***PERFORMANCE TESTING:***

Performance Testing is performed to evaluate the performance of components of a particular system under a particular workload. During this testing, system components are monitored to verify the stability of the system under test. Performance Testing is the type of Non-Functional Testing.

Performance testing is a testing measure that evaluates the speed, responsiveness and stability of a computer, network, software program or device under a workload. Organizations will run performance tests to identify performance-related bottlenecks.

### **Why use performance testing?**

* For testing vendor claims to verify that a system meets the specifications claimed by its manufacturer or vendor. The process can compare two or more devices or programs.
* For providing information to stakeholders to inform project stakeholders about application performance updates surrounding speed, stability and scalability.
* For avoiding gaining a bad reputation, as an application released without performance testing might lead it to run poorly, which can lead to negative word of mouth.
* For comparing two or more systems to enable an organization to compare software speed, responsiveness and stability.

**Performance testing challenges:**

Some challenges within performance testing are as follows:

* Some tools may only support web applications.
* Free variants of tools may not work as well as paid variants, and some paid tools may be expensive.
* Tools may have limited compatibility.
* It can be difficult for some tools to test complex applications.
* Organizations should watch out for performance bottlenecks in the following:
  + 1. CPU.
    2. Memory.
    3. Network utilization.
    4. Disk usage.
    5. OS limitations.
* Other common performance problems may include the following:
  + 1. Long load times.
    2. Long response times.
    3. Insufficient hardware resources.
    4. Poor scalability.

**ATTRIBUTES OF PERFORMANCE TESTING:**

* ***Speed***- It determines whether the software product responds rapidly.
* ***Scalability***- It determines amount of load the software product can handle at a time.
* ***Stability***- It determines whether the software product is stable in case of varying workloads.
* ***Reliability***- It determines whether the software product is secure or not.

**Types of Performance Testing:**

**1. Load testing:** It checks the product’s ability to perform under anticipated user loads. The objective is to identify performance congestion before the software product is launched in market.

**2. Stress testing:** It involves testing a product under extreme workloads to see whether it handles high traffic or not. The objective is to identify the breaking point of a software product.

**3. Endurance/Soak testing:** It is performed to ensure the software can handle the expected load over a long period of time.

**4. Spike testing:** It tests the product’s reaction to sudden large spikes in the load generated by users.

**5. Volume testing:** In volume testing large number of data is saved in a database and the overall software system’s behavior is observed. The objective is to check product’s performance under varying database volumes.

**6. Scalability testing:** In scalability testing, software application’s effectiveness is determined in scaling up to support an increase in user load. It helps in planning capacity addition to your software system.

**7. Capacity testing:** Capacity testing is similar to stress testing in that it tests traffic loads based on the number of users but differs in the amount. Capacity testing looks at whether a software application or environment can handle the amount of traffic it was specifically designed to handle.

**8. Production Activity testing:** The production activity test ensures that the system can handle the load related to the number of transactions/hour expected in production. This test will load and validate the behaviour of the business components within the database. Two main requirements for this type of test are the number of transactions/hour per user journey and the appropriate think times.

**TOOLS OF PERFORMANCE TESTING:**

We have various types of performance testing tools available in the market; some of the most used performance (load) testing tools are as follows:

* Apache JMeter
* LoadRunner[HP]
* LoadNinja
* WebLOAD
* LoadComplete
* NeoLoad
* LoadView

**Apache JMeter:**

It is used to test the performance of both static and dynamic resources and dynamic web applications. This tool is completely designed on the JAVA application to load the functional test behavior and measure the performance of the application. It is an open-source tool that facilitates users or developers to use the source code for the development of other applications.

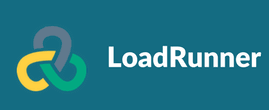
It can be used to reproduce the huge load on a server, object, or network, group of servers to test its power, or to explore the complete performance in multiple load types. Previously it was used to test the web application, but now it is expanded to other test functions also.



**LoadRunner:**

It is one of the most powerful tools of performance testing, which is used to support the performance testing for the extensive range of protocols, number of technologies, and application environments.

It quickly identifies the most common causes of performance issues. And also accurately predict the application scalability and capacity.



