Professional Master's Degree
Pentesting and Red Team

MPRT

tech technological university

tech technological university

Professional Master's Degree

Pentesting and Red Team

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**
- Target Group: **University Graduates who have previously completed any of the degrees in the fields of Social and Legal Sciences, Administrative and Business Sciences**

Website: **www.techtitute.com/pk/school-of-business/professional-master-degree/master-pentesting-red-team**

Index

01

Welcome

Nowadays, cyber attacks have taken on considerable prominence and strength, worrying both the public and the companies themselves. As a result, companies have suffered exponentially from these threats and have had to implement maximum protection of databases and sensitive customer information. Thus, this sector is in constant search of highly qualified experts in cybersecurity, so TECH has designed this academic program, counting with technological resources and other developments around the tactics, techniques and procedures used by malicious actors. All this, through the Relearning methodology and a very complete 100% online platform, which offers flexibility and time convenience.

Professional Master's Degree in Pentesting and Network Team
TECH Technological University

Thanks to this 100% online program, you will specialize in promoting ethical and legal practices in the execution of attacks and tests on Windows systems"

02

Why Study at TECH?

TECH is the world's largest 100% online business school. It is an elite business school, with a model based on the highest academic standards. A world-class center for intensive managerial skills education.

> *TECH is a university at the forefront of technology, and puts all its resources at the student's disposal to help them achieve entrepreneurial success"*

At TECH Technological University

Innovation

The university offers an online learning model that balances the latest educational technology with the most rigorous teaching methods. A unique method with the highest international recognition that will provide students with the keys to develop in a rapidly-evolving world, where innovation must be every entrepreneur's focus.

"Microsoft Europe Success Story", for integrating the innovative, interactive multi-video system.

The Highest Standards

Admissions criteria at TECH are not economic. Students don't need to make a large investment to study at this university. However, in order to obtain a qualification from TECH, the student's intelligence and ability will be tested to their limits. The institution's academic standards are exceptionally high...

95% | **of TECH students successfully complete their studies**

Networking

Professionals from countries all over the world attend TECH, allowing students to establish a large network of contacts that may prove useful to them in the future.

+100000

executives prepared each year

+200

different nationalities

Empowerment

Students will grow hand in hand with the best companies and highly regarded and influential professionals. TECH has developed strategic partnerships and a valuable network of contacts with major economic players in 7 continents.

+500 | **collaborative agreements with leading companies**

Talent

This program is a unique initiative to allow students to showcase their talent in the business world. An opportunity that will allow them to voice their concerns and share their business vision.

After completing this program, TECH helps students show the world their talent.

Multicultural Context

While studying at TECH, students will enjoy a unique experience. Study in a multicultural context. In a program with a global vision, through which students can learn about the operating methods in different parts of the world, and gather the latest information that best adapts to their business idea.

TECH students represent more than 200 different nationalities.

Learn with the best

In the classroom, TECH's teaching staff discuss how they have achieved success in their companies, working in a real, lively, and dynamic context. Teachers who are fully committed to offering a quality specialization that will allow students to advance in their career and stand out in the business world.

Teachers representing 20 different nationalities.

> *At TECH, you will have access to the most rigorous and up-to-date case analyses in academia"*

TECH strives for excellence and, to this end, boasts a series of characteristics that make this university unique:

Analysis

TECH explores the student's critical side, their ability to question things, their problem-solving skills, as well as their interpersonal skills.

Academic Excellence

TECH offers students the best online learning methodology. The university combines the Relearning method (postgraduate learning methodology with the best international valuation) with the Case Study. Tradition and vanguard in a difficult balance, and in the context of the most demanding educational itinerary.

Economy of Scale

TECH is the world's largest online university. It currently boasts a portfolio of more than 10,000 university postgraduate programs. And in today's new economy, **volume + technology = a ground-breaking price**. This way, TECH ensures that studying is not as expensive for students as it would be at another university.

03

Why Our Program?

Studying this TECH program means increasing the chances of achieving professional success in senior business management.

It is a challenge that demands effort and dedication, but it opens the door to a promising future. Students will learn from the best teaching staff and with the most flexible and innovative educational methodology.

We have highly qualified teachers and the most complete syllabus on the market, which allows us to offer you education of the highest academic level"

This program will provide you with a multitude of professional and personal advantages, among which we highlight the following:

01

A Strong Boost to Your Career

By studying at TECH, students will be able to take control of their future and develop their full potential. By completing this program, students will acquire the skills required to make a positive change in their career in a short period of time.

70% of students achieve positive career development in less than 2 years.

02

Develop a strategic and global vision of the company

TECH offers an in-depth overview of general management to understand how each decision affects each of the company's different functional fields.

Our global vision of companies will improve your strategic vision.

03

Consolidate the student’s senior management skills

Studying at TECH means opening the doors to a wide range of professional opportunities for students to position themselves as senior executives, with a broad vision of the international environment.

You will work on more than 100 real senior management cases.

04

You will take on new responsibilities

The program will cover the latest trends, advances and strategies, so that students can carry out their professional work in a changing environment.

45% of graduates are promoted internally.

05

Access to a powerful network of contacts

TECH connects its students to maximize opportunities. Students with the same concerns and desire to grow. Therefore, partnerships, customers or suppliers can be shared.

You will find a network of contacts that will be instrumental for professional development.

06

Thoroughly develop business projects.

Students will acquire a deep strategic vision that will help them develop their own project, taking into account the different fields in companies.

20% of our students develop their own business idea.

07

Improve *soft skills* and management skills

TECH helps students apply and develop the knowledge they have acquired, while improving their interpersonal skills in order to become leaders who make a difference.

Improve your communication and leadership skills and enhance your career.

08

You will be part of an exclusive community

Students will be part of a community of elite executives, large companies, renowned institutions, and qualified teachers from the most prestigious universities in the world: the TECH Technological University community.

We give you the opportunity to study with a team of world-renowned teachers.

04

Objectives

This program will provide students with innovative updates regarding regulations and compliance in cybersecurity projects in the area of Pentesting, bringing more value to their professional career. In this sense, TECH will provide didactic resources throughout the development of the program, enhancing skills related to anomaly detection and suspicious behavior. Thus, at the end of this program, the graduate will have broadened his or her knowledge of Pentesting and Red Team. All this, over 12 months of online learning.

