PENETRATION TESTING FOR ANDROID USING METASPLOIT FRAMEWORK

TAN CHUN YONG

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: Penetration Testing for Android Using Metasploit Framework

SESI PENGAJIAN: 2020 / 2021

Saya: TAN CHUN YONG

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

_____ SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____ TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
✓ TIDAK TERHAD	

(TANDATANGAN PELAJAR)

Alamat tetap: 105, Jalan Intan Mas,
Taman Intan Mas, 36000 Teluk Intan,
Perak.

Tarikh: 12/9/2021

(TANDATANGAN PENYELIA)

PROF DR SHAHRIN SAHIB

Nama Penyelia

Tarikh: 12/9/2021

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

PENETRATION TESTING FOR ANDROID USING METASPLOIT FRAMEWORK

TAN CHUN YONG

This report is submitted in partial fulfilment of the requirements for the Bachelor of Degree Computer Science Software Development with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

DECLARATION

I hereby declare that this project report entitled

PENETRATION TESTING FOR ANDROID USING METASPLOIT FRAMEWORK

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : _____ Date : 12/9/2021

(TAN CHUN YONG)

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of Degree Computer Science Software Development with Honours.

SUPERVISOR : _____ Date : 12/9/2021

([PROF DR SHAHRIN SAHIB])

DEDICATION

I dedicated to my beloved parents, who taught and showered me never ending prayers and support throughout the whole process inside this project. I also dedicate this work to all hardworking teachers and friends in our college that assisted me with this project.

ACKNOWLEDGEMENTS

First of all, I think this project would not have been possible without the help of the following people, who have shared their knowledge, experience and skills to me in achieving the completeness of this project. Firstly, I would like to express my appreciation to my project's supervisor, Prof. Ts. Dr. Shahrin Bin Sahib for assisting me in completing this project successfully. He gave me a lot of valuable guidance and advice that prompted me to complete this project involve system development and project reporting. Next, I would also like to express my appreciation to my project's evaluator in this project which is Prof. Dr. Nor Azman Bin Abu for taking the time to evaluating my project. Finally, I would also like to thank my beloved parents for their continuous support and encouragement during my project.

ABSTRACT

Penetration Testing is a simulated cyberattack on your computer to check for vulnerabilities that can be exploited in order to improve and enhance an organization security system. Unfortunately, many users do not really understand what are the vulnerabilities on their devices behind the pentest implementation. This project is about developing an pentesting tool with other penetration tools which is not only to extract the information from the targeting victim's devices, but also will help the victim to understand what was the vulnerabilities of their devices and help improve their security knowledge during the pentest execution. The objective of this project is to test the developed pentesting tool and secure the target device in the pre-setup testbed, to develop an pentesting tool with application file using MSFvenom tool to extract information about the targeting android devices, to set up a listener to receive the connection from the reverse TCP connection from targeting victim's devices in order to obtain the information from the devices, and lastly is generate a risk report to educate victim about the knowledge on how to secure their devices from being exploit by the attackers. This project is designed by combining all the 5 stages on pentesting which include reconnaissance, scanning, gain access, risk analysis & recommendation and report generation. Lastly, as the penetration tester, you should look into security points for an android device to conduct a risk report to victim by including all information from the pentesting process to prevent information exploit by the attackers which include disable the enable option unknown resources by downloading application from third-party website applications other than Google Play Store which contains high security level and also can installed anti-virus into devices to detect the virus of the application.

ABSTRAK

Ujian Penetrasi adalah serangan siber yang disimulasikan di komputer anda untuk memeriksa kelemahan yang dapat dimanfaatkan untuk memperbaiki dan meningkatkan sistem keselamatan organisasi. Malangnya, banyak pengguna tidak benar-benar memahami kerentanan pada peranti mereka di sebalik pelaksanaan ujian penetrasi. Projek ini adalah untuk mengembangkan alat pentesting dengan alat penembusan lain yang bukan hanya untuk mengekstrak maklumat dari alat mangsa yang menjadi sasaran, tetapi juga akan membantu mangsa memahami apa kelemahan peranti mereka dan membantu meningkatkan pengetahuan keselamatan mereka semasa pentest dilaksanakan. Objektif projek ini adalah untuk menguji alat pentesting yang dikembangkan dan mengamankan peranti sasaran di tempat ujian pra-persediaan