SECURITY TEST PLAN

Your Ally Against Cyber-Security Threats

PEN TESTING - STEP-BY-STEP

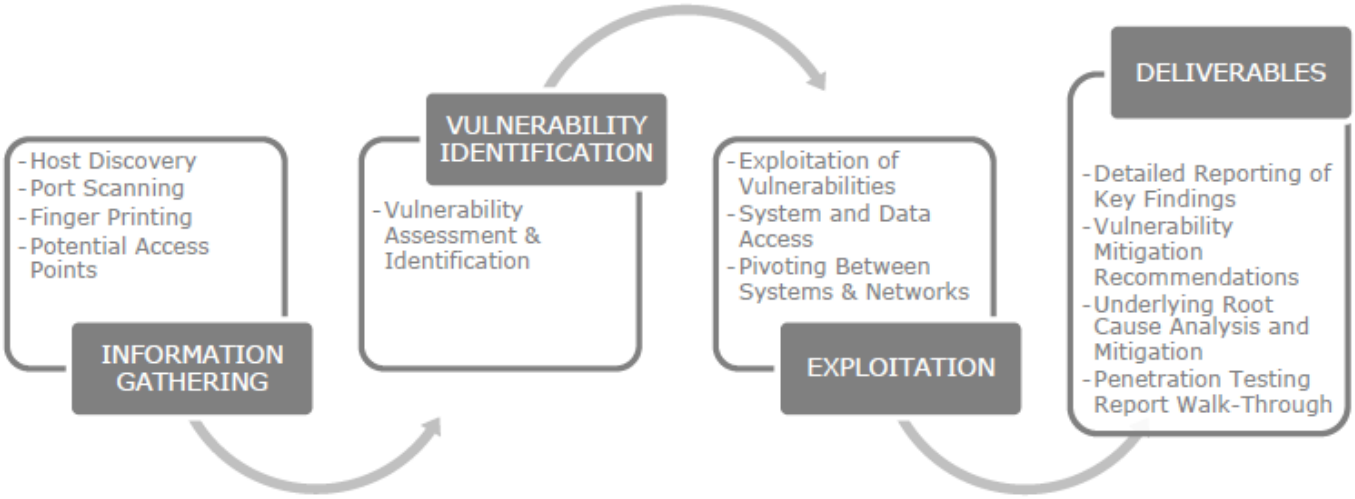


Table of Contents

The Need

With reports of breaches across Australia and around the world daily, it is important to be diligent about assessing your network, data and application security from the perspective of a malicious actor that is trying to compromise your systems and data.

The What, Why, Who and Types of Pen Testing: A penetration test is used to evaluate the security of an informational technology environment whether that be on-premise, cloud or hybrid, or testing applications, systems, networks or human controls.

The goals of penetration testing are to:

I. Proactively identify vulnerabilities that leave the organisation exposed to malicious actions;
II. Actively exploit vulnerable systems to prove that the identified vulnerability actually poses a risk to the organisation; and
III. Prove access gained to systems via exploitation leads to the exposure of sensitive or personal data.

Outcomes of a successful penetration testing program include identification of vulnerabilities, crosschecking of the effectiveness of existing security controls to protect against identified exposure, compliance regulation and the ability to prioritise risks, and manage mitigation and remediation of those risks.

Choose the Right Pen Test for your Organisation

There are a variety of tests within the penetration testing suite. Most of these can vary in scale and scope greatly and use a large variety of tools, techniques and applicable skillsets.

Types of Penetration Tests

External Infrastructure Penetration Test The penetration tester will identify vulnerabilities in the external network and Internet exposed systems to try and gain control or "own" a system using a series of tools that breach Internet exposed systems and data or the perimeter of the network.

Internal Infrastructure Penetration Test This type of test takes place behind your firewall and simulates an environment where a malicious actor is already within your network. This type of test starts with the tester given the mandate to compromise systems and credentials. They then attempt to gain unauthorised access to systems, devices and data, then escalate privileges to access higher levels of confidential information.

Web Application Penetration Test This type of test simulates an attack on your company's website or published web applications. Testing is performed against web applications such as customer/user portals, support portals and employee intranets. Testing is generally performed authenticated and unauthenticated, to simulate both attacks where a malicious actor has no prior access and also where credentials have already been compromised by other means. Web application penetration testing requires a significant amount of manual effort.

Mobile Application Penetration Test This type of test finds vulnerabilities in this ever-evolving remote technology. The goal is to review the mobile application, infrastructure and Application Programming Interfaces (APIs) to investigate insecure development practices, authentication and access controls, settings and configuration, storage and the APIs the mobile application uses to communicate with backend services and data stores.

Scope and Research:
Understanding the environment, scope and determining an effective methodology is critical to effective penetration testing. With a large amount of options, plus the blend of automated versus manual testing, creates a need for a defined testing structure and a clear picture of the environment boundaries, gained through extensive research.

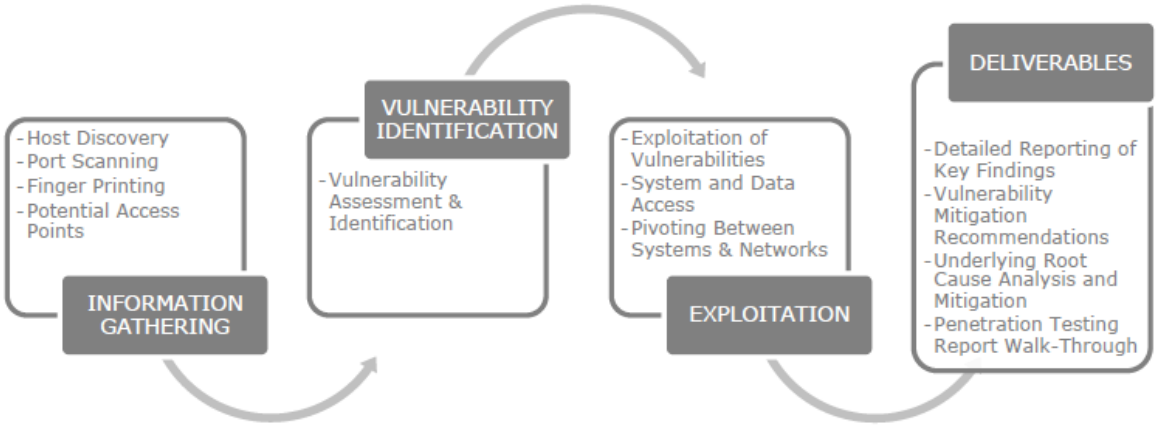
Testing Objectives: The objective of security testing of the product is to:

- define security goals through understanding security requirements of the applications;
- identify the security threats;
- validate that the security controls operate as expected;
- eliminate the impact of security issues on the safety and integrity of the product;
- guarantee that the product will function correctly under malicious attacks;

Reporting and Mitigation:
Finally, when a testing phase is completed there is a required need for reporting and mitigation strategies. Interpreting complex vulnerability and exploit data and its potential impact on the business being tested, requires analysis and commercial translation, as well as effective mitigation strategies to address the identified vulnerabilities but also understanding root cause mitigation to reduce vulnerabilities in future.

Penetration Testing: Step by Step

BitSecure's Pen-Tester will commence a penetration testing engagement with limited knowledge about the target. Using automated tools and scripts, along with manual testing techniques, the security team will identify targets and areas of potential vulnerability which may lead to exploitation, and the impact this may have on the target application, systems or infrastructure. Based on this information, a structured test plan is used to execute the penetration test. The output of this exercise is a detailed report, and this is presented to the client.



Penetration testing is going to be done in two ways: *automatically* and *manually*.

Penetration testing is done manually using the procedures developed for a particular application and type of threat

OR

automatically using:

a. web application vulnerability scanners, binary analysis tools,
b. proxy tools.

The main attacks performed during penetration testing are listed below:

- Cross site scripting;
- SQL injection;
- Server misconfiguration;
- Form manipulation;
- Cookies poisoning;
- Platforms vulnerabilities;
- Weak session management;
- Buffer overflows;
- Command injection.

Roles & Responsibilities

The team members will be performing the following roles:

Role	Responsibilities	Contact information
✓**Team Lead** ✓**Team Designer** ✓**Test Engineer**	• Test process setting up and adjusting • Security test plan creation • Test strategy authoring • Test activities tracking • Giving conclusion about the quality • Security models creation • Test cases and test suites creation and updating • Running test cases • Defects authoring • Test results analysis • Test reports creation	info@bitsecure.com.au

Methodology

Dependencies (dependency testing): The dependency type of testing supposes that the 3-rd part modules (or libraries, code, etc.) are tested. During this procedure a test engineer verifies whether:

- An application has vulnerabilities of (3-rd part) components it uses;
- Modules that provide security services fail;
- There are security vulnerabilities in the file system;
- There are security vulnerabilities in the registry.

Client-side testing: During this type of testing a test engineer works with the user interface exclusively. He/she tries to enter incorrect input sequences, like:

- Escape characters;
- Long strings;
- Parts of some code in a programming language;
- Incorrect input values;
- Testing for error handling;

- Perform cross site scripting.

Exposed design vulnerabilities (design testing): The design vulnerabilities can be caused by an immature design or development process.

- On this stage the next issues are controlled:
- Open unsecured ports;
- Insecure default values and accounts;
- Debug code intertwined with implementation code;

Exposed implementation vulnerabilities (implementation testing): This type of vulnerabilities may occur because of implementation errors:

- Developers who develop only their modules could unintentionally reveal data: for example, incorrect validation;
- Time-of-check-to-time-of-use issues.

Test Results

Test results are sent to all interested parties and may contain:

- List of features which were tested;
- List of vulnerabilities found during testing;
- List of executed test cases with their statuses;
- List of risks which were defined during testing;
- Conclusion about the quality of the product.

List of Deliverables

- List of Vulnerabilities (Included in the Test Report)
- Test Report