STARTECH
Information Security

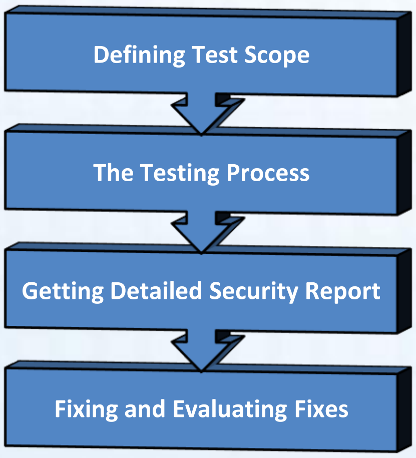
Penetration Testing

What is Penetration Testing?

Penetration testing is a process in which a certain asset of an organization is being analyzed and tested for security vulnerabilities. The purpose of the test is to identify actual vulnerabilities that could damage the security of the organization, and manage ways to solve them.

Whether your organization contains an internal computer network or you are developing a mobile application, security should be taken into consideration. Penetration testing is a cost-effective test method for finding the most critical vulnerabilities within your organization.

Our Penetration Test Process



Defining Test Scope

The Testing Process

Getting Detailed Security Report

Fixing and Evaluating Fixes

Penetration Testing - Should I Use It?

Find out what are the benefits from conducting a penetration test:

1. **Secure your organization.** As mentioned, the purpose of the penetration testing is to make your organization more secure.
2. **Meet regulatory standards.** Security standards such as PCI-DSS or government standards require organizations to conduct penetration testing to keep a high level of security.
3. **Get a clear status about the security of your organization.** Do you know what is the status of your security? Even if you did implement some security measures, can you be certain that they are actually covering you from attacks? Penetration testing is the way to test it.
4. **Prevent disasters**. An insecure organization can be subject to:
   - Defacement
   - Confidential information compromise
   - Damage to the image and reputation
   - Lawsuits
5. **Improve your business partnerships.** Would anyone be interested in making business with an insecure organization? Would you? Serious organizations care about their security, and will prefer to make business with similar companies. In order to have added value in any business interaction you have, utilize the process of penetration testing.
6. **Give added value to your developers and improve future projects**. During the process of penetration testing and discovering security vulnerabilities, your developers will gain new security knowledge. This knowledge is practical and relevant to their code, which is a great added value to the team. Furthermore, your development team will use the acquired knowledge for future projects, keeping your organization secured.

What Can Be Tested?

The following can be tested using Penetration Testing:

- Applications
  - **Software / Desktop Applications**
  - **Websites**
  - **Mobile Applications**

- Networks
  - **External Network**
  - **Internal Network**
  - **Wireless Network**

Black, White and Gray Box : Three Types of Penetration Tests

Black, White and Gray box defines the level of knowledge given prior to the testing.

- **Black box penetration testing** mimics an external attacker who is trying to attack the organization without any prior knowledge about the system.

- **White box penetration testing** is a test conducted with full knowledge about the tested system. Prior and during the tests, access to the source code of the system is granted, along with all the documentation about the system.

- **Gray box penetration testing** is a mixture between the last two. The information about the system while conducting the test is limited. For example, access to the system can be granted, but not to the source code.

Which type of test is right for you? the answer is different per company and project. We at Startech have the knowledge and experience to give you the best answer. Contact us and we will build the best security solution for your needs.

Contact us today to get your organization secured

for more information, contact us :

- Website: www.startechsecurity.com
- Email : info@startechsecurity.com
- Phone : +972-9-9708610