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.

# About 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

The project is about a collection of penetration testing tools. More specifically, it is a collection of independent programs that test vulnerabilities on different areas like computer systems, files, and websites. Moreover, the application will be a desktop app aiming to work on Windows operating system and after some period we will aim to launch it on Linux and iOS. Also, the thought behind this project was about implementing some of the famous penetration testing tools on the same application.

The target audience would be mostly users that would like to see how these programs work and how they can help with the security of their systems or how those programs can harm another computer. However, it would be possible to be addressed to companies rather than individuals only, after some updates that are planned to be done in the future, so it is more efficient and effective for large organizations.

Lastly, due to the increased need of protection on the IT field, companies and organizations are depended on this kind of apps in order to ensure their computer system’s security.

# 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

There are plenty of statistical analysis that cover the impact of hacking activities and the use of cyber security. In this section we will be viewing some of the statistical data that have been observed and documented.

Statistical data about hacking and cyber-crime:

* There Is a malicious attack on a computer system or network approximately every 39 seconds
* Over 300.000 new malware is created every day
* Hackers steal 75 records of their targets every second
* More than half of the businesses that have been attacked were not sure they could recover the damage
* 92% of malware is delivered by e-mail
* For mobile devices most of the malware target the Android system
* Most of the malware target Windows operating systems
* Cybercrime is more profitable than global illegal drug trade

Statistical data about cyber security:

* In the US the cyber security budget was around 15 billion dollars in 2019
* White hat hackers earned around 19 million dollars in 2018
* Around 95% of breaches in cyber security are caused by human error
* There will be 3.5 million cyber security job openings in 2021

(Galov, 2021)

Considering all the statistical facts stated above, companies, organizations, and individuals must be aware of the threats about cyber-crime and also the effort that focuses on cyber-security expenses as well as its growth over the years.

# Tools

## Port Scanner

A Port Scanner is a program that checks for network ports to see if it is open or closed. They are often used to diagnose a network and check for connectivity issues. Also, it is used by hackers that want to detect any possible access point of a network and decide in which access point to attack.

It works by using a TCP or UDP network packet and asks the port their status. If the computer responds to the current port and asks if there is something to be done, then it means that the port is open. However, if the port is currently in use, then the port is closed. Bellow in Algorithm 1 is shown the logic used on the implementation.

|  |
| --- |
| **Algorithm 1** Port Scanner |
| Use **socket** library |
| Listen on IPv4  Try: |
| SocketObject.connect(ip\_address, port)  Port is open  Except: |
| Pass (Port is closed) |
|  |

The main concept is very simple. Using the socket library, we create a socket Object that trying to have a connection of a specific ip address to a specific port. If the connection is successful, then the program prints that the port Is open. However, if the port is occupied, we pass because in general we don’t care to print all the closed ports for the reason that we are trying to see which access point of a network is vulnerable to attacks.

## DDoS

A distributed denial-of-service (DDoS) attack is a malicious software that loads the traffic of a computer network, overwhelming it and making it unable to perform. Most of the times, DDoS is performed by using a lot of other computers, usually hacked ones, thus it helps flooding the network of a computer much faster.

There are many different types of DDoS attacks such as:

* Application layer attacks
* Protocol attacks
* Volumetric attacks

The Algorithm 2 was implemented shown an example of a protocol syn flood attack.

|  |
| --- |
| **Algorithm 2** DDoS Attack |
| Make a IPv4 connection  Sending random bytes to a **port** from an **IP address** |

## IP Finder

IP Finder is a tool that simply scans a domain name of a website at outputs its IP address. It alone does not have any penetration testing meaning but it can be very useful with the combination of other tools like a port scanner, DDoS attack and more.

IP Finder is simple to be implemented due to the socket library that python and other programming languages provide as shown in Algorithm 3.

|  |
| --- |
| **Algorithm 3** IP Finder |
| Use **socket** library |
| Enter a **domain name**  Socket.gethostbyname(**domain name)** |
|  |

## Keylogger

The keylogger is a program that monitors keystrokes made by a user. Cyber-criminals use keyloggers to steal private information of users such as passwords of credit cards and other accounts. Bellow in Algorithm 4 is shown the specific keylogger that we used.

|  |
| --- |
| **Algorithm 4** Keylogger |
| Set a **path** for the keylogger **file** to be created  Open **file** on append mode  Append **keys**  Count += 1    If count >= 1:    Write **keys** on file |
|  |

The user sets the path for the keylogger file to be created and then when the keylogger is activated it stored any keystroke on the file.

## Wordlist Generator

Wordlist Generator is a tool mostly used in combination with SSH BruteForce and Hash Cracker. It generates a list of possible passwords in order to use it for crack them. In Algorithm 5 it shows a simple implementation of the Wordlist Generator with the option of making a text file with alphabetical, numeric or alphanumeric passwords.

|  |
| --- |
| **Algorithm 5** Wordlist Generator |
| Create Wordlist Generator text file  Choose from **alphabetical**, **number** or **alphanumeric**  Open file on write mode |
| For i in range of (**min** size of word, **max** size of word:  Write in file all combinations of number between **min** and **max** |

## 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 6 the logic behind this tool is presented.

|  |
| --- |
| **Algorithm 6** 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

Backdoor is a program that a user can have authorized or unauthorized root access to

(high level access) on target’s computer or network. It can be used both maliciously and for other reasons. To be more specific, a hacker can use Backdoor to have access on the target’s personal information and retrieve or destroy any files of its computer system. However, it can also be used to help clients with computer errors. For this specific Backdoor we used a server side that connects with a specific local IP address and gain access to the root using the Backdoor program. The Algorithm 7 and 8 bellow shows both the server and the Backdoor program.

|  |
| --- |
| **Algorithm 7** Server |
| Make a connection for IPv4 address  Bind the local IP to an unoccupied **port**  Listen to **port**  While **True:** |
| If user chooses a **command**: |
| Execute the **command** |

|  |
| --- |
| **Algorithm 8** Backdoor |
| Make a connection to IPv4 address  Make the connection with the server  While True:  If user chooses a **command**:  Execute the **command** |

The server makes a connection to a specific unoccupied port from a local IP address and when the Backdoors runs the user Is able to execute implemented commands to the targets computer system.

## Hash Cracker

Hash Cracker is a tool that takes a list of possible passwords and a hash, and compares them until it finds the password that matches with the hash. Nowadays, most of the databases save passwords with the aid of hashes. This is the reason that a hash cracker is needed in order to find passwords. Also, it is a very fast procedure and take less time than a BruteForce Attack.

|  |
| --- |
| **Algorithm 9** Hash Cracker |
| Use hashlib library  Open **file** **of passwords** on read mode  Based on the chosen **hash type** enter the hash  Decrypt the hash if it exists on **file of passwords** |
|  |

## 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 10 is the logic behind the encryption developed in the ransomware tool:

|  |
| --- |
| **Algorithm 10** 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 11 is the logic behind the decryption:

|  |
| --- |
| **Algorithm 11** 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 12 shows the logic behind our tool.

|  |
| --- |
| **Algorithm 12** 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 13 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 13** 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