Postgraduate Certificate

Pentesting Team Management

tech technological university

tech technological university

Postgraduate Certificate
Pentesting Team Management

- Modality: **online**
- Duration: **6 weeks**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/in/information-technology/postgraduate-certificate/pentesting-team-management

Index

01

Introduction

The management of pentesting teams is a fundamental aspect for institutions. The reason is that it allows to make the most of the available human and technological resources, performing penetration tests. Companies are therefore increasingly demanding the incorporation of cybersecurity experts to identify and resolve problems in an optimal manner. Faced with the rise of computer *hacking*, these professionals must regularly update their knowledge and apply the latest tools in order to prevent computer attacks. For this reason, TECH is launching an innovative program for students to implement the most cutting-edge *pentesting*tactics. In addition, this program is based on a 100% online modality, guaranteeing the comfort and flexibility of the students.

It features the most powerful arsenal of offensive auditing through 150 hours of the best digital teaching"

Thanks to audits conducted by experts in equipment management, entities are aware of their potential obstacles, risks and problems before it is too late. In this sense, pentesters facilitate communication between team members, allowing them to share their knowledge and information. In addition, resources are monitored and control strategies are applied to achieve the objectives set by the organizations (both in the short and long term).

Aware of this reality, TECH has developed a pioneering training program ranging from vulnerability analysis to advanced intrusion techniques. The syllabus will delve into a series of methodologies oriented to offensive security, among which the Cyber Security Kill Chain stands out. In addition, it will encourage creativity through the think outside the box technique and promote innovative solutions to differentiate themselves from the rest. They will also explore the different roles of *pentestings*, emphasizing the need for in-depth investigations. In turn, they will delve into the Metasploit tool, with the aim of performing simulated attacks in a controlled manner. Finally, the main challenges that affect offensive security will be presented and the graduates will be encouraged to turn them into opportunities to demonstrate their full potential and ingenuity.

It should be noted that, in order to consolidate the mastery of the contents, this training applies the state-of-the-art *Relearning*system. TECH is a pioneer in the use of this teaching model, which promotes the assimilation of complex concepts through their natural and progressive reiteration. In this line, the program also uses materials in various formats such as infographics, interactive summaries or explanatory videos. All this in a convenient 100% online mode, which allows students to adjust their schedules according to their responsibilities and personal circumstances.

This **Postgraduate Certificate in Pentesting Team Management** contains the most complete and up-to-date program on the market. The most important features include:

- The development of case studies presented by experts in pentesting team management
- The graphic, schematic and practical contents with which it is conceived provide cutting- Therapeutics and practical information on those disciplines that are essential for professional practice
- Practical exercises where the self-assessment process can be carried out to improve learning
- Its special emphasis on innovative methodologies
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

Do you want to experience a professional leap in your career? Become an Open Source Intelligence expert thanks to this training"

You will achieve your objectives thanks to TECH's didactic tools, including explanatory videos and interactive summaries"

You will delve into researching to perform the most exhaustive investigations and differentiate yourself from the rest.

Master the Metasploit program at the best digital university in the world according to Forbes.

The program's teaching staff includes professionals from the field who contribute their work experience to this educational program, as well as renowned specialists from leading societies and prestigious universities.

The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive education programmed to learn in real situations.

This program is designed around Problem-Based Learning, whereby the professional must try to solve the different professional practice situations that arise during the academic year For this purpose, the students will be assisted by an innovative interactive video system created by renowned and experienced experts.

02

Objectives

The design of this program will provide a deep dive into the tactics and techniques employed by offensive security professionals. In this line, it will focus on the development of penetration testing skills and strategies to exploit vulnerabilities in both systems and networks. In this way, solid knowledge will be provided to perform security assessments in an effective and ethical manner. Students will conduct hands-on sessions to learn theoretical concepts in simulated environments, preparing them to face real-world challenges in *Red Team*.

Looking to implement the most innovative offensive security measures? Achieve it thanks to this program in just 6 weeks"

General Objectives

- Acquire advanced skills in penetration testing and Red Team simulations, addressing the identification and exploitation of vulnerabilities in systems and networks
- Develop leadership skills to coordinate teams specialized in offensive cybersecurity, optimizing the execution of Pentesting and Red Team projects
- Develop skills in the analysis and development of malware, understanding its functionality and applying defensive and educational strategies
- Refine communication skills by preparing detailed technical and executive reports, presenting findings effectively to technical and executive audiences
- Promote an ethical and responsible practice in the field of cybersecurity, considering ethical and legal principles in all activities
- Keep students up-to-date with emerging trends and technologies in cybersecurity

During your learning process, you will have the support of the best professionals in Cybersecurity"

