding the most current threats and attacker motivations is also important. Some consider

penetration testing an art; however, this art needs to start out with a methodology if it is to be effective. Furthermore, you need to spend some time understanding the different types of testing and the industry methods used. Finally, this is a hands-on concept, and you need to know how to get your hands dirty by properly building a lab environment for testing.

1.0.2 What Will I Learn in This Module?

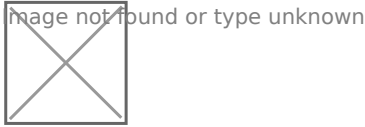
Module Title: Introduction to Ethical Hacking and Penetration Testing

Module Objective: Explain the importance of methodological ethical hacking and penetration testing.

Topic Title	Topic Objective
Understanding Ethical Hacking and Penetration Testing	Explain the importance of ethical hacking and penet
Exploring Penetration Testing Methodologies	Explain different types of penetration testing method frameworks.
Building Your Own Lab	Configure a virtual machine for your penetration test experience.

1.1.1 Overview

1.1.1 Overview



Protego Security Solutions

Alex here! We will be meeting periodically over the next few weeks so you can get oriented to working at Protego and also build your skills and knowledge as we increase your involvement in our customer engagements.

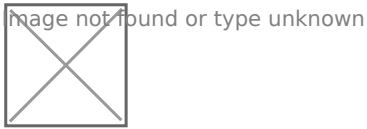
At the very heart of what we do is our purpose. You need to understand why we do what we do and who our enemies are. Once you have a strong foundation here, we can move on to understanding how we accomplish our purpose.

As a refresher, the term **ethical hacker** describes a person who acts as an attacker and evaluates the security posture of a computer network for the purpose of minimizing risk. The NIST Computer Security Resource Center (CSRC) defines a *hacker* as an “unauthorized user who attempts to or gains access to an information system.” Now, we all know that the term *hacker* has been used in many different ways and has many different definitions. Most people in a computer technology field would consider themselves hackers based on the simple fact that they like to tinker. This is obviously not a malicious thing. So, the key factor here in defining ethical versus nonethical hacking is that the latter involves malicious intent. The *permission to attack* or permission to test is crucial and what will keep you out of trouble! This permission to attack is often referred to as “the scope” of the test (what you are allowed and not allowed to test). More on this later in this module.

A security researcher looking for vulnerabilities in products, applications, or web services is considered an ethical hacker if he or she responsibly discloses those vulnerabilities to the vendors or owners of the targeted research. However, the same type of “research” performed by someone who then uses the same **vulnerability** to gain unauthorized access to a target network/system would be considered a nonethical hacker. We could even go so far as to say that someone who finds a vulnerability and discloses it publicly without working with a vendor is considered a nonethical hacker – because this could lead to the compromise of networks/systems by others who use this information in a malicious way.

The truth is that as an ethical hacker, you use the same tools to find vulnerabilities and exploit targets as do nonethical hackers. However, as an ethical hacker, you would typically report your findings to the vendor or customer you are helping to make the network more secure. You would also try to avoid performing any tests or exploits that might be destructive in nature.

An ethical hacker's goal is to analyze the security posture of a network's or system's infrastructure in an effort to identify and possibly exploit any security weaknesses found and then determine if a compromise is possible. This process is called *security **penetration testing*** or *ethical hacking*.

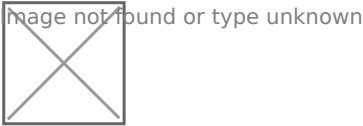


TIP Hacking is NOT a Crime (hackingisnotacrime.org) is a nonprofit organization that attempts to raise awareness about the pejorative use of the term *hacker*. Historically, *hackers* have been portrayed as evil or illegal. Luckily, a lot of people already know that hackers are curious individuals who want to understand how things work and how to make them more secure.

1.1.2 Why Do We Need to Do Penetration Testing?

So, why do we need penetration testing? Well, first of all, as someone who is responsible for securing and defending a network/system, you want to find any possible paths of compromise before the bad guys do. For years we have developed and implemented many different defensive techniques (for instance, antivirus, firewalls, intrusion prevention systems [IPSs], anti-malware). We have deployed defense-in-depth as a method to secure and defend our networks. But how do we know if those defenses really work and whether they are enough to keep out the bad guys? How valuable is the data that we are protecting, and are we protecting the right things? These are some of the questions that should be answered by a penetration test. If you build a fence around your yard with the intent of keeping your dog from getting out, maybe it only needs to be 4 feet tall. However, if your concern is not the dog getting out but an intruder getting in, then you need a different fence – one that would need to be much taller than 4 feet. Depending on what you are protecting, you might also want razor wire on the top of the fence to deter the bad guys even more. When it comes to information security, we need to do the same type of assessments on our networks and systems. We need to determine what it is we are protecting and whether our defenses can hold up to the threats that are imposed on them. This is where penetration testing comes in. Simply implementing a firewall, an IPS, anti-malware, a VPN, a web application firewall (WAF), and other modern security defenses isn't enough. You also need to test their validity. And you need to do this on a regular basis. As you know, networks and systems change constantly. This means the attack surface can change as well, and when it does, you need to consider reevaluating the security posture by way of a penetration test.