> *After this Professional Master's Degree program, you will be up to speed on the usefulness of Digital Forensic Investigation (DFIR) in solving cybercrimes"*

TECH makes the goals of their students their own goals too Working together to achieve them

The **Professional Master's Degree in Pentesting and Network Team** will qualify the student to:

01 Study and understand the tactics, techniques and procedures used by malicious actors, enabling the identification and simulation of threats

02 Apply theoretical knowledge in practical scenarios and simulations, facing real challenges to strengthen Pentesting skills

03 Learn how to efficiently allocate resources within a cybersecurity team, considering individual skills and maximizing productivity on projects

04 Improve communication skills specific to technical environments, facilitating understanding and coordination among team members

05 Learn project monitoring and control techniques, identifying deviations and taking corrective actions as necessary

06 Develop competencies to evaluate and improve security configurations in Windows systems, ensuring the implementation of effective measures

07 Promote ethical and legal practices in the execution of attacks and tests on Windows systems, considering the ethical principles of cybersecurity

08 Familiarize the graduate with the evaluation of security in APIs and web services, identifying possible points of vulnerability and strengthening security in programming interfaces

09 Foster effective collaboration with security teams, integrating strategies and efforts to protect network infrastructure

10 Promote ethical and legal practices in malware analysis and development, ensuring integrity and accountability in all activities

11 Apply theoretical knowledge in simulated environments, participate in hands-on exercises to understand and counter malicious attacks

12 Acquire a solid understanding of the fundamental principles of digital forensic investigation (DFIR) and their application in the resolution of cyber incidents

13 Learn to prepare detailed reports documenting findings, methodologies used and recommendations derived from advanced Red Team exercises

14 Develop skills to formulate actionable and practical recommendations aimed at mitigating vulnerabilities and improving security posture

15 Familiarize the learner with best practices for executive reporting, adapting technical information for non-technical audiences

05 Skills

This academic proposal will provide the graduate with a current vision of Pentesting. This will give you the opportunity to increase your skills, taking on management roles, facing challenging and changing situations, and even working hand in hand and effectively with other companies in the IT sector. In this way, the professional will have at his disposal multiple tools, such as infographics and videos, which will present a more practical perspective in this field of study.

Empower your skills for effective malware detection and prevention, solving the most challenging situations in the IT sector"

01

Acquire *coaching* skills for the professional development of team members, fostering growth and improvement

02

Develop skills for strategic decision making in cybersecurity situations, considering the short and long term impact on organizational security

03

Acquire skills in the identification, assessment and mitigation of risks specific to cyber security projects

04

Develop skills to implement active defense measures, strengthening the security of systems and systems-based networks

05

Learn web traffic analysis techniques to identify anomalous patterns and behaviors, facilitating the detection of possible threats

06 Acquire skills in forensic analysis applied to network environments, enabling effective identification and response to cyber incidents

07 Learn strategies for effective malware detection and prevention, including the deployment of advanced security solutions.

08 Develop skills in identifying indicators of compromise (IoC) during forensic investigation, facilitating incident detection and response

09 Acquire skills for strategic planning of Red Team exercises, considering objectives, scope, resources and realistic scenarios

10 Acquire skills in identifying and prioritizing vulnerabilities, standing out those that represent the greatest security risks

06

Structure and Content

The program in Pentesting and Red Team is a program essentially focused on the graduate acquiring competencies related to computer forensics in cybersecurity. Thus, this academic program is oriented towards a theoretical-practical structure, accompanied by the wide experience and the great background of a highly specialized team of experts.

No predefined schedules or continuous evaluations: TECH Technological University guarantees you the fastest and most flexible access to its academic content"

Syllabus

This university program consists of 1,500 hours of continuous learning through teaching of the highest standards, thanks to which the graduate will obtain the best positions in the IT and business sector. In this way, students will overcome the various obstacles imposed by the work environment. This program will facilitate multiple skills that address advanced Kerberos techniques, mitigations and protections.

On the other hand, the teaching team has developed an exclusive syllabus, which incorporates 10 modules, with the purpose of enabling the student to acquire fundamental competencies related to the evaluation of security in APIs and web services, identifying possible points of vulnerability.

The professional will also delve into actionable and practical recommendations aimed at mitigating vulnerabilities and improving the security posture. In this sense, they will become important specialists in the field of measurement methods and conflict prevention.

For this academic program, entrepreneurs will be supported by the exclusive Relearning methodology, through which they will be able to examine complex concepts and assimilate their daily application in a fluid manner. At the same time, the degree will be taught from an innovative 100% online learning platform, which is not subject to fixed schedules or continuous evaluation chronograms.

This Professional Master's Degree takes place over 12 months and is divided into 10 modules:

Module 1	Offensive Security
Module 2	Cybersecurity Team Management
Module 3	Security Project Management
Module 4	Network and Windows System Attacks
Module 5	Advanced Web Hacking
Module 6	Network Architecture and Security
Module 7	Malware Analysis and Development
Module 8	Forensic Fundamentals and DFIR
Module 9	Advanced Red Team Exercises
Module 10	Technical and Executive Report

Where, When and How is it Taught?

TECH offers the possibility of taking this Professional Master's Degree Pentesting and Red Team online Throughout the 12 months of the educational program, you will be able to access all the contents of this program at any time, allowing you to self-manage your study time.

> *A unique, key, and decisive educational experience to boost your professional development and make the definitive leap.*

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. Researching: The Art of Research

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

Module 2. Cybersecurity Team Management

2.1. Team Management

2.1.1. Who is Who
2.1.2. The Director
2.1.3. Conclusions

2.2. Roles and Responsibilities

2.2.1. Role Identification
2.2.2. Effective Delegation
2.2.3. Expectation Management

2.3. Team Training and Development

2.3.1. Stages of Team Building
2.3.2. Group Dynamics
2.3.3. Evaluation and Feedback

2.4. Talent Management

2.4.1. Talent Identification
2.4.2. Capacity Building
2.4.3. Talent Retention

2.5. Team Leadership and Motivation

2.5.1. Leadership Styles
2.5.2. Theories of Motivation
2.5.3. Recognition of Achievements

2.6. Communication and Coordination

2.6.1. Communication Tools
2.6.2. Communication Barriers
2.6.3. Coordination Strategies

2.7. Strategic Staff Professional Development Planning

2.7.1. Identification of Training Needs
2.7.2. Individual Development Plans
2.7.3. Supervision and evaluation

2.8. Conflict Resolution

2.8.1. Conflict Identification
2.8.2. Measurement Methods
2.8.3. Conflict Prevention

2.9. Quality Management and Continuous Improvement

2.9.1. Quality Principles
2.9.2. Techniques for Continuous Improvement
2.9.3. Feedback

2.10. Tools and Technologies

2.10.1. Collaboration Platforms
2.10.2. Project Management
2.10.3. Conclusions

Module 3. Security Project Management

3.1. Security Project Management

3.1.1. Definition and Purpose of Cybersecurity Project Management

3.1.2. Main Challenges

3.1.3. Considerations

3.2. Life Cycle of a Security Project

3.2.1. Initial Stages and Definition of Objectives

3.2.2. Implementation and Execution

3.2.3. Evaluation and Review

3.3. Resource Planning and Estimation

3.3.1. Basic Concepts of Economic Management

3.3.2. Determination of Human and Technical Resources

3.3.3. Budgeting and Associated Costs

3.4. Project Implementation and Control

3.4.1. Monitoring and Follow-Up

3.4.2. Adaptation and Changes in the Project

3.4.3. Mid-Term Evaluation and Reviews

3.5. Project Communication and Reporting

3.5.1. Effective Communication Strategies

3.5.2. Preparation of Reports and Presentations

3.5.3. Communication with the Customer and Management

3.6. Tools and Technologies

3.6.1. Planning and Organization Tools

3.6.2. Collaboration and Communication Tools

3.6.3. Documentation and Storage Tools

3.7. Documentation and Protocols

3.7.1. Structuring and Creation of Documentation

3.7.2. Action Protocols

3.7.3. Guidelines

3.8. Regulations and Compliance in Cybersecurity Projects

3.8.1. International Laws and Regulations

3.8.2. Compliance

3.8.3. Audits

3.9. Risk Management in Security Projects

3.9.1. Risk Identification and Analysis

3.9.2. Mitigation Strategies

3.9.3. Risk Monitoring and Review

3.10. Project Closing

3.10.1. Review and Assessment

3.10.2. Final Documentation

3.10.3. Feedback

Module 4. Network and Windows System Attacks

4.1. Windows and Active Directory

4.1.1. History and Evolution of Windows
4.1.2. Active Directory Basics
4.1.3. Active Directory Functions and Services
4.1.4. General Architecture of the Active Directory

