Stages

Penetration tests can have a wide variety of objectives and targets within scope. Because of this, no penetration test is the same, and there are no one-case fits all as to how a penetration tester should approach it.

The steps a penetration tester takes during an engagement is known as the methodology. A practical methodology is a smart one, where the steps taken are relevant to the situation at hand. For example, having a methodology that you would use to test the security of a web application is not practical when you have to test the security of a network.

Before discussing some different industry-standard methodologies, we should note that all of them have a general theme of the following stages:

Stage	Description
Information Gathering	This stage involves collecting as much publically accessible information about a target/organisation as possible, for example, OSINT and research. **Note**: This does not involve scanning any systems.
Enumeration/Scanning	This stage involves discovering applications and services running on the systems. For example, finding a web server that may be potentially vulnerable.
Exploitation	This stage involves leveraging vulnerabilities discovered on a system or application. This stage can involve the use of public exploits or exploiting application logic.
Privilege Escalation	Once you have successfully exploited a system or application (known as a foothold), this stage is the attempt to expand your access to a system. You can escalate horizontally and vertically, where horizontally is accessing another account of the same permission group (i.e. another user), whereas vertically is that of another permission group (i.e. an administrator).
Post-exploitation	This stage involves a few sub-stages: 1. What other hosts can be targeted (pivoting) 2. What additional information can we gather from the host now that we are a privileged user 3. Covering your tracks 4. Reporting

Revision #2
Created 2023-02-11 21:14:06 UTC by Fettlaus

Updated 2023-02-11 21:16:51 UTC by Fettlaus