Networking Academy

Increasing Cybersecurity Resilience Using a New **Ethical Hacker** Course

Special IPD Session

Jozef Janitor

Product Manager

2023/08/17

Agenda

- The Unknown Unknowns
- Ethical Hackers in Cybersecurity Careers
- Course Overview
- Course Demo
- Labs Demo
- Learner’s Journey and Use Cases
- Instructor’s Resources
- Q&A

I didn’t see anything out of the ordinary.

Victim

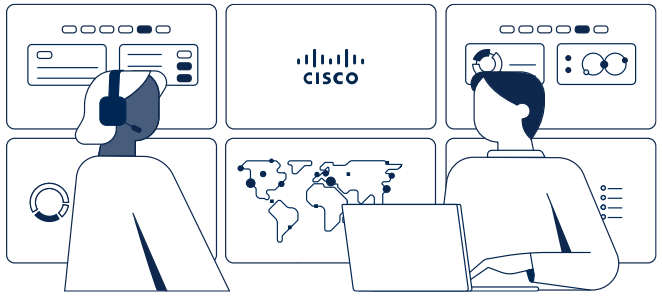
Most of the organizations

Meet the cybersecurity heroes team

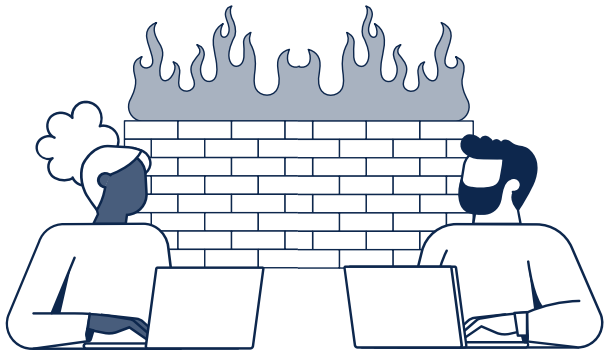
Red Team: Offensive security

Ethical Hackers

Blue Team: Defensive security

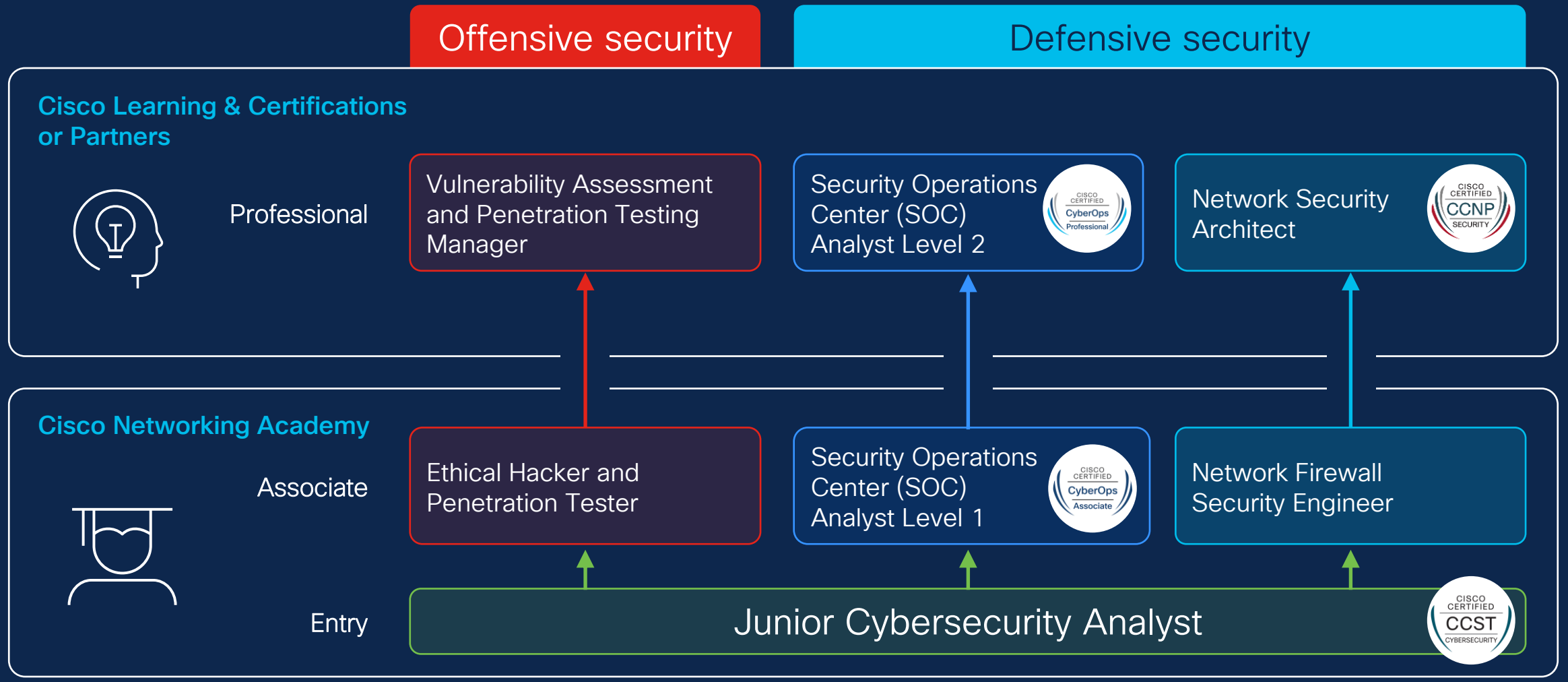


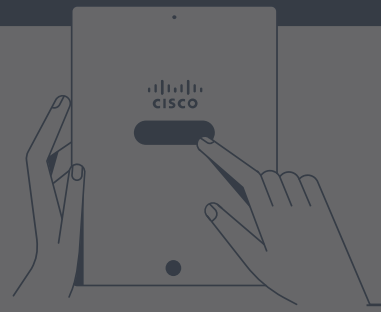
Security Operations Center



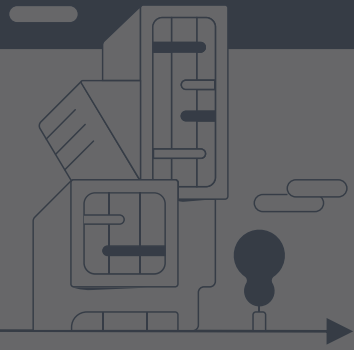
Firewall & Security

Cybersecurity Career Progressions





Learning pathways from zero to jobs



