Unit 5

Penetration Testing and Analysis

Computer Science and Engineering Department@SoEEC
SQAT(CSE5310)

Outline:

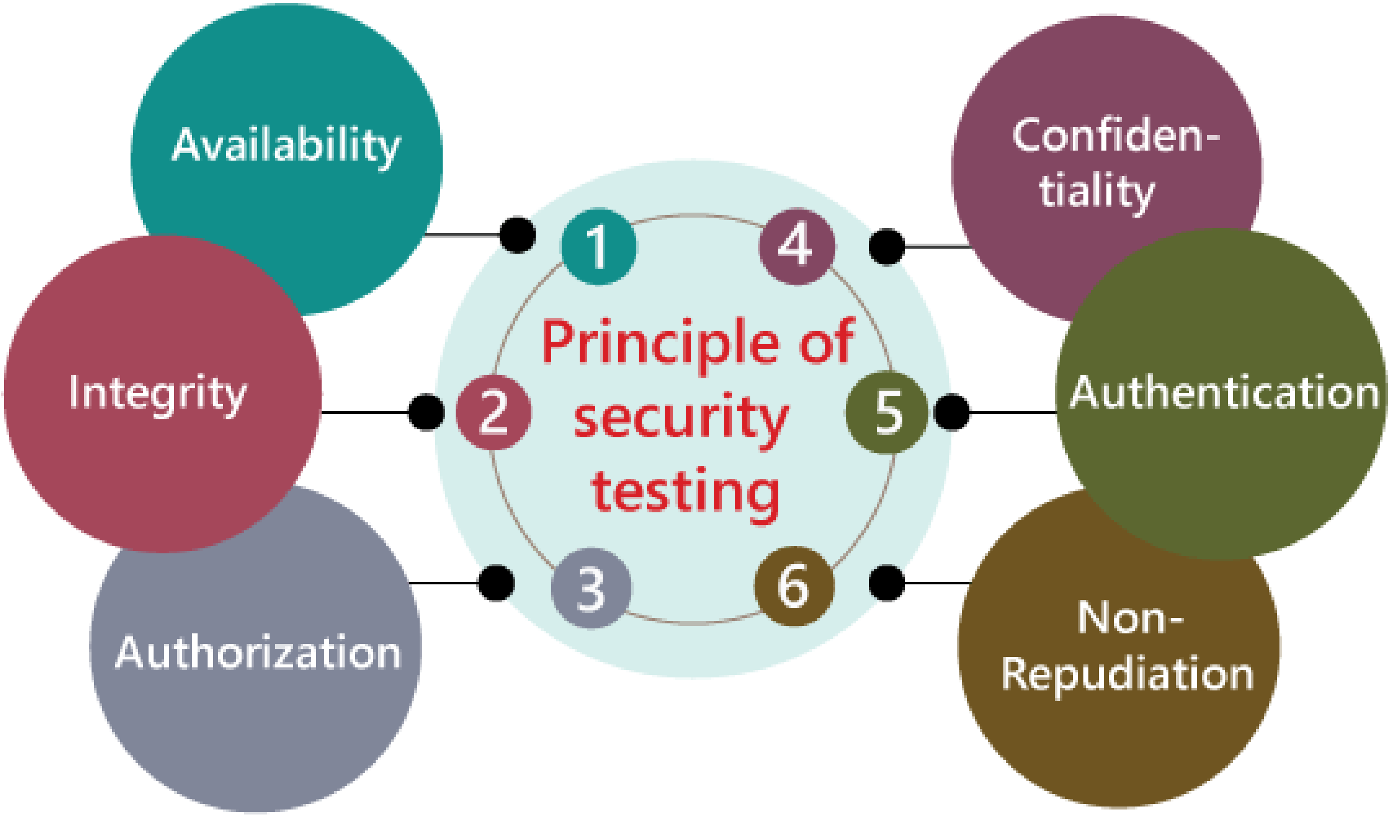
- Web Security, Quality vs Security.
- Penetration testing and static analysis for security.
- Web security testing techniques and tools.
- A case study on penetration testing.

Security Testing

What is security testing?

