Thomas Efthymiadis, Theodosios Dotsas, Sarantis Tsitsos.

Pandora’s Box  | Mediterranean College

Penetration testing toolkit documentation

# Introduction

Cyber security is a collection of defensive techniques in order to protect electronic devices, servers, computers, networks, databases, mobile phones and more, from malicious attacks and hackers.

Nowadays, most of the people and organizations are relied mostly to technology for the purpose of developing their work or making their personal everyday needs easier to be accomplished. For the fact stated, companies need cyber security to have their data, information and systems secured from hackers that want to harm the company or to sell their data to other rival companies, since their work’s implementations is mostly stored on the cyberspace or locally on a computer system.

The most important aspect of cyber security is that protects companies from cybercrime. Information theft is the most profitable part of cybercrime. This type of crime has been exponentially increased throughout the years because of the technological development. Additionally, another reason is the anonymity of the users on the internet that people think it is safer to make cybercrimes rather than more traditional type of crimes. Cybercriminals are becoming more sophisticated, differentiating between what they target, how they affect companies or individuals, and developing a plethora of attacking methods for different attacking methods.

There are many different categories of cyber-attacks used at present. The easiest method by far is social engineering, which means trying to retrieve valuable information through social skills. It is the most common method because it does not need any programming or computing skills. Another type of attack is malware. It is a software that aims on harming a computer system with the aid of computer virus, spyware, worms, and Trojan horses. Moreover, ransomware which is a type of malware is an attack which locks the target’s computer system or files with the use of an encryption method. The only way of decrypting those files is using the decryption key which only the hackers owns. Thus, the hacker, most of the cases, demands to be paid in order to unlock the system or the files. Last but not least, another type of cyber fraud, is the phising method. On this type of attack, the hacker sends emails to his victims that consists of a link of a websites that looks like the legit one (bank, social media, or other platform that require payments like amazon) , but it is a clone of it. With this method the hacker aims to retrieve the personal information of his victim to take advantage of his money or image.

Lack of cyber security can impact companies in two major ways. Firstly, it can result on economic cost because due to the damage that is done through a cyber-attack the company will need to pay computer experts to repair the damage done. Secondly, it can affect the reputation of the company. Due to a malicious attack, customer will loss trust on the organization and thus those customers might influence future customers to not give a chance to this company.

There are plenty of benefits using cyber security on a company. The most obvious one that it can protect the business, but in order to achieve this the business should hire cyber security experts. Another one is that it allows employees to work on a safe environment and also protect their productivity of their work. Lastly, It protects the company’s website from going down and also protects from different types of malicious attack that discussed above.

# History of Hacking

## Definition of Hacking

Hacking refers to unauthorised intrusion into an individual computer system or network, it is usually used to describe a malicious cyber-attack. However, there is also the non-malicious hacking. At first hacking was referred to students at Massachusetts Institute of Technology (MIT) during 50s and 60s who implemented solutions. Over time the term hacker has changed and now it describes someone who exploits individuals or organizations in order to retrieve personal information and sell it. (Haslam, J. 2020)

## Types of Hackers

There are plenty types of hackers, the following are three major categories:

There are plenty types of hackers, the following are three major categories:

* White Hat: This type of hackers try to find bugs and vulnerabilities in companies in order to secure them and fix their security issues. They are usually working as security system experts and they prevent black hat hackers from attacking them.
* Grey Hat: This type of hackers are not always harmful or helpful. They are searching for bugs and exploits for organizations, but they are not employed to the company. Lastly, they do not tend to harm the company but instead they sometimes help the company by providing useful information about how to prevent some of their security issues.
* Black Hat: This type of hackers try to find exploits and vulnerabilities on websites and systems for profit. Also, they steal data from companies and organizations to sell their information to their rivals.

# About the project: what is this project, what does it do, who is its audience, why is this needed

# Purpose: why do we need such an application

# Statistical data: about cyber security, hacking etc.

# Tools: explanation of the tools and the algorithms behind them

## Port Scanner

## DDoS

## IP Finder

## Keylogger

## Wordlist Generator

## SSH BruteForce

## Backdoor

## Hash Cracker

## Ransomware

## SQL Injection

## OS Detection

# Manual

# References