Master's Degree
Pentesting and Red Team

tech global university

Master's Degree
Pentesting and Red Team

» Modality: **online**
» Duration: **12 months**
» Certificate: **TECH Global University**
» Accreditation: **60 ECTS**
» Schedule: **at your own pace**
» Exams: **online**

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

Index

01
Introduction to the Program

In a global context where cyber threats evolve at an accelerated pace, organizations face increasingly complex challenges to protect their digital assets. In response to this situation, Pentesting and Red Teaming emerge as essential approaches in proactive security assessment, allowing specialists to detect vulnerabilities before they can be exploited by malicious actors. Therefore, it is crucial for professionals to acquire advanced skills to handle the latest techniques for simulating attacks and strengthening the digital infrastructures of organizations. To support them in this endeavor, TECH has launched a revolutionary university program focused on implementing these offensive strategies.

With this 100% online Master's degree, you will lead offensive security strategies and strengthen digital resilience against advanced threats"

Targeted attacks, such as ransomware and zero-day vulnerability exploitation, pose critical threats to digital infrastructures across multiple sectors. Although conventional defense systems provide a first line of protection, sophisticated attackers are able to bypass these barriers. This highlights the importance of specialists staying up to date with the most innovative Pentesting and Red Team methodologies to evaluate the effectiveness of existing security systems, identify undetected weaknesses, and strengthen cybersecurity policies in institutions.

In response to this scenario, TECH has created a cutting-edge Master's Degree in Pentesting and Red Team. The academic itinerary will cover topics ranging from the fundamentals of offensive security and optimal management of cybersecurity teams to advanced attack simulation techniques and evaluation of digital infrastructure resilience. Additionally, strategies for evading defenses and the use of advanced software to detect vulnerabilities will be explored. As a result, students will develop technical skills to anticipate threats, mitigate risks, and reinforce the digital defenses of organizations.

Furthermore, this degree not only offers deep technical learning but also a strategic outlook. Its 100% online methodology, based on the Relearning method, allows for flexible and autonomous learning, with no fixed schedules or commutes, facilitating the balancing of work and personal responsibilities. Additionally, it boasts a faculty of experts in the field, ensuring that theory is combined with real-world cases for more effective preparation. In this way, graduates will only need a device with internet access to immerse themselves in the Virtual Campus.

This **Master's Degree in Pentesting and Red Team** contains the most complete and up-to-date program on the market. The most important features include:

- The development of practical cases presented by Pentesting and Red Team experts
- The graphic, schematic, and practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional practice
- Practical exercises where self-assessment can be used to improve learning
- Special emphasis on innovative methodologies in Pentesting and Red Team
- 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

"You will use advanced security analysis and evaluation tools to identify vulnerabilities in various digital environments"

You will manage the most sophisticated strategies to assess and improve the response capabilities of digital architectures against threats"

The program includes faculty members from the Pentesting and Red Team field, who bring their real-world experience to this program, along with recognized 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 an immersive learning experience designed to prepare for real-life situations.

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

You will dive deeper into conducting realistic cyberattack simulations using Red Teaming techniques.

You will have access to a library of specialized resources available 24/7, with high-level technical materials and real-world applicability.

02
Why Study at TECH?

TECH is the world's largest online university. With an impressive catalog of more than 14,000 university programs, available in 11 languages, it is positioned as a leader in employability, with a 99% job placement rate. In addition, it has a huge faculty of more than 6,000 professors of the highest international prestige.

Study at the largest online university in the world and ensure your professional success. The future begins at TECH"

The world's best online university, according to FORBES

The prestigious Forbes magazine, specialized in business and finance, has highlighted TECH as "the best online university in the world" This is what they have recently stated in an article in their digital edition in which they echo the success story of this institution, "thanks to the academic offer it provides, the selection of its teaching staff, and an innovative learning method oriented to form the professionals of the future".

The best top international faculty

TECH's faculty is made up of more than 6,000 professors of the highest international prestige. Professors, researchers and top executives of multinational companies, including Isaiah Covington, performance coach of the Boston Celtics; Magda Romanska, principal investigator at Harvard MetaLAB; Ignacio Wistumba, chairman of the department of translational molecular pathology at MD Anderson Cancer Center; and D.W. Pine, creative director of TIME magazine, among others.

The world's largest online university

TECH is the world's largest online university. We are the largest educational institution, with the best and widest digital educational catalog, one hundred percent online and covering most areas of knowledge. We offer the largest selection of our own degrees and accredited online undergraduate and postgraduate degrees. In total, more than 14,000 university programs, in ten different languages, making us the largest educational institution in the world.

The most complete syllabuses on the university scene

TECH offers the most complete syllabuses on the university scene, with programs that cover fundamental concepts and, at the same time, the main scientific advances in their specific scientific areas. In addition, these programs are continuously updated to guarantee students the academic vanguard and the most demanded professional skills. and the most in-demand professional competencies. In this way, the university's qualifications provide its graduates with a significant advantage to propel their careers to success.