- Security testing is an integral part of software testing, which is used to discover the weaknesses, risks, or threats in the software application and also help us to stop the nasty attack from the outsiders and make sure the security of our software applications.
- The primary objective of security testing is to find all the potential ambiguities and vulnerabilities of the application so that the software does not stop working. If we perform security testing, then it helps us to identify all the possible security threats and also help the programmer to fix those errors.
- It is a testing procedure, which is used to define that the data will be safe and also continue the working process of the software.

Principle of Security testing



Availability

In this, the data must be retained by an official person, and they also guarantee that the data and statement services will be ready to use whenever we need them.

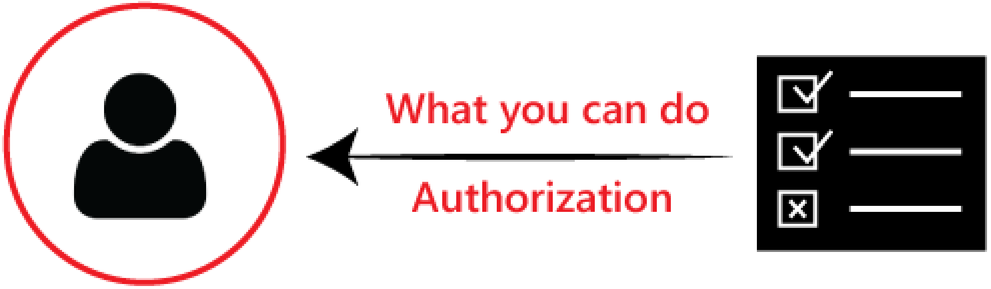
Integrity

In this, we will secure those data which have been changed by the unofficial person. The primary objective of integrity is to permit the receiver to control the data that is given by the system.

The integrity systems regularly use some similar fundamental approaches as confidentiality structures. Still, they generally include the data for the communication to create the source of an algorithmic check rather than encrypting all of the communication. And also verify that correct data is conveyed from one application to another.

Authorization

It is the process of defining that a client is permitted to perform an action and also receive the services. An example of authorization is Access control.



Confidentiality

It is a security process that protracts the leak of the data from the outsider's because it is the only way where we can make sure the security of our data.

Authentication

The authentication process comprises confirming the individuality of a person, tracing the source of a product that is necessary to allow access to the private information or the system.

Who you are
Authentication

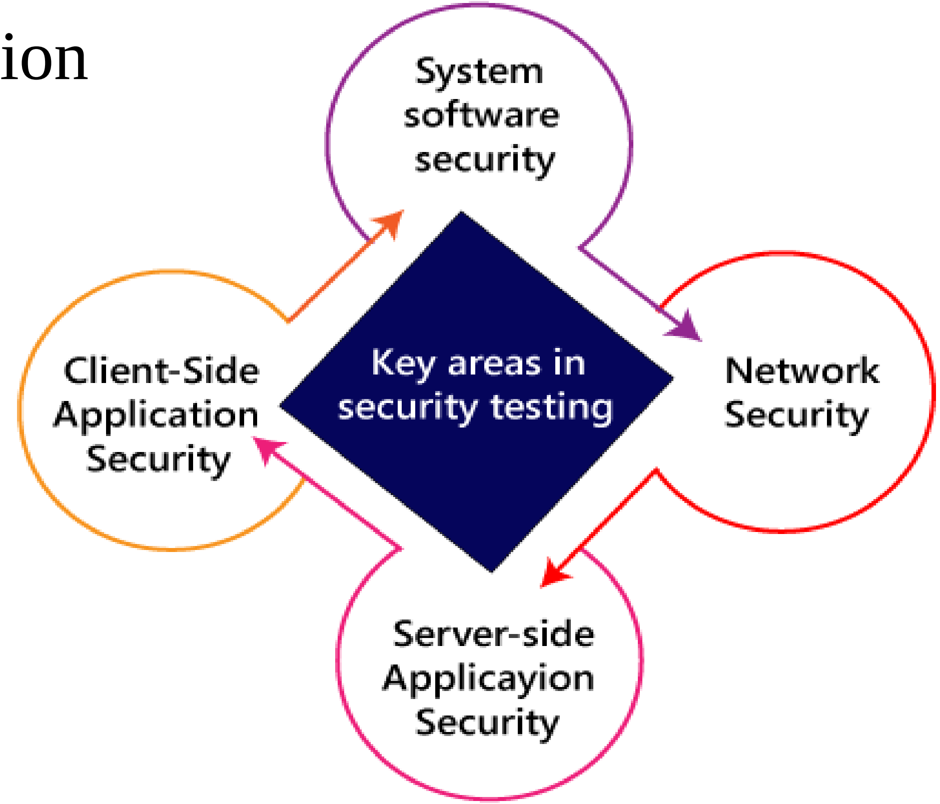
Non- repudiation

It is used as a reference to the digital security, and it a way of assurance that the sender of a message cannot disagree with having sent the message and that the recipient cannot repudiate having received the message.