Specific Objectives

- Familiarize the graduate with penetration testing methodologies, including key phases such as information gathering, vulnerability analysis, exploitation and documentation
- Develop practical skills in the use of specialized Pentesting tools to identify and assess vulnerabilities in systems and networks
- Study and understand the tactics, techniques and procedures used by malicious actors, enabling the identification and simulation of threats.
- Apply theoretical knowledge in practical scenarios and simulations, facing real challenges to strengthen Pentesting skills
- Develop effective documentation skills, creating detailed reports reflecting findings, methodologies used, and recommendations for safety improvement
- Practice effective collaboration in offensive security teams, optimizing the coordination and execution of Pentesting activities

03

Course Management

In its commitment to offer the highest quality education, TECH has a first class teaching staff. These experts are characterized by a deep knowledge in cybersecurity, at the same time that they have a broad professional background. Therefore, this academic pathway provides students with the best tools and tactics to acquire multiple skills during the course. Students have the guarantees they need to specialize in a digital sector that offers numerous job opportunities.

You will have access to a learning system based on repetition, with natural and progressive teaching throughout the entire syllabus.

Management

Mr. Gómez Pintado, Carlos

- Manager of Cybersecurity and Network Team Cipherbit in Oesía Group
- Manager *Advisor & Investor* at Wesson App
- Graduate in Software Engineering and Information Society Technologies, Polytechnic University of Madrid
- Collaboration with educational institutions for the development **of Higher Level Training Cycles** in cybersecurity

Professors

Mr. Mora Navas, Sergio

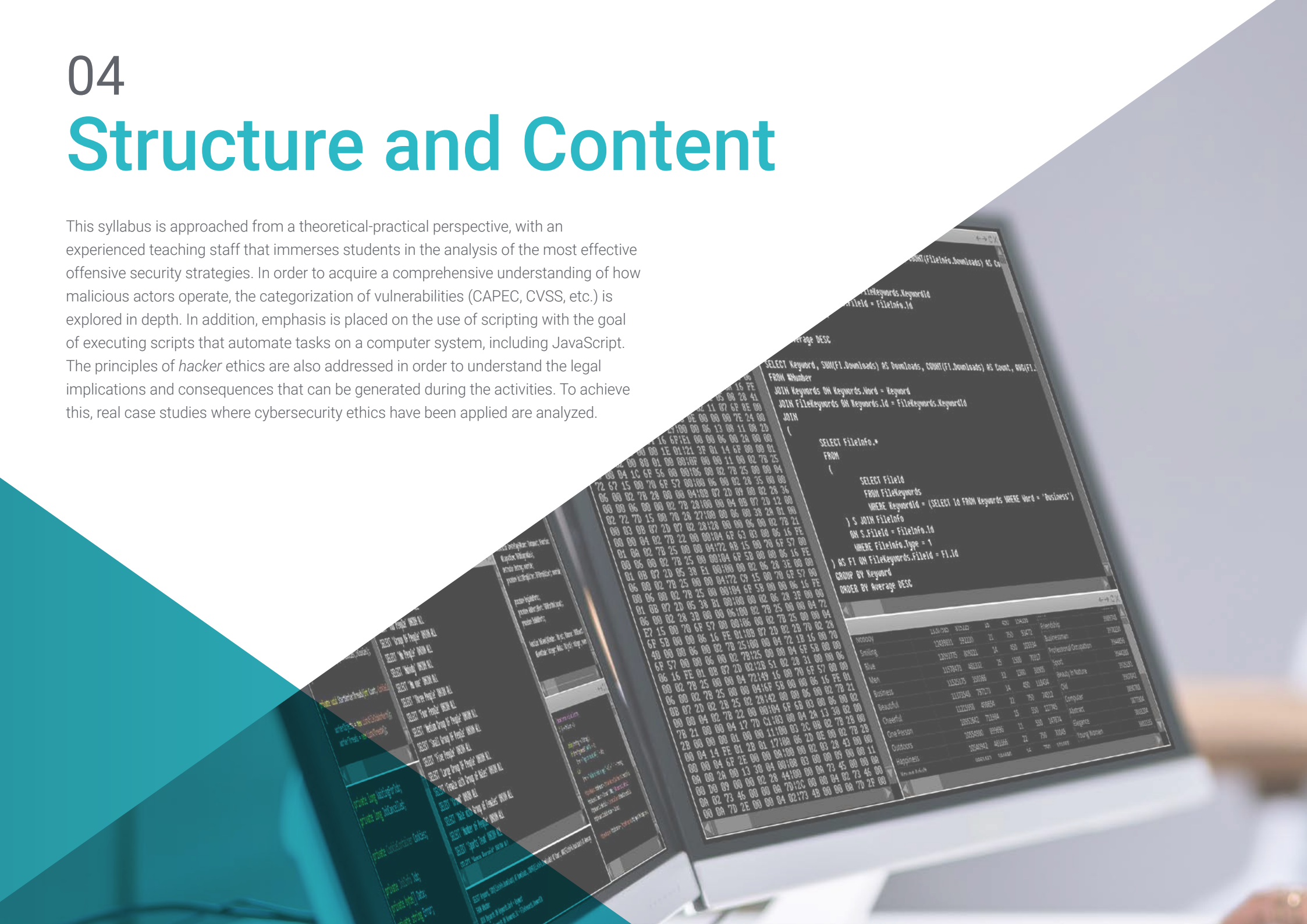
- Cybersecurity Consultant in Oesía Group
- Cybersecurity Engineer from Rey Juan Carlos University
- Computer Engineer from the University of Burgos

