LAB CYBER
Cybersecurity made easy

CYBER RISK MANAGEMENT FOR

CYBER SECURITY MANAGERS

INTRODUCTION

First let me just say a big thank you for enrolling in this cyber risk management course.

Cyber risk management is a relatively new field under cyber security but the demand for cyber risk management specialists is increasing rapidly due to the consistent cyber attacks companies continue to face today.

I developed this hand book to provide you with all the key points of the course and is meant to act as a summary of the entire course. If you ever need to retrieve some information from the course, you can use this book as a quick reference.

I sincerely hope this course will provide you with both the theoretical and practical skills necessary to help you manage risks from a cyber security perspective.

Do not forget to follow my company page on LinkedIn

https://www.linkedin.com/company/lab-cyber/

Alexander Oni

What is Risk (Business Perspective)?

Risk refers to the chance of loss of assets that can disrupt a business, function or system.

Assets include software, hardware and even people.

What is Risk (Cyber Security Perspective)?

The likelihood that a vulnerability will be exploited by a threat

Vulnerability refers to a weakness in a security system or setup

Threats could be from black hats, malware, insider attacks or even naive employees

Reduction in threats or vulnerabilities will lower risks.

Scenario (Email)

Loss of email could mean loss of sensitive data such as contracts or access to customers.

Could be caused by loss of email server.

The loss of the server could be due to an outage by the hosting service.

The risks can be reduced by using a reliable host with minimal disruption in service.

Types of Risk

Every cyber security manager needs to be able to manage risks from a business perspective especially when it comes to budget allocation.

- **Operational Risk -** Refers to risks associated with internal failures from people or systems such as employees failing to adhere to security policies and power outages.
- **Strategic Risk** - Refers to risks associated with operations in a specific industry within a specific period of time.
- **Financial Risk -** Refers to the risks associated with how the business handles finances including accepting payments, sending payments and payment options.
- **Reputational Risk -** Refers to the loss of a company's reputation as a result of data breaches, product failures, lawsuits & negative publicity.
- **Compliance Risk -** Refers to an organization's potential exposure to legal penalties and material loss resulting from a failure to act in accordance with industry laws and regulations.

Cyber Risk Management

The process of eliminating as much risk as possible at all times and limiting the effects of risks that cannot be completely eliminated.

It involves;

- Identifying factors or threats that can cause damage
- Evaluate factors for asset value and countermeasures
- Implement cost saving solutions for reducing risk
- Maintaining a secure environment

Risk Management Types

- **Risk Management Sessions -** Brainstorming sessions around what could possibly go wrong with assets.
- **Compliance Risk Management -** Using pre-established risk management criteria e.g checklists
- **Technical/Vulnerability Risk Management -** Deals with technical risks or operating system flaws.
- **Risk Management Through Threat Monitoring -** Monitoring the environment actively for threats

Risk Management is a continuous cycle.

Risk Management Scope & Roles

Risk management deals with data, IT hardware as well as files, documentation and archives.

There are 4 main roles under cyber security risk management but this also depends on the size of the organization.

- **Risk Manager -** who assumes the leadership role and is also responsible for establishing the framework.
- **Risk Management Specialists -** responsible for executing the phases of risk management
- **Subject Matter Experts -** responsible for risk identification recommendations
- **Risk Owner -** responsible for making the final decisions on any cyber risk management related issues.

Threats

- Black hats
- Hactivists
- Nation States
- Employees
- Disgruntled Ex-Employees
- Insider Threats

Risk Identification

A risk register is a tool used by risk managers to document risk management activities.