Offensive security

Defensive security

Cisco Networking Academy

Associate

Ethical Hacker

CyberOps Associate

Network Security

Entry

Cybersecurity Essentials or Junior Cybersecurity Analyst Career Path:
Endpoint Security, Network Defense, and Cyber Threat Management

Awareness

Introduction to Cybersecurity

Ethical Hacker

Description:

Security personnel that designs and performs penetration tests to discover vulnerabilities and recommend mitigation strategies. They check cases to determine if infrastructure components, systems, and applications meet confidentiality, integrity, and availability standards, analyze the findings, and communicate appropriate remediation within a report.

Aliases:

- Penetration Tester
- Penetration Testing Analyst
- Vulnerability Assessor
- Bug Bounty Hunter

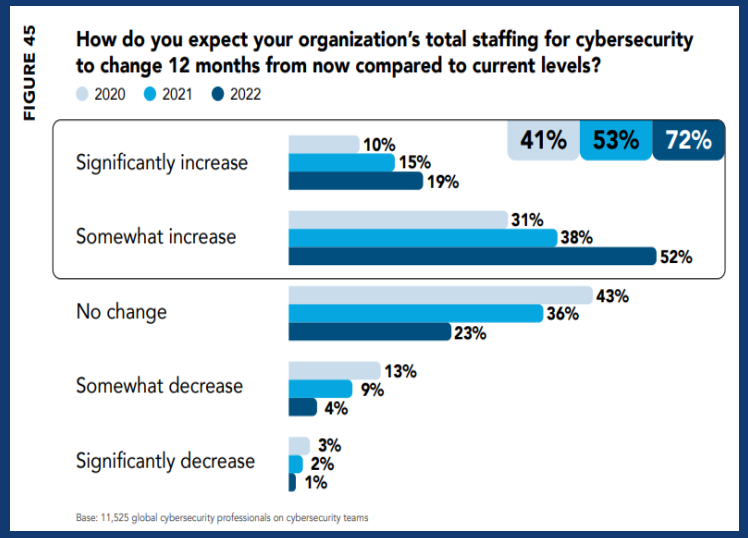
Experience level:

1-3 years

Skills:

- ✓ Understand legal and compliance requirements
- ✓ Oversee vulnerability assessment and penetration testing activities
- ✓ Define and translate requirements into test plans and procedures
- ✓ Perform security assessments of infrastructure components and computer systems
- ✓ Manage penetration testing activities, including reporting and documentation
- ✓ Review and assess existing security policies and procedures

Market Size



src: (ISC)² Cybersecurity Workforce Study, 2022

Due to a talent shortage and a strong growth in the new open job roles, Cybersecurity Ventures predicts 3.5M cybersecurity jobs globally will go unfilled by 2025.

src: Cybersecurity Jobs Report 2021, Cybersecurity Ventures

The Global Penetration Testing Market size is forecast to reach $2.87 billion by 2025, growing at a CAGR of 15.87% during 2020-2025.

src: IndustryARC Penetration Testing Market - Forecast(2023 - 2028)

Penetration tester employment is projected to grow 31% from 2019 to 2029, much faster than the average for all occupations.

src: U.S. Bureau of Labor Statistics (BLS).

- 15.9% YoY employment growth (147k to 171k in 2020 to 2021).
- 15,212 Unique Job Postings (over the last 12 months).
- The national median salary for Penetration Testers is $112,480

src: Lightcast Occupation Snapshot Report: Penetration Testers in United States 2023/06/07

Ethical Hacker
Course Overview

Networking Academy

Ethical Hacker

Course Overview

The Ethical Hacker course prepares learners with skills to proactively discover vulnerabilities before the cybercriminals do. Learners will become proficient in the art of scoping, executing, and reporting on vulnerability assessments, while recommending mitigation strategies.

Benefits

Through the gamified narrative in the course and real-world inspired hands-on practice labs, students develop essential workforce readiness skills, laying a solid foundation in offensive security.

Prepare for Careers

- ✓ Get job-ready for Offensive Security roles such as Ethical Hacker or Penetration Tester.
- ✓ Understand the mindset and tactics of cybercriminals to strengthen your defensive security skillset.
- ✓ Gain needed skills for implementing security controls and monitoring, analyzing, and responding to current security threats.

Course Details

Target Audience: College/university students or vocational school students

Estimated Time to Completion: 70 hours

Prerequisites:
- Entry-level cybersecurity knowledge: CCST Cybersecurity certification or Cybersecurity Essentials or Junior Cybersecurity Analyst Career Path, or equivalent
- Basic programming knowledge

Course Delivery: Instructor-led and Self-paced

Learning Component Highlights:
- ✓ 10 modules and 34 labs
- ✓ 86 interactive practice activities and quizzes
- ✓ 1 final exam
- ✓ 1 skills-based assessment

Course Recognitions: Digital Badge

Recommended Next Course:
CyberOps Associate, Network Security

Requirements

- ASC Alignment: Recommended
- Instructor Training: Recommended
- Basic Equipment: Computer and Internet
- Additional Equipment: No

skillsforall.com

Gamified Narrative

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.

Matt Willis
CEO, Founder

Janice Katz
V.P. Finance

Fernando Gomes
V.P Technology

Alex Prevost
Director, Customer Engagement

PIXEL Paradise

Elizabeth deGray
Creative Director & CEO

William A. Hurst
Technical Director

Alphonse Luis Silva
V.P. Marketing & Sales

Our mission is to push the boundaries of creativity and innovation in the gaming industry to the next level. Our quest is to create immersive engaging gaming experiences that captivate players and inspire them to explore rich new worlds, conquer new challenges, and take off on thrilling adventures.