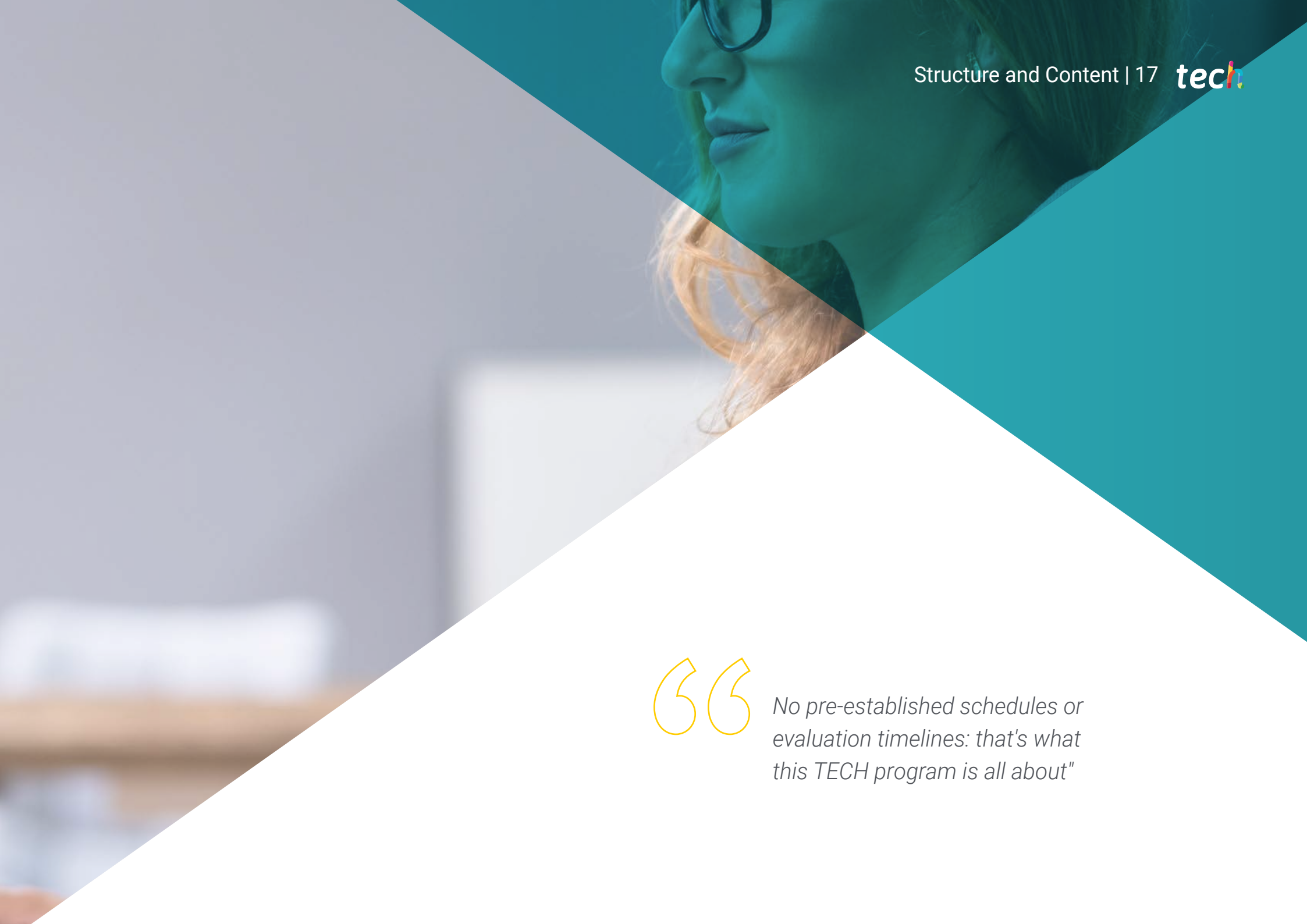

Backspace

04

Structure and Content

This syllabus is approached from a theoretical-practical perspective, with an experienced teaching staff that immerses students in the analysis of the most effective offensive security strategies. In order to acquire a comprehensive understanding of how malicious actors operate, the categorization of vulnerabilities (CAPEC, CVSS, etc.) is explored in depth. In addition, emphasis is placed on the use of scripting with the goal of executing scripts that automate tasks on a computer system, including JavaScript. The principles of *hacker* ethics are also addressed in order to understand the legal implications and consequences that can be generated during the activities. To achieve this, real case studies where cybersecurity ethics have been applied are analyzed.