4.2. Networking in Active Directory Environments

4.2.1. Network Protocols in Windows
4.2.2. DNS and its Operation in the Active Directory
4.2.3. Network Diagnostic Tools
4.2.4. Implementation of Networks in Active Directory

4.3. Authentication and Authorization in Active Directory

4.3.1. Authentication Process and Flow
4.3.2. Credential Types
4.3.3. Credentials Storage and Management
4.3.4. Authentication Security

4.4. Permissions and Policies in Active Directory

4.4.1. GPOs
4.4.2. Application and Management of GPOs
4.4.3. Active Directory Permissions Management
4.4.4. Vulnerabilities and Mitigations in Permits

4.5. Kerberos Basics

4.5.1. What Is Kerberos?
4.5.2. Components and Operation
4.5.3. Kerberos Tickets
4.5.4. Kerberos in the Context of Active Directory

4.6. Advanced Kerberos Techniques

4.6.1. Common Kerberos Attacks
4.6.2. Mitigations and Protections
4.6.3. Kerberos Traffic Monitoring
4.6.4. Advanced Kerberos Attacks

4.7. Active Directory Certificate Services (ADCS)

4.7.1. PKI Basics
4.7.2. ADCS Roles and Components
4.7.3. ADCS Configuration and Deployment
4.7.4. Safety at ADCS

4.8. Attacks and Defenses in Active Directory Certificate Services (ADCS)

4.8.1. Common ADCS Vulnerabilities
4.8.2. Attacks and Exploitation Techniques
4.8.3. Defenses and Mitigations
4.8.4. ADCS Monitoring and Auditing

4.9. Active Directory Audit

4.9.1. Importance of Auditing in the Active Directory
4.9.2. Audit Tools
4.9.3. Detection of Anomalies and Suspicious Behaviors
4.9.4. Incident Response and Recovery

4.10. Azure AD

4.10.1. Azure AD Basics
4.10.2. Synchronization with Local Active Directory
4.10.3. Identity Management in Azure AD
4.10.4. Integration with Applications and Services

Module 5. Advanced Web Hacking

5.1. Operation of a Website

5.1.1. The URL and Its Parts
5.1.2. HTTP Methods
5.1.3. The Headers
5.1.4. How to View Web Requests with Burp Suite

5.2. Session

5.2.1. Cookies
5.2.2. JWT Tokens
5.2.3. Session Hijacking Attacks
5.2.4. Attacks on JWT

5.3. Cross Site Scripting (XSS)

5.3.1. What is a XSS
5.3.2. Types of XSS
5.3.3. Exploiting an XSS
5.3.4. Introduction to XSLeaks

5.4. Database Injections

5.4.1. What Is a SQL Injection
5.4.2. Exfiltrating Information with SQLi
5.4.3. SQLi Blind, Time-Based and Error-Based
5.4.4. NoSQLi Injections

5.5. Path Traversal and Local File Inclusion

5.5.1. What They Are and Their Differences
5.5.2. Common Filters and How to Bypass Them
5.5.3. Log Poisoning
5.5.4. LFIs in PHP

5.6. Broken Authentication

5.6.1. User Enumeration
5.6.2. Password Bruteforce
5.6.3. 2FA Bypass
5.6.4. Cookies with Sensitive and Modifiable Information

5.7. Remote Command Execution

5.7.1. Command Injection
5.7.2. Blind Command Injection
5.7.3. Insecure Deserialization PHP
5.7.4. Insecure Deserialization Java

5.8. File Uploads

5.8.1. RCE through Webshells
5.8.2. XSS in File Uploads
5.8.3. XML External Entity (XXE) Injection
5.8.4. Path traversal in File Uploads

5.9. Broken Access Control

5.9.1. Unrestricted Access to Panels
5.9.2. Insecure Direct Object References (IDOR)
5.9.3. Filter Bypass
5.9.4. Insufficient Authorization Methods

5.10. DOM Vulnerabilities and More Advanced Attacks

5.10.1. Regex Denial of Service
5.10.2. DOM Clobbering
5.10.3. Prototype Pollution
5.10.4. HTTP Request Smuggling

Module 6. Network Architecture and Security

6.1. Computer Networks

6.1.1. Basic Concepts: LAN, WAN, CP, CC Protocols
6.1.2. OSI and TCP/IP Model
6.1.3. Switching: Basic Concepts
6.1.4. Routing: Basic Concepts

6.2. Switching

6.2.1. Introduction to VLAN' s
6.2.2. STP
6.2.3. *EtherChannel*
6.2.4. Layer 2 Attacks

6.3. VLAN´s

6.3.1. Importance of VLAN's
6.3.2. Vulnerabilities in VLAN's
6.3.3. Common Attacks on VLAN's
6.3.4. Mitigations

6.4. Routing

6.4.1. IP Addressing - IPv4 and IPv6
6.4.2. Routing: Key Concepts
6.4.3. Static Routing
6.4.4. Dynamic Routing: Introduction

6.5. IGP Protocols

6.5.1. RIP
6.5.2. OSPF
6.5.3. RIP vs OSPF
6.5.4. Topology Needs Analysis

6.6. Perimeter Protection

6.6.1. DMZs
6.6.2. Firewalls
6.6.3. Common Architectures
6.6.4. *Zero Trust Network Access*

6.7. IDS and IPS

6.7.1. Features
6.7.2. Implementation
6.7.3. SIEM and SIEM CLOUDS
6.7.4. Detection based on HoneyPots

6.8. TLS and VPN´s

6.8.1. SSL/TLS
6.8.2. TLS: Common Attacks
6.8.3. VPNs with TLS
6.8.4. VPNs with IPSEC

6.9. Security in Wireless Networks

6.9.1. Introduction to Wireless Networks
6.9.2. Protocols
6.9.3. Key Elements
6.9.4. Common Attacks

6.10. Business Networks and How to Deal with Them

6.10.1. Logical Segmentation
6.10.2. Physical Segmentation
6.10.3. Access Control
6.10.4. Other Measures to Take into Account

