

Methodologies

- [Stages](#)
- [OSSTMM](#)
- [OWASP](#)
- [NIST Cybersecurity Framework 1.1](#)
- [NCSC CAF](#)

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

OSSTMM

[The Open Source Security Testing Methodology Manual](#) provides a detailed framework of testing strategies for systems, software, applications, communications and the human aspect of cybersecurity.

The methodology focuses primarily on how these systems, applications communicate, so it includes a methodology for:

- 1. **Telecommunications (phones, VoIP, etc.)**
- 2. Wired Networks
- 3. Wireless communications

Advantages	Disadvantages
Covers various testing strategies in-depth.	The framework is difficult to understand, very detailed, and tends to use unique definitions.
Includes testing strategies for specific targets (i.e. telecommunications and networking)	<i>Intentionally left blank.</i>
The framework is flexible depending upon the organisation's needs.	<i>Intentionally left blank.</i>
The framework is meant to set a standard for systems and applications, meaning that a universal methodology can be used in a penetration testing scenario.	<i>Intentionally left blank.</i>

OWASP

The "[Open Web Application Security Project](#)" framework is a community-driven and frequently updated framework used solely to test the security of web applications and services.

The foundation regularly [writes reports](#) stating the top ten security vulnerabilities a web application may have, the testing approach, and remediation.

Advantages	Disadvantages
Easy to pick up and understand.	It may not be clear what type of vulnerability a web application has (they can often overlap).
Actively maintained and is frequently updated.	OWASP does not make suggestions to any specific software development life cycles.
It covers all stages of an engagement: from testing to reporting and remediation.	The framework doesn't hold any accreditation such as CHECK.
Specialises in web applications and services.	<i>Intentionally left blank.</i>

NIST Cybersecurity Framework 1.1

The [NIST Cybersecurity Framework](#) is a popular framework used to improve an organisations cybersecurity standards and manage the risk of cyber threats. This framework is a bit of an honourable mention because of its popularity and detail.

The framework provides guidelines on security controls & benchmarks for success for organisations from critical infrastructure (power plants, etc.) all through to commercial. There is a limited section on a standard guideline for the methodology a penetration tester should take.

Advantages	Disadvantages
The NIST Framework is estimated to be used by 50% of American organisations by 2020.	NIST has many iterations of frameworks, so it may be difficult to decide which one applies to your organisation.
The framework is extremely detailed in setting standards to help organisations mitigate the threat posed by cyber threats.	The NIST framework has weak auditing policies, making it difficult to determine how a breach occurred.
The framework is very frequently updated.	The framework does not consider cloud computing, which is quickly becoming increasingly popular for organisations.
NIST provides accreditation for organisations that use this framework.	<i>Intentionally left blank.</i>
The NIST framework is designed to be implemented alongside other frameworks.	<i>Intentionally left blank.</i>

NCSC CAF

The [Cyber Assessment Framework](#) (CAF) is an extensive framework of fourteen principles used to assess the risk of various cyber threats and an organisation's defences against these.

The framework applies to organisations considered to perform "vitally important services and activities" such as critical infrastructure, banking, and the likes. The framework mainly focuses on and assesses the following topics:

- Data security
- System security
- Identity and access control
- Resiliency
- Monitoring
- Response and recovery planning

Advantages	Disadvantages
This framework is backed by a government cybersecurity agency.	The framework is still new in the industry, meaning that organisations haven't had much time to make the necessary changes to be suitable for it.
This framework provides accreditation.	The framework is based on principles and ideas and isn't as direct as having rules like some other frameworks.
This framework covers fourteen principles which range from security to response.	Intentionally left blank.