Professional Master's Degree

Pentesting and Red Team

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**

Website: www.techtitute.com/us/information-technology/professional-master-degree/master-pentesting-red-team

Index

01 Introduction p. 4

02 Objectives p. 8

03 Skills p. 16

04 Course Management p. 20

05 Structure and Content p. 24

06 Methodology p. 34

07 Certificate p. 42

01

Introduction

The number and sophistication of cyberattacks have reached alarming proportions. With the exponential increase in threats, from ransomware attacks to advanced intrusions, the need for highly skilled cybersecurity professionals is crucial. It is in this context that the present program arises, which will not only offer a complete immersion in advanced security techniques, but will also address the reality of a constantly evolving digital environment. In this way, students will delve into attack and defense techniques, facing the most sophisticated security challenges. Driven by the need to strengthen cyber defenses, this syllabus is distinguished by its 100% online methodology and the effective use of the Relearning method to optimize learning.

You will design impregnable security protocols thanks to this pioneering program, with TECH's guarantee"

Staying current is vital to preserve effectiveness in defending against current and emerging threats. In this regard, the rapid evolution of technology and cyber tactics has made constant updating an imperative. The proliferation of threats underscores the urgency of having highly enabled professionals.

In this context, this university program proves to be an essential answer, as it will not only provide an in-depth understanding of the most advanced techniques in cybersecurity, but will also ensure that professionals are at the forefront of the latest trends and technologies.

In the syllabus of this Professional Master's Degree in Pentesting and Network Team, the graduate will comprehensively address the demands in the field of cybersecurity. In this way, you will implement effective network security measures, including firewalls, intrusion detection systems (IDS) and network segmentation. To this end, specialists will apply digital forensic investigation methodologies to solve cases, from identification to documentation of findings.

In addition, they will develop skills in advanced threat simulation, replicating the tactics, techniques and procedures most commonly used by malicious actors. In addition, TECH's innovative approach will ensure the acquisition of applicable and valuable skills in the cybersecurity work environment.

The methodology of the educational itinerary reinforces its innovative character, as it will offer a 100% online educational environment. This program will be tailored to the needs of busy professionals looking to advance their careers. In addition, it will employ the Relearning methodology, based on the repetition of key concepts to fix knowledge and facilitate learning. In this way, the combination of flexibility and robust pedagogical approach will not only make it accessible, but also highly effective in preparing computer scientists for the dynamic challenges of cybersecurity.

This **Professional 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 case studies presented by experts in Pentesting and Red Team
- The graphic, schematic and eminently practical contents of the book provide up-to-date and practical information on those disciplines that are essential for professional practice
- Practical exercises where self-assessment can be used to improve learning
- Its special emphasis on innovative methodologies
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

In just 12 months you will give your career the boost it needs. Enroll now and experience immediate progress!"

Do you want to experience a leap in quality in your career? With TECH you will enable you in the implementation of strategies for the effective execution of cybersecurity projects"

You will delve into the identification and assessment of vulnerabilities in web applications, thanks to the best digital university in the world according to Forbes.

You will master forensic techniques in Pentesting environments. Position yourself as the cybersecurity expert that every company is looking for!

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

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

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

02

Objectives

The main objective of this educational program is to enable graduates in penetration testing and Red Team simulations. Throughout the program, computer scientists will be immersed in a practical and specialized approach, developing skills to address the identification and exploitation of vulnerabilities in systems and networks. Furthermore, this syllabus is designed to provide an in-depth understanding of cybersecurity tactics and strategies, preparing students to meet real-world challenges and lead in the effective implementation of cybersecurity measures.

You will delve into malware analysis and development to position yourself as a stand out professional. Reach your goals by the hand of TECH!"

General Objectives

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

You will achieve your objectives thanks to TECH's didactic tools, among which the explanatory videos and interactive summaries stand out"

Specific Objectives

Module 1. Offensive Security

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

Module 2. Cybersecurity Team Management

- Develop leadership skills specific to cybersecurity teams, including the ability to motivate, inspire, and coordinate efforts to achieve common goals
- 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 strategies to identify and manage conflicts within the cybersecurity team, promoting a collaborative and efficient work environment

- Learn how to establish metrics and evaluation systems to measure cybersecurity team performance and make adjustments as needed
- Promote the integration of ethical practices in the management of cybersecurity teams, ensuring that all activities are conducted in an ethical and legal manner
- Develop competencies for the preparation and efficient management of cybersecurity incidents, ensuring a rapid and effective response to threats