Module 7. Malware Analysis and Development

7.1. Malware Analysis and Development

7.1.1. History and Evolution of Malware
7.1.2. Classification and Types of Malware
7.1.3. Malware Analysis
7.1.4. Malware Development

7.2. Preparing the Environment

7.2.1. Configuration of Virtual Machines and Snapshots
7.2.2. Malware Analysis Tools
7.2.3. Malware Development Tools

7.3. Windows Basics

7.3.1. PE file format (Portable Executable)
7.3.2. Processes and Threads
7.3.3. File System and Registry
7.3.4. Windows Defender

7.4. Basic Malware Techniques

7.4.1. Shellcode Generation
7.4.2. Execution of Shellcode on Disk
7.4.3. Disk vs Memory
7.4.4. Execution of *Shellcode* in Memory

7.5. Intermediate Malware Techniques

7.5.1. Persistence in Windows
7.5.2. Home Folder
7.5.3. Registration Keys
7.5.4. Screensaver

7.6. Advanced Malware Techniques

7.6.1. Shellcode Encryption (XOR)
7.6.2. Shellcode Encryption (RSA)
7.6.3. String Obfuscation
7.6.4. Process Injection

7.7. Static Malware Analysis

7.7.1. Analyzing Packers with DIE (Detect It Easy)
7.7.2. Analyzing Sections with PE-Bear
7.7.3. Decompilation with Ghidra

7.8. Dynamic Malware Analysis

7.8.1. Observing Behavior with Process Hacker
7.8.2. Analyzing Calls with API Monitor
7.8.3. Analyzing Registry Changes with Regshot
7.8.4. Observing Network Requests with TCPView

7.9. Analysis in .NET

7.9.1. Introduction to .NET
7.9.2. Decompiling with dnSpy
7.9.3. Debugging with dnSpy

7.10. Analyzing Real Malware

7.10.1. Preparing the Environment
7.10.2. Static Malware Analysis
7.10.3. Dynamic Malware Analysis
7.10.4. YARA Rule Creation

Module 8. Forensic Fundamentals and DFIR

8.1. Digital Forensics

8.1.1. History and Evolution of Computer Forensics
8.1.2. Importance of Computer Forensics in Cybersecurity
8.1.3. History and Evolution of Computer Forensics

8.2. Fundamentals of Computer Forensics

8.2.1. Chain of Custody and Its Application
8.2.2. Types of Digital Evidence
8.2.3. Evidence Acquisition Processes

8.3. File Systems and Data Structure

8.3.1. Main File Systems
8.3.2. Data Hiding Methods
8.3.3. Analysis of File Metadata and Attributes

8.4. Operating Systems Analysis

8.4.1. Forensic Analysis of Windows Systems
8.4.2. Forensic Analysis of Linux Systems
8.4.3. Forensic Analysis of macOS Systems

8.5. Data Recovery and Disk Analysis

8.5.1. Data Recovery from Damaged Media
8.5.2. Disk Analysis Tools
8.5.3. Interpretation of File Allocation Tables

8.6. Network and Traffic Analysis

8.6.1. Network Packet Capture and Analysis
8.6.2. Firewall Log Analysis
8.6.3. Network Intrusion Detection

8.7. Malware and Malicious Code Analysis

8.7.1. Classification of Malware and Its Characteristics
8.7.2. Static and Dynamic Malware Analysis
8.7.3. Disassembly and Debugging Techniques

8.8. Log and Event Analysis

8.8.1. Types of Logs in Systems and Applications
8.8.2. Interpretation of Relevant Events
8.8.3. Log Analysis Tools

8.9. Respond to Security Incidents

8.9.1. Incident Response Process
8.9.2. Creating an Incident Response Plan
8.9.3. Coordination with Security Teams

8.10. Evidence and Legal Presentation

8.10.1. Rules of Digital Evidence in the Legal Field
8.10.2. Preparation of Forensic Reports
8.10.3. Appearance at Trial as an Expert Witness

Module 9. Advanced Red Team Exercises

9.1. Advanced Recognition Techniques

9.1.1. Advanced Subdomain Enumeration
9.1.2. Advanced Google Dorking
9.1.3. Social Networks and theHarvester

9.2. Advanced Phishing Campaigns

9.2.1. What is Reverse-Proxy Phishing?
9.2.2. 2FA Bypass with Evilginx
9.2.3. Data Exfiltration

9.3. Advanced Persistence Techniques

9.3.1. Golden Tickets
9.3.2. Silver Tickets
9.3.3. DCShadow Technique

9.4. Advanced Avoidance Techniques

9.4.1. AMSI Bypass
9.4.2. Modification of Existing Tools
9.4.3. Powershell Obfuscation

9.5. Advanced Lateral Movement Techniques

9.5.1. Pass-the-Ticket (PtT)
9.5.2. Overpass-the-Hash (Pass-the-Key)
9.5.3. NTLM Relay

9.6. Advanced Post-Exploitation Techniques

9.6.1. LSASS Dump
9.6.2. SAM Dump
9.6.3. DCSync Attack

9.7. Advanced Pivoting Techniques

9.7.1. What Is Pivoting
9.7.2. Tunneling with SSH
9.7.3. Pivoting with Chisel

9.8. Physical Intrusions

9.8.1. Surveillance and Reconnaissance
9.8.2. Tailgating and Piggybacking
9.8.3. Lock-Picking

9.9. Wi-Fi Attacks

9.9.1. WPA/WPA2 PSK Attacks
9.9.2. AP Rogue Attacks
9.9.3. Attacks on WPA2 Enterprise

9.10. RFID Attacks

9.10.1. RFID Card Reading
9.10.2. RFID Card Manipulation
9.10.3. Creation of Cloned Cards

Module 10. Technical and Executive Report

10.1. Report Process

10.1.1. Report Structure
10.1.2. Report Process
10.1.3. Key Concepts
10.1.4. Executive vs Technical

10.2. Guidelines

10.2.1. Introduction
10.2.2. Guide Types
10.2.3. National Guides
10.2.4. Case Uses

10.3. Methods

10.3.1. Assessment
10.3.2. Pentesting
10.3.3. Common Methodologies Review
10.3.4. Introduction to National Methodologies

10.4. Technical Approach to the Reporting Phase

10.4.1. Understanding the Limits of Pentester
10.4.2. Language Usage and Clues
10.4.3. Information Presentation
10.4.4. Common Errors

10.5. Executive Approach to the Reporting Phase

10.5.1. Adjusting the Report to the Context
10.5.2. Language Usage and Clues
10.5.3. Standardization
10.5.4. Common Errors

10.6. OSSTMM

10.6.1. Understanding the Methodology
10.6.2. Assessment
10.6.3. Documentation
10.6.4. Creating a Report

10.7. LINCE

10.7.1. Understanding the Methodology
10.7.2. Assessment
10.7.3. Documentation
10.7.4. Creating a Report

10.8. Reporting Vulnerabilities

10.8.1. Key Concepts
10.8.2. Scope Quantification
10.8.3. Vulnerabilities and Evidence
10.8.4. Common Errors

10.9. Focusing the Report on the Customer

10.9.1. Importance of Job Testing
10.9.2. Solutions and Mitigations
10.9.3. Sensitive and Relevant Data
10.9.4. Practical Examples and Cases

10.10. Reporting Retakes

10.10.1. Key Concepts
10.10.2. Understanding Legacy Information
10.10.3. Error Checking
10.10.4. Adding Information

07

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"*

TECH Business School uses the 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"*

This program prepares you to face business challenges in uncertain environments and achieve business success.