No pre-established schedules or evaluation timelines: that's what this TECH program is all about"

Module 1. Offensive Security

1.1. Definition and Context
- 1.1.1. Fundamental Concepts of Offensive Security
- 1.1.2. Importance of Cybersecurity Today
- 1.1.3 Offensive Security Challenges and Opportunities

1.2. Basis of Cybersecurity
- 1.2.1. Early Challenges and Evolving Threats
- 1.2.2. Technological Milestones and Their Impact on Cybersecurity
- 1.2.3. Cybersecurity in the Modern Era

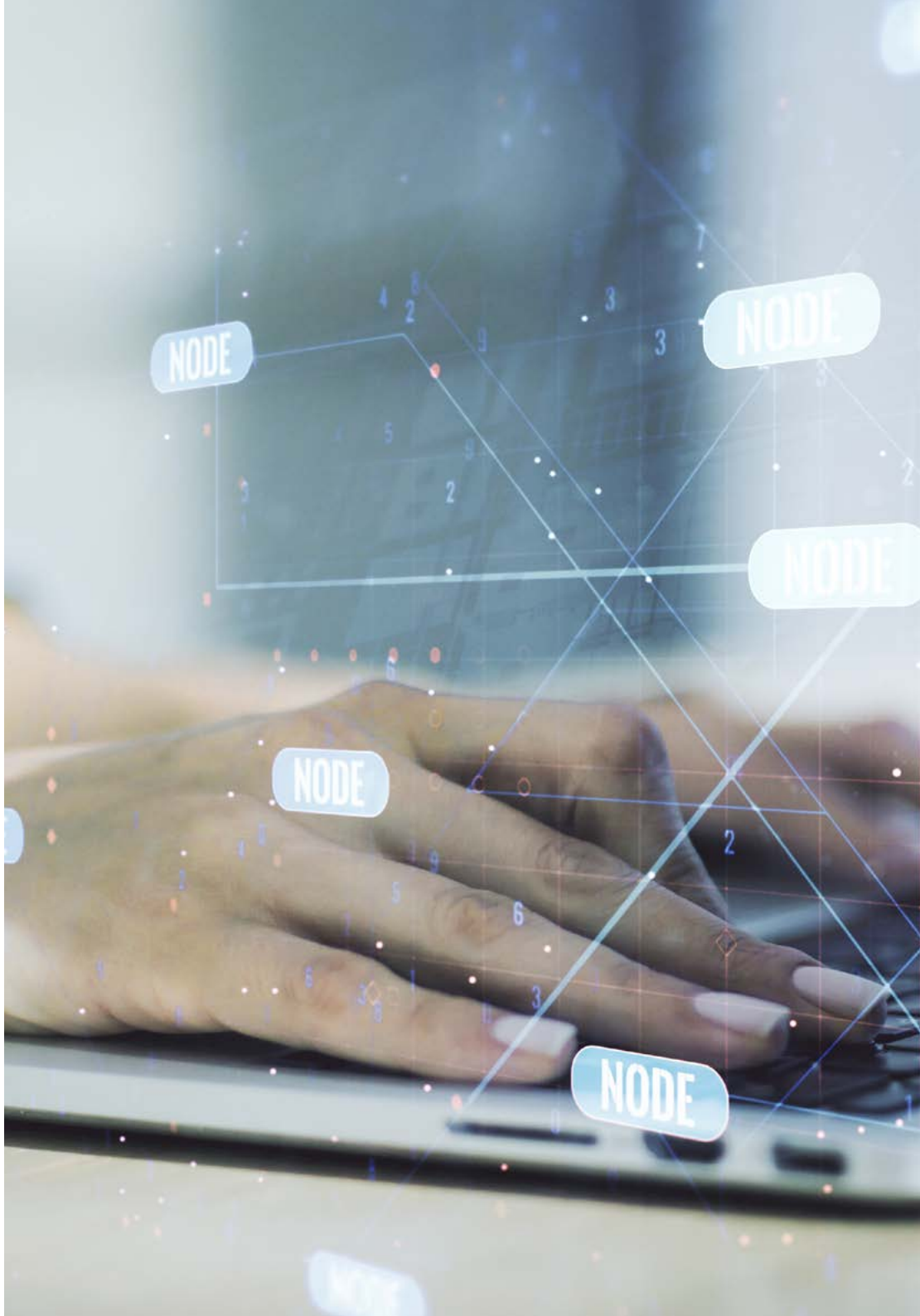
1.3. Basis of Offensive Security
- 1.3.1. Key Concepts and Terminology
- 1.3.2. Think Outside the Box
- 1.3.3. Differences between Offensive and Defensive Hacking

