Cisco Certs - Network Academy - Ethical Hacker

Cisco Network Acadmeny - Ethical Hacker

Kieran Collins

2024-10-30

Contents

1 Cisco - Network Academy - Ethical Hacker

1.1 Course Introduction

1.1.1 Welcome to the Ethical Hacking Course

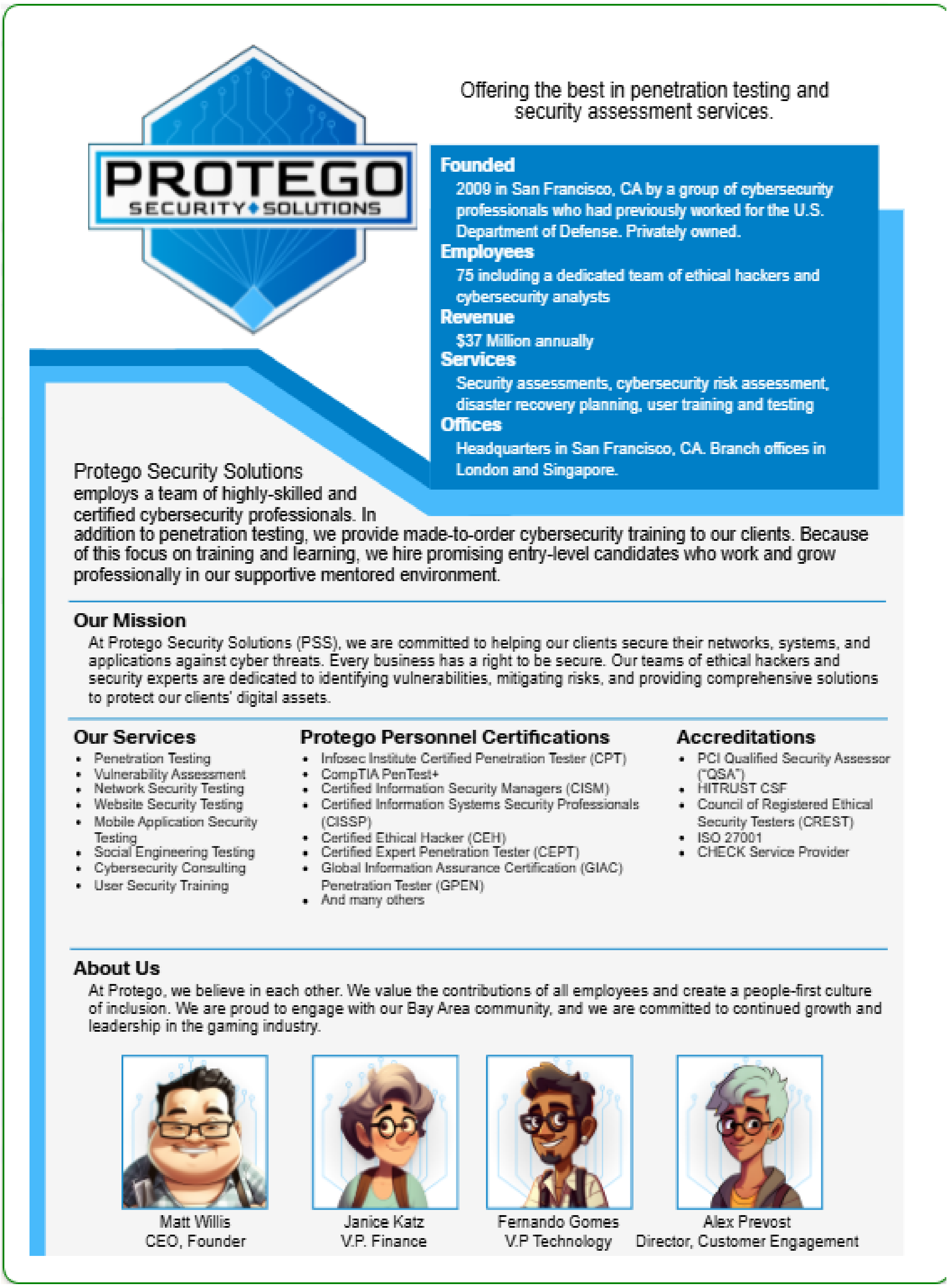
This starts with a video with a breif introduction and below is a summary

This Ethical Hacking course, taught by Cisco principal engineer Omar Santos, aims to train future cybersecurity professionals to proactively identify vulnerabilities. The course uses a gamified approach where students role-play as junior penetration testers at a fictional company. Under the guidance of a virtual mentor, they'll conduct vulnerability assessments, solve challenges, and learn to think like hackers. Though intense, the course promises to be a rewarding experience, equipping students with essential ethical hacking skills and a strong cybersecurity mindset.

1.1.2 The Fictional Companies in the Ethical Hacking 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.



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.

