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

Penetration testing (from here on pen-testing) is considered as a collection of actions that are being executed in order to test the integrity of information systems (Bacudio, Yuan, Bill Chu and Jones, 2011). Usually this revolves around identifying vulnerabilities that could be exploited by an adversary in order to gain access and possibly cause harm to a system. Nowadays, there are regulations that oblige organizations to pass certain security tests and implement various security measures, especially when they handle personal user information (like medical data) or financial assets (Kosseff, 2017).

The process of pen-testing usually involves a security expert who tries to gain unauthorized access with various ways in an information system. To do that, the expert employs automated, manual (and sometimes both) tools in order to identify possible vulnerabilities in different parts of the system. There are various cases where certain organizations had to pay huge amounts of money in law-suits and recovery efforts, after their systems have been breached. Apart from the revenue, an organization’s credibility greatly depends on how secure its users’ information is. Pen-testing can help prevent this by providing very valuable information, enabling an organization to always be one step ahead. Apart from identifying any possible vulnerabilities pen-testing can lead to a ranking between them, helping the organization prioritize measures against those with the higher risk of being exploited and also the higher chances of causing harm.

# 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

In general brute-force attacks are a type of dictionary attacks that iteratively try a combination of username/password in order to gain access to an account or system. In our scenario the target is an SSH server that uses a username and a password for a login. The main purpose of this attack is to gain access in the case of a weak username/password combination that is present in the dictionary databases. In Algorithm 3 the logic behind this tool is presented.

|  |
| --- |
| **Algorithm 3** SSH Brute-force |
| **Require** usernames **dictionary file** |
| **Require** passwords **dictionary file** |
| **for** username **in** usernames: |
| **for** password **in** passwords: |
| **try connect(**username, password**)** |
| **if success**: |
| **store(**username, password**)** |

As simple as it may look there are many people that fail to create a strong username/password combination which makes them vulnerable to such attacks. The biggest drawback of this type of attacks is time complexity since for our case it is O(n2).

## Backdoor

## Hash Cracker

## Ransomware

A ransomware is a type of malware that is generally used to extort a user/victim into paying the attacker in order to revert any actions taken by it. The most commonly used action is the encryption of a user’s most important files, which generally are personal images and videos, important documents, system files etc. To get the ransomware to the user/victim, an attacker usually fools them into thinking that the file is to be trusted and thus leading him into executing it on their personal computer. After being ran the ransomware immediately begins encrypting user files and then displays a message prompting the user to pay the attacker (usually in Bitcoin) in order to get their files back.

For the purposes of this team project, we created a tool that, once ran, it encrypts all of the user’s important files under the specified directory. Before running the ransomware script, the attacker must generate a pair of private/public encryption keys by using the also developed *key generator.* The generator uses the RSA algorithm to create the keys, from which the private key must stay with the attacker and the public is used for encryption purposes in the ransomware. Presented in Algorithm 1 is the logic behind the encryption developed in the ransomware tool:

|  |
| --- |
| **Algorithm 1** Ransomware encrypt |
| Generate Fernet key |
| Initialize Fernet crypter with key |
| Encrypt Fernet key with public RSA key |
| Store encrypted Fernet key |
| **targets = [**list of file extensions**]** |
| **for** file **in** directory: |
| **if** file.extension **in** targets: |
| **encrypt()** |

As shown in Algorithm 1 the Crypter used to encrypt files is Fernet, which is said to be a military grade encryption algorithm that is unbreakable. The ransomware tool also employs a decryption function that is used to decrypt all previously encrypted files. Algorithm 2 is the logic behind the decryption:

|  |
| --- |
| **Algorithm 2** Ransomware decrypt |
| Decrypt Fernet key with private RSA key |
| Initialize Fernet crypter with key |
| **targets = [**list of file extensions**]** |
| **for** file **in** directory: |
| **if** file.extension **in** targets: |
| **decrypt()** |

In the case of the decryption the logic is that the victim will provide the encrypted Fernet key to the attacker and the attacker will use his private RSA key to decrypt it and send it to the victim in order to restore his files. Since the files were encrypted with the original Fernet key, the victim can’t use the encrypted one to decrypt his files, so he needs to get the original by decrypting it.

## SQL Injection

One of the most common hacking techniques is that of the SQL Injection. In general this attack occurs when there is an input that requires the user to type in something and then based on that return the result from the database, where instead of the expected text the user sends SQL code which runs unbeknownst to the administrator on the database. This can result in data leaks and data loss since the user is able to run any SQL code in order to get the desired results. For this project our tool checks a given webpage for SQL injection vulnerabilities by entering the [ ‘ ] character along with some random text hoping to get an SQL error, that indicates that we can run SQL code. Algorithm 5 shows the logic behind our tool.

|  |
| --- |
| **Algorithm 5** SQL Injection |
| Find all forms in webpage |
| Find all inputs for all forms |
| **for** input **in** inputs: |
| **getattributes()** |
| Set value for input random string + ‘ |
| Send post or get request with the value |
| Get page response and match regexp of error |
| **if** match found: |
| **return** SQL injection vulnerable |

After we send the payload that includes the special character we read the response page and try to find a match using regular expressions to the most common SQL errors. If a match is found then the page is SQL injectable.

## OS Detection

OS Detection refers to the process of identifying the operating system that runs on a computer. Most popular OSes are Windows and Unix/Linux. The simplest method (though not foolproof) of identifying a computer’s OS is to send a packet and then read the TTL (Time To Live) value that comes in the response. Generally, Windows and Linux have different TTL values as listed in Table 1.

Table 1 OS TTL Values

|  |  |
| --- | --- |
| **OS** | **TTL** |
| Linux | 64 |
| Windows | 128 |

In order to identify the OS, Algorithm 4 was employed. It is to be noted that the TTL value can be easily changed by a system administrator in order to counter detection tools that use this method. There are other much more sophisticated ways to detect the OS, but are outside the scope of this project.

|  |
| --- |
| **Algorithm 4** OS Detection |
| Create packet with the target’s IP |
| Send packet and read response |
| **if** response.TTL **≤** 64: |
| **return** Linux |
| **else if** response.TTL **≤** 128: |
| **return** Windows |

# Manual

# References