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

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch to present executives with challenges and business decisions at the highest level, whether at the national or international level. 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 business reality is taken into account.

> *You will learn, through collaborative activities and real cases, how to solve complex situations in real business environments"*

The case method has been the most widely used learning system among the world's leading business 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 we face in the case method, an action-oriented learning method. Throughout the program, the studies will be presented with multiple real cases. They must integrate all their knowledge, research, argue and defend their ideas and decisions.

Relearning Methodology

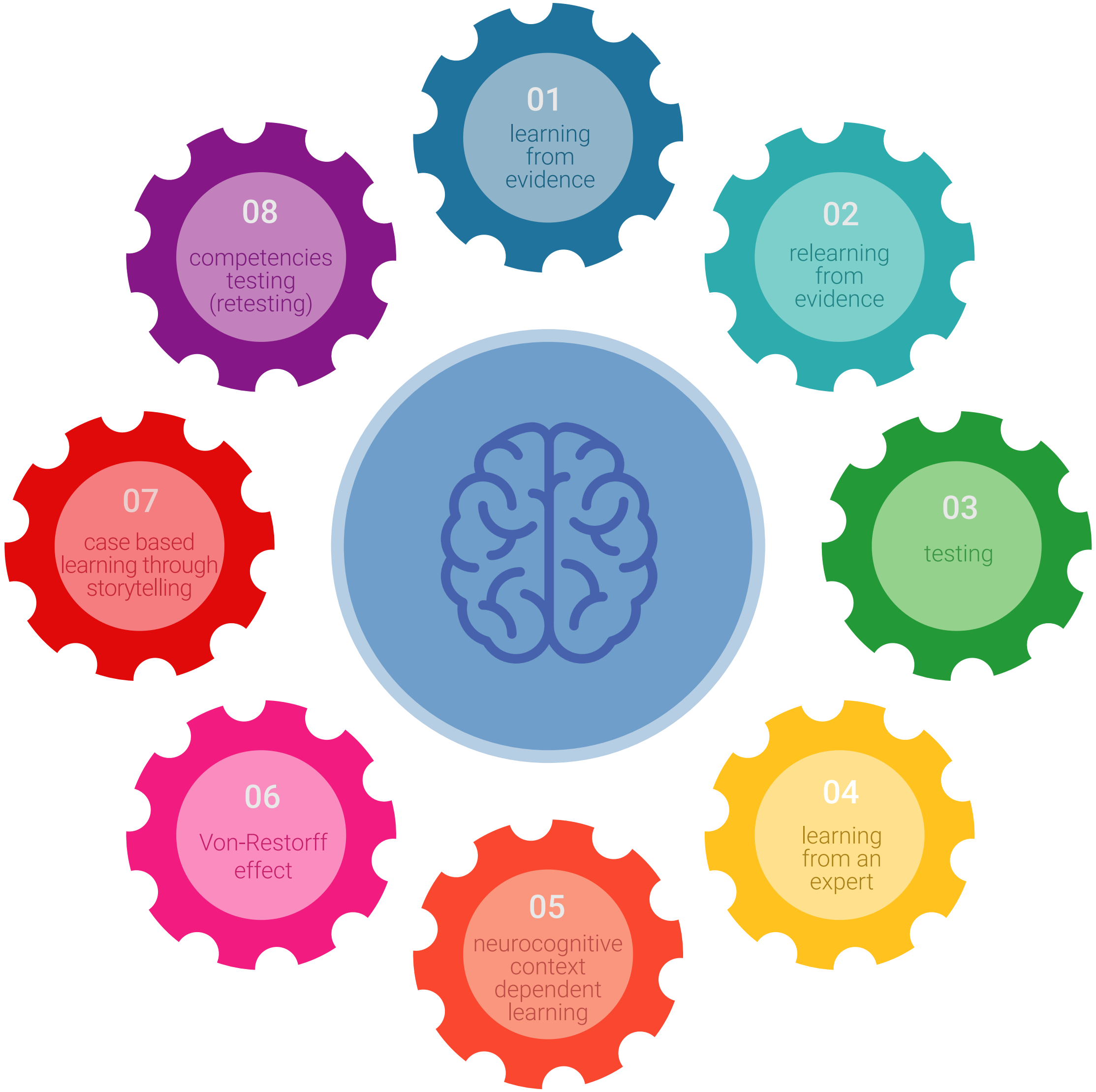
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

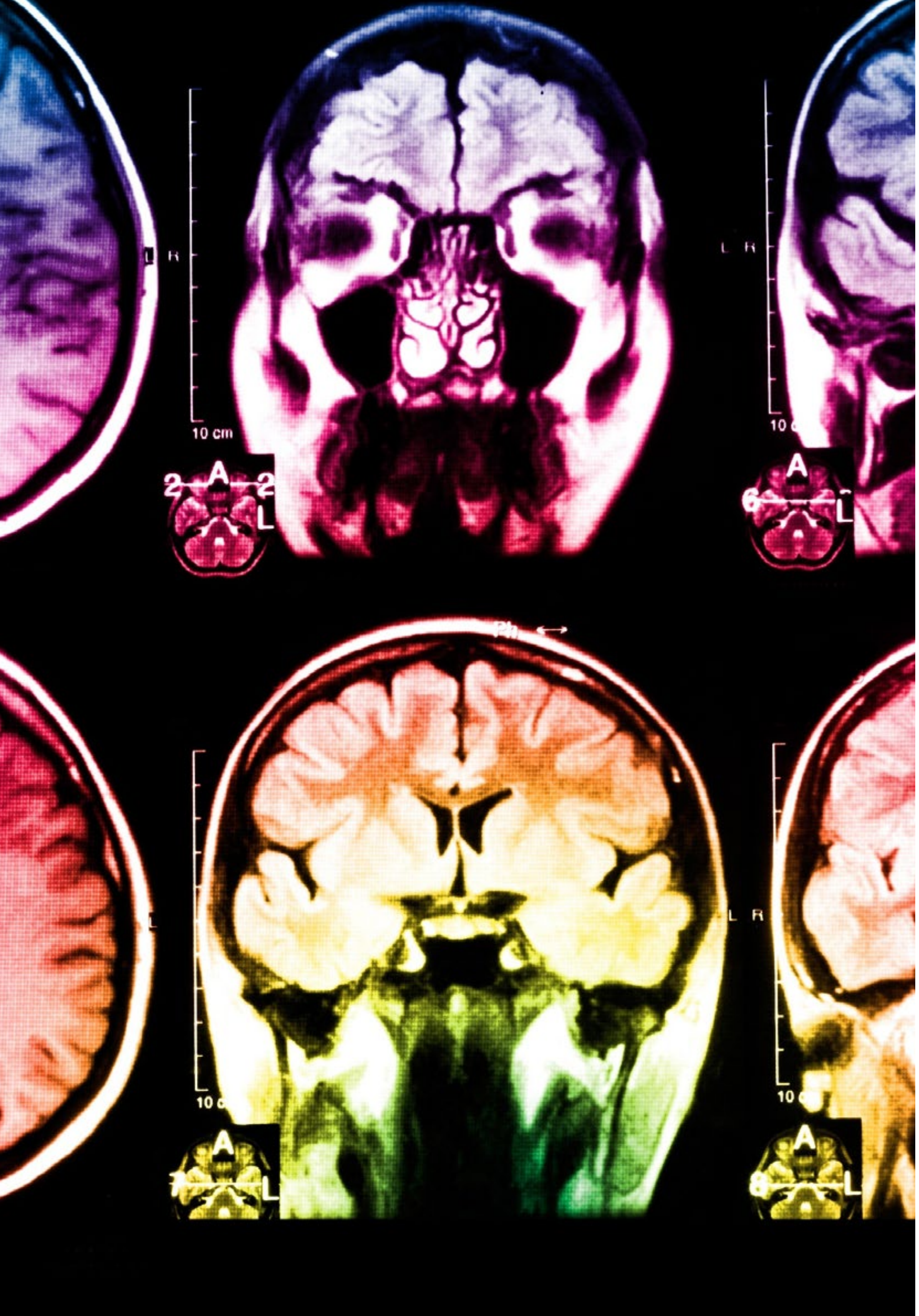
We enhance the Case Study with the best 100% online teaching method: Relearning.