A unique learning method

TECH is the first university to use Relearning in all its programs. This is the best online learning methodology, accredited with international teaching quality certifications, provided by prestigious educational agencies. In addition, this innovative academic model is complemented by the "Case Method", thereby configuring a unique online teaching strategy. Innovative teaching resources are also implemented, including detailed videos, infographics and interactive summaries.

The official online university of the NBA

TECH is the official online university of the NBA. Thanks to our agreement with the biggest league in basketball, we offer our students exclusive university programs, as well as a wide variety of educational resources focused on the business of the league and other areas of the sports industry. Each program is made up of a uniquely designed syllabus and features exceptional guest hosts: professionals with a distinguished sports background who will offer their expertise on the most relevant topics.

Leaders in employability

TECH has become the leading university in employability. Ninety-nine percent of its students obtain jobs in the academic field they have studied within one year of completing any of the university's programs. A similar number achieve immediate career enhancement. All this thanks to a study methodology that bases its effectiveness on the acquisition of practical skills, which are absolutely necessary for professional development.

Google Premier Partner

The American technology giant has awarded TECH the Google Premier Partner badge. This award, which is only available to 3% of the world's companies, highlights the efficient, flexible and tailored experience that this university provides to students. The recognition not only accredits the maximum rigor, performance and investment in TECH's digital infrastructures, but also places this university as one of the world's leading technology companies.

The top-rated university by its students

Students have positioned TECH as the world's top-rated university on the main review websites, with a highest rating of 4.9 out of 5, obtained from more than 1,000 reviews. These results consolidate TECH as the benchmark university institution at an international level, reflecting the excellence and positive impact of its educational model.

03

Syllabus

The educational materials that make up this university degree have been developed by renowned experts in the application of cutting-edge Pentesting and Red Team techniques. In this way, the syllabus will cover topics ranging from the specific functioning of cybersecurity teams or the implementation of innovative security protocols to the use of state-of-the-art software to carry out attack simulations such as malware. In this way, students will develop advanced skills to identify critical vulnerabilities, design personalized offensive strategies, and perform comprehensive protection assessments.

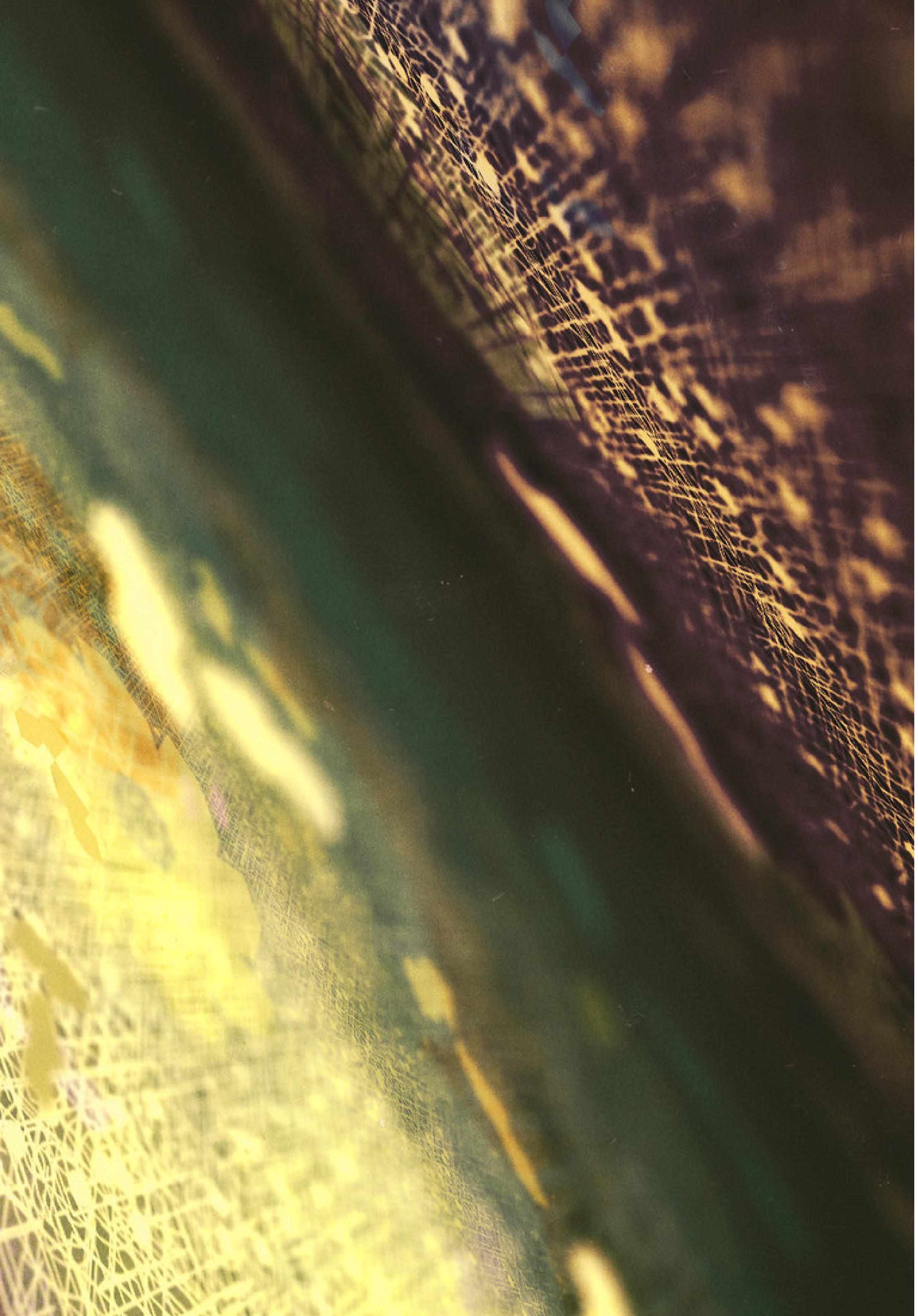
You will design methods to simulate complex attacks and measure the effectiveness of organizational defense systems"