A typical risk register should contain the following information about a risk:

- Risk Statement
- Risk ID
- Asset
- Risk Rating
- Risk Treatment
- Mitigation/Transference Plan

A risk register may also contain further information like:

- Risk Impact
- Risk Cause
- Cost of immigation

Here is a sample of a risk register

Risk Statement - Sensitive data can be compromised with phishing attacks

Risk ID - 4

Asset - Confidential data

Risk Rating - High

Risk Treatment - Risk must be mitigated

Mitigation Plan - Formal training for employees and use of phishing detection software

SIMPLE BUSINESS RISK REGISTER TEMPLATE

PROBABILITY					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	IMPACT				

RISK DESCRIPTION	IMPACT DESCRIPTION	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL	MITIGATION NOTES	OWNER
Brief summary of the risk.	What will happen if the risk is not mitigated or eliminated.	Rate 1 (LOW) to 5 (HIGH)	Rate 1 (LOW) to 5 (HIGH)	(IMPACT X PROBABILITY) Address highest first.	What can be done to lower or eliminate the impact or probability.	Who's responsible?
Material delivery is delayed	Production stops	5	2	10	Keep in contact with supplier. Have alternative suppliers on retainer.	Sheila
Machinery breakdowns	Production delayed	4	1	4	Increase inspections. Have spare parts on site.	Rashad
		3	5	15		
		5	5	25		
		4	2	8		

Risks can be identified by using the CIA triad.

Risk Assessment

In assessing risks, there are two main things we consider

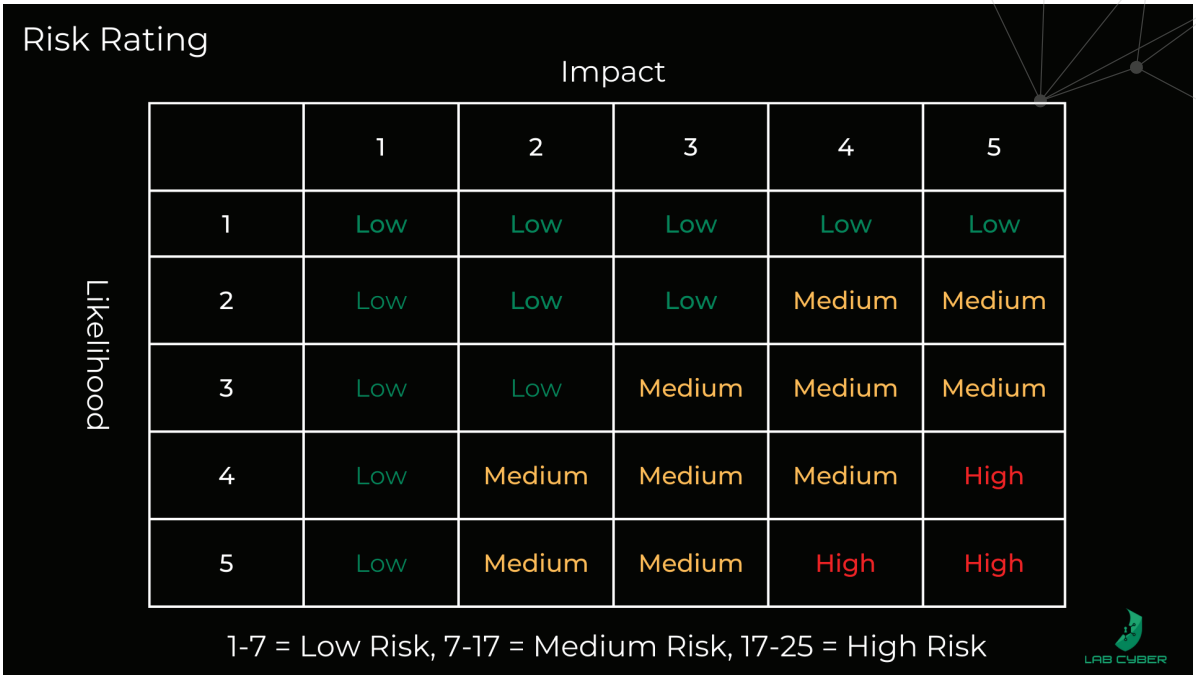
- Likelihood - What are the chances of an event occurring?
- Impact - How much damage will the event cause?