**LoadNinja:**

LoadNinja is powered by SmartBear. With the help of this tool, product teams and the test engineer will construct the application with more concentration rather than writing the load testing scripts. We can keep track of user interactions, find the performance issues directly, and debug them in real-time. It will change the load emulators with the real browsers.



**WebLOAD:**

WebLOAD testing tool is used to test the test application with the help of load testing, performance testing, and stress testing. For the authentication of web and mobile applications, the WebLOAD tool combines the performance, scalability, and integrity as a single process. It will support the multi-protocols such as HTTPS, XML, HTTP, and so on, which helps us to control the load of the large number of users.



**LoadComplete:**

It is another performance (load) testing tool. It is used to create and run automated tests for web services and web servers. It supports all types of browsers, web services. It will check our web server's performance when we have encountered a huge load. With the help of this tool, we can observe multiple server metrics such as CPU usage, throughout the test runs.



**NeoLoad:**

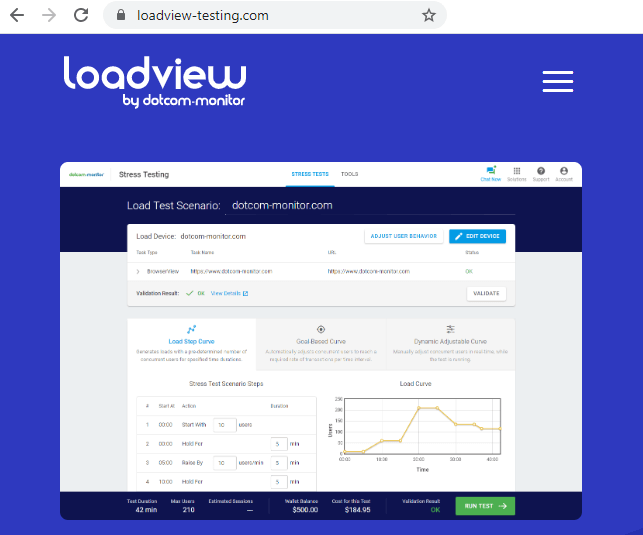
Neotys develop a testing tool which is called NeoLoad. The NeoLoad is used to test the performance test scenarios. With the help of NeoLoad, we can find the bottleneck areas in the web and the mobile app development process.

The NeoLoad testing tool is faster as compared to traditional tools. It will support the complete range of web, mobile, and packaged applications, like SAP, Oracle, Salesforce, and so on, which cover all our testing needs. And also share and manage the test resources.

Performance testing tools

**LoadView:**

The By dotcom-monitor powers it. With the help of this tool, we can display the real performance of the application. It is used to perform load testing in the real browsers that will give the correct data. It is a cloud-based tool that can be deployed in less time.



***SECURITY TESTING:***

* Security Testing is a type of Software Testing that uncovers vulnerabilities of the system and determines that the data and resources of the system are protected from possible intruders. It ensures that the software system and application are free from any threats or risks that can cause a loss.
* Security testing of any system is focused on finding all possible loopholes and weaknesses of the system which might result in the loss of information or repute of the organization.
* Security testing is a type of software testing that focuses on evaluating the security of a system or application.
* The goal of security testing is to identify vulnerabilities and potential threats, and to ensure that the system is protected against unauthorized access, data breaches, and other security-related issues.

**Goal of Security Testing:**

* To identify the threats in the system.
* To measure the potential vulnerabilities of the system.
* To help in detecting every possible security risks in the system.
* To help developers in fixing the security problems through coding.