The non-repudiation is used to ensure that a conveyed message has been sent and received by the person who claims to have sent and received the message.

Key Areas in Security Testing

While performing the security testing on the web application, we need to concentrate on the following areas to test the application


System software security
Network Security
Key areas in security testing
Client-Side Application Security
Server-side Applicayion Security

Key Areas in Security Testing

System software security

In this, we will evaluate the vulnerabilities of the application based on different software such as **Operating system, Database system**, etc.

Network security

In this, we will check the weakness of the network structure, such as **policies and resources**.

Server-side application security

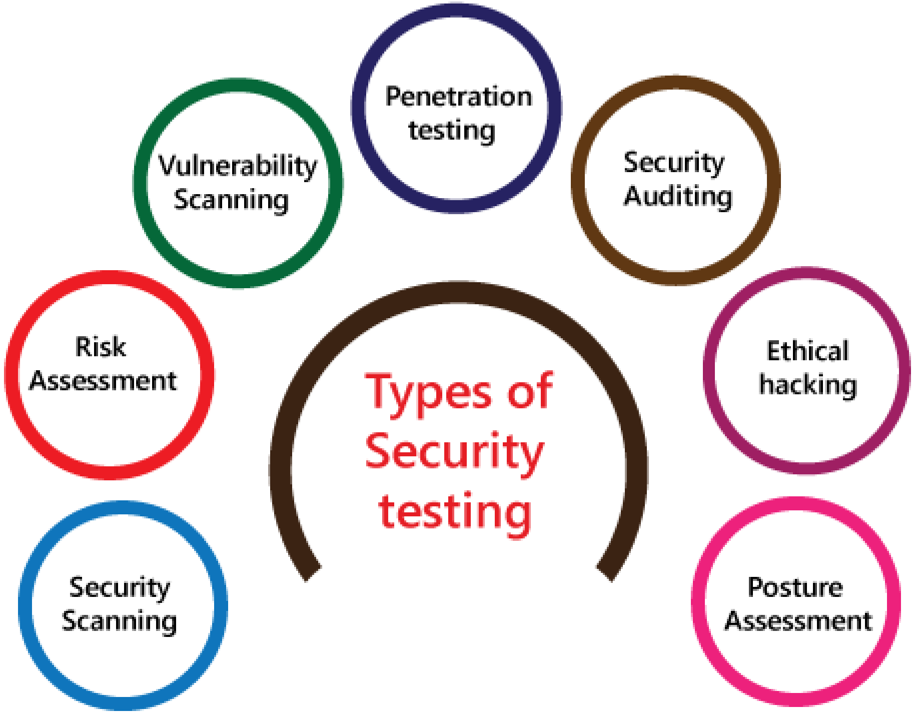
We will do the server-side application security to ensure that the server encryption and its tools are sufficient to protect the software from any disturbance.

Client-side application security

In this, we will make sure that any intruders cannot operate on any browser or any tool which is used by customers.

Types of Security testing

- As per Open Source Security Testing techniques, we have different types of security testing which as follows:
  - Security Scanning
  - Risk Assessment
  - Vulnerability Scanning
  - Penetration testing
  - Security Auditing
  - Ethical hacking
  - Posture Assessment



Security Scanning: Security scanning can be done for both automation testing and manual testing. This scanning will be used to find the vulnerability or unwanted file modification in a web-based application, website, network, or file system. After that, it will deliver the results which help us to decrease those threats. Security scanning is needed for those systems, which depends on the structure they use.

Risk Assessment: To moderate the risk of an application, we will go for risk assessment. In this, we will explore the security risk, which can be detected in the association. The risk can be further divided into three parts, and those are high, medium, and low. The primary purpose of the risk assessment process is to assess the vulnerabilities and control the significant threat.