Module 3. Security Project Management

- Develop skills to plan cyber security projects, defining objectives, scope, resources and execution deadlines
- Learn strategies for the effective execution of security projects, ensuring the successful implementation of planned measures
- Develop skills for efficient budget management and resource allocation in security projects, maximizing efficiency and minimizing costs
- Improve effective communication with stakeholders, presenting reports and updates in a clear and understandable manner
- Learn project monitoring and control techniques, identifying deviations and taking corrective actions as necessary
- Familiarize students with Agile Pentesting methodologies
- Develop skills in detailed documentation and reporting, providing a clear view of project progress and results obtained
- Promote effective collaboration between different teams and disciplines within security projects, ensuring a comprehensive and coordinated vision
- Learn strategies to evaluate and measure the effectiveness of implemented measures, ensuring continuous improvement of the organization's security posture

Module 4. Network and Windows System Attacks

- Develop skills to identify and assess specific vulnerabilities in Windows operating systems
- Learn advanced tactics used by attackers to infiltrate and persist in networks based on Windows environments
- Acquire skills in strategies and tools to mitigate specific threats targeting Windows operating systems
- Familiarize the graduate with forensic analysis techniques applied to Windows systems, facilitating the identification and response to incidents
- Apply theoretical knowledge in simulated environments, participating in practical exercises to understand and counteract specific attacks on Windows systems
- Learn specific strategies for securing enterprise environments using Windows operating systems, considering the complexities of enterprise infrastructures
- 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
- Keep the student up-to-date with the latest trends and threats in Windows system attacks, ensuring the continued relevance and effectiveness of the skills acquired

Module 5. Advanced Web Hacking

- Develop skills to identify and assess vulnerabilities in web applications, including SQL injections, Cross-Site Scripting (XSS) and other common attack vectors
- Learn how to perform security testing on modern web applications
- Acquire skills in advanced web hacking techniques, exploring strategies for evading security measures and exploiting sophisticated vulnerabilities
- Familiarize the graduate with the evaluation of security in APIs and web services, identifying possible points of vulnerability and strengthening security in programming interfaces
- Develop skills to implement effective mitigation measures in web applications, reducing exposure to attacks and strengthening security
- Participate in hands-on simulations to assess security in complex web environments, applying knowledge to real-world scenarios
- Develop competencies in the formulation of effective defense strategies to protect web applications against cyber threats
- Learn how to align advanced web hacking practices with relevant security regulations and standards, ensuring adherence to legal and ethical frameworks
- Foster effective collaboration between development and security teams

Module 6. Network Architecture and Security

- Acquire advanced knowledge of network architecture, including topologies, protocols and key components
- Develop skills to identify and assess specific vulnerabilities in network infrastructures, considering potential threats
- Learn how to implement effective network security measures, including firewalls, intrusion detection systems (IDS) and network segmentation
- Familiarize the student with emerging networking technologies, such as software-defined networking (SDN), and understand their impact on security
- Develop skills to secure network communications, including protection against threats such as sniffing and man-in-the-middle attacks
- Learn how to evaluate and improve security configurations in enterprise network environments, ensuring adequate protection
- Develop skills to implement effective mitigation measures against threats in enterprise networks, from internal attacks to external threats
- Foster effective collaboration with security teams, integrating strategies and efforts to protect network infrastructure
- Promote ethical and legal practices in the implementation of network security measures, ensuring adherence to ethical principles in all activities

Module 7. Malware Analysis and Development

- Acquire advanced knowledge of the nature, functionality and behavior of malware, understanding its various forms and targets
- Develop skills in forensic analysis applied to malware, enabling the identification of indicators of compromise (IoC) and attack patterns
- Learn strategies for effective malware detection and prevention, including the deployment of advanced security solutions

- Familiarize the student with the development of malware for educational and defensive purposes, allowing a deep understanding of the tactics used by attackers
- Promote ethical and legal practices in malware analysis and development, ensuring integrity and accountability in all activities
- Apply theoretical knowledge in simulated environments, participate in hands-on exercises to understand and counter malicious attacks
- Develop skills to evaluate and select anti-malware security tools, considering their effectiveness and adaptability to specific environments
- Learn how to implement effective mitigation against malicious threats, reducing the impact and spread of malware on systems and networks
- Foster effective collaboration with security teams, integrating strategies and efforts to protect against malware threats
- Keep the graduate up-to-date with the latest trends and techniques used in malware analysis and development, ensuring the continued relevance and effectiveness of the skills acquired