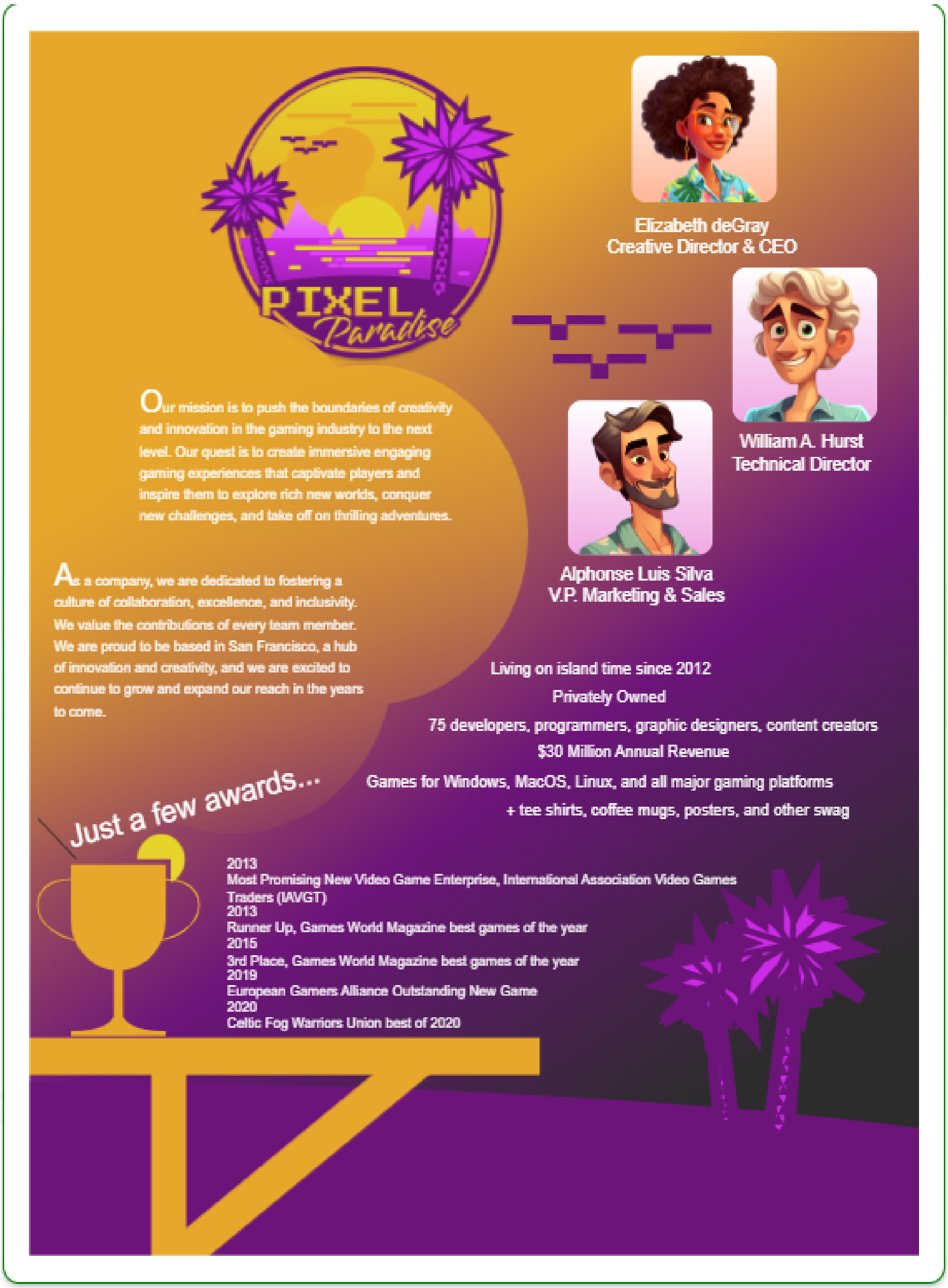
Matt Willis
CEO, Founder

Janice Katz
V.P. Finance

Fernando Gomes
V.P Technology

Alex Prevost
Director, Customer Engagement

Figure 1.1: Protego-Security-Solutions



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

Figure 1.2: Pixel-Paradise

1.1.3 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 Objectives
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 Application-Based Vulnerabilities	Explain how to exploit wired and wireless network 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.

1.2 Module 1 - Introduction to Ethical Hacking and Penetration Testing

1.2.1 1.0 Introdution - Skipping

I am skipping 1.0 Introduction due to not it is not required due to is have parts that are not relevient at this point of time.

1.2.2 1.1 Understanding Ethical Hacking and Penetration Testing

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 **Hacking is not a Crime** 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.

1.2.3 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.

1.2.4 1.1.3 Lab - Researching Pentesting Careers

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

2 Labs Questions and Answers

> [!WARNING] This will the machines and courses answers, so please see this a **Warning**.

2.1 1.1.3