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 formating 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

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

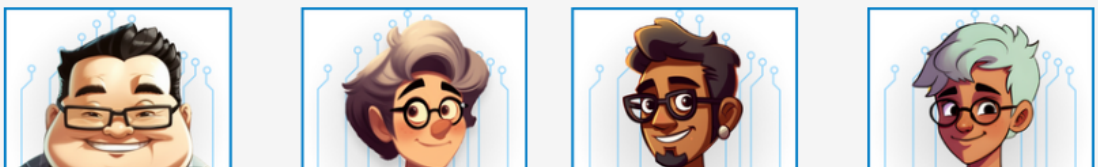
- Infosec Institute Certified Penetration Tester (CPT)
- CompTIA PenTest+
- Certified Information Security Managers (CISM)
- Certified Information Systems Security Professionals (CISSP)
- Certified Ethical Hacker (CEH)
- Certified Expert Penetration Tester (CEPT)
- Global Information Assurance Certification (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**.

Revision #1
Created 30 August 2023 16:25:53 by naruzkurai
Updated 30 August 2023 17:57:59 by naruzkurai