Module 8. Forensic Fundamentals and DFIR

- Acquire a solid understanding of the fundamental principles of digital forensic investigation (DFIR) and their application in the resolution of cyber incidents
- Develop skills in the secure and forensic acquisition of digital evidence, ensuring the preservation of the chain of custody
- Learn how to perform forensic analysis of file systems
- Familiarize the student with advanced techniques for log and log analysis, allowing the reconstruction of events in digital environments
- Learn how to apply digital forensic investigation methodologies in case resolution, from identification to documentation of findings
- Familiarize the student with the analysis of digital evidence and the application of forensic techniques in Pentesting environments
- Develop skills in the preparation of detailed and clear forensic reports, presenting findings and conclusions in an understandable manner
- Foster effective collaboration with incident response (IR) teams, optimizing coordination in threat investigation and mitigation
- Promote ethical and legal practices in digital forensics, ensuring adherence to cybersecurity regulations and standards of conduct

Module 9. Advanced Red Team Exercises

- Develop skills in advanced threat simulation, replicating tactics, techniques and procedures (TTP) used by attractive malicious actors
- Learn to identify weaknesses and vulnerabilities in the infrastructure through realistic Red Team exercises, strengthening the security posture
- Familiarize the graduate with advanced techniques for evasion of security measures, allowing to evaluate the resistance of the infrastructure against desirable attacks
- Develop effective coordination and collaboration skills among Red Team team members, optimizing the execution of tactics and strategies to comprehensively assess the security of the organization
- Learn how to simulate current threat scenarios, such as ransomware attacks or advanced

phishing campaigns, to assess the organization's response capabilities

- Familiarize the student with post-exercise analysis techniques, evaluating the performance of the Red Team and extracting lessons learned for continuous improvement
- Develop skills to assess organizational resilience to simulated attacks, identifying areas for improvement in policies and procedures
- Learn to prepare detailed reports documenting findings, methodologies used and recommendations derived from advanced Red Team exercises
- Promote ethical and legal practices in the conduct of Red Team exercises, ensuring adherence to cybersecurity regulations and ethical standards

Module 10. Technical and Executive Report

- Develop skills to prepare detailed technical reports, presenting clearly and completely the findings, methodologies used and recommendations
- Learn to communicate effectively with technical audiences, using precise and appropriate language to convey complex technical information
- Develop skills to formulate actionable and practical recommendations aimed at mitigating vulnerabilities and improving security posture
- Learn to assess the potential impact of identified vulnerabilities, considering technical, operational and strategic aspects
- Familiarize the learner with best practices for executive reporting, adapting technical information for non-technical audiences
- Develop competencies to align findings and recommendations with the strategic and operational objectives of the organization
- Learn how to use data visualization tools to graphically represent the information contained in the reports, facilitating comprehension
- Promote the inclusion of relevant information on compliance with regulations and standards in reports, ensuring adherence to legal requirements
- Foster effective collaboration between technical and executive teams, ensuring understanding and support for the improvement actions proposed in the report

03

Skills

Thanks to this syllabus, graduates will enable them with specialized skills to implement active defense measures, strengthening the security of systems and networks based on cybersecurity best practices. In addition, students will acquire advanced skills in penetration testing and Red Team simulations, standing out in proactive vulnerability identification and mitigation. In this sense, professionals will master the technical skills necessary to face real-world threats, preparing them to lead effective security assessment and fortification strategies in dynamic cyber environments. In addition, the 100% online approach makes learning more flexible.

Become an expert in cybersecurity through 1,500 hours of the best multimedia content, with the TECH quality seal"

General Skills

- Acquire competencies in the planning, execution and management of cyber security projects, ensuring effective results and compliance with objectives
- Acquire advanced knowledge in network architecture and its security aspects, assessing vulnerabilities and applying strategies to strengthen the infrastructure
- Develop competencies in digital forensics and incident response, from evidence collection to threat mitigation and operational restoration
- Apply advanced tactics in the planning and execution of Red Team exercises, simulating real-world scenarios to assess infrastructure resilience, detect weaknesses and improve preparedness for cyber threats

Get up-to-date on the process of identifying, assessing and mitigating risks specific to cybersecurity projects. Bet on TECH!"