As a company, we are dedicated to fostering a culture of collaboration, excellence, and inclusivity. We value the contributions of every team member. We are proud to be based in San Francisco, a hub of innovation and creativity, and we are excited to continue to grow and expand our reach in the years to come.

Living on island time since 2012

Privately Owned

75 developers, programmers, graphic designers, content creators

$30 Million Annual Revenue

Games for Windows, MacOS, Linux, and all major gaming platforms

+ tee shirts, coffee mugs, posters, and other swag

Just a few awards...

2013
Most Promising New Video Game Enterprise, International Association Video Games Traders (IAVGT)
2013
Runner Up, Games World Magazine best games of the year
2015
3rd Place, Games World Magazine best games of the year
2019
European Gamers Alliance Outstanding New Game
2020
Celtic Fog Warriors Union best of 2020

Ethical Hacking Statement

Ethical Hacking Statement

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**.

Submit | Show feedback

Course Outline

Hands-on Labs and Practice Items

1.2.3 Environmental Considerations

There are, of course, a number of different types of penetration tests. Often they are combined in the overall scope of a penetration test; however, they can also be performed as individual tests as well.

The following is a list of some of the most common environmental considerations for the types of penetration tests today:

Network Infrastructure Tests | **Application-Based Tests** | **Penetration Testing in the Cloud**

Network Infrastructure Tests

Testing of the network infrastructure can mean a few things. For the purposes of this course, we say it is focused on evaluating the security posture of the actual network infrastructure and how it is able to help defend against attacks. This often includes the switches, routers, firewalls, and supporting resources, such as authentication, authorization, and accounting (AAA) servers and IPSs. A penetration test on wireless infrastructure may sometimes be included in the scope of a network infrastructure test. However, additional types of tests beyond a wired network assessment would be performed. For instance, a wireless security tester would attempt to break into a network via the wireless network either by bypassing security mechanisms or breaking the cryptographic methods used to secure the traffic. Testing the wireless infrastructure helps an organization to determine weaknesses in the wireless deployment as well as the exposure. It often includes a detailed heat map of the signal disbursement.

NOTE Many penetration testers find the physical aspect of testing to be the most fun because they are essentially being paid to break into the facility of a target. This type of test can help expose any weaknesses in the physical perimeter as well as any security mechanisms that are in place, such as guards, gates, and fencing. The result should be an assessment of the external physical security controls. The majority of compromises today start with some kind of social engineering attack. This could be a phone call, an email, a website, an SMS message, and so on. It is important to test how your employees handle these types of situations. This type of test is often omitted from the scope of a penetration testing engagement mainly because it primarily involves testing people instead of the technology. In most cases, management does not agree with this type of approach. However, it is important to get a real-world view of the latest attack methods. The result of a social engineering test should be to assess the security awareness program so that you can enhance it. It should not be to identify individuals who fail the test. One of the tools that we talk about more in a later module is the Social-Engineer Toolkit (SET), created by Dave Kennedy. This is a great tool for performing social engineering testing campaigns.

TIP Bug bounty programs enable security researchers and penetration testers to get recognition (and often monetary compensation) for finding vulnerabilities in websites, applications, or any other types of systems. Companies like Microsoft, Apple, and Cisco and even government institutions such as the U.S. Department of Defense (DoD) use bug bounty programs to reward security professionals when they find vulnerabilities in their systems. Many security companies, such as HackerOne, Bugcrowd, Intigriti, and SynAck, provide platforms for businesses and security professionals to participate in bug bounty programs. These programs are different from traditional penetration testing engagements but have a similar goal: finding security vulnerabilities to allow the organization to fix them before malicious attackers are able to exploit such vulnerabilities. I have included different bug bounty tips and resources in my GitHub repository at: *https://github.com/The-Art-of-Hacking/h4cker/tree/master/bug-bounties*.

