Ethical Hacking Methodologies

Santiago Hernández Ramos
@santiagohramos

IMPORTANCE OF METHODOLOGIES

- Methodologies help us carry out a set of activities in a specific order, establishing proper priorities to ensure success and achieve a final goal.

MAIN METHODOLOGIES

- OSSTMM (Open-Source Security Testing Methodology Manual): https://www.isecom.org/OSSTMM.3.pdf
- The Penetration Testing Execution Standard: http://www.pentest-standard.org/index.php/Main_Page
- ISSAF (Information Systems Security Assessment Framework)
- OTP (OWASP Testitng Project)

METHODOLOGY OF THIS COURSE

- Definition of the Scope of the Penetration Test (Ethical Hacking)
- Information Gathering
- Vulnerability Identification and Analysis
- Vulnerability Exploitation
- Post-Exploitation
- Reporting

DEFINITION OF THE SCOPE

- Before taking any action, discuss with the client the tasks the analyst will perform during the Ethical Hacking process, as well as the roles and responsibilities of both parties.
- Ensure through a signed contract that the actions carried out are on behalf of the client.
- Analyze the organization's policies that define how users interact with systems and infrastructure.
- Procedure in case a third-party intrusion is detected.