**Penetration Testing for Web Applications**

Penetration testing, commonly known as pentesting or security testing is the process by which organizations test their applications by simulating an attack to identify vulnerabilities and security loopholes in your web applications. The aim of a penetration test is to find out what information can be accessed by a real hacker in case of a real attack on a system and to fix the identified security weaknesses.

**What are the Benefits?**

By carrying out a penetration test, a pentester aims to achieve the following objectives:

* To determine the possibility of specific attack vectors
* To determine a combination of high and low risk vulnerabilities exploited in a specific sequence
* To determine vulnerabilities that cannot be detected easily by automated vulnerability scanning software
* To measure the potential impact of real attacks on the business operations
* To measure the ability of automated network software to detect attacks and respond to them
* To ensure that all data security compliance protocols are being met, particularly in the Payment Card Industry
* To report obtained evidence for ensuring satisfactory measures in improving organizational information by investing more in technology and security staff

A successful web application penetration test requires you to hire one or a team of skilled hackers, otherwise known as ethical hackers or penetration testers. They are not provided any access to source code and are asked to attempt an attack to access your system.

**Why is a Penetration Test Important for Web Applications?**

Penetration Tests are important for a wide number of reasons, the basic one being that it allows you to discover the loopholes in your information security systems. Other than that, regular penetration tests are also important because,

* They help the information security staff gain experience to deal with a potential incident of breach. If conducted without prior notice, it can help determine whether your security policies are in effect or not, and how much awareness and training is needed by organizational employees to ensure security and safety of organizational data and information.
* They allow you to discover the flaws in your security policy, and the areas where it lacks. Some organizational policies, for instance, focus on how to prevent and detect attacks but have no proper stance on dislodging an ongoing attack. A penetration test may allow you to discover that due to an incomplete policy, your security personnel could not remove the hacker from your organizational system before he inflicted enough damage.
* Penetration testing reports allow you to prioritize your areas of security investment by identifying the weakest and most risky links in your web applications.
* Penetration testing reports allow web application developers identify their mistakes and train them for perfection. When developers see how the hacker was able to break into their application, they will improve their mistakes and avoid similar ones to build stronger and securer web applications.

**How to Build an Effective Web Application Pentesting Methodology?**

It was not until 2010 that a standard was developed for a widely accepted penetration testing methodology. In 2010, a Penetration Testing Execution Standard (PTES) was developed which is divided into the following sections:

* Pre-engagement Interactions
* Intelligence Gathering
* Threat Modeling
* Vulnerability Analysis
* Exploitation
* Post Exploitation
* Reporting

To better understand what makes an effective penetration testing methodology, and to make it easier for organizations to follow a standard way of carrying out penetration testing, we will provide a brief elaboration to each of these sections.

**Pre-engagement Interactions**

When hiring a penetration tester, you need to choose a reliable individual or team as they will have access to your organization’s sensitive information. Furthermore, you need to be clear with your requirements and to convey them to the penetration tester. Some of the concerns that must be catered for are:

* Scope of the Penetration test. Would you want it to be done on a particular business area or your entire business? What is included and what is not?
* Schedule of the Penetration test. At what time would the test be performed and what will be the duration while the business is still running?
* Whitebox or Blackbox test. In a blackbox test, the tester is not given any information, just like an outsider. In a whitebox test, a tester is given basic access or information to start with.
* Communication channels. Contacts of all involved individuals and parties must be provided before the start of the pentest process to avoid unintended consequences.

**Intelligence Gathering**

The penetration testing provider prepares to plan its attack. To make it successful, an experienced tester will have clear idea of what is within scope and what is not. However, if your provider is not looking at each and every area of scope to ferret out information every possible way, you should know that they are not doing their job correctly.

**Threat Modelling**

After gathering relevant information, a pentesting methodology works upon building up your company profile along with its assets. The penetration testing provider will work to look for assets with the highest value and could include organizational policies and procedures, customer data, employee information, etc.

**Vulnerability Analysis**

For ensuring that desired outcomes are met, a good methodology for web application penetration testing will clearly define project scope. With clear target assets in line, the penetration testing provider will determine how to enter and exploit them. All vulnerabilities within the given assets are identified and assessed for extent. Their weakness level is determined and it is also revealed what sensitive information they might be exposing.

**Exploitation and Post Exploitation**

Once the entry points and related vulnerabilities are identified, the penetration tester then simulates a real attack, as would a real hacker do. After gaining access to the system, the will try to remain undetected, and also gain more access to the system to extract maximum sensitive information.

In the post-exploitation phase, the penetration tester assesses the value of compromised system and identifies its potential to be exploited for later use.

**Reporting**

A good penetration testing methodology for web application cannot be complete without good reporting. A report is a true essence of a penetration test that provides detailed account of exploitations and vulnerabilities in an organization to work upon.

Penetration testing report must include high-level recommendations for problems with the web applications, how the exploitations were carried out and what was the risk level of the discovered vulnerabilities.

If your organization has not yet undergone regular penetration tests for testing the security of its web applications and the organizational systems as a whole, it must do so now. The initial penetration test results will be eye-opening as it may highlight a number of vulnerabilities you were least likely expecting to be there.