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 Market 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. Characteristics
- 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 The Harvester
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 TheTicket (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. Use Cases

10.3. Methods
- 10.3.1. Evaluation
- 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 Mistakes

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 Mistakes

10.6. OSSTMM
- 10.6.1. Understanding the Methodology
- 10.6.2. Detection
- 10.6.3. Documentation
- 10.6.4. Creating a Report

10.7. LINCE
- 10.7.1. Understanding the Methodology
- 10.7.2. Detection
- 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 Mistakes

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

04

Teaching Objectives

The Master's Degree in Pentesting and Red Team aims to prepare experts in offensive cybersecurity capable of identifying, analyzing, and exploiting vulnerabilities in complex environments. Graduates will be able to lead security teams, manage projects, and execute advanced penetration tests on networks, systems, and web applications. They will learn to design effective defense strategies and respond to incidents using cutting-edge forensic techniques.

You will develop the ability to lead specialized teams, manage security projects, and coordinate cybersecurity defense strategies.

General Objectives

- Apply theoretical knowledge in practical scenarios and simulations, facing real challenges to strengthen Pentesting skills
- Learn how to efficiently allocate resources within a cybersecurity team, considering individual skills and maximizing productivity on projects
- Improve communication skills specific to technical environments, facilitating understanding and coordination among team members
- Learn project monitoring and control techniques, identifying deviations and taking corrective actions as necessary
- Develop competencies to evaluate and improve security configurations in Windows systems, ensuring the implementation of effective measures
- Promote ethical and legal practices in the execution of attacks and tests on Windows systems, considering the ethical principles of cybersecurity
- Familiarize the graduate with the evaluation of security in APIs and web services, identifying possible points of vulnerability and strengthening security in programming interfaces
- Foster effective collaboration with security teams, integrating strategies and efforts to protect network infrastructure

Specific Objectives

Module 1. Offensive Security
- Identify and apply offensive security methodologies used in penetration tests and system audits
- Understand the legal and ethical framework within which offensive cybersecurity operates

Module 2. Cybersecurity Team Management
- Develop leadership and coordination strategies in offensive and defensive security teams
- Implement agile and management methodologies for optimizing cybersecurity processes

Module 3. Security Project Management
- Plan and execute cybersecurity projects aligned with the strategic objectives of organizations
- Evaluate risks and define effective mitigation plans to improve enterprise security

Module 4. Network and Windows System Attacks
- Analyze and exploit vulnerabilities in networks and Windows environments using specialized tools
- Apply evasion and persistence techniques to assess the effectiveness of implemented security measures

Module 5. Advanced Web Hacking
- Identify and exploit vulnerabilities in web applications through specialized penetration tests
- Apply advanced techniques like SQL Injection, Cross-Site Scripting, and Server-Side Request Forgery

Module 6. Network Architecture and Security
- Design secure infrastructures by applying segmentation principles and traffic control
- Analyze attacks on corporate networks and propose effective mitigation solutions

Module 7. Malware Analysis and Development
- Design and analyze malicious code to understand its operation and attack mechanisms
- Implement reverse engineering techniques to detect and neutralize advanced threats

Module 8. Forensic Fundamentals and DFIR
- Apply forensic analysis techniques for the collection and preservation of digital evidence
- Implement incident response strategies to contain and mitigate cyberattacks in real-time

Module 9. Advanced Red Team Exercises
- Develop simulated attack campaigns to assess the resilience of critical infrastructures
- Apply advanced Red Teaming methodologies to replicate realistic attack scenarios

Module 10. Technical and Executive Report
- Prepare detailed technical reports with findings, analysis, and security recommendations
- Write executive reports for senior management with strategies for risk management and mitigation

05

Career Opportunities

With this comprehensive Master's Degree in Pentesting and Red Team, professionals will master the most advanced techniques for detecting vulnerabilities, running attack simulations, and strengthening digital infrastructures. Thanks to this approach, they will be highly prepared to access strategic roles of great importance in companies, such as cybersecurity analysts or consultants in offensive security. This will provide them with advanced competencies in threat detection and proactive defense.