When talking about penetration testing methods, you are likely to hear the terms unknown-environment (previously known as *black-box*), known-environment (previously known as *white-box*), and partially known environment (previously known as *gray-box*) testing. These terms are used to describe the perspective from which the testing is performed, as well as the amount of information that is provided to the tester:

Unknown-Environment Test | **Known-Environment Test** | **Partially Known Environment Test**

Unknown-Environment Test

In an unknown-environment penetration test, the tester is typically provided only a very limited amount of information. For instance, the tester may be provided only the domain names and IP addresses that are in scope for a particular target. The idea of this type of limitation is to have the tester start out with the perspective that an external attacker might have. Typically, an attacker would first determine a target and then begin to gather information about the target, using public information, and gain more and more information to use in attacks. The tester would not have prior knowledge of the target's organization and infrastructure. Another aspect of unknown-environment testing is that sometimes the network support personnel of the target may not be given information about exactly when the test is taking place. This allows for a defense exercise to take place as well, and it eliminates the issue of a target preparing for the test and not giving a real-world view of how the security posture really looks.

1.2.4 Practice - Types of Penetration Tests

Protego has been contracted to do a network infrastructure test as part of a broader penetration testing engagement. What will you be targeting in this test? (Choose all that apply.)

- [ ] IPS devices
- [ ] switches
- [ ] AAA servers
- [ ] virtual machines (VM) that are running in the cloud
- [x] the digital storefront

Reset | Show feedback

Show correct answer

1.3.6 Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM)

Protego Security Solutions Task

Kali is a great tool! We are providing you with a working version of it that you can use to learn new tools and practice penetration testing techniques. The Kali Linux version that I am giving you contains all of the Kali tools and several networked simulated targets that you can practice on without risking legal problems. I encourage you to use the simulated targets and other networks that you have permission to scan, such as your home network. Be careful though, Kali provides some very powerful tools!

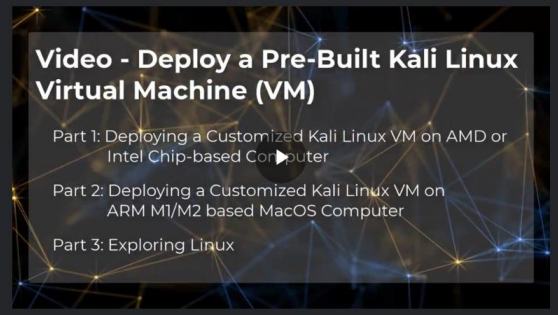
First you need to install and run the virtual machine, and then the fun begins!

In this lab, you will complete the following objectives:

- Part 1: Deploying a Customized Kali Linux VM on AMD or Intel Chip-based Computer
- Part 2: Deploying a Customized Kali Linux VM on ARM M1/M2 based MacOS Computer
- Part 3: Exploring Linux

Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM)

Select play to watch a demonstration of the lab.



Please answer the following questions after you have completed the lab.

Skills Check

You have just downloaded and installed VirtualBox or UTM. You start the application, but you do not see the Kali VM running. What step did you forget?

- ○ You need to update the install files to the latest version.
- ○ You must download and import or run the Kali VM file in VirtualBox or UTM.
- ○ There may be an issue with the installation. Remove and reinstall VirtualBox or UTM.
- ○ You must use VirtualBox or UTM to browse to the virtual machine on the kali.org website.

Submit | Show feedback

Lab Survey

Please tell us about your experience with the lab by indicating your level of agreement with the following statements.

I feel confident about the skills I practiced with this lab.