Vulnerability Scanning: It is an application that is used to determine and generates a list of all the systems which contain desktops, servers, laptops, virtual machines, printers, switches, and firewalls related to a network. The vulnerability scanning can be performed over the automated application and also identifies that software and systems which have acknowledged the security vulnerabilities.

Penetration testing: Penetration testing is a security implementation where a cyber-security professional tries to identify and exploit weaknesses in the computer system. The primary objective of this testing is to simulate outbreaks and also find loopholes in the system and similarly save from the intruders who can take the benefits.

Types of Security testing ..Contd..

Security Auditing: Security auditing is a structured method for evaluating the security measures of the organization. In this, we will do an inside review of the application and the control system for security faults.

Ethical hacking: Ethical hacking is used to discover the weakness in the system and also helps the organization to fix those security loopholes before the nasty hacker exposes them. Ethical hacking will help us to increase the security position of the association because sometimes ethical hackers use the same tricks, tools, and techniques that nasty hackers will use, but with the approval of the official person.

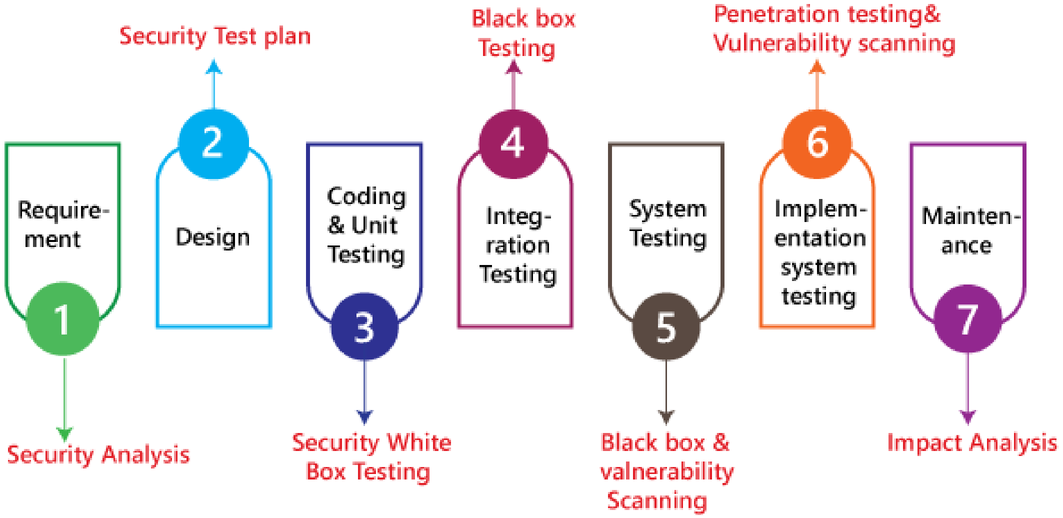
The objective of ethical hacking is to enhance security and protect the systems from malicious users attacks.

Posture Assessment: It is a combination of ethical hacking, risk assessments, and security scanning, which helps us to display the complete security posture of an organization.

How we perform security testing

- The security testing is needed to be done in the initial stages of the software development life cycle because if we perform security testing after the software execution stage and the deployment stage of the SDLC, it will cost us more.
- Now let us understand how we perform security testing parallel in each stage of the software development life cycle(SDLC).

Security Testing along with SDLC



Step1 : SDLC: Requirement stage

Security Procedures: In the requirement phase of SDLC, we will do the security analysis of the business needs and also verify which cases are manipulative and waste.

Step2 : SDLC: Design stage

Security Procedures: In the design phase of SDLC, we will do the security testing for risk exploration of the design and also embraces the security tests at the development of the test plan.

Step3 : SDLC: Development or coding stage

Security Procedures: In the coding phase of SDLC, we will perform the white box testing along with static and dynamic testing.

Step4 : SDLC: Testing (functional testing, integration testing, system testing) stage

Security Procedures: In the testing phase of SDLC, we will do one round of vulnerability scanning along with black-box testing.

Step 5 : SDLC: Implementation stage

Security Procedures: In the implementation phase of SDLC, we will perform vulnerability scanning again and also perform one round of penetration testing.