You will work as a Red Teaming Specialist, creating exhaustive simulations to assess the resilience of digital infrastructures and the response capacity of teams"

Graduate Profile

Graduates of this university program will be highly trained experts capable of identifying vulnerabilities, executing cyberattack simulations, and strengthening digital infrastructures. They will also be prepared to lead offensive security operations, manage incidents, and develop proactive defense strategies, ensuring the protection of systems against advanced threats. In addition, they will be able to advise organizations on implementing cybersecurity policies, comply with international regulations, and coordinate multidisciplinary teams to address complex challenges in digital environments.

You will design proactive security strategies, enabling companies to respond effectively to a variety of incidents.

- **Malware Analysis and Reverse Engineering:** Competency in creating, detecting, and dismantling malicious software to understand its mechanisms and develop effective countermeasures.
- **Red Teaming and Attack Simulation:** Ability to conduct advanced Red Team exercises, replicating real-world threats to evaluate the resilience of critical infrastructures.
- **Incident Response and Forensic Analysis:** Ability to identify, contain, and mitigate security incidents using advanced forensic techniques
- **Network Design and Security:** Knowledge in implementing secure infrastructures by applying principles of segmentation, traffic control, and mitigating attacks on corporate networks

After completing the Master's Degree, you will be able to use your knowledge and skills in the following positions:

1. **Pentesting and Offensive Security Specialist:** Responsible for conducting penetration tests on digital infrastructures, identifying and exploiting vulnerabilities to strengthen corporate security.
2. **Red Team Leader and Attack Simulation:** Responsible for designing and executing advanced Red Teaming exercises, replicating realistic attack scenarios to assess the resilience of systems.
3. **Cybersecurity Manager in Companies and Government Organizations:** Overseeing offensive and defensive security strategies, ensuring compliance with regulations and mitigating digital risks.
4. **Malware Analyst and Reverse Engineering:** Specialist in studying, developing, and dismantling malicious software, applying reverse engineering techniques to detect and neutralize threats.
5. **Web Security Consultant and Vulnerability Assessment:** Advising companies on identifying and mitigating risks in web applications using advanced ethical hacking methodologies.
6. **Incident Response and Digital Forensics Director:** Responsible for coordinating the detection, analysis, and mitigation of cyberattacks.
7. **Network and Security Architect:** In charge of designing and maintaining secure infrastructures, implementing protective measures to prevent attacks on corporate networks.
8. **Information Security Project Manager:** Leading the planning and execution of cybersecurity strategies, ensuring alignment with business objectives and international regulations.
9. **Cyber Threat Intelligence Specialist:** Analyzing trends and techniques used by malicious actors, providing key insights for anticipating and mitigating attacks.
10. **Offensive Cybersecurity Instructor and Trainer:** Responsible for training security teams, imparting advanced knowledge in Pentesting, Red Teaming, and incident management.

You will manage actions to contain, analyze, and reduce the impact of cyberattacks, ensuring the protection of sensitive information"

06 Study Methodology

TECH is the world's first university to combine the **case study** methodology with **Relearning**, a 100% online learning system based on guided repetition.

This disruptive pedagogical strategy has been conceived to offer professionals the opportunity to update their knowledge and develop their skills in an intensive and rigorous way. A learning model that places students at the center of the educational process giving them the leading role, adapting to their needs and leaving aside more conventional methodologies.

“TECH will prepare you to face new challenges in uncertain environments and achieve success in your career”

The student: the priority of all TECH programs

In TECH's study methodology, the student is the main protagonist.
The teaching tools of each program have been selected taking into account the demands of time, availability and academic rigor that, today, not only students demand but also the most competitive positions in the market.

With TECH's asynchronous educational model, it is students who choose the time they dedicate to study, how they decide to establish their routines, and all this from the comfort of the electronic device of their choice. The student will not have to participate in live classes, which in many cases they will not be able to attend. The learning activities will be done when it is convenient for them. They can always decide when and from where they want to study.

At TECH you will NOT have live classes (which you might not be able to attend)"

The most comprehensive study plans at the international level

TECH is distinguished by offering the most complete academic itineraries on the university scene. This comprehensiveness is achieved through the creation of syllabi that not only cover the essential knowledge, but also the most recent innovations in each area.