> *Our online system will allow you to organize your time and learning pace, adapting it to your schedule. You will be able to access the contents from any device with an internet connection.*

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 online business school is the only one in the world licensed to incorporate 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.


01
learning from evidence
02
relearning from evidence
03
testing
04
learning from an expert
05
neurocognitive context dependent learning
06
Von-Restorff effect
07
case based learning through storytelling
08
competencies testing (retesting)



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. With this methodology we have 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, markets, and financial 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 specialization, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation to 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.

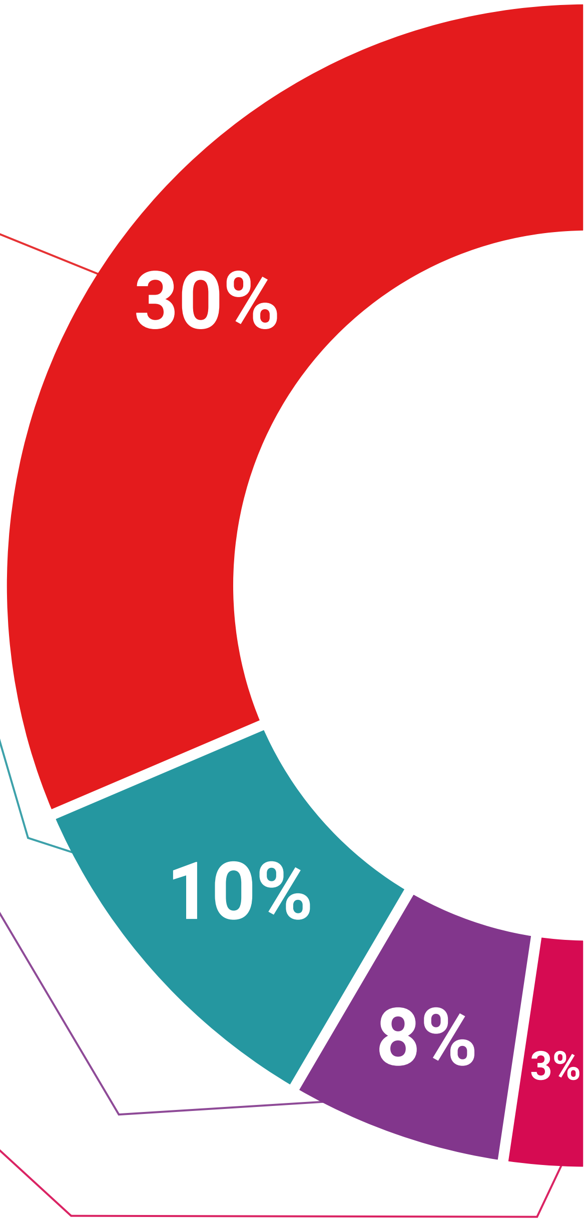
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

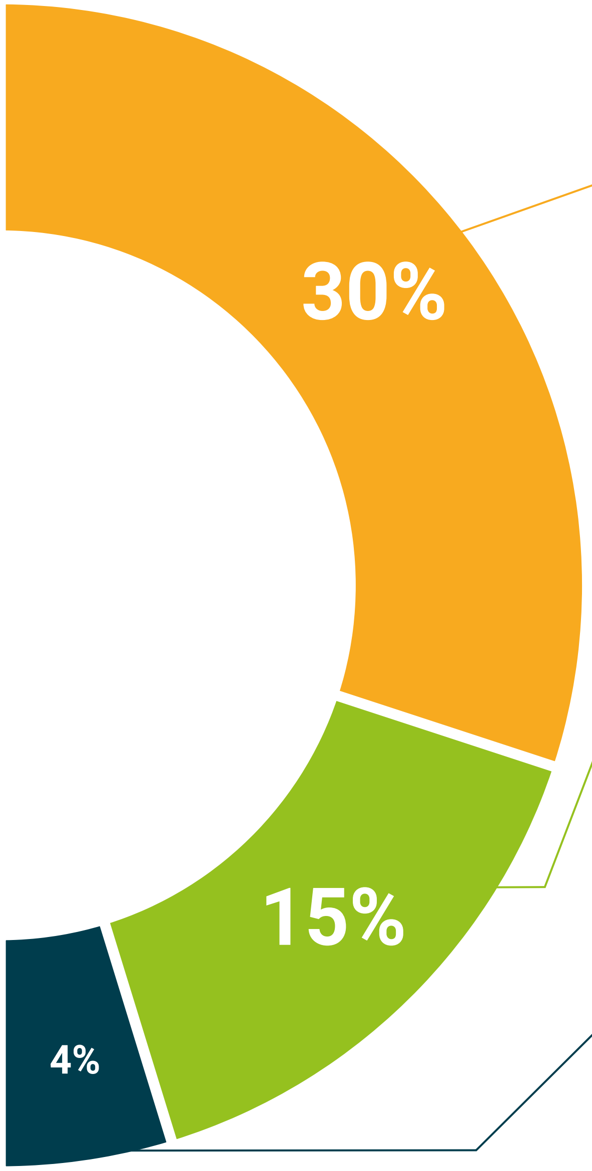
Management Skills Exercises

They will carry out activities to develop specific executive competencies in each thematic area. Practices and dynamics to acquire and develop the skills and abilities that a high-level manager needs to develop in the context of the globalization we live in.