Step 6 : SDLC: Maintenance stage

Security Procedures: In the Maintenance phase of SDLC, we will do the impact analysis of impact areas.

And the test plan should contain the following:

- The test data should be linked to security testing.
- For security testing, we need the test tools.
- With the help of various security tools, we can analyze several test outputs.
- Write test scenarios or test cases that rely on security purposes.

Example of security testing

- Generally, the type of security testing includes problematic steps based on overthinking, but sometimes the simple tests will help us to uncover the most significant security threats.
- Let us see a sample example to understand how we do security testing on a web application:
  - Firstly, log in to the web application.
  - And then log out of the web application.
  - Then click the BACK button of the browser to verify that it was asking us to log in again, or that we are already logged in to the application.

Why security testing is essential for web applications :

- At present, web applications are growing day by day, and most of the web application is at risk. Here we are going to discuss some common weaknesses of the web application.
  - Client-side attacks
  - Authentication
  - Authorization
  - Command execution
  - Logical attacks
  - Information disclosure

Client-side attacks

The client-side attack means that some illegitimate implementation of the external code occurs in the web application. And the data spoofing actions have occupied the place where the user believes that the particular data acting on the web application is valid, and it does not come from an external source.

Note: Here, Spoofing is a trick to create duplicate websites or emails.

Authentication

In this, the authentication will cover the outbreaks which aim to the web application methods of authenticating the user identity where the user account individualities will be stolen. The incomplete authentication will allow the attacker to access the functionality or sensitive data without performing the correct authentication.

For example, the brute force attack, the primary purpose of brute force attack, is to gain access to a web application. Here, the invaders will attempt n-numbers of usernames and password repeatedly until it gets in because this is the most precise way to block brute-force attacks.

After all, once they try all defined number of an incorrect password, the account will be locked automatically.

Authorization

The authorization comes in the picture whenever some intruders are trying to retrieve the sensitive information from the web application illegally.

For example, a perfect example of authorization is directory scanning. Here the directory scanning is the kind of outbreaks that deeds the defects into the webserver to achieve the illegal access to the folders and files which are not mentioned in the pubic area.

And once the invaders succeed in getting access, they can download the delicate data and install the harmful software on the server.

Command execution

The command execution is used when malicious attackers will control the web application.

Logical attacks

The logical attacks are being used when the DoS (denial of service) outbreaks, avoid a web application from helping regular customer action, and also restrict the application usage.

Information disclosure

The information disclosures are used to show sensitive data to the invaders, which means that it will cover bouts that are planned to obtain precise information about the web application. Here information leakage happens when a web application discloses delicate data, like the error message or developer comments that might help the attacker for misusing the system.

For example, the password is passed to the server, which means that the password should be encoded while being communicated over the network.

Note: The web application needs more security regarding its access along with data security; that's why the web developer will make the application in such a way to protect the application from **Brute Force Attacks, SQL Injections, Session Management, failure to Restrict URL Access and Cross-site scripting (XSS).** And also, if the web application simplifies the remote access points, then it must be protected too.

Here, **Session management:** Is used to check whether the cookies can be re-used in another computer system during the login stage.

SQL injection: It is a code injection approach where the destructive SQL Statements are implanted into some queries, and it is implemented by the server.
Cross-site scripting (XSS): This is the technique through which the user introduces the client-side script or the HTML in the user interface of a web application and those additions are visible to other users.

Security testing tools

Security testing tools are used to make sure that the data is saved and not accessible by any unauthorized user. To protect our application data from threats, we will use these tools. These tools help us to find the flaws and security leakage of the system in the earlier stage and fix it, and test whether the application has encoded security code or not and is accessible by unauthorized users.

These may initially work on authorization, confidentiality, authentication, and availability types of aspects. With the help of these tools, we can avoid the loss of relevant information, the client's trust, sudden breakdown, additional costs required for repairing websites after an attack, and unpredictable website performance.

For this, we have the following tools available in the market:

- SonarQube
- ZAP
- Netsparker
- Arachni
- IronWASP

Security Testing Tools
SonarQube
ZAP
Netsparker
Arachni
IRONWASP

Features of SonarQube

- It will integrate with multiple development environments like Visual Studio, Eclipse, and IntelliJ IDEA over the SonarLint plug-ins.
- It also supports some external tools such as GitHub, LDAP, and Active Directory.
- It can record the metric history and deliver the evolution graphs.
- It will help us to identify the complex issues.
- It will provide application security.