1.1.3 Lab - Researching PenTesting Careers



Protego Security Solutions

I think it is important for you to understand the employment landscape and the different roles and responsibilities that cybersecurity professions include. A good general reference to explore for descriptions of different job roles is The National Initiative for Cybersecurity Careers and Studies (NICCS) [Cyber Career Pathways Tool](#). It offers a visual way to discover and compare different job roles in our profession.

In this activity, you discover and compare ethical hacking jobs that are listed on various job boards. Don't worry, we are not trying to get rid of you! We just want you to understand where you fit in to the big picture in our profession. I think that you will find that we are treating you very well, and rest assured that you have a lot of room to grow with us.

In this lab, you will complete the following objectives:

- Conduct a Penetration Tester Job Search
- Analyze Penetration Tester Job Requirements
- Discover Resources to Further Your Career

Lab - Researching PenTesting Careers

email naruzkurai@gmail.com to link the html hosting sheet

Skills Check

This is a multiple choice question. Once you have selected an option, select the submit button below

the following three internet job boards allow filtering job postings by seniority or experience level.

glassdoor.com

indeed.com

linkedin.com jobs

At the time of this writing, monster.com did not have a filter for level of expertise or seniority in its job search results. but allows searching of weather or not you want to be at home part time etc.



Lab - Researching PenTesting Careers

[Download HTML](#)

Lab - Researching PenTesting Careers

Objectives

In this lab, you will complete the following objectives:

- Conduct a Penetration Tester Job Search
- Analyze Penetration Tester Job Requirements
- Discover Resources to Further Your Career

Background / Scenario

When preparing for any career, it is important to understand the prospective job market. The help wanted postings on internet job boards contain a wealth of information regarding the qualifications and preparation required for the jobs that you will be applying for. For careers in ethical hacking, you can see the certifications, knowledge, and skills that are required along with descriptions of what the ethical hacker will be doing for the company. In addition, you can see the kinds of organizations that hire ethical hackers, their locations, and other corporate information that is useful to know when applying for positions.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

Part 1: Conduct a Penetration Tester Job Search

In this part of the lab, you will conduct a search for ethical hacker/penetration tester jobs on various internet employment sites.

Step 1: Search internet job boards.

- Open a browser and search for jobs related to ethical hacking and penetration testing. Use employment sites such as **indeed.com**, **glassdoor.com**, **linkedin.com**, **monster.com**, etc.
- Consult at least three different employment sites. Search specifically for entry-level postings, although feel free to look at more senior positions. Find some jobs that look interesting to you.
- Complete **Table 1: Jobs Table** with at least five jobs that you have found from different employment sites. You can complete the tables in this document, or recreate the tables in another file or on a piece of paper.
- Bookmark these jobs or open each job in a new tab. Keep the sites available for the next part of the lab.

Table 1: Jobs Table

--	--	--	--	--

1.1.4 Threat Actors

Before you can understand how an ethical hacker or penetration tester can mimic a **threat actor** (or malicious attacker), you need to understand the different types of threat actors. The following are the most common types of malicious attackers we see today. Select each for more information.

Organized Crime

Several years ago, the cybercrime industry took over the number-one spot, previously held by the drug trade, for the most profitable illegal industry. As you can imagine, it has attracted a new type of cybercriminal. Just as it did back in the days of Prohibition, organized crime goes where the money is. Organized crime consists of very well-funded and motivated groups that will typically use any and all of the latest attack techniques. Whether that is ransomware or data theft, if it can be monetized, organized crime will use it.

Hacktivists

This type of threat actor is not motivated by money. Hacktivists are looking to make a point or to further their beliefs, using cybercrime as their method of attack. These types of attacks are often carried out by stealing sensitive data and then revealing it to the public for the purpose of embarrassing or financially affecting a target.

State-Sponsored Attackers

Cyber war and cyber espionage are two terms that fit into this category. Many governments around the world today use cyber attacks to steal information from their opponents and cause disruption. Many believe that the next Pearl Harbor will occur in cyberspace. That's one of the reasons the United States declared cyberspace to be one of the operational domains that U.S. forces would be trained to defend.

Insider Threats

An insider threat is a threat that comes from inside an organization. The motivations of these types of actors are normally different from those of many of the other common threat actors. Insider threats are often normal employees who are tricked into divulging sensitive information or mistakenly clicking on links that allow attackers to gain access to their computers. However, they could also be malicious insiders who are possibly motivated by revenge or money.