Please select an option

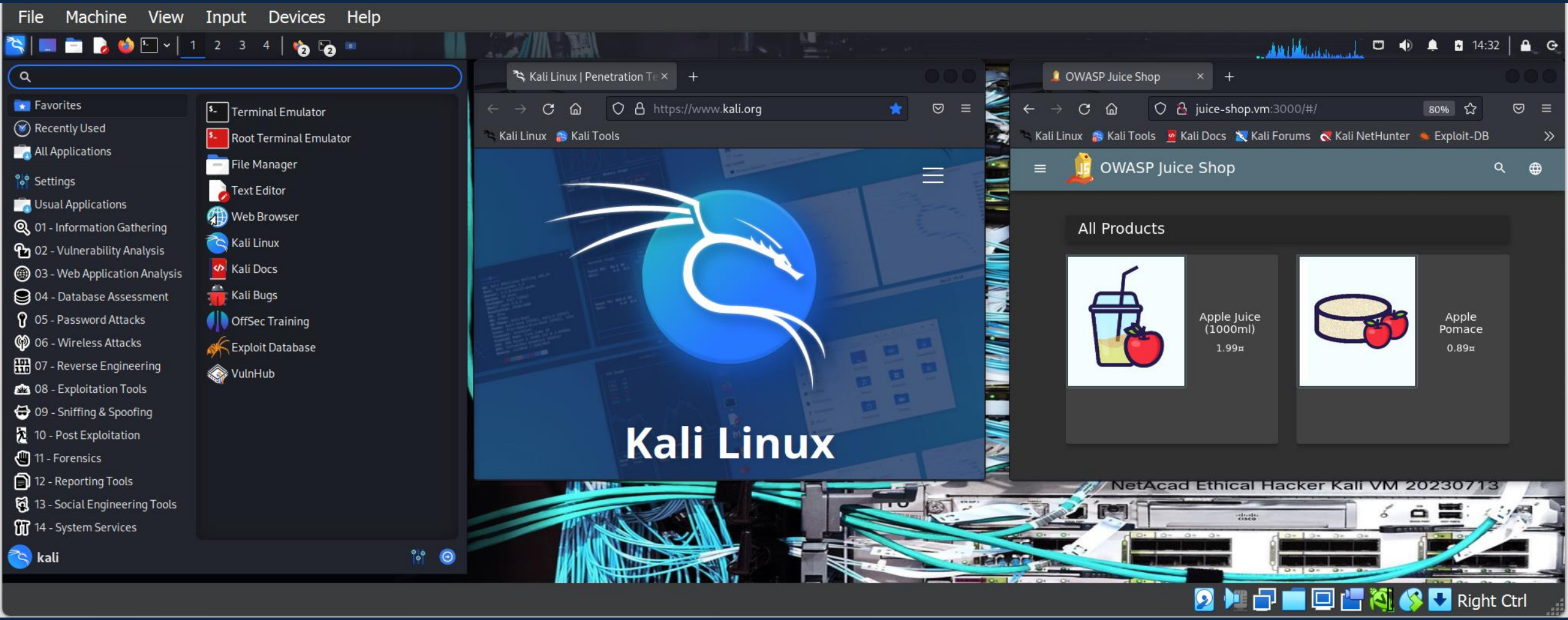
Completing this lab was a good use of my time.

Please select an option

Submit | Show feedback

Course Outline

Lab Environment



Module 1: Introduction to Ethical Hacking and Penetration Testing

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.

- Researching PenTesting Careers
- Compare Pentesting Methodologies
- Deploy a Pre-Built Kali Linux Virtual Machine
- Investigate Kali Linux

Module 2: Planning and Scoping a Penetration Testing Assessment

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.

- Compliance Requirements and Local Restrictions
- Pre-engagement Scope and Planning
- Create a Pentesting Agreement
- Personal Code of Conduct

Module 3: Information Gathering and Vulnerability Scanning

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.

- Using OSINT People Tools
- DNS Lookups
- Finding Out About Personnel
- Finding Information From SSL certificates
- Finding Out About the Organization
- Advanced Searching
- Shodan Searches
- Enumeration with Nmap
- Packet Crafting with Scapy
- Network Sniffing with Wireshark
- Vulnerability Scanning with Kali Tools
- Investigate Vulnerability Information Sources

Module 4: Social Engineering Attacks

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.

- Explore the Social Engineer Toolkit (SET)
- Using the Browser Exploitation Framework (BeEF)

Module 5: Exploiting Wired and Wireless Networks

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.

- Scanning for SMB Vulnerabilities with enum4linux
- On-Path Attacks with Ettercap

Module 6: Exploiting Application-Based 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.

