

REGISTRATION FORM FOR THE QUALITY MANAGEMENT SYSTEM

 <p>OMNITECHIT</p>	<p><i>COURSE SPECIFICATION</i></p>	<p>STC – Course Specification <i>Model: SRA-r1</i></p>
--	---	---

Title of Course: *PENETRATION TEST*

Code: *PT*

COURSE DESCRIPTION	Practical base course on Penetration Test methodologies
COURSE RECIPIENTS	ITC Personnel
EDUCATIONAL GOALS	<p>Introduction to Penetration Testing. Penetration Test is a methodology to evaluate the security of a system or a net. The analysis is made up of phases, whose objective is to highlight the weaknesses of the platform, revealing the most information possible about the vulnerabilities that have allowed the unauthorized access. The analysis is conducted as a potential attacker would, and consists in exploiting the revealed weaknesses to extract as much information as possible to access the system illicitly. A pen-test therefore tests the security of a system by threatening to breach it with a number of different types of attacks. The objective is to single out the eventual vulnerabilities available to third parties which could access the system fraudulently.</p>
ADMISSION REQUIREMENTS	The must have base knowledge of computer networks (architectures and types), Web apps (communication protocols used and functioning), base IT Security concepts (though not fundamental).
COURSE PROGRAM	<p>First day</p> <ul style="list-style-type: none"> • Introduction to Security Audit • Introduction to Penetration test • How to find vulnerabilities through the Penetration test • Methodology used: what is OSSTMM • PT audit phases • Exercises and Laboratory <p>Second Day</p> <ul style="list-style-type: none"> • Vulnerability, most common attacks and typologies • Examples of tools and instruments to be used • Results analysis phase: <ul style="list-style-type: none"> ○ Metrics for result's measuring ○ How to use results in Risk analysis • Exercises and Laboratory