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 senior management 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.

08

Our Students' Profiles

The program is aimed at University Graduates who have previously completed any of the following programs in the fields of Social and Legal Sciences, Administration and Economics.

This program uses a multidisciplinary approach as the students have a diverse set of academic profiles and represent multiple nationalities.

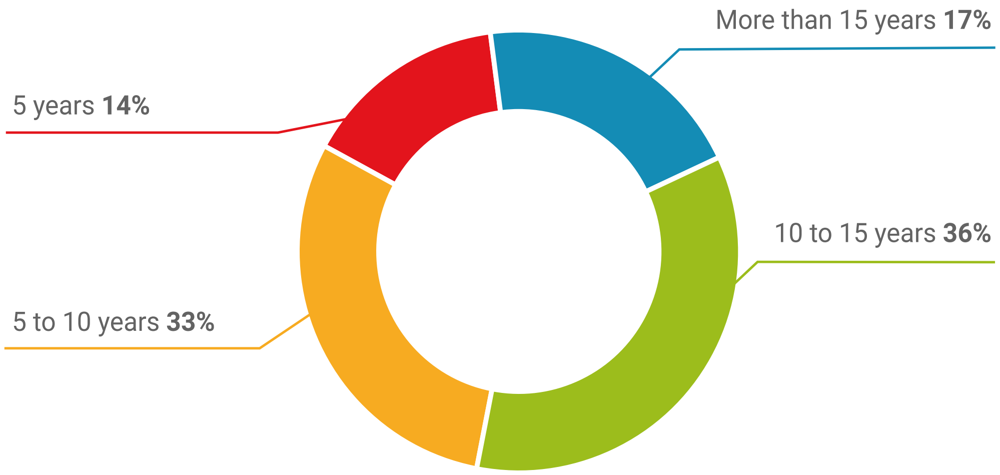
The program is also open to professionals who, being university graduates in any field, have two years of work experience in the IT field.

If you have experience in Pentesting and Red Team, and you are looking for an interesting improvement in your career while you continue working, this is the program for you"

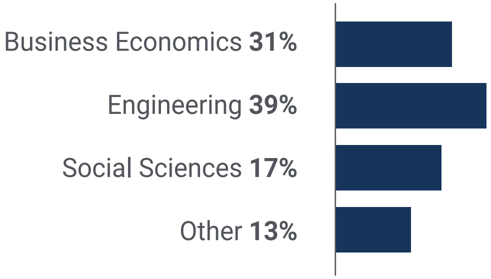
Average Age

Between **35** and **45** years old

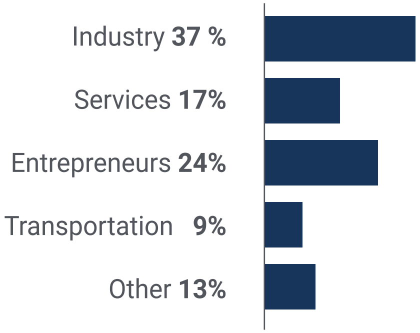
Years of Experience



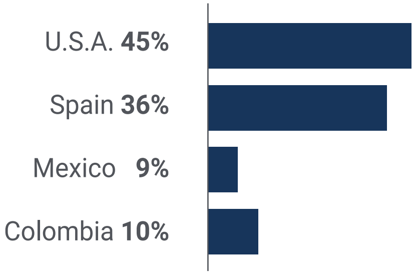
Training



Educational Profile



Geographical Distribution



Salomón Galvis

Information Security Analyst

"From this program I highlight that I managed to deepen my understanding of the importance of regular assessments and how essential it is to measure cyber security. A great investment that will be reflected in the future, thanks to the key tools that the teaching team implements in the development of the program"

09 Course Management

This Professional Master's Degree has at its disposal a teaching team of great international recognition and with significant expertise in Software and Technologies of the Information Society and Cybersecurity in Business Technology Integration. Thus, elite education is reflected in a dynamic and innovative approach to the curriculum, implementing the latest trends in cybersecurity. In this way, simulated cases and the analysis of real situations are combined so that the students obtain a first level praxis, allowing them to assume the different professional challenges in the work environment.

Leading experts in Pentesting and Network Team will teach this innovative and rigorous program"

Management

Mr. Carlos Gómez Pintado

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

Professors

Mr. Marcelino Siles Rubia

- Cibersecurity Engineer
- Cybersecurity Engineering at the Rey Juan Carlos University
- Knowledge: Competitive Programming, Web Hacking, Active Directory, and Malware Development
- AdaByron Contest Winner

Mr. Marcos González Sanz

- Cybersecurity Consultant-Network Teamer Cipherbit in Oesía Group
- Software Engineer, Polytechnic University of Madrid
- Cybersecurity Specialist Tutor and Core *Dumped*

Mr. Pablo Redondo Castro

- Pentester in Oesia Group
- Cybersecurity Engineer from Rey Juan Carlos University
- Extensive experience as a Cybersecurity Evaluator Traineer
- He has accumulated teaching experience, giving programs related to Capture The Flag tournaments

Mr. Alejandro Gallego Sánchez

- Pentester in Oesia Group
- Cybersecurity Consultant in Integrated Technology Business, S.L
- Audiovisual Technician in Audiovisual Engineering S.A
- Graduate in Cybersecurity Engineering from the Rey Juan Carlos University

Mr. Sergio Mora Navas

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

Mr. Yuba González Parrilla

- Offensive Security Line and Network Team Coordinator
- Predictive Project Management Specialist at the Project Management Institute
- SmartDefense Specialist
- Expert in Web Application Penetration Tester at eLearnSecurity
- Junior Penetration Tester in eLearnSecurity
- Graduated in Computer Engineering at the Polytechnic University of Madrid

> *"A unique, key, and decisive educational experience to boost your professional development"*

10
Impact on Your Career

This university program has been designed with the intention of orienting the graduate on the knowledge that will lead him/her to face any situation in the field of cybersecurity. In this way, TECH will specifically focus on teaching of the highest quality, seeking efficiency in each of its programs. Thus, the professional will be guaranteed a specialized learning in Pentesting and Red Team.

> *Red Team and other IT aspects of cybersecurity can be integrated into Pentesting through this intensive program”*

Are you ready to take the leap?
Excellent professional development awaits you

The Professional Master's Degree in Pentesting and Network Team of TECH is an intensive program that prepares you to face challenges and business decisions in the field of Information Technology. The main objective is to promote your personal and professional growth. Helping you achieve success.

If you want to improve yourself, make a positive change at a professional level, and network with the best, then this is the place for you.

Take advantage of this rigorous and comprehensive opportunity to expand your Pentesting skills through TECH, the best online university in the world according to Forbes.

Advanced pivoting techniques are some of the skills you will have in your hands after this comprehensive 12-month program.