By being constantly up to date, these programs allow students to keep up with market changes and acquire the skills most valued by employers. In this way, those who complete their studies at TECH receive a comprehensive education that provides them with a notable competitive advantage to further their careers.

And what's more, they will be able to do so from any device, pc, tablet or smartphone.

TECH's model is asynchronous, so it allows you to study with your pc, tablet or your smartphone wherever you want, whenever you want and for as long as you want"

Case Studies and Case Method

The case method has been the learning system most used by the world's best business schools. Developed in 1912 so that law students would not only learn the law based on theoretical content, its function was also to present them with real complex situations. In this way, they could make informed decisions and value judgments about how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

With this teaching model, it is students themselves who build their professional competence through strategies such as Learning by Doing or Design Thinking, used by other renowned institutions such as Yale or Stanford.

This action-oriented method will be applied throughout the entire academic itinerary that the student undertakes with TECH. Students will be confronted with multiple real-life situations and will have to integrate knowledge, research, discuss and defend their ideas and decisions. All this with the premise of answering the question of how they would act when facing specific events of complexity in their daily work.

Relearning Methodology

At TECH, case studies are enhanced with the best 100% online teaching method: Relearning.

This method breaks with traditional teaching techniques to put the student at the center of the equation, providing the best content in different formats. In this way, it manages to review and reiterate the key concepts of each subject and learn to apply them in a real context.

In the same line, and according to multiple scientific researches, reiteration is the best way to learn. For this reason, TECH offers between 8 and 16 repetitions of each key concept within the same lesson, presented in a different way, with the objective of ensuring that the knowledge is completely consolidated during the study process.

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.

A 100% online Virtual Campus with the best teaching resources

In order to apply its methodology effectively, TECH focuses on providing graduates with teaching materials in different formats: texts, interactive videos, illustrations and knowledge maps, among others. All of them are designed by qualified teachers who focus their work on combining real cases with the resolution of complex situations through simulation, the study of contexts applied to each professional career and learning based on repetition, through audios, presentations, animations, images, etc.

The latest scientific evidence in the field of Neuroscience points to the importance of taking into account the place and context where the content is accessed before starting a new learning process. Being able to adjust these variables in a personalized way helps people to remember and store knowledge in the hippocampus to retain it in the long term. This is a model called Neurocognitive context-dependent e-learning that is consciously applied in this university qualification.

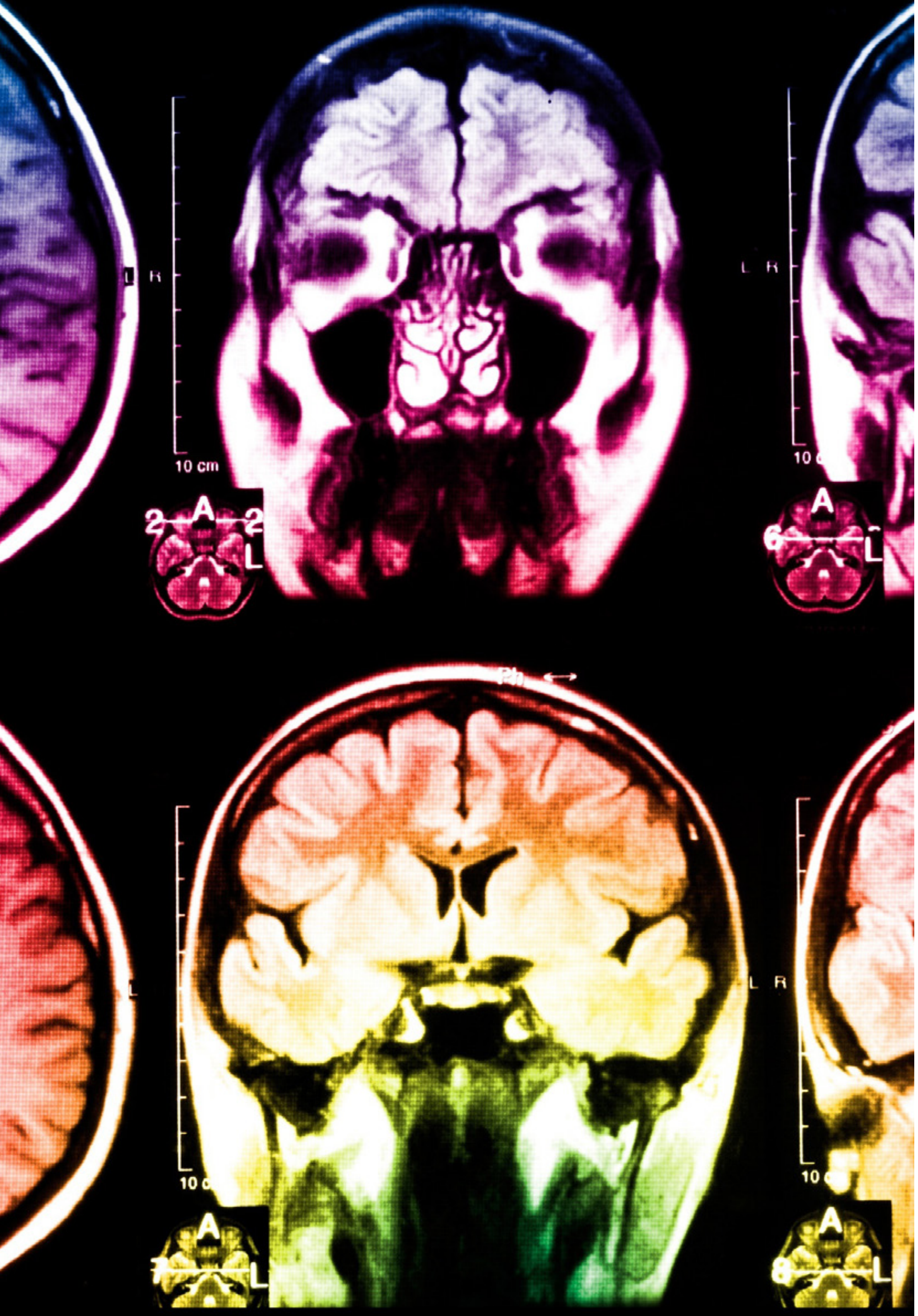
In order to facilitate tutor-student contact as much as possible, you will have a wide range of communication possibilities, both in real time and delayed (internal messaging, telephone answering service, email contact with the technical secretary, chat and videoconferences).

