Penetration Testing Standards

Penetration tests should not be performed without any rules or guidelines. There must always be a specifically defined scope for a pentest, and the owner of a network must have a signed legal contract with pentesters outlining what they're allowed to do and what they're not allowed to do. Pentesting should also be conducted in such a way that minimal harm is done to a company's computers and networks. Penetration testers should avoid making changes wherever possible (such as changing an account password) and limit the amount of data removed from a client's network. For example, instead of removing sensitive documents from a file share, a screenshot of the folder names should suffice to prove the risk.

In addition to scope and legalities, there are also various pentesting standards, depending on what kind of computer system is being assessed. Here are some of the more common standards you may use as a pentester.

PTES

The Penetration Testing Execution Standard (PTES) can be applied to all types of penetration tests. It outlines the phases of a penetration test and how they should be conducted. These are the sections in the PTES:

1. **Pre-engagement Interactions**:
   - Establishing communication channels, understanding client requirements, and defining the rules of engagement.
2. **Intelligence Gathering**:
   - Collecting information about the target system through passive and active means without triggering any alarms.
3. **Threat Modelling**:
   - Identifying potential threats and attack vectors that could be exploited against the target system.
4. **Vulnerability Analysis**:
   - Identifying and analysing security weaknesses in the target system.
5. **Exploitation**:
   - Attempting to exploit identified vulnerabilities to gain unauthorised access.
6. **Post Exploitation**:
   - Maintaining access, collecting evidence, and understanding the impact of exploitation.
7. **Reporting**:
   - Documenting the findings, providing a risk assessment, and recommending remediation steps.

OSSTMM

OSSTMM is the Open Source Security Testing Methodology Manual, another set of guidelines pentesters can use to ensure they're doing their jobs properly. It can be used alongside other pentest standards.

OSSTMM is divided into five different channels for five different areas of pentesting:

1. **Human Security**:
    - Assessing human susceptibility to social engineering attacks.
2. **Physical Security**:
    - Evaluating the security of physical barriers and controls.
3. **Wireless Communications**:
    - Assessing the security of wireless technologies like WiFi and Bluetooth.
4. **Telecommunications**:
    - Analysing the security of telecommunication systems.
5. **Data Networks**:
    - Evaluating the security of data networks and communication channels.

NIST

The NIST (National Institute of Standards and Technology) is well known for their NIST Cybersecurity Framework, a system for designing incident response policies and procedures. NIST also has a Penetration Testing Framework. The phases of the NIST framework include:

1. **Planning**:
    - Defining the scope, objectives, and rules of engagement for the penetration test.
2. **Discovery**:
    - Gathering information about the target system and identifying potential vulnerabilities.
3. **Attack**:
    - Attempting to exploit identified vulnerabilities to gain unauthorised access.
4. **Reporting**:
    - Documenting the findings, providing a risk assessment, and recommending remediation steps.

OWASP

OWASP stands for the Open Web Application Security Project. They're typically the go-to organisation for defining testing standards and classifying risks to web applications.

OWASP maintains a few different standards and helpful guides for assessing various technologies:

1. **Web Security Testing Guide (WSTG)**:
    - A comprehensive guide for testing the security of web applications, covering various testing techniques and methodologies.
2. **OWASP Top Ten**:
    - A list of the top ten most critical web application security risks, updated periodically to reflect the evolving threat landscape.
3. **Application Security Verification Standard (ASVS)**:
    - A framework for verifying the security of web applications, providing a basis for designing, developing, and testing secure applications.
4. **Mobile Security Testing Guide (MSTG)**:
    - A comprehensive guide for testing the security of mobile applications, covering both iOS and Android platforms.
5. **Software Assurance Maturity Model (SAMM)**:
    - A framework for evaluating and improving the security practices of software development organisations.

Conclusion

Penetration testing standards provide a structured approach to conducting security assessments, ensuring that tests are thorough, systematic, and legally compliant. By adhering to these standards, penetration testers can effectively identify and mitigate security vulnerabilities, helping organisations enhance their overall security posture.