Metodologías de pruebas de penetración y análisis de vulnerabilidades

Proceso de evaluación de seguridad que simula un ataque cibernético para identificar y explotar vulnerabilidades en sistemas, redes y aplicaciones. Su objetivo es simular el comportamiento de un atacante malicioso para encontrar puntos débiles antes de que puedan ser aprovechados por delincuentes reales

Diferencias entre metodologías

- Número de fases
- Enfoque de la metodología
- Superficie de Ataque
- Guías técnicas o referencias de fases

ALGUNAS METODOLOGÍAS Y LÍNEAS GUÍA TÉCNICAS

ISSAF

NIST

OWASP

PTES

OSSTMM

STANDARDS
(Process & Structure)

- **PTES (Penetration Testing Execution Standard)**
  - Focus: Lifecycle & 7 Phases of an Engagement
- **ISSAF (Information Systems Security Assessment Framework)**
  - Focus: Business & Technical Integration, Broad Organizational Audit

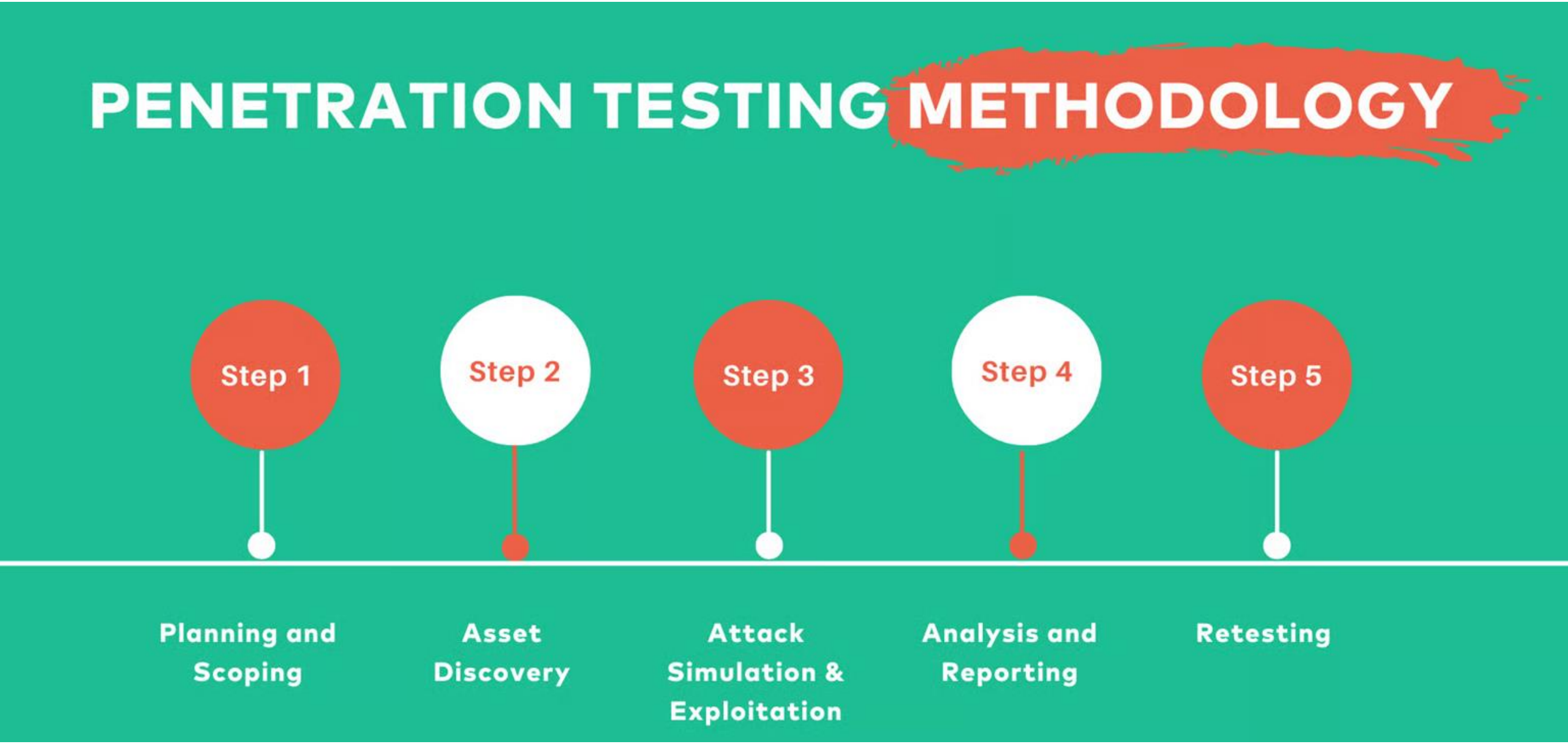
TECHNICAL GUIDELINES
(Methodology & Metrics)

- **NIST SP 800-115 (National Institute of Standards and Technology)**
  - Focus: Formal Methodology, Compliance, & Control Assessment
- **OSSTMM (Open Source Security Testing Methodology Manual)**
  - Focus: Operational Security, Metrics, & Scientific Approach

TESTING GUIDES
(Domain-Specific Cookbooks)

- **OWASP WSTG**
  (Open Web Application Security Project Web Security Testing Guide)
  - Focus: Web App Specific, Tactical Tests, & Command Checklists

PENETRATION TESTING METHODOLOGY



ENFOQUES Y SUPERFICIES

- **Blackbox**

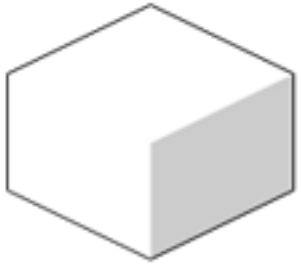
Perimetral

IoT

- **Graybox**

Wi-FI

Endpoints



- **Whitebox**

Red

Servidores