Features of ZAP

- It will support the command-line access for advance users.
- It can be used as a scanner.
- It will provide the automatic scanning of the web application.
- It supports different operating systems like Windows, OS X, and Linux.
- It uses the powerful and Old AJAX spiders.

Features of Netsparker

- It will automatically scan modern web applications like Web 2.0, HTML5, and SPA (single page applications), and all types of legacy.
- For different purposes, it will provide a multitude of out-of-the-box reports for both developers and management.
- We can generate custom reports with the help of our templates.
- We can collaborate this tool with CI/CD platforms such as Bamboo, Jenkins, or TeamCity to protect our application.

Features of Arachni

- It will provide vulnerability exposure, test coverage, and correctness of the web application technologies.
- It supports the various platform and all-important Operating systems like Linus, Mac, OS X, and MS Windows.
- It will support different technologies like HTML5, JavaScript, AJAX, and DOM manipulation.

Features of IronWASP

- It will support the recording login sequence.
- It will produce the reports for both RTF and HTML formats.
- It is a GUI based tool.
- It will support false Positives and negatives detection.

Conclusion

For an application or software, it is necessary to perform security testing to verify that the sensitive information is still private. In software testing, security testing is essential because it helps us to save our necessary data ultimately. In this, the test engineer will act as an invader and test the system or detect security defects.

What is Penetration Testing

- Penetration testing, also called as pen testing, ensures that information security experts use security bugs in a computer program to find and take advantage of them. These specialists, often classified as white-hat hackers or ethical hackers, make things simpler by detecting attacks by cyber attackers known as black-hat hackers in the modern environment.
- In reality, performing penetration testing is equivalent to hiring experienced analysts to conduct a safe facility security breach to figure out how it could be achieved by actual criminals. Businesses and companies are using the results to make the frameworks more stable.

Need for Penetration Testing:

- Pen testing often demonstrates that where and how the system might be abused by a malicious intruder. This helps you to eliminate any vulnerabilities before a real attack happens.
- According to a recent Optimistic Technologies study, every other business has vulnerabilities that can be abused by attackers. Pen testers have been able to violate the company network and enter the network in 93 percent of instances. Four days was the average time taken to do so. An untrained hacker would've been able to access the internal system at 71 percent of the firms.

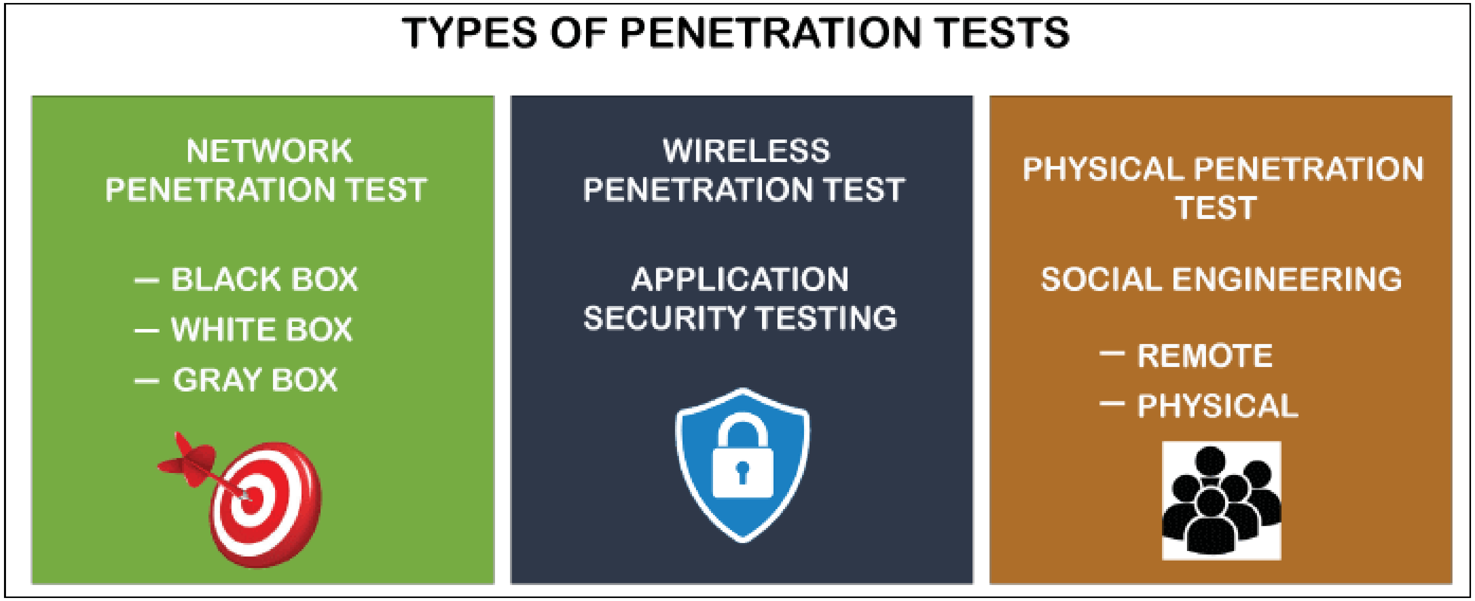
Working Functionality of Penetration Testing :

