Penetration Testing Execution Standards

SNOWCAP CYBER

There are various standards that relate to and include Penetration Testing such as ISO27001 and NIST 800-53. We define penetration testing as follows:

> *"A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."*

However, the following are standards that expressly relate to Penetration Testing.

- NIST 800-171
    - NIST offers more specific guidelines for penetration testers to follow. The National Institute of Standards and Technology (NIST) provides a manual that is best suited to improve the overall Cybersecurity of an organization. The most recent version, 1.1, places more emphasis on the Critical Infrastructure Cybersecurity. Complying with the NIST framework is often a regulatory requirement for various American providers and business partners. With this framework, NIST set its sight on guaranteeing information security in different industries, including banking, communications, and energy.
- OSSTMM
    - The OSSTMM framework, one of the most recognized standards in the industry, provides a scientific methodology for network penetration testing and vulnerability assessment. This framework contains a comprehensive guide for testers to identify security vulnerabilities within a network (and its components) from various potential angles of attack. The OSSTMM methodology (Open Source Security Testing Methodology Manual) allows testers to customize their assessment to fit the specific needs or the technological context of your company. With this set of standards, you will obtain an accurate overview of your network's cybersecurity, as well as reliable solutions adapted to your technological context to help your stakeholders make the right decisions to secure your networks.
- OWASP
    - This framework provides a methodology for web application penetration testing that can not only identify vulnerabilities commonly found within web and mobile applications, but also complicated logic flaws that stem from unsafe development practices.
- PTES
    - The PTES Framework (Penetration Testing Methodologies and Standards) highlights the most recommended approach to structure a penetration test. This standard guides testers on various steps of a penetration test including initial communication, gathering information, as well as the threat modelling phases. Following this penetration testing standard, testers acquaint themselves with the organization and their technological context as much as possible before they focus on exploiting the potentially vulnerable areas, allowing them to identify the most advanced scenarios of attacks that could be attempted.
- ISSAF
    - The ISSAF standard (Information System Security Assessment Framework) contains an even more structured and specialized approach to penetration testing than the previous standard. If your organization's unique situation requires an advanced methodology entirely personalized to its context, then this manual should prove useful for the specialists in charge of your penetration test. These sets of standards enable a tester to meticulously plan and document every step of the penetration testing procedure, from planning and assessment to reporting and destroying artefacts. This standard caters for all steps of the process.