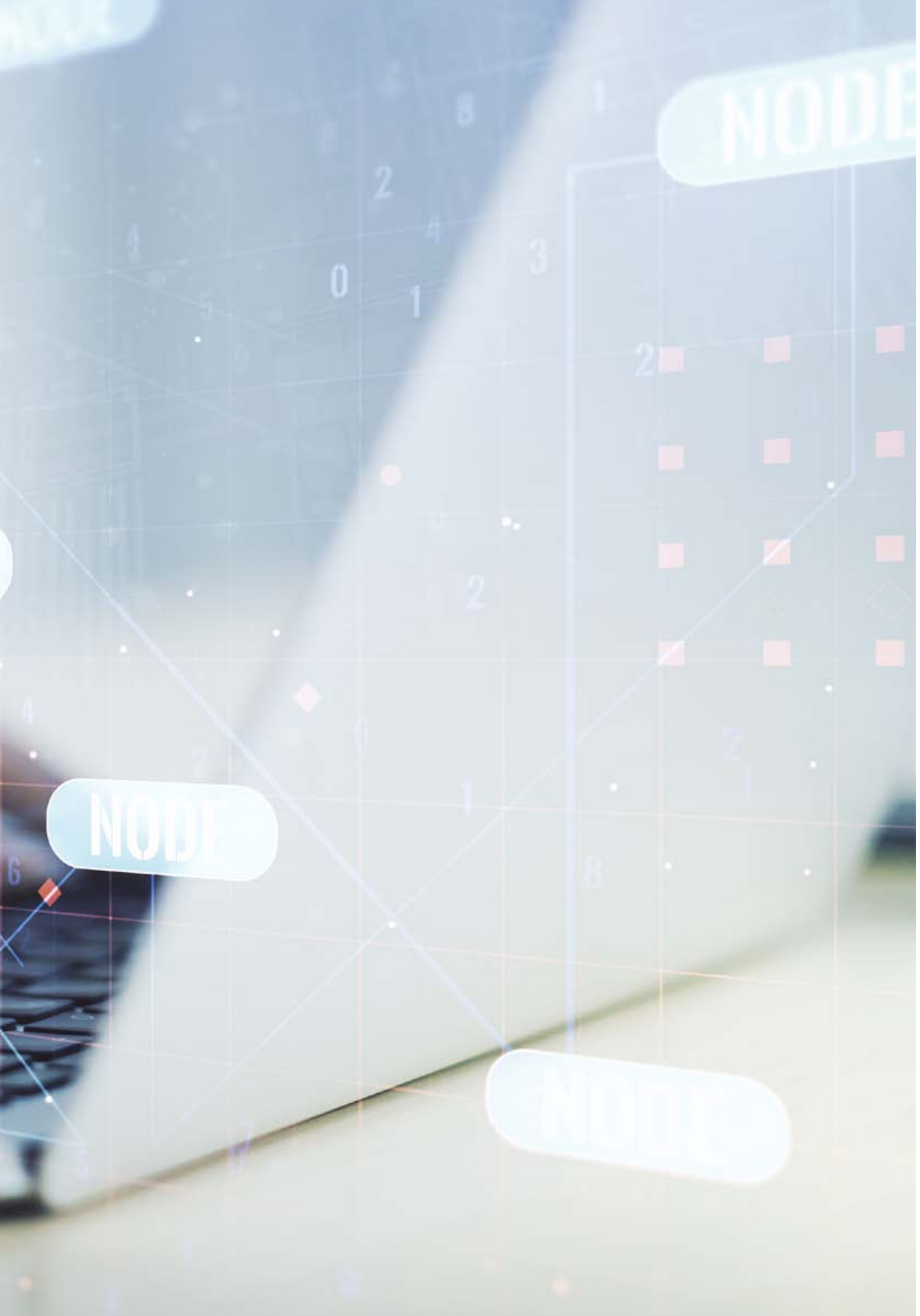
1.4. Offensive Security Methodologies
- 1.4.1. PTES (Penetration Testing Execution Standard)
- 1.4.2. OWASP (Open Web Application Security Project)
- 1.4.3. Cyber Security Kill Chain

1.5. Offensive Security Roles and Responsibilities
- 1.5.1. Main Profiles
- 1.5.2. Bug Bounty Hunters
- 1.5.3. The art of researching

1.6. Offensive Auditor's Arsenal
- 1.6.1. Operating Systems for Hacking
- 1.6.2. Introduction to C2
- 1.6.3. Metasploit: Fundamentals and Use
- 1.6.4. Useful Resources

1.7. OSINT Open Source Intelligence
- 1.7.1. OSINT Fundamentals
- 1.7.2. OSINT Tools and Techniques
- 1.7.3. OSINT Applications in Offensive Security