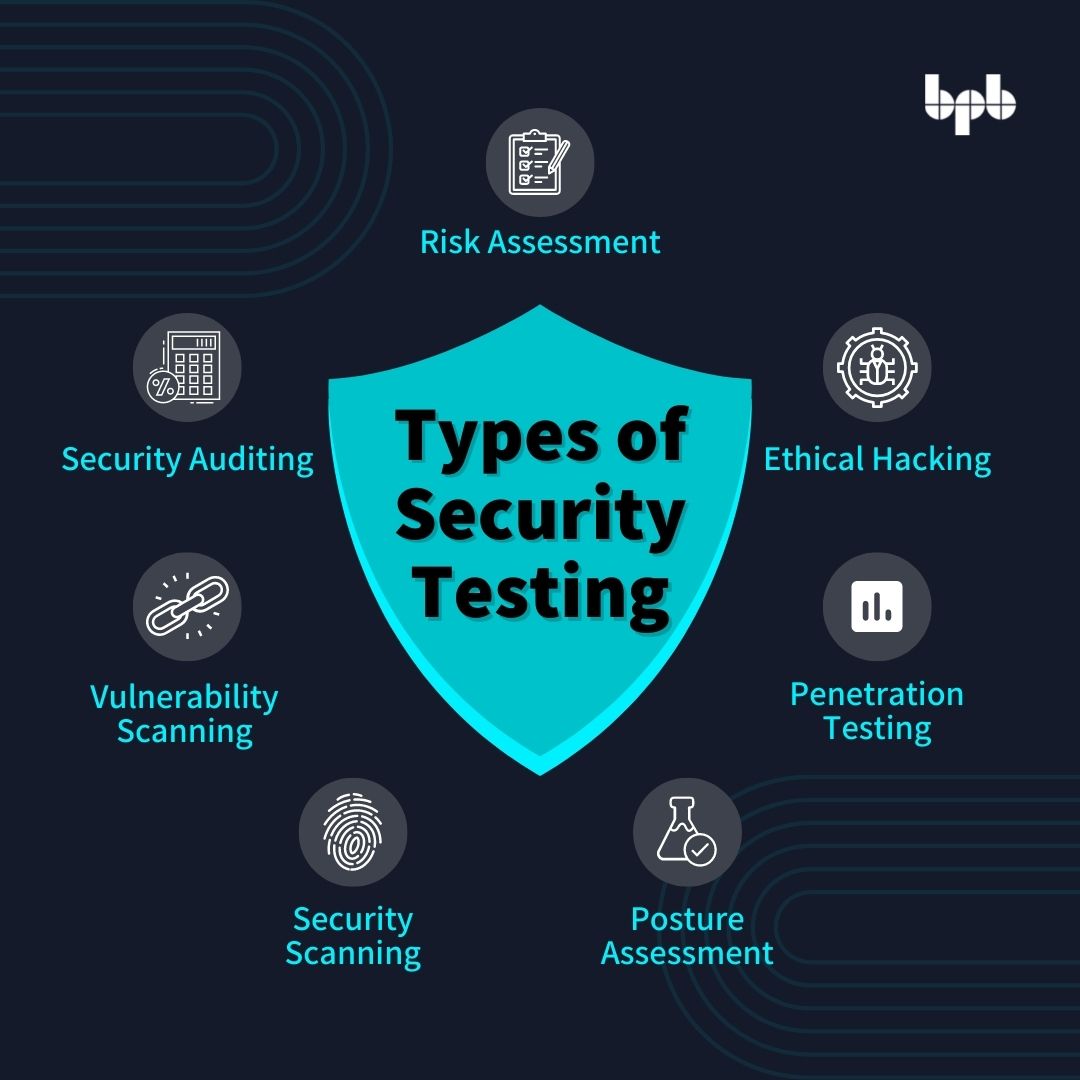
**Principle of Security Testing:**

* Confidentiality
* Integrity
* Authentication
* Authorization
* Availability
* Non-repudiation

**Major Focus Areas in Security Testing:**

1. Network Security
2. System Software Security
3. Client-side Application Security
4. Server-side Application Security
5. Authentication and Authorization
6. Network and Infrastructure Security
7. Database Security
8. Application Security
9. Data Security
10. Compliance
11. Cloud Security

**TYPES OF SECURITY TESTING:**



*1. Vulnerability Scanning:*

Vulnerability scanning is performed with the help of automated software to scan a system to detect the known vulnerability patterns.

*2. Security Scanning:*

Security scanning is the identification of network and system weaknesses. Later on it provides solutions for reducing these defects or risks. Security scanning can be carried out in both manual and automated ways.

*3. Penetration Testing:*

Penetration testing is the simulation of the attack from a malicious hacker. It includes an analysis of a particular system to examine for potential vulnerabilities from a malicious hacker that attempts to hack the system.

*4. Risk Assessment:*

In risk assessment testing security risks observed in the organization are analyzed. Risks are classified into three categories i.e., low, medium and high. This testing endorses controls and measures to minimize the risk.