Likewise, this very complete Virtual Campus will allow TECH students to organize their study schedules according to their personal availability or work obligations. In this way, they will have global control of the academic content and teaching tools, based on their fast-paced professional update.

The online study mode of this program will allow you to organize your time and learning pace, adapting it to your schedule"

The effectiveness of the method is justified by four fundamental achievements:

1. Students who follow this method not only achieve the assimilation of concepts, but also a development of their mental capacity, through exercises that assess real situations and the application of knowledge.
2. Learning is solidly translated into practical skills that allow the student to better integrate into the real world.
3. Ideas and concepts are understood more efficiently, given that the example situations are based on real-life.
4. Students like to feel that the effort they put into their studies is worthwhile. This then translates into a greater interest in learning and more time dedicated to working on the course.



The university methodology top-rated by its students

The results of this innovative teaching model can be seen in the overall satisfaction levels of TECH graduates.

The students' assessment of the teaching quality, the quality of the materials, the structure of the program and its objectives is excellent. Not surprisingly, the institution became the top-rated university by its students according to the global score index, obtaining a 4.9 out of 5.

Access the study contents from any device with an Internet connection (computer, tablet, smartphone) thanks to the fact that TECH is at the forefront of technology and teaching.

You will be able to learn with the advantages that come with having access to simulated learning environments and the learning by observation approach, that is, Learning from an expert.

As such, the best educational materials, thoroughly prepared, will be available in this program:

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.

This content is then adapted in an audiovisual format that will create our way of working online, with the latest techniques that allow us to offer you high quality in all of the material that we provide you with.

Practicing Skills and Abilities

You will carry out activities to develop specific competencies and skills in each thematic field. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop within the framework of the globalization we live in.