1.8. Scripting Introduction to Automation
- 1.8.1. Scripting Fundamentals
- 1.8.2. Scripting in Bash
- 1.8.3. Scripting in Python

1.9. Vulnerability Categorization
- 1.9.1. CVE (Common Vulnerabilities and Exposure)
- 1.9.2. CWE (Common Weakness Enumeration)
- 1.9.3. CAPEC (Common Attack Pattern Enumeration and Classification)
- 1.9.4. CVSS (Common Vulnerability Scoring System)
- 1.9.5. MITRE ATT & CK

1.10. Ethics and Hacking
- 1.10.1. Principles of Hacker Ethics
- 1.10.2. The Line between Ethical Hacking and Malicious Hacking
- 1.10.3. Legal Implications and Consequences
- 1.10.4. Case Studies: Ethical Situations in Cybersecurity

Library full of multimedia resources in different audiovisual formats"

05

Methodology

This academic program offers students a different way of learning. Our methodology uses a cyclical learning approach: **Relearning.**

This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

Discover Relearning, a system that abandons conventional linear learning, to take you through cyclical teaching systems: a way of learning that has proven to be extremely effective, especially in subjects that require memorization"

Case Study to contextualize all content

Our program offers a revolutionary approach to developing skills and knowledge. Our goal is to strengthen skills in a changing, competitive, and highly demanding environment.

At TECH, you will experience a learning methodology that is shaking the foundations of traditional universities around the world"

You will have access to a learning system based on repetition, with natural and progressive teaching throughout the entire syllabus.

The student will learn to solve complex situations in real business environments through collaborative activities and real cases.

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch, which presents the most demanding challenges and decisions in this field, both nationally and internationally. This methodology promotes personal and professional growth, representing a significant step towards success. The case method, a technique that lays the foundation for this content, ensures that the most current economic, social and professional reality is taken into account.

> *Our program prepares you to face new challenges in uncertain environments and achieve success in your career"*

The case method has been the most widely used learning system among the world's leading Information Technology schools for as long as they have existed. The case method was developed in 1912 so that law students would not only learn the law based on theoretical content. It consisted of presenting students with real-life, complex situations for them to make informed decisions and value judgments on how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue and defend their ideas and decisions.

Relearning Methodology

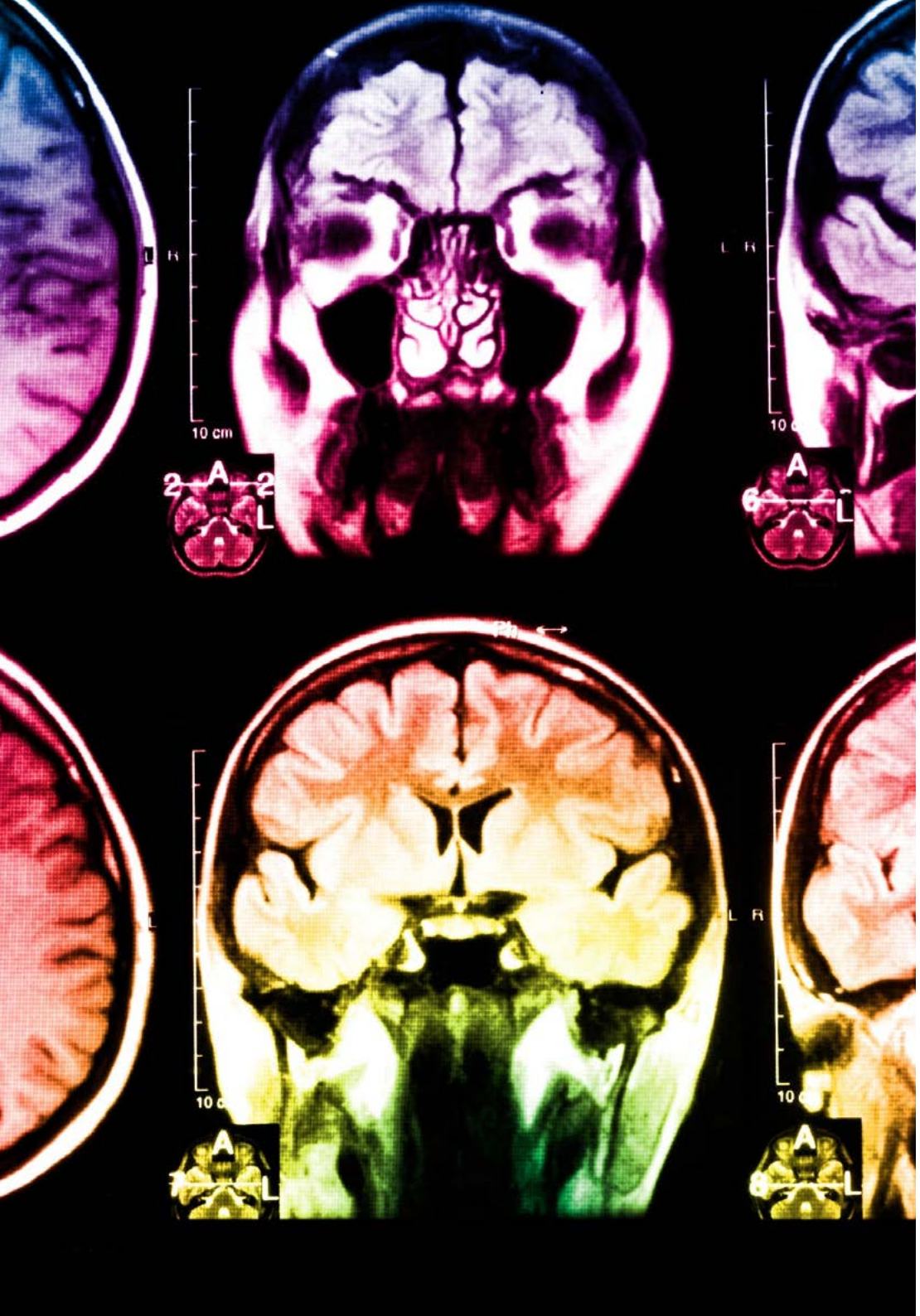
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