Specific Skills

- Acquire coaching skills for the professional development of team members, fostering growth and improvement
- Develop skills for strategic decision making in cybersecurity situations, considering the short and long term impact on organizational security
- Acquire skills in the identification, assessment and mitigation of risks specific to cyber security projects
- Develop skills to implement active defense measures, strengthening the security of systems and systems-based networks
- Learn web traffic analysis techniques to identify anomalous patterns and behaviors, facilitating the detection of possible threats
- Acquire skills in forensic analysis applied to network environments, enabling effective identification and response to cyber incidents
- Learn strategies for effective malware detection and prevention, including the deployment of advanced security solutions
- Develop skills in identifying indicators of compromise (IoC) during forensic investigation, facilitating incident detection and response
- Acquire skills for strategic planning of Red Team exercises, considering objectives, scope, resources and realistic scenarios
- Acquire skills in identifying and prioritizing vulnerabilities, standing out those that represent the greatest security risks

04

Course Management

For the preparation of the teaching staff of the Professional Master's Degree in Pentesting and Network Team, TECH has brought together the best specialists, who have an extensive and recognized professional background in leading companies in the sector. In this regard, each member of the teaching staff will contribute their practical experience and expertise, ensuring that students will benefit from the teaching of highly qualified professionals. Furthermore, the careful selection of these experts will not only ensure academic quality, but also the immediate relevance and applicability of the content in the dynamic cybersecurity environment.

Cybersecurity industry giants will catapult you to success in as little as 12 months with this exclusive TECH University program"

