INTRODUCTION TO PENETRATION TESTING OR ETHICAL HACKING.

Threat

Possibility of a harmful event to occur

Attack

Taking advantage of the weakness found

Vulnerability

Weakness that makes a target susceptible to an attack

**What is a penetration testing?** It is an authorized simulated and legal

cyberattack on a computer system and to check for exploitable vulnerabiliti**es.**

**Why penetration attack?**

* To analyze and strengthen an organization’s security posture.
* To prevent hackers from gaining access to an organization’s information systems
* To uncover vulnerabilities
* To provide adequate preventive measures
* To enhance security awareness at all levels in a business
* To help safeguard customer data available in business transactio**n**

**WHEN TO PERFORM PENTRATION TESTING**

* When security system discovers new threat attacks
* When you relocate your office
* When you set up a new end -user policy
* Before and after the deployment of the system
* When the system is no longer in a state of constant change
* Before a system is launched

**HOW IS IT BENEFICAL**

Saves recuperation downtime

Comply with regulation or security certification

Increase business continuity

Customer protection

Enhancement of the management system

Detect security threats

Protects financial and reputational loss

**TYPES OF PEN TESTING**

**Web application hacking**

System hacking

Web server hacking

Social engineering – it paves way to verify a human network on a system.

This pen test imitates attacks which the employees a company to upgrade its security.

**REMOTE TEST –** it intends to tricks an engineer or employee to compromise confidential data by using phising attack.

**PHYSICAL TEST –** vishing – using phone calls

**Smishing** -sending sms

Wireless network hacking – intends to analyze the wireless devices deployed on the client site eg: smartphones.

Protocols used for configuring wireless it helps find out the weak areas.

Access point for wireless setup it helps identift those violating the access rights.

Network service hacking – it’s main aim is to find vulnerabilities

It si done both inside and in the autside world.

TARGETED AREAS FOR PEN TEST

DMZ

**Dns level attack which include:**

**Zone transfer testing**

**Switching or routing based testing**

**Any miscellaneous network parameter testing**

There are a set of sorftware modules which the penetration test should cover are as follows.

**SSH** CLIENT/SERVER TESTS

**Exchange or SMTP mail servers**

**FTP client/server tests.**

**Network database.**

**Types of hackers**

**Ethical hacker or white hat hackers**

**Black hat hackers**

**Grey hat hackers**

**ETHICAL OR WHITE HAT HACKERS**

**BLACK HAT HACKERS**

**Their intentions is to fulfil their selfish motives**

**GREY HAT**

**They are a combination of white and black hat hackers .They hack without any malicious intentions for fun**

**HACKING PHASE**

Pre-engagement

Reconnaissance

Scanning

Gaining Access

Maintaining Access

Analysis

**Network database**