SERIES: CYBERSECURITY

PENETRATION TESTING

ALL I.T

CONTACT US

INTERNAL PENETRATION TESTING

SCOPING OF THE INTERNAL PENETRATION TEST

A well-thought-out scope is imperative for the success Internal Penetration Test. Without developing and aligning on the scope, there is a risk of unauthorised testing of systems, wasted time and effort, or unexpected disruption (including permanent damage) to the organisation.

The scope of the test should include the following:

- The list of assets or targets in scope. This could include domain names, URLs, hostnames, or IP addresses. Anything not listed in the scope should not be tested without first seeking approval to have it added to the scope.
- The timeframe for the engagement.
- The objectives (also known as flags) of the penetration test. *For example*, an objective may be to gain domain administrator access or access to a certain system that holds sensitive information.
- Whether the test is full-knowledge, zero-knowledge, or partial-knowledge.

During a **full-knowledge penetration test** (also known as a whitebox penetration test), the penetration testers will be provided with complete documentation of the network. This may include descriptions of all systems, such as their IP addresses, the services running on them, and the security controls implemented. Full-knowledge penetration tests allow the penetration testers to spend more time attempting to exploit vulnerabilities and less time performing reconnaissance and discovery.

In **zero-knowledge penetration tests** (also known as blackbox penetration tests), the testers will need to start by performing reconnaissance tasks such as network and port scanning. Zero-knowledge penetration tests are usually more realistic but not as thorough as full-knowledge tests as the testers are more likely to miss weaknesses.
In partial-knowledge penetration tests (also known as greybox penetration tests), the testers are given some information about the target network.

SERIES: CYBERSECURITY

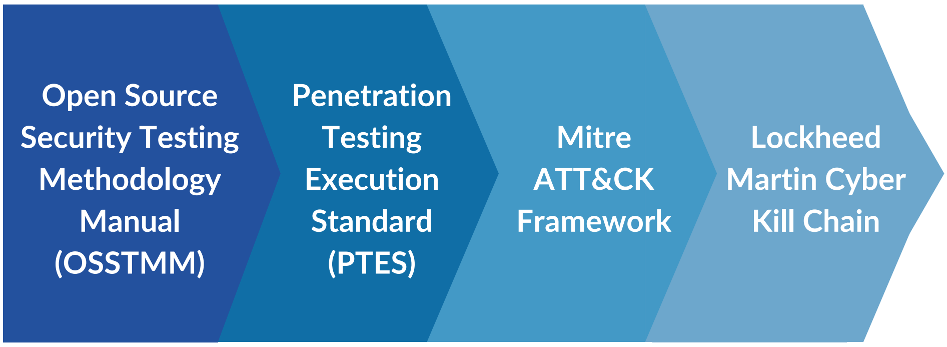
PENETRATION TESTING

CONTACT US

OUR METHODOLOGY

We follow a structured Penetration Testing methodology to ensure a comprehensive and systematic approach to identifying vulnerabilities and assessing the security of a system. While all engagements will vary based on the organisation or the nature of the test, there are many similarities in the approach.

We have integrated several industry recognised Penetration Testing frameworks into our methodology:



- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- Mitre ATT&CK Framework
- Lockheed Martin Cyber Kill Chain

EXTERNAL PENETRATION TESTING

WHAT IS AN EXTERNAL PENETRATION TEST?

An External Penetration Test is a simulated cyber attack on an organisation's external perimeter, which entails their network and systems. The goal of the test is to identify and demonstrate weaknesses in an organisation's public-facing infrastructure in order to identify and remediate those vulnerabilities. Penetration tests. may also be referred to as pen-testing, ethical hacking, red-teaming, offensive security, or adversarial simulations.

During an External Penetration Test, security professionals simulate the actions of real attackers by attempting to exploit weaknesses in the network and gain access to sensitive data or systems. They may use a variety of tools and techniques, such as scanning for open ports, attempting to guess passwords, or exploiting known vulnerabilities in software or operating systems.

The outcome of an External Penetration Test is a comprehensive report, detailing the findings of the engagement and recommendations for remediating any identified weaknesses. It's important to note that penetration tests are not meant to identify all weaknesses, as much of the engagement will be spent attempting to exploit the vulnerabilities that will have the greatest impact or allow the attacker to reach their goal the soonest. Therefore, a penetration test should not replace a robust, ongoing Vulnerability Management program.

SCOPING OF THE EXTERNAL PENETRATION TEST

A well-thought-out scope is imperative for the success External Penetration Test. Without developing and aligning on the scope, there is a risk of unauthorised testing of systems, wasted time and effort, or unexpected disruption (including permanent damage) to the organisation.

The scope of the test should include the following:

- The list of assets or targets in scope. This could include domain names, URLs, hostnames, or IP addresses. Anything not listed in the scope should not be tested without first seeking approval to have it added to the scope.
- The timeframe for the engagement.
- The objectives (also known as flags) of the penetration test. *For example*, an objective may be to gain domain administrator access or access to a certain system that holds sensitive information.
- Whether the test is full-knowledge, zero-knowledge, or partial-knowledge.

During a **full-knowledge penetration test** (also known as a whitebox penetration test), the penetration testers will be provided with complete documentation of the network. This may include descriptions of all systems, such as their IP addresses, the services running on them, and the security controls implemented. Full-knowledge penetration tests allow the penetration testers to spend more time attempting to exploit vulnerabilities and less time performing reconnaissance and discovery.

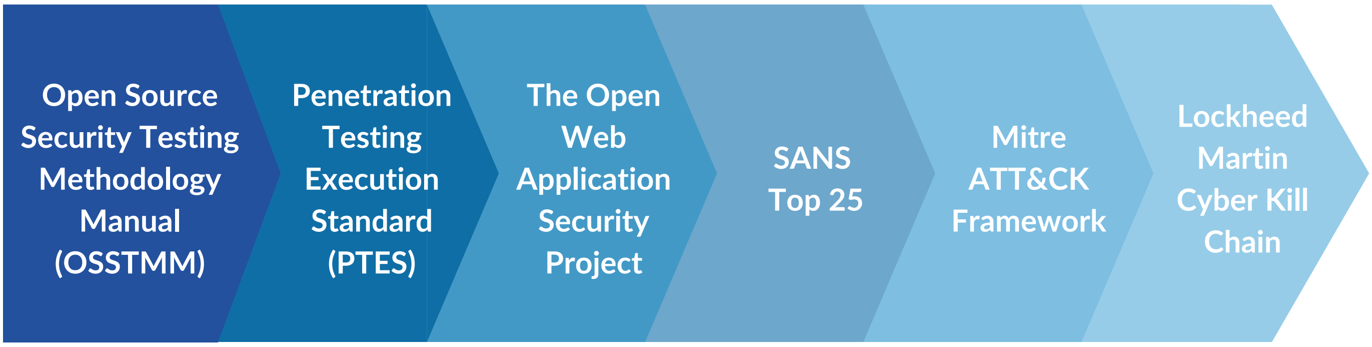
In **zero-knowledge penetration tests** (also known as blackbox penetration tests), the testers will need to start by performing reconnaissance tasks such as network and port scanning. Zero-knowledge penetration tests are usually more realistic but not as thorough as full-knowledge tests as the testers are more likely to miss weaknesses.
In partial-knowledge penetration tests (also known as greybox penetration tests), the testers are given some information about the target network.

PENETRATION TESTING

CONTACT US

OUR METHODOLOGY

We follow a structured Penetration Testing methodology to ensure a comprehensive and systematic approach to identifying vulnerabilities and assessing the security of a system. While all engagements will vary based on the organisation or the nature of the test, there are many similarities in the approach. **We have integrated several industry recognised Penetration Testing frameworks into our methodology:**



Open Source Security Testing Methodology Manual (OSSTMM)

Penetration Testing Execution Standard (PTES)

The Open Web Application Security Project

SANS Top 25

Mitre ATT&CK Framework

Lockheed Martin Cyber Kill Chain

OUR PROCESS

PLANNING & RECONNAISSANCE

- Understand the scope and objectives of the penetration test.
- Gather information about the target system, including IP addresses, domain names, network architecture, and application details.
- Conduct passive reconnaissance, such as searching for publicly available information, open ports, or DNS records.

THREAT MODELLING

- Identify potential attack vectors and prioritise them based on their risk and impact.
- Determine the level of access and knowledge available to the penetration tester (e.g., blackbox, graybox, or whitebox).
- Define the rules of engagement and establish clear boundaries for the test.

VULNERABILITY SCANNING

- Perform automated scans using specialised tools to identify common vulnerabilities like outdated software versions, misconfigurations, or weak encryption algorithms.
- Conduct network scanning to discover open ports, services, and potential entry point

SERIES: CYBERSECURITY

PENETRATION TESTING

CONTACT US

EXPLOITATION

- Attempt to exploit identified vulnerabilities manually or using exploit tools to gain unauthorised access, escalate privileges, or manipulate the target system.
- Exploit weaknesses in applications, networks, or other components to determine the extent of potential damage.

POST-EXPLOITATION

- Maintain access and conduct further exploration of the compromised system.
- Collect evidence of the successful exploitation for later reporting and analysis.
- Identify potential pivoting points for lateral movement within the network.

ANALYSIS AND REPORTING

- Evaluate the impact and severity of the vulnerabilities identified during the penetration test.
- Document all findings, including detailed descriptions, screenshots, and steps to reproduce the issues.
- Provide recommendations and best practices to address the identified vulnerabilities.
- Prepare a comprehensive report summarising the test, findings, and remediation suggestions.

REMEDIATION & VERIFICATION

- Analysis and Reporting.
- Evaluate the impact and severity of the vulnerabilities identified during the penetration test.
- Document all findings, including detailed descriptions, screenshots, and steps to reproduce the issues.
- Provide recommendations and best practices to address the identified vulnerabilities.
- Prepare a comprehensive report summarising the test, findings, and remediation suggestions.

ADDITIONAL SERVICES

- Wireless Penetration testing
- Physical Penetration Testing
- Simulations (Phishing, Social Engineering)
- Perimeter Assessment
- OSINT Assessment

Our team can meet with you to determine the best test and assessment to achieve the right outcomes for your organisation.