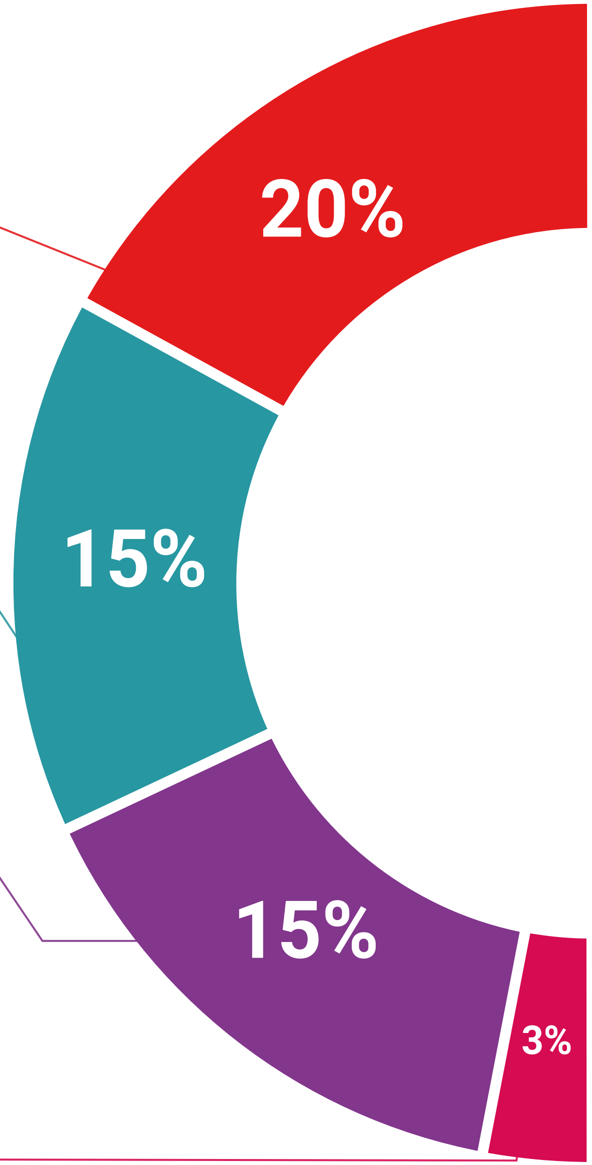
Interactive Summaries

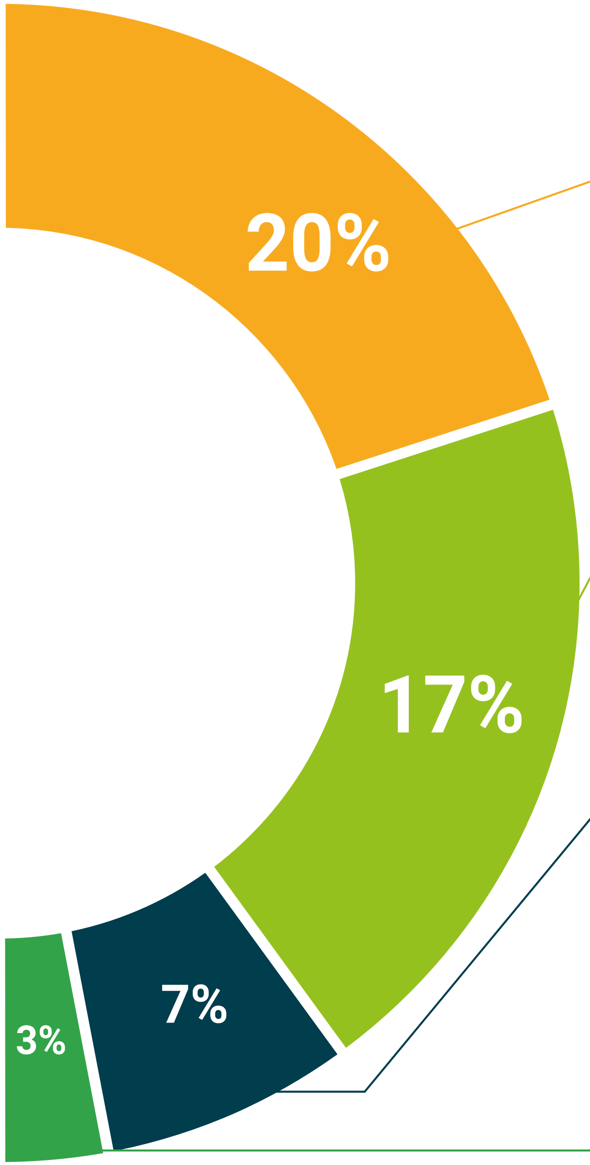
We present the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

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

Additional Reading

Recent articles, consensus documents, international guides... In our virtual library you will have access to everything you need to complete your education.





Case Studies

Students will complete a selection of the best case studies in the field. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Testing & Retesting

We periodically assess and re-assess your knowledge throughout the program. We do this on 3 of the 4 levels of Miller's Pyramid.

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 for future difficult decisions.

Quick Action Guides

TECH offers the most relevant contents of the course in the form of worksheets or quick action guides. A synthetic, practical and effective way to help students progress in their learning.

07

Teaching Staff

This university program boasts a prestigious international faculty, composed of experts in Pentesting and Red Team. In this way, they have developed numerous educational materials that stand out both for their high quality and for being tailored to the demands of the current job market. As a result, graduates will engage in a high-intensity experience that will significantly expand their career prospects.

You will gain access to a university degree designed by true leaders in the application of Pentesting and Red Team solutions in organizational settings"

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

Teachers

Mr. Siles Rubia, Marcelino

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

Mr. Redondo Castro, Pablo

- 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. Gallego Sánchez, Alejandro
- 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. Mora Navas, Sergio
- Cybersecurity Consultant in Oesía Group
- Cybersecurity Engineer from Rey Juan Carlos University.
- Computer Engineer from the University of Burgos

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

Mr. González Sanz, Marcos
- Cybersecurity Consultant at Cipherbit
- eLearnSecurity Certified eXploit Developer
- Offensive Security Certified Professional
- Offensive Security Wireless Professional
- Virtual Hacking Labs Plus
- Graduate in Software Engineering from the Polytechnic University of Madrid