Firstly, penetration testers need to think about the operating systems that they are going to try to hack. Then, to identify vulnerabilities, they usually use a collection of software tools. Penetration monitoring can also include hacking risks from social engineering. By entrapping a member of the group into having access, testers will attempt to obtain access to a device.

Penetration testers also provide the company with the outcomes of their checks, and that is responsible for introducing improvements that either fix the vulnerabilities or minimize them.

Classification of Penetration Tests

- Penetration testing contains the following essential types that are listed below.
  - Blind Tests
  - White box Tests
  - External tests
  - Double-blind tests
  - Internal Tests



TYPES OF PENETRATION TESTS

NETWORK PENETRATION TEST

- BLACK BOX
- WHITE BOX
- GRAY BOX

WIRELESS PENETRATION TEST

APPLICATION SECURITY TESTING

PHYSICAL PENETRATION TEST

SOCIAL ENGINEERING

- REMOTE
- PHYSICAL

Blind Tests: The Companies offer penetration testers with little security details about the device being exploited in a blind test, referred to as a black-box test. The aim is to find vulnerabilities that wouldn't ever be discovered.

White box Tests: A white box test is one where companies offer a range of security details related to their structures to penetration testers to help them improve vulnerabilities.

External Tests: An external test is one where, globally, penetration testers aim to identify vulnerabilities. They are carried out on macro environment-facing software such as domains because of the existence of these kinds of testing.

Double-blind Tests: A double-blind test that is also defined as a covert test is one where sensitive data is not only given to penetration testers by companies. They still may not make the assessments known to their own information security experts. Traditionally, such experiments are strongly regulated by those conducting them.

Internal Tests: An internal examination is one where the examination of penetration exists within the boundaries of an entity. Typically, these checks concentrate on the security weaknesses of which full advantage could be taken by anyone operating from inside an organization.

Advantages of Penetration Testing Tools

Here, some advantages of pen-testing tools are defined below.

1. Arrangement and Detection of Security Threats

A penetration test calculates the capability of the organization to secure their apps, servers, users and data sources from international and domestic attempts to avoid its security measures in order to obtain restricted or unsanctioned access to secured properties. The pen test result confirms the danger posed by specific security problems or defective systems, enabling abatement initiatives to be arranged by IT management and intelligence analysts.

2. Subvert the channel failure intensity

Recovering from a security flaw is costly. IT rescue station, retention measures, consumer security, commercial-grade, reduced sales, decreased employee productivity, and frustrated trade representatives can be included in recovery. Penetration testing helps a company to prevent these financial difficulties by recognizing and resolving risks constructively before data breaches or attacks occur.

3. Meet the needs of tracking and mitigate penalties

The ultimate monitoring/implementation aspects of activities such as HIPAA, SARBANES-OXLEY, and GLBA are discussed by IT agencies, as well as the monitoring needs to be acknowledged in the federal NIST / FISMA and PCI-DSS directions. The detailed reports provided by the vulnerability scanners will help organizations escape significant non-adherence consequences and allow them to demonstrate continuing due diligence in evaluators by retaining the appropriate safety controls for auditors.