We enhance the Case Study with the best 100% online teaching method: Relearning.

In 2019, we obtained the best learning results of all online universities in the world.

At TECH you will learn using a cutting-edge methodology designed to train the executives of the future. This method, at the forefront of international teaching, is called Relearning.

Our university is the only one in the world authorized to employ this successful method. In 2019, we managed to improve our students' overall satisfaction levels (teaching quality, quality of materials, course structure, objectives...) based on the best online university indicators.



In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. This methodology has trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, genetics, surgery, international law, management skills, sports science, philosophy, law, engineering, journalism, history, and financial markets and instruments. All this in a highly demanding environment, where the students have a strong socio-economic profile and an average age of 43.5 years.

Relearning will allow you to learn with less effort and better performance, involving you more in your training, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation for success.

From the latest scientific evidence in the field of neuroscience, not only do we know how to organize information, ideas, images and memories, but we know that the place and context where we have learned something is fundamental for us to be able to remember it and store it in the hippocampus, to retain it in our long-term memory.

In this way, and in what is called neurocognitive context-dependent e-learning, the different elements in our program are connected to the context where the individual carries out their professional activity.

This program offers the best educational material, prepared with professionals in mind:

Study Material

All teaching material is produced by the specialists who teach the course, specifically for the course, so that the teaching content is highly specific and precise.

These contents are then applied to the audiovisual format, to create the TECH online working method. All this, with the latest techniques that offer high quality pieces in each and every one of the materials that are made available to the student.

Classes

There is scientific evidence suggesting that observing third-party experts can be useful.

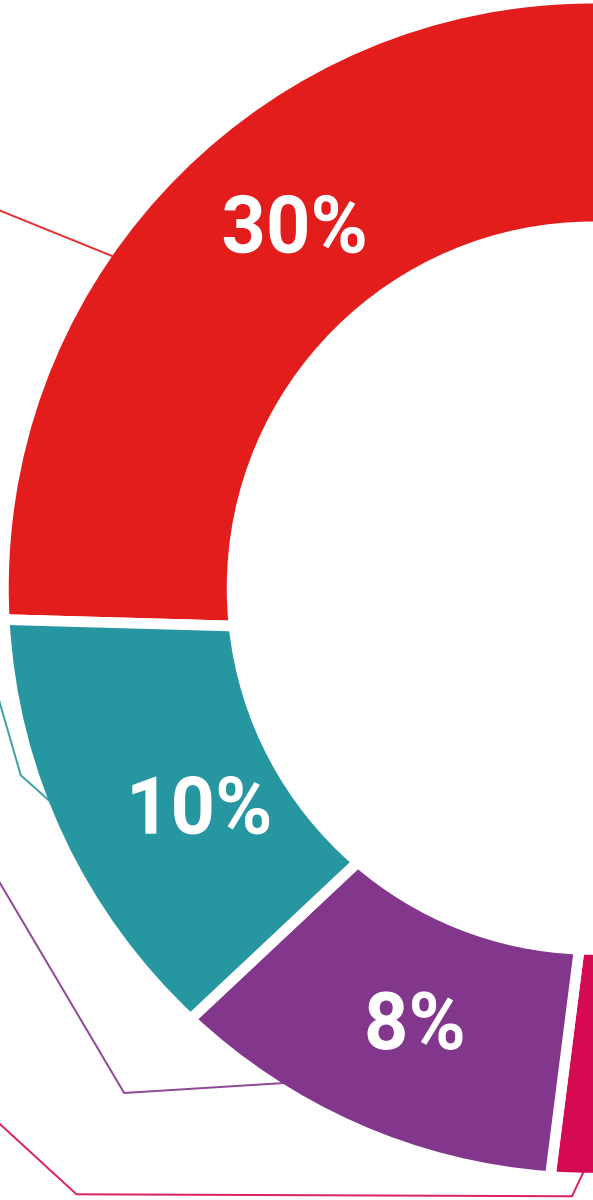
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