Likelihood Rating

Qualitative	Quantitative	Definition
Very Unlikely	1	Expected to occur once in 5 years
Unlikely	2	Expected to occur once in 3 years
Probably	3	Expected to occur once every year
Likely	4	Expected to occur few times in a year
Very Likely	5	Expected to occur every month

Impact Rating

Qualitative	Quantitative	Definition
Insignificant	1	Loss of assets worth < $5,000
Minor	2	Loss of assets worth between $5000 & $25,000
Moderate	3	Loss of assets worth between $25,000 & $50,000
High	4	Loss of assets worth over $50,000
Disastrous	5	Company reputation, legal fines, license



	1	2	3	4	5
1	Low	Low	Low	Low	Low
2	Low	Low	Low	Medium	Medium
3	Low	Low	Medium	Medium	Medium
4	Low	Medium	Medium	Medium	High
5	Low	Medium	Medium	High	High

Risk Management Processes

Before risks can be managed, they need to be analyzed

Risk Analysis Steps;

- Identify assets - humans, data, emails, hardware (Scoping)
- Identify vulnerabilities - weak passwords, unpatched systems
- Identify exploits & threats - hackers, natural disasters
- Determine safeguards & countermeasures - security policies, backups, patches, updates etc
- Determine which risks are acceptable or not

Risk control refers to how we respond to a determined risk and there are 4 ways we can choose to do so.

Risk Mitigation - This is the most common method of handling risk and typically involves the use of countermeasure or safe guards.

Risk Avoidance - The cost of the risk is too high and must be avoided.

Mitigation means the risk probabilities are reduced to the maximum while avoidance means the risk is eliminated completely.

Risk Transference - This involves assigning or transferring the risk to another entity or organization. In other words, the risk is outsourced because the organization cannot mitigate the risk on its own due to cost.

Risk Acceptance - The cost of mitigating the risk outweighs the cost of losing the asset. Risks are also accepted when there is no better solution. In certain situations, management may choose to reject the risk.

Information Classification

This involves organizing data into categories.

Personal Information

This includes clients names, addresses and telephone numbers.

Internal Company Data

This refers to data like employee information, salaires and company technical information.

Confidential Data

This refers to data that should only be accessed by authorized users.

Public Information

This refers to information that can be accessed by anyone.

Information Security Controls

Security controls serve to protect assets as well as reduce the risk against assets.

Security controls include:

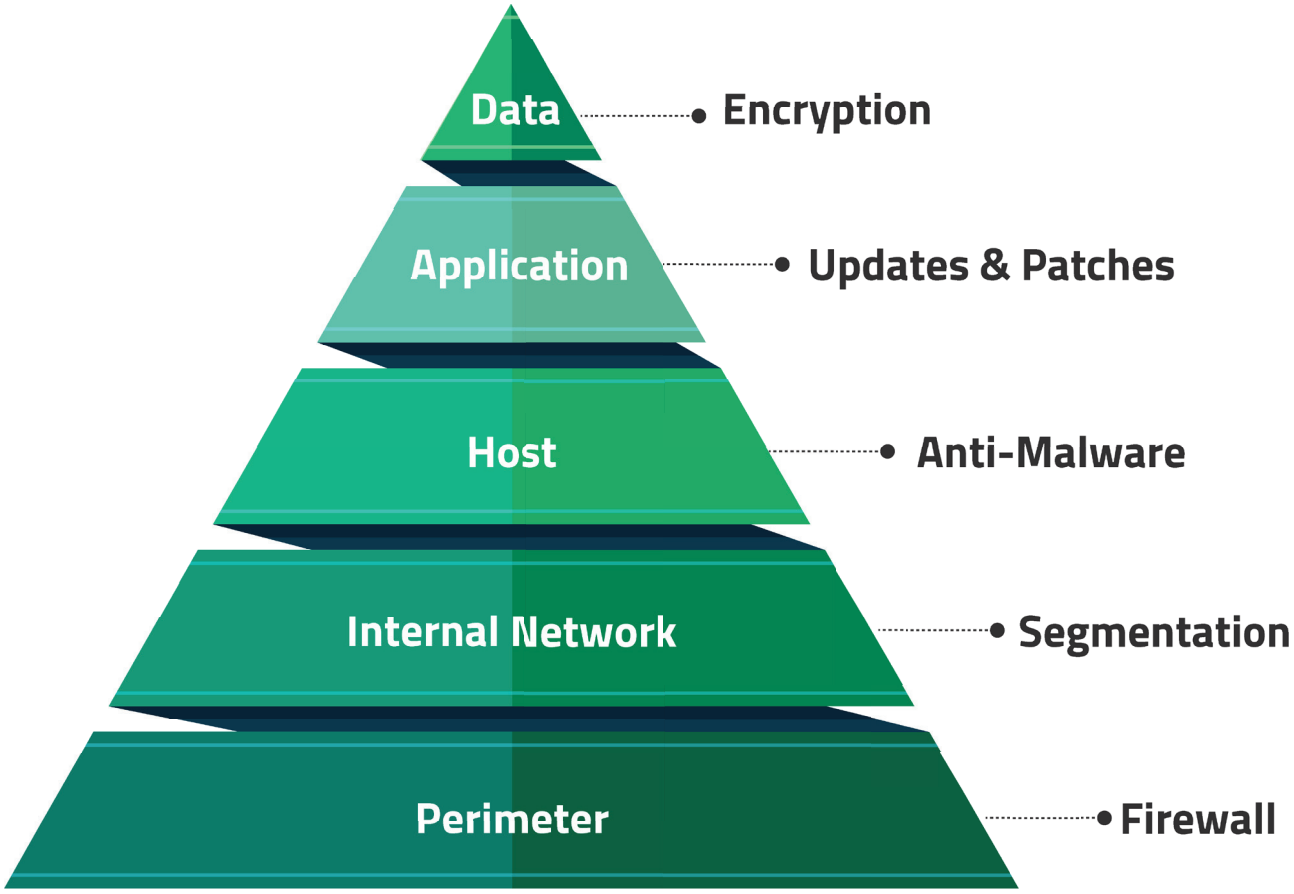
- **Logical Controls -** Networks, databases & applications
- **Physical Controls -** Doors, Walls and Security
- **Administrative Controls -** Security Policies & company culture
- **Detective Controls -** Cameras, Alarms
- **Preventive Controls -** Passwords, firewalls, encryption
- **Corrective Controls -** Backups, Anti-malware

Implementing Security Controls

There should be several layers of protection and multiple security controls used.

DEFENSE IN DEPTH

A cybersecurity approach that uses multiple layers of security for holistic protection. A layered defense helps security organizations reduce vulnerabilities, contain threats, and mitigate risk.



Security Controls can also be divided into **4 main categories**

- **Protection**
- **Detection**
- **Slow Downs**
- **Recovery**

PROTECTION CONTROLS:

These are the first line of defense and include

- **Anti-malware**
- **Firewalls**
- **Encryption**
- **Security Policies**
- **Training**

DETECTION CONTROLS:

The second line of defense and focus on situations where a hacker bypasses one or more security controls

- **Intrusion Detection Systems**
- **Trip wires**
- **Honeypots**
- **Security Cameras & Doors**

SLOW DOWNS:

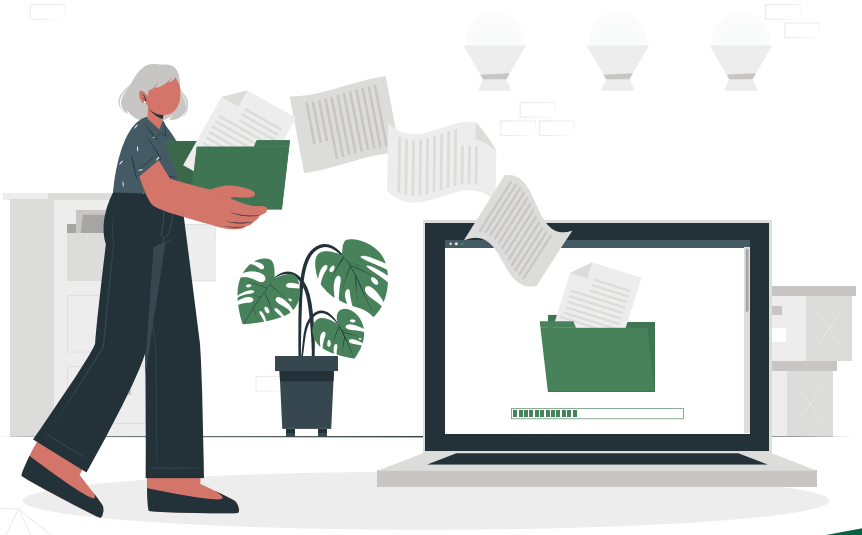
Designed to impede the amount of damage a hacker can cause after successfully gaining entry.

- **Obfuscation**
- **Time outs**
- **Large Files Transfer Controls**

RECOVERY CONTROLS:

If all other controls have failed, these controls allow for quick resumption of normal operations.

- **Backups**
- **Warm/Hot Sites**



Third Party Cyber Risk Management *(TPCRM)*

SUPPLY CHAIN ATTACKS -

These occur when cyber criminals infiltrate a target through an outside partner or provider with access to the target's systems, network and data.

Supply chain attacks are expected to increase because it's a very attractive method of attack for cyber criminals.

Third-party cyber risk management (TPCRM) is an organized approach of analyzing, controlling, monitoring and mitigating cyber risks associated with third-party vendors, suppliers and service providers.

There are two kinds of risks that are discussed in TPCRM:

Inherent Risk - The risks involved just by dealing with the third party absent of any security controls.

Residual Risk * - The risks that remain after all security controls have been accounted for.

6 Steps for TPCRM

VENDOR IDENTIFICATION

Create a list of all vendors starting with those that provide important services or have access to sensitive data.

RISK EVALUATION

Classify vendors based on inherent risk.

USE QUESTIONNAIRES

Your organization may be required to comply with standards like ISO 27001, NIST SP 800-53, CSA CCM, etc. Your questionnaire should cover questions related to such frameworks and compliance requirements.

ASSIGN RATINGS TO RISKS

Use a scorecard to determine the level of threat posed by the risks.

High Risk - Deploy mitigation steps immediately

Medium Risk - Deploy mitigation steps within a stipulated time frame

Low Risk - Accept the risk or deploy mitigation steps over an extended period of time.

ADDRESS RISKS BY PRIORITY

Risks are mitigated based on importance & security.

CONTINUOUS RISK MONITORING

Risks are constantly changing and evolving and thus continuous monitoring is necessary.

Vulnerability Management

This is the process of identifying, assessing, treating and reporting security vulnerabilities.

Vulnerabilities refer to actual security weaknesses while Risks refer to the probability of a vulnerability being exploited.

Vulnerability Example:

Vulnerability = Adobe Reader version 4.3 is vulnerable to a buffer overflow attack.

Vulnerability Treatment = Update Adobe Reader version 4.3 to 4.4

Ways to Discover Vulnerabilities

- **Third party software/services**
- **https://nvd.nist.gov/**
- **https://www.cvedetails.com/**
- **Ethical Hacking**
- **Penetration Testing**