Advantages of Penetration testing …Contd

4. Service delays and security problems are costly

Security vulnerabilities and the corresponding performance disturbances in service providers can result in crippling economic harm, damage the credibility of an enterprise, decimate customer loyalties, elicit negative attention, and impose unexpected financial penalties. Frequent recruitment in penetration testing by the company prevents these expenses.

Checking penetration enables the company to prevent invaders of the infrastructure. It is safer for the company to protect its protection promptly than to suffer drastic failures, both in terms of its brand value and its financial stability.

5. Secure brand recognition and corporate image

Only a single instance of stolen consumer data may kill the reputation of a business and affect its end result negatively. Penetration testing can help an entity eliminate data accidents that can place the integrity and reliability of the business at risk.

Case Study: Global Oil and Energy Provider Penetration Test

- Industry:

  Oil and Energy

- Business Challenge:

  Meeting compliance and regulation standards

  Protecting employees and customer data

- IT Environment:

  Cisco Servers,

  Windows Tech Stack

- Solution:

  Custom-developed security roadmap, built post pentest to help meet compliance and regulations

- Results:

  - Met compliance standards

  - Increased customer trust and Retention security practices

Background:

One of the world’s leading international oil and gas companies, providing fuel, energy, retail services and petrochemicals, best known to the public for its service stations and for exploring and producing oil and gas on land and at sea. Prominent in over 140 countries and territories and employing more than 112,000 people around the globe.

“Under Defense stands out in the field of penetration testing because they understand the importance of security risks and are able to map it to the domain in which its client is operating. Their services are very much tailored to the particular application being examined. Simply using automated scanning tools is not a replacement for smart, intelligent people with a deep understanding of security-related issues. Under Defense takes penetration testing to the next level, using real people to test systems and interpret the results”.

CISO - Oil and Energy Company

The Challenge:

Holding a major global presence and continuously being targeted, our clients understood the risks they faced on a daily basis. In order to meet compliance and regulation standards they engaged the Security Team at UnderDefense to conduct and full black-box Organizational pentest, to learn more about the vulnerabilities they have and how they can be remediated Additionally, the customer had specific business continuity and compliance requirements, relating to its duty of care to maintain employees' and clients personal and financial data With a multinational presence the pentest itself was conducted on multiple territories to ensure the highest level of results.

People, Process, & Technology:

Penetration testing can be conducted in many ways and methodologies. Usually we follow this process:

Test Planning	Vulnerabilities Identification	Vulnerabilities Exploiting	Post Exploitation	Reporting and Recommendation
Meetting with customer	Potential vulnerabilities detection	Vulnerabilities testing	Escalating privileges	Create report for system owner, including found vulnerabilities and recommendations how to eliminate them
Allign test goals and scope	Threat modeling	Vulnerabilities validation	Infrastructure analysis	
Intelligance gathering	Business process analysis	Vulnerabilities research	Vulnerabilities research	

- For our client’s specific requirements and geographical locations we agreed to pursue the following methods: black box tests, social engineering , email phishing , and onsite red teaming.

Standard/Methodology

1. Penetration Testing Execution Standard
2. OWASP Application security verification standard
3. Information Systems Security Assessment Framework (ISSAF)
4. SANS: Network Penetration Testing and Ethical Hacking

With a team of 4 engineers and a duration of 4 weeks, we were able to fully compromise not only the organizations infrastructure but also, web applications as well as expose critical data related to key organizational stakeholders.

The Result:

Penetration testing is often done for varying reasons. Two of the key goals we and our client aimed for, were to increase upper management awareness of security issues and to test intrusion detection and response capabilities. After conducting the pentests and compromising the organization UnderDefense engaged the client in a controlled offensive / defensive threat detection challenge, allowing the client several days to identify and remediate active threats within their systems.

After this challenge was complete UnderDefense was commissioned to conduct training for the key internal security team as well as further advisory on remediation tactics. In the end our client was able to meet the highest level of compliance and regulation standards, develop better security practices and reassure their customers, employees, and board of their continued dedication to best business practices and continued growth.

Key Benefits:

Increase Business Continuity

Protect Clients, Partners and Third Parties

Help to evaluate Security Investments

Thank You!!