Mr. Villaverde, David
- Cybersecurity Consultant at Cipherbit
- Expert in Hacking Challenge Platforms and HackTheBox
- Pentesting Specialist
- Malware Expert
- Software Engineer specializing in cybersecurity from Las Rozas University Center for Technology and Digital Art

Mr. Castillo, Carlos
- Cybersecurity Consultant and Red Teamer at Cipherbit
- Offensive Security Wireless Professional
- eLearnSecurity Web Application Penetration Tester
- eLearnSecurity Certified Professional Penetration Tester v2
- eLearnSecurity Junior Penetration Tester
- Cybersecurity Consultant
- Software Engineer from the Polytechnic University of Madrid

“ *A unique, essential and decisive learning experience to boost your professional development”*

08
Certificate

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

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

This private qualification will allow you to obtain a diploma for the **Master's Degree in Pentesting and Red Team** endorsed by TECH Global University, the world's largest online university.

TECH Global University, is an official European University publicly recognized by the Government of Andorra (***official bulletin***). Andorra is part of the European Higher Education Area (EHEA) since 2003. The EHEA is an initiative promoted by the European Union that aims to organize the international training framework and harmonize the higher education systems of the member countries of this space. The project promotes common values, the implementation of collaborative tools and strengthening its quality assurance mechanisms to enhance collaboration and mobility among students, researchers and academics.

This **TECH Global University** private qualification, is a European program of continuing education and professional updating that guarantees the acquisition of competencies in its area of knowledge, providing a high curricular value to the student who completes the program.

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

Modality: **online**

Duration: **12 months**

Accreditation: **60 ECTS**


tech global university

D/Dña ________________, con documento de identificación ___________ ha superado con éxito y obtenido el título de:

Máster Título Propio en Pentesting y Red Team

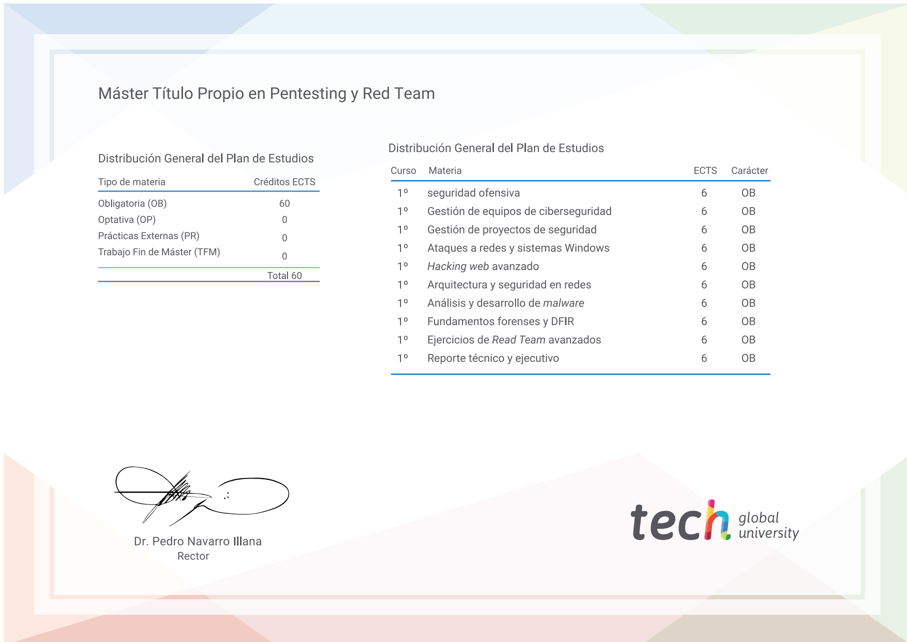
Se trata de un título propio de 1.800 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos


Máster Título Propio en Pentesting y Red Team

Distribución General del Plan de Estudios

Tipo de materia	Créditos ECTS
Obligatoria (OB)	60
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 60

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	seguridad ofensiva	6	OB
1º	Gestión de equipos de ciberseguridad	6	OB
1º	Gestión de proyectos de seguridad	6	OB
1º	Ataques a redes y sistemas Windows	6	OB
1º	*Hacking web* avanzado	6	OB
1º	Arquitectura y seguridad en redes	6	OB
1º	Análisis y desarrollo de *malware*	6	OB
1º	Fundamentos forenses y DFIR	6	OB
1º	Ejercicios de *Read Team* avanzados	6	OB
1º	Reporte técnico y ejecutivo	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

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

global university

Master's Degree
Pentesting and Red Team

» Modality: **online**
» Duration: **12 months**
» Certificate: **TECH Global University**
» Accreditation: **60 ECTS**
» Schedule: **at your own pace**
» Exams: **online**

Master's Degree
Pentesting and Red Team

tech global university