*5. Security Auditing:*

Security auditing is an internal inspection of applications and operating systems for security defects. An audit can also be carried out via line-by-line checking of code.

*6. Ethical Hacking:*

Ethical hacking is different from malicious hacking. The purpose of ethical hacking is to expose security flaws in the organization’s system.

*7. Posture Assessment:*

It combines security scanning, ethical hacking and risk assessments to provide an overall security posture of an

*8. Application security testing:*

Application security testing is a type of testing that focuses on identifying vulnerabilities in the application itself. It includes testing the application’s code, configuration, and dependencies to identify any potential vulnerabilities.

*9. Network security testing:*

Network security testing is a type of testing that focuses on identifying vulnerabilities in the network infrastructure. It includes testing firewalls, routers, and other network devices to identify potential vulnerabilities.

*10. Social engineering testing:*

Social engineering testing is a type of testing that simulates phishing, baiting, and other types of social engineering attacks to identify vulnerabilities in the system’s human element.

**TOOLS USED FOR SECURITY TESTING:**

**1. Invicti-**It is a web vulnerability management system. It is an automatic, deadly accurate, and easy-to-use web application security scanner. It is used to automatically identify security issues such as Cross-Site Scripting (XSS) and in websites, web applications, and web services.

**2. Acunetix-**It is an easy yet powerful solution to secure your website, web applications and APIs. It detects over 4500 web vulnerabilities such as Cross Site Scripting (XSS), SQL injection, etc.,

**3. Zed Attack Proxy (ZAP)-** Zed Attack Proxy popularly known as ZAP is an open source security testing tool for a web application which was developed by OWASP (Open Web Application Security Project). It runs on all operating systems that support Java 8. It is one of the world’s most popular free security tools and is actively maintained by volunteers.

**4. Wfuzz-**This is a web application security fuzzer tool which is developed in Python. It doesn’t come with GUI Interface, so security testers who want to use this tool have to work on command line interface. This tool is designed for bruteforcing web applications.

**5. Wapiti**-It is a web application vulnerability scanner. It allows us to audit the security of websites or web applications. It performs black box scans of the web application by crawling the web pages of the deployed webapp, looking for scripts and forms where it can inject data.

**6. W3af-**It is a web application attack and audit framework that is developed using pythont helps developers and penetration testers identify and exploit vulnerabilities in web applications.It supports authentication types such as HTTP basic authentication, NTLM authentication, Form authentication, Cookie authentication.

**7. Vega-**This is a free and open source web security scanner and web security testing platform to test the security of web applications. It is written in Java and has a well designed graphical user interface (GUI) runs on Linux, OS X, and Windows.

**8. SQLMap-**This is an open source penetration testing tool. It allows us to automate the process of detecting and exploiting SQL injection vulnerabilities in a website’s database. It comes with a powerful detection engine and many features to detect vulnerabilities.

**9. SonarQube-**It is an open source security testing tool developed by SonarSource. It is an automatic code review tool to detect bugs, vulnerabilities and code smells in your code.

**10. Nogotofail-**It is a network security testing tool (network vulnerability scanner tool) designed to help developers and penetration testers. As a network security scanner, it includes testing for common SSL certificate verification issues, HTTPS and TLS/SSL library bugs, SSL and STARTTLS stripping issues, cleartext issues, and more.

**11. Grabber-**It is an open source web application scanner that detects some kind of vulnerabilities in a website or web applications. It is designed to scan small websites such as forums and personal websites. It is absolutely not for big application. It will take a too long time and flood your network when you use it for a big application. It doesn’t come with GUI interface. It was developed in Python.

**12. Arachni-**This is an open source security testing tool aimed towards helping penetration testers and administrators evaluate the security of web applications. It is a feature-full, modular, high-performance Ruby framework. It supports all major operating systems such as MS Windows, Mac OS X, and Linux.

**13. Skipfish-**It is an active web application security testing tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. It is available for Linux, Mac OS X, and Windows.

**14. Ratproxy-**This is an open source security testing tool. It is a semi-automated, largely passive web application security audit tool. Ratproxy assessments take little bandwidth or time to run and proceed in an intuitive, distraction-free manner.