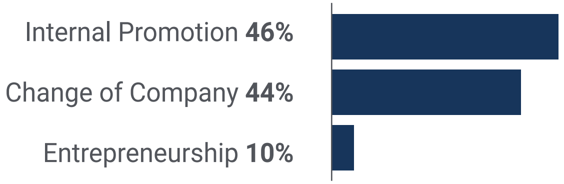
Time of Change

During the program
13%

During the first year
64%

After 2 years
23%

Type of change



Salary increase

This program represents a salary increase of more than **25.55%** for our students

Salary before

$55,465

A salary increase of

25.55%

Salary after

$74,500

11
Benefits for Your Company

This program contributes to elevating the organization's talent to its maximum potential through the instruction of high-level leaders.

In addition, participating in this university option is a unique opportunity to access a powerful network of contacts in which to find future professional partners, customers or suppliers.

In the digital era, managers must integrate new processes and strategies that bring about significant changes and organizational development. This is only possible through university training and updating"

Developing and retaining talent in companies is the best long-term investment.

01

Growth of talent and intellectual capital

The professional will introduce the company to new concepts, strategies, and perspectives that can bring about significant changes in the organization.

02

Retaining high-potential executives to avoid talent drain

This program strengthens the link between the company and the professional and opens new avenues for professional growth within the company.

03

Building agents of change

You will be able to make decisions in times of uncertainty and crisis, helping the organization overcome obstacles.

04

Increased international expansion possibilities

Thanks to this program, the company will come into contact with the main markets in the world economy.

05

Project Development

The professional can work on a real project or develop new projects in the field of R & D or business development of your company.

06

Increased competitiveness

This program will equip students with the skills to take on new challenges and drive the organization forward.

12

Certificate

The Professional Master's Degree in Pentesting and Red Team guarantees students, in addition to the most rigorous and up-to-date education, access to a Professional Master's Degree diploma issued by TECH Technological University.

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

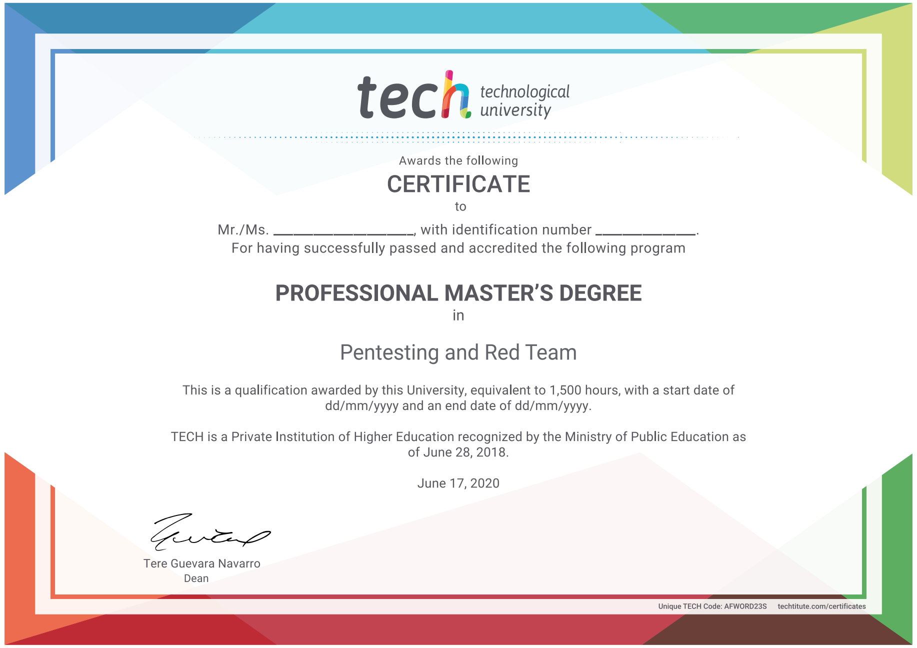
This **Professional Master's Degree in Pentesting and Red Team** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Professional Master's Degree** issued by **TECH Technological University** via tracked delivery*.

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

Title: **Professional Master's Degree in Pentesting and Red Team**

Official Nº of Hours: **1,500 h.**



tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. ________________ with identification number ____________.

For having successfully passed and accredited the following program

PROFESSIONAL MASTER'S DEGREE

in

Pentesting and Red Team

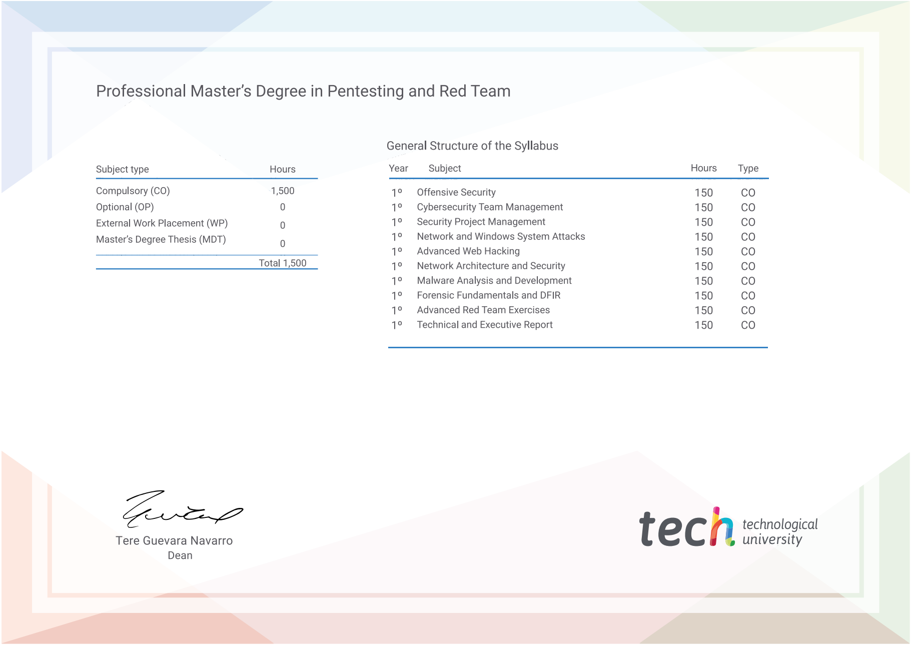
This is a qualification awarded by this University, equivalent to 1,500 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

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



Professional Master's Degree in Pentesting and Red Team

Subject type	Hours
Compulsory (CO)	1,500
Optional (OP)	0
External Work Placement (WP)	0
Master's Degree Thesis (MDT)	0
	Total 1,500

General Structure of the Syllabus

Year	Subject	Hours	Type
1º	Offensive Security	150	CO
1º	Cybersecurity Team Management	150	CO
1º	Security Project Management	150	CO
1º	Network and Windows System Attacks	150	CO
1º	Advanced Web Hacking	150	CO
1º	Network Architecture and Security	150	CO
1º	Malware Analysis and Development	150	CO
1º	Forensic Fundamentals and DFIR	150	CO
1º	Advanced Red Team Exercises	150	CO
1º	Technical and Executive Report	150	CO

Tere Guevara Navarro
Dean

tech technological university

*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

Professional Master's Degree
Pentesting and Red Team

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Professional Master's Degree

Pentesting and Red Team

tech technological university