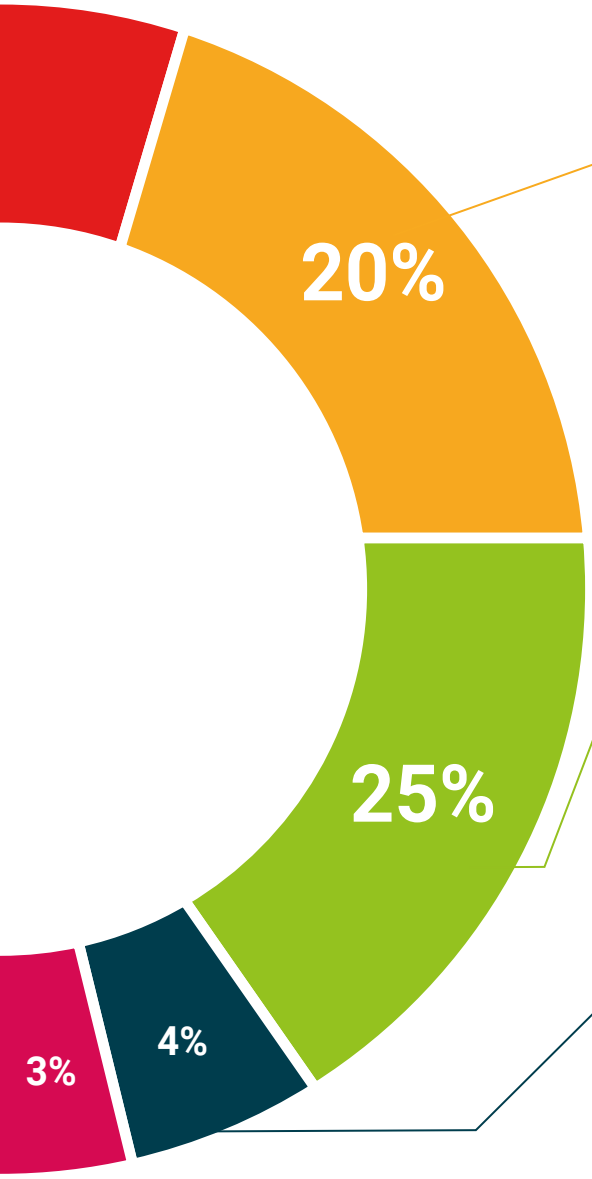
Practising Skills and Abilities

They will carry out activities to develop specific skills and abilities in each subject area. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop in the context of the globalization that we are experiencing.

Additional Reading

Recent articles, consensus documents and international guidelines, among others. In TECH's virtual library, students will have access to everything they need to complete their course.





Case Studies

Students will complete a selection of the best case studies chosen specifically for this program. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Interactive Summaries

The TECH team presents the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

Testing & Retesting

We periodically evaluate and re-evaluate students' knowledge throughout the program, through assessment and self-assessment activities and exercises, so that they can see how they are achieving their goals.

06

Certificate

The Postgraduate Certificate in Pentesting Team Management guarantees students, in addition to the most rigorous and up-to-date education, access to a Postgraduate Certificate issued by TECH Technological University.

Successfully complete this program and receive your university qualification without having to travel or fill out laborious paperwork"

This **Postgraduate Certificate in Pentesting Team Management** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Postgraduate Certificate** issued by **TECH Technological University** via tracked delivery*.

The certificate issued by **TECH Technological University** will reflect the qualification obtained in the Postgraduate Certificate, and meets the requirements commonly demanded by labor exchanges, competitive examinations and professional career evaluation committees.

Title: **Postgraduate Certificate in Pentesting Team Management**

Official Nº of Hours: **150 h.**


tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _____, with identification number _____.

For having passed and accredited the following program

POSTGRADUATE CERTIFICATE

in

Pentesting Team Management

This is a qualification awarded by this University, equivalent to 150 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates

*Apostille Convention. In the event that the student wishes to have their paper certificate issued with an apostille, TECH EDUCATION will make the necessary arrangements to obtain it, at an additional cost.

tech technological university

Postgraduate Certificate
Pentesting Team Management

- Modality: **online**
- Duration: **6 weeks**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Postgraduate Certificate

Pentesting Team Management

tech technological university