Management

Mr. Gómez Pintado, Carlos

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

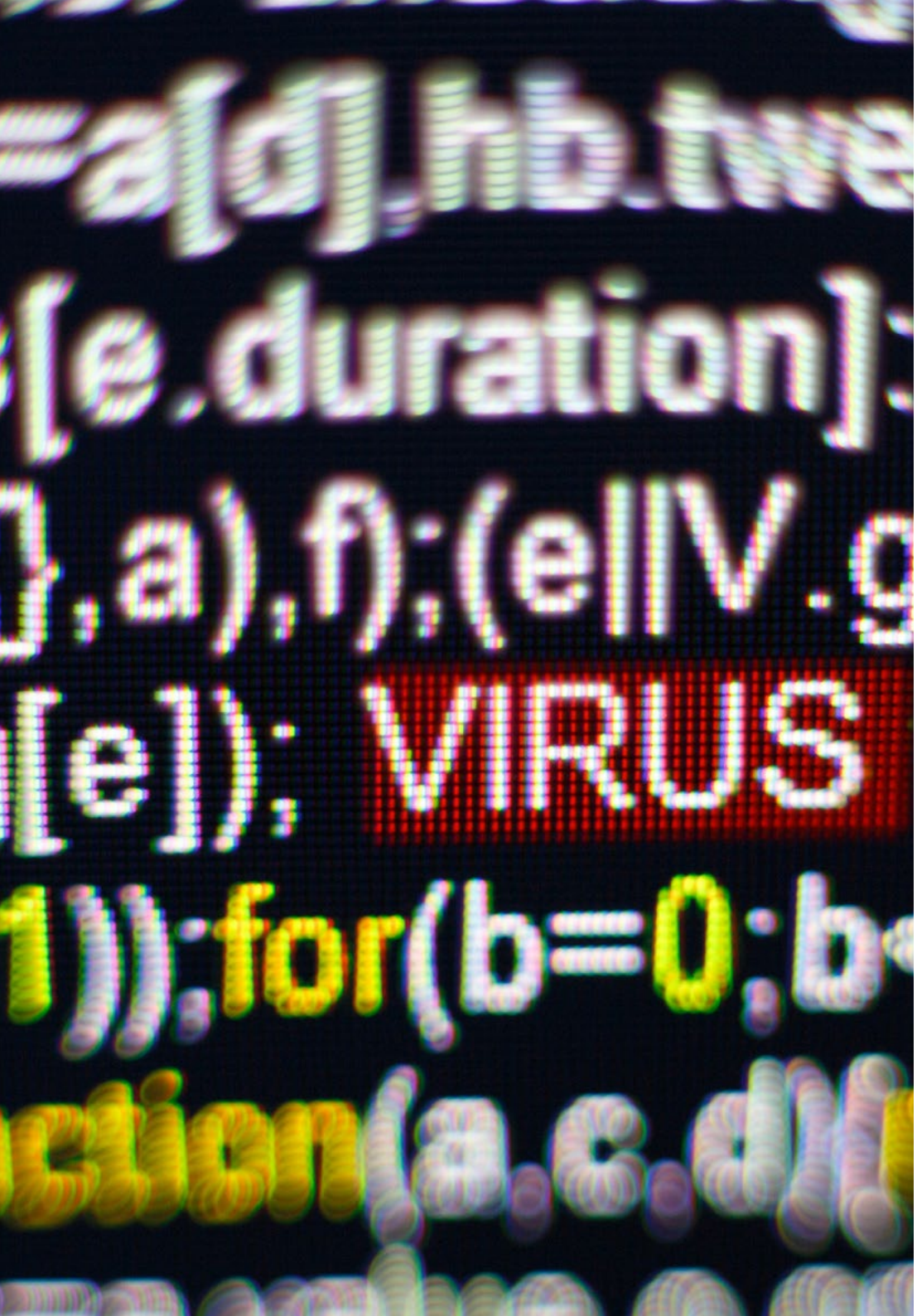
Professors

Mr. 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

- 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. González Sanz, Marcos

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

Mr. Mora Navas, Sergio

- Cybersecurity Consultant in Oesía Group
- Cybersecurity Engineer, Rey Juan Carlos University Computer Science Engineer, University of Burgos