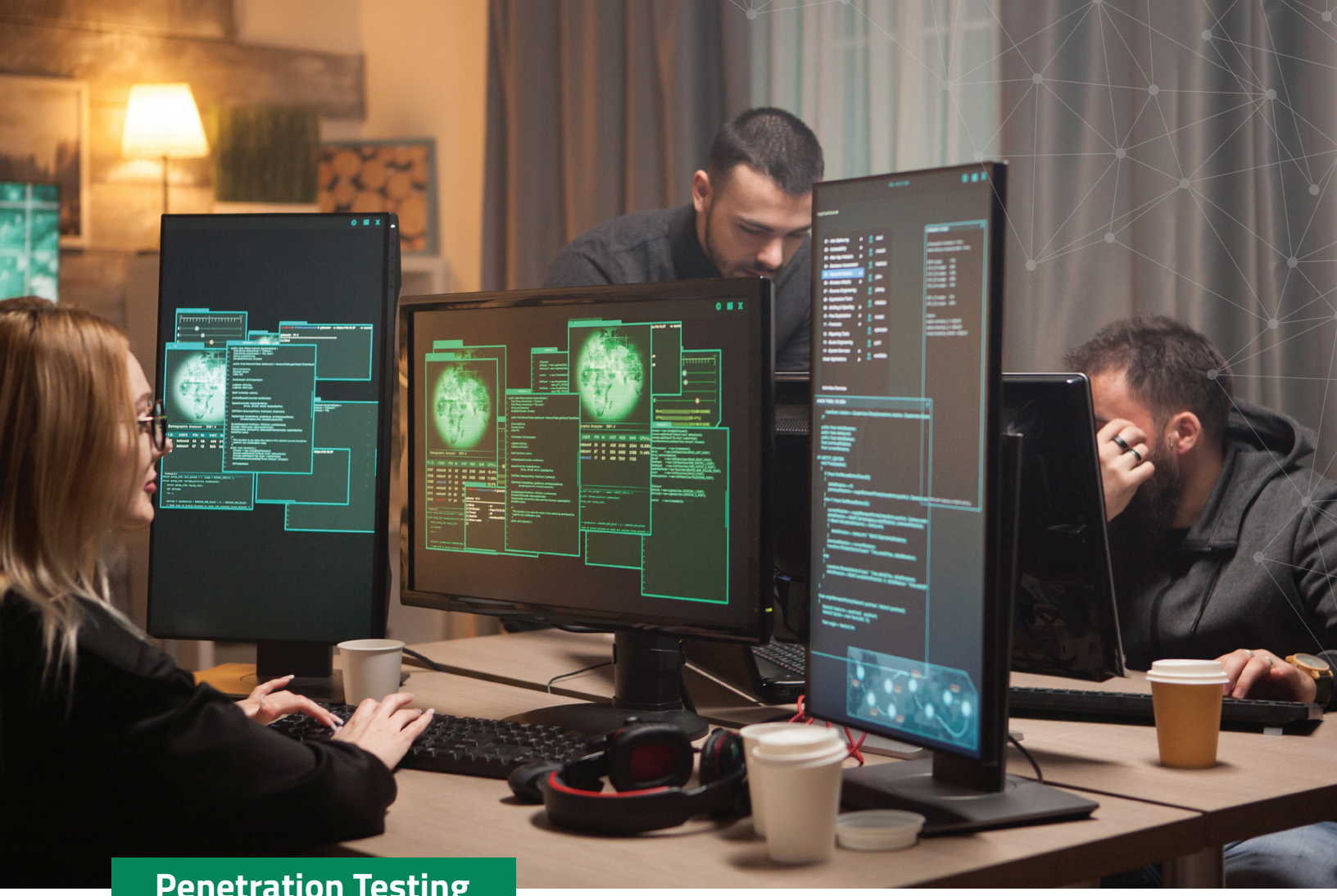
Ethical Hacking

A typical ethical hacking team is comprised of two teams:

Red Team - which are offensive. They actively look for vulnerabilities and weaknesses in a security target.

Blue Team - They are defensive.

In certain situations, there might be a purple team whose objective is to ensure that both red and blue teams are working together optimally.



Penetration Testing

An authorized and legal process aiming to assess and evaluate the security posture of an organization.

There are three stages of pen testing which are the:

- **Pre-Attack which is the reconnaissance stage**
- **Attack**
- **Post- Attack which is the reporting stage**

There are also three types of pentesting which are:

- **Black Box -** This is where the pen testers have no prior information about the target and have to begin from scratch.
- **Gray Box -** The pen testers have limited knowledge about the target
- **White Box -** The pen testers have all the information about the target