- Website Vulnerability Scanning
- Using the GVM Vulnerability Scanner
- Injection Attacks
- Using Password Tools
- Cross Site Scripting
- Use the OWASP Web Security Testing Guide

Module 7: Cloud, Mobile, and IoT Security

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

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

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.

- Explore PenTest Reports
- Recommend Remediation Based on Findings

Module 10: Tools and Code Analysis

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.

- Analyze Exploit Code
- Analyze Automation Code

LAB

Demo

Learner's Journey

Networking Academy

Cybersecurity Essentials

Version 3.0, Instructor-Led only (70h)

Basic programming knowledge

Ethical Hacker

Version 1.0, Instructor-Led or Self-paced (70h)

Learner's Journey

Networking Academy

Cybersecurity Essentials
Version 3.0, Instructor-Led only (70h)

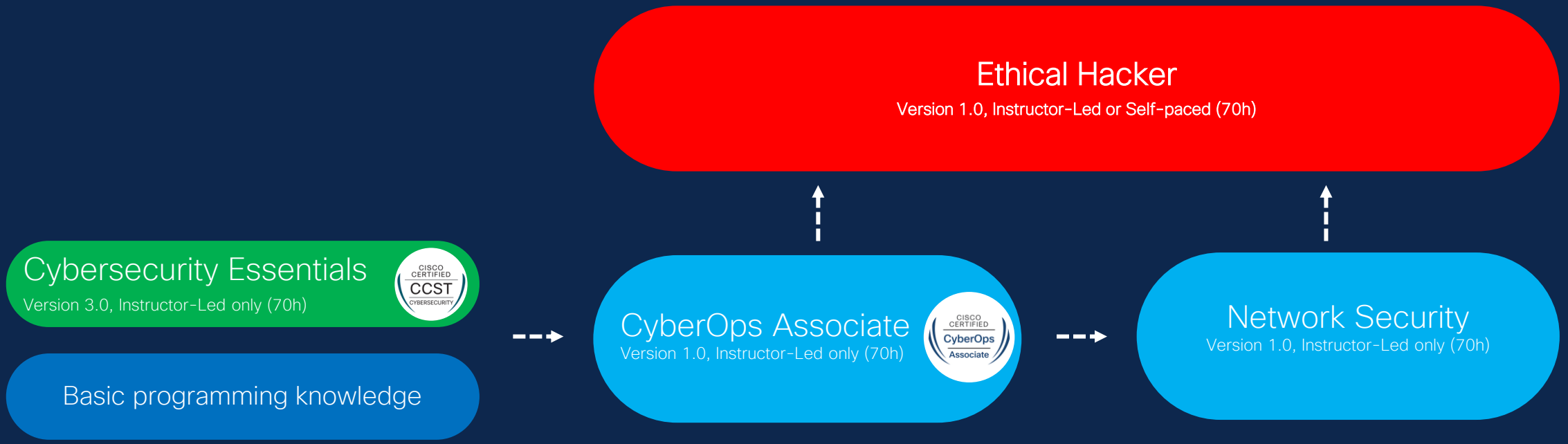
Basic programming knowledge

CyberOps Associate
Version 1.0, Instructor-Led only (70h)

Ethical Hacker
Version 1.0, Instructor-Led or Self-paced (70h)

Learner's Journey

Networking Academy



Instructor's Resources

- Scope & Sequence
- Course Overview Slide
- Course PPTs
- Instructor activated Final Exam & Skills Based Assessment (Capstone)
- IoT Security course to Ethical Hacker course Transitioning Guide

- Where to find these resources?
  https://skillsforall.com/catalog?audience=instructor
  https://www.netacad.com/portal/content/skills-all-cisco-networking-academy

- Subscribe to future IPD Week sessions

Launch Date

August 23

https://skillsforall.com

I didn’t see anything out of the ordinary.

Victim

Most of the organizations

Thank you,
for discovering all those vulnerabilities.

Happy CISO ;-)

Organizations with Ethical Hackers/Penetration Testers

The bridge to possible