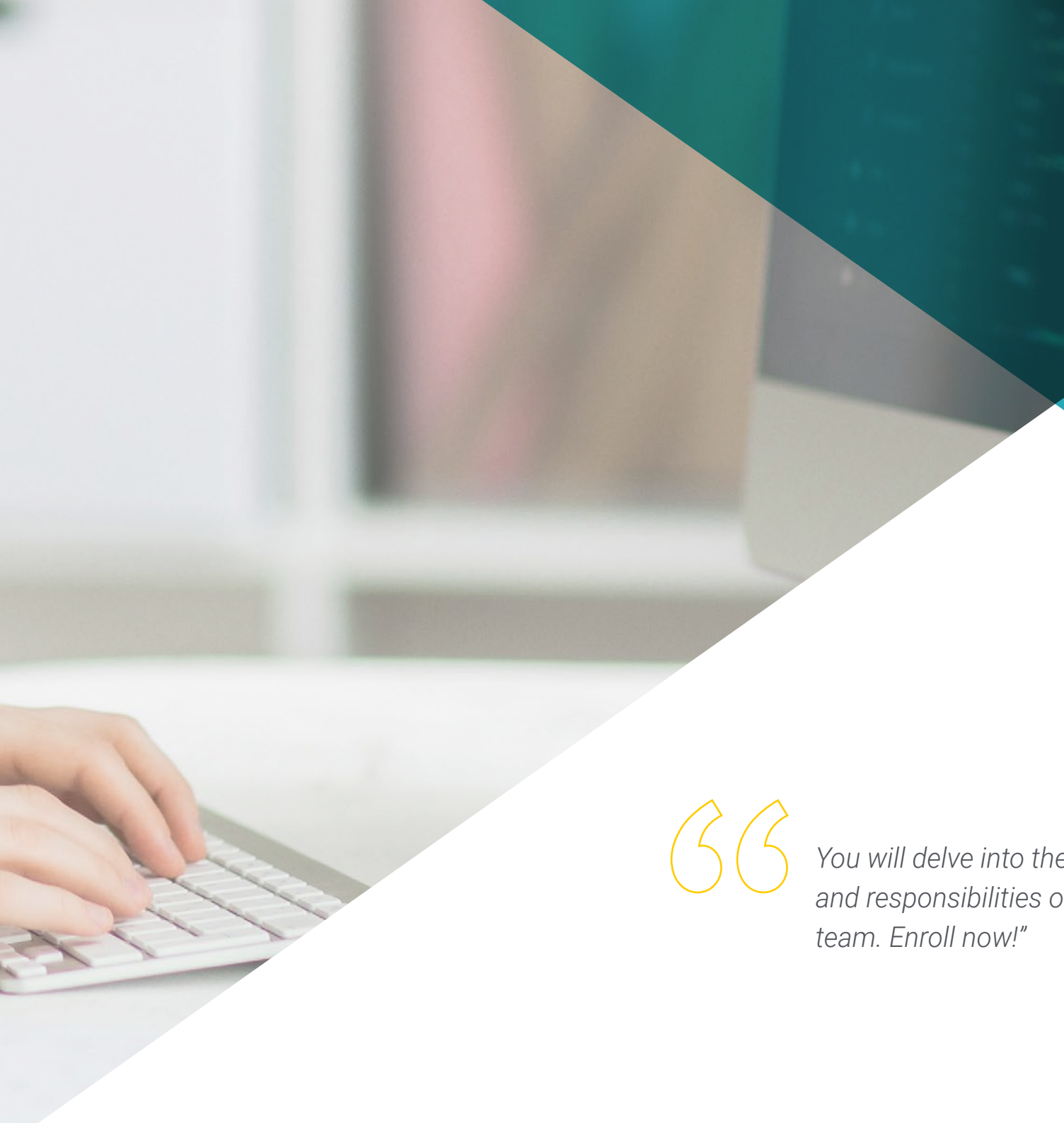
Mr. González Parrilla, Yuba

- 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

05

Structure and Content

This university program offers a complete immersion in the crucial disciplines of penetration testing and Red Team simulations. Throughout the program, graduates will develop advanced skills to identify and exploit vulnerabilities in systems and networks, using modern techniques and tools. This program, designed with a hands-on approach, will enable cybersecurity professionals to meet real-world challenges. In this regard, students will benefit from a unique combination of theory and practice, guided by industry experts, to strengthen their understanding and effectively apply security assessment strategies in cyber environments.



You will delve into the different roles and responsibilities of the cybersecurity team. Enroll now!"

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. Preparation 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. Reporting 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

06

Methodology

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

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

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

Case Study to contextualize all content

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

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

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

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

A learning method that is different and innovative

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

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

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

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

Relearning Methodology

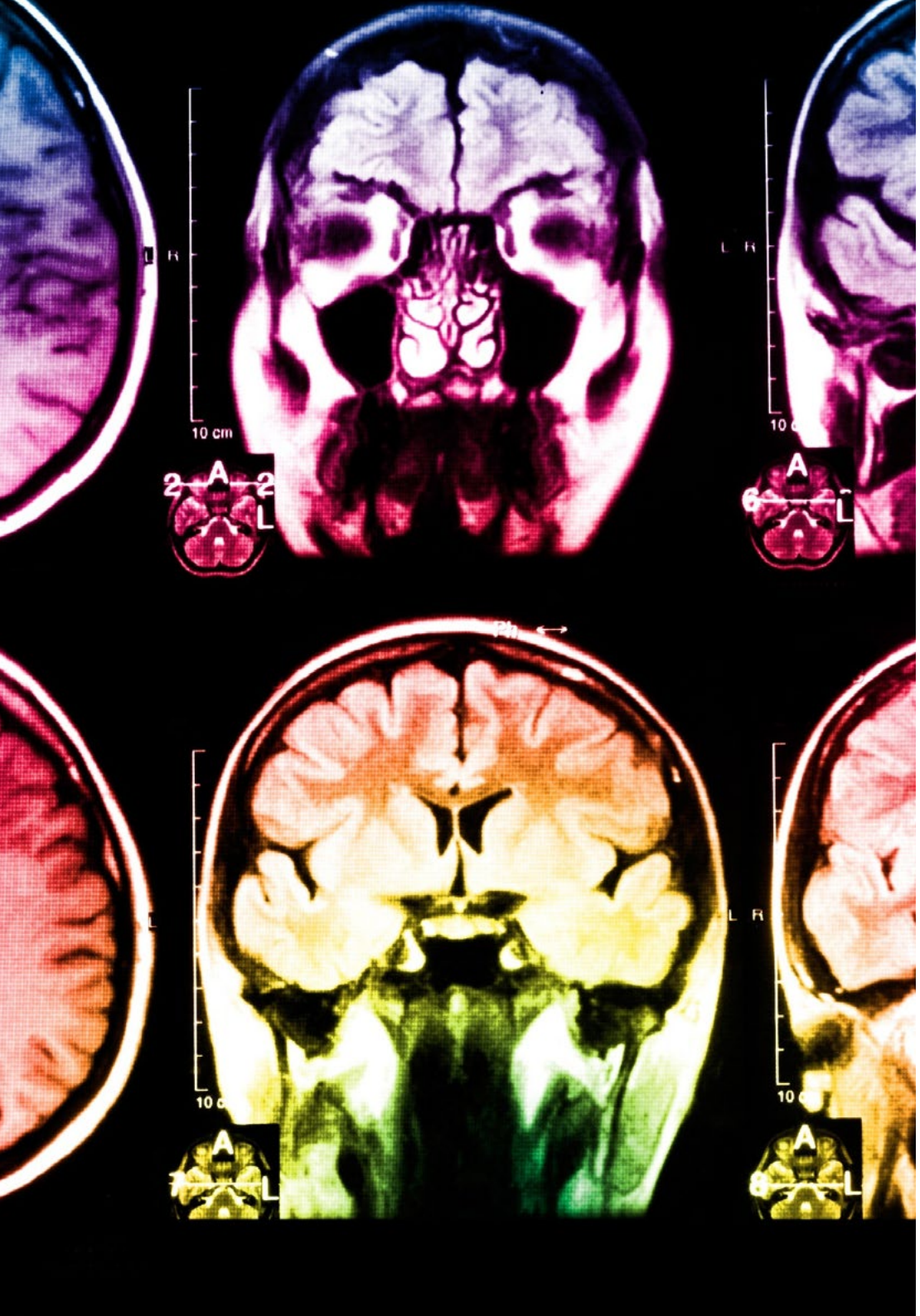
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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

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

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

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



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

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

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

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

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

Study Material

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

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

Classes

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

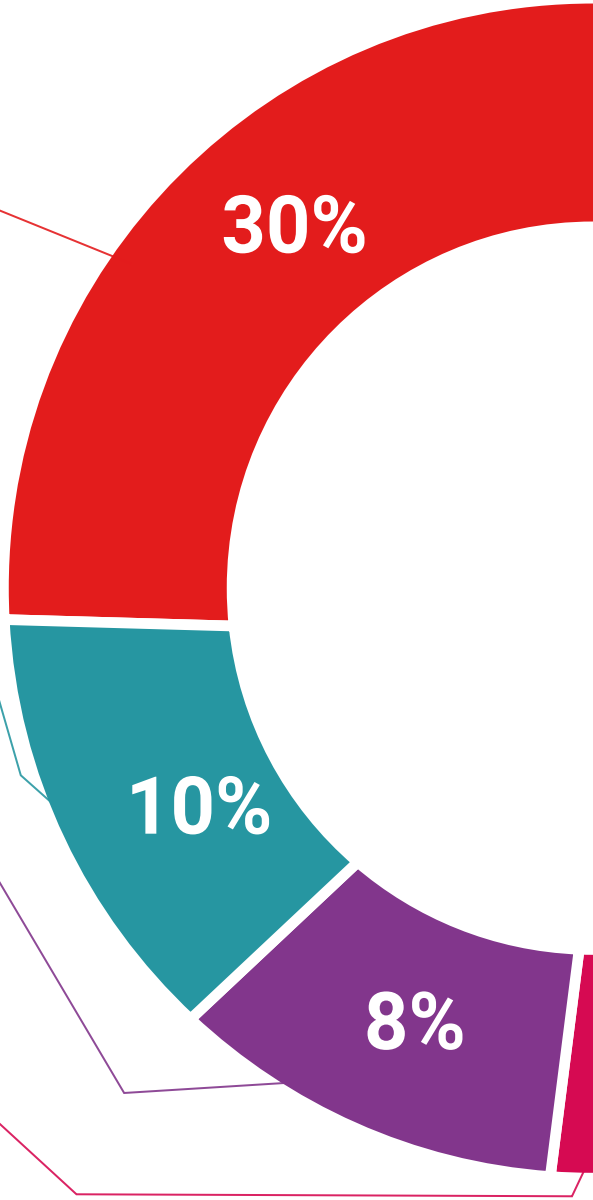
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

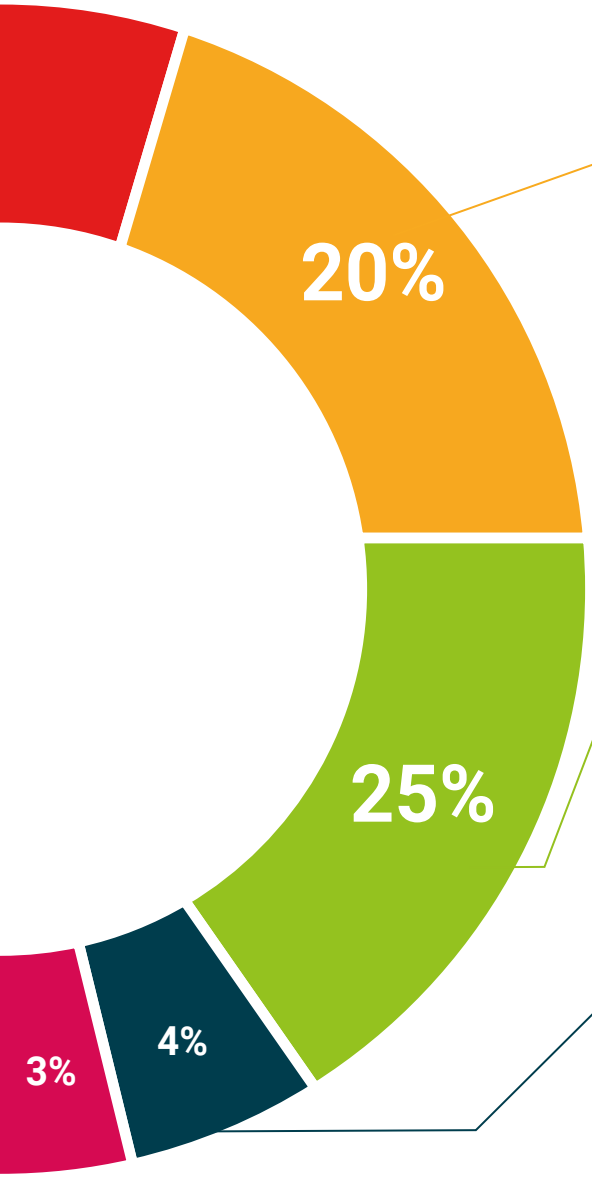
Practising Skills and Abilities

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

Additional Reading

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





Case Studies

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

Interactive Summaries

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

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

Testing & Retesting

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

07

Certificate

The Professional Master's Degree in Pentesting and Red Team guarantees, in addition to the most rigorous and up-to-date program, access to a Professional Master's Degree 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 diploma 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: **1500 h.**


tech technological university

Awards the following

DIPLOMA

to

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

For having successfully passed and accredited the following program

PROFESSIONAL MASTER'S DEGREE

in

Pentesting and Red Team

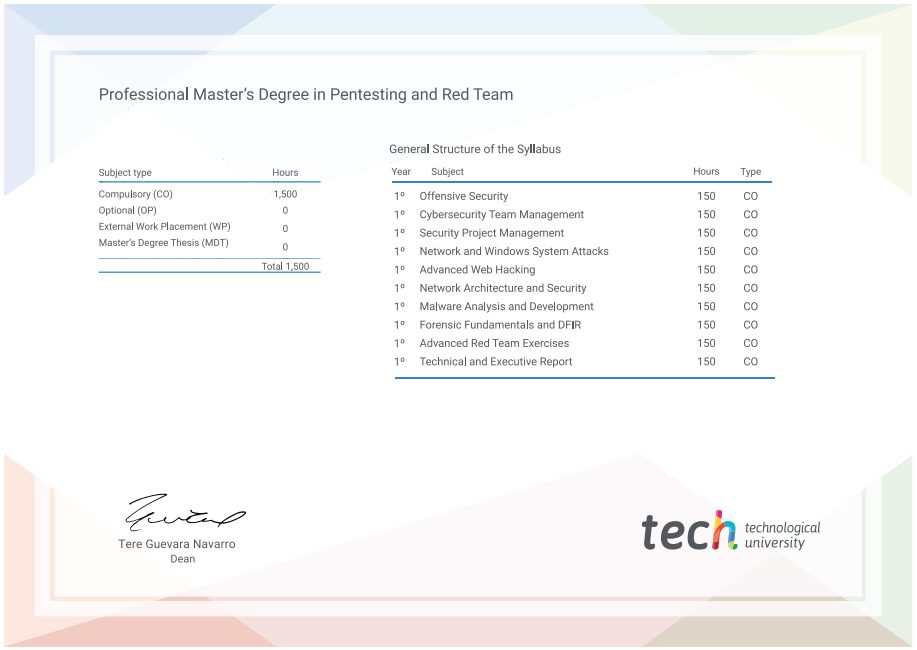
This is a qualification awarded by this University, equivalent to 1,500 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

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 diploma 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