

TESTING

REPORTING

SECURITY
REPORT

Manual Penetration Testing

By mitigating risks you stay in control

A Penetration test

– is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities.

The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit.

Experienced ImmuneSecurity security testers offer the following services:

- Review of Network Design
- Review of Web Application Design
- Network Layer Attacks
- Pre-investigation and Web Application Layer Testing
- WiFi Testing
- Risks

Penetration testing can be an invaluable technique to any organization's information security program. Basic white box penetration testing is often done as a fully automated inexpensive process. However, black box penetration testing is a labor-intensive activity and requires expertise to minimize the risk to targeted systems. At a minimum, it may slow the organization's networks response time due to network scanning and vulnerability scanning.

Risks from penetration tests are mitigated by the use of experienced penetration testers, but it can never be fully eliminated.



Black Box vs. White Box

Two Levels of Testing

The most common difference is the amount of knowledge of the implementation details of the system being tested that are available to the testers. Black box testing assumes no prior knowledge of the infrastructure to be tested. The testers must first determine the location and extent of the systems before commencing their analysis. At the other end of the spectrum, white box testing provides the testers with complete knowledge of the infrastructure to be tested, often including network diagrams, source code, and IP addressing information. There are also several variations in between, known as grey box tests.

Penetration tests may also be described as “full disclosure”, “partial disclosure” or “blind” tests based on the amount of information provided to the testing party.

Black box testing simulates an attack from someone who is unfamiliar with the system. White box testing simulates what might happen during an “inside job” or after a “leak” of sensitive information, where the attacker has access to source code, network layouts, and possibly even some passwords.

Web Application Penetration Test Application Vulnerability and Risks

Web application penetration testing refers to a set of services used to detect various security issues with web applications.

Web Application Penetration Testing services help identify vulnerabilities and risks in web applications, including:

Known vulnerabilities in COTS applications

Technical vulnerabilities: URL manipulation, SQL injection, cross site scripting, back-end authentication, password in memory, session hijacking, buffer overflow, web server configuration, credential management, Click-jacking etc.

Business logic errors: Day-to-Day threat analysis, unauthorized logins, personal information modification, pricelist modification, unauthorized funds transfer, breach of customer trust etc.

OSSTMM

Open Source Security Testing Methodology Manual

The Open Source Security Testing Methodology Manual is a peer-reviewed methodology for performing security tests and metrics. The OSSTMM test cases are divided into five channels which collectively test: information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases.

The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test, and how to measure the results. OSSTMM is also known for its Rules of Engagement which define for both the tester and the client how the test needs to properly run starting from denying false advertising from testers to how the client can expect to receive the report. New tests for international best practices, laws, regulations, and ethical concerns are regularly updated and added to our tool-box.



Manual Penetration Tests offers the extra level of security

Contact Your local sales office to hear how we can assess the level of security in your IT infrastructure and get inspiration from what we have done with other customers in all industries.

More information:

WWW.IMMUNESecurity.COM

Denmark

Corporate Headquarter
ImmuneSecurity A/S
Aldersrogade 6A
DK-2100 Copenhagen O
Denmark

Phone: +45 70 266 286

Fax : +45 70 266 287

E-mail: info@immunesecurity.com

Sweden

ImmuneSecurity
Solna Business Park
Svetsarvägen 15
SE-171 41 Solna
Sweden

Phone: +46 85 052 1230

Fax : +45 70 266 287

E-mail: info@immunesecurity.com

France (Southern Europe)

ImmuneSecurity
121 bis, rue de la Pompe
FR-75116 Paris
France

Phone: +33 1 58 36 08 40

Fax : +45 70 266 287

E-mail: info@immunesecurity.com

BENELUX

ImmuneSecurity
Baronieweg 12
5321 JW Hedel
The Netherlands

Phone: +31 73 5997121

Fax : +45 70 266 287

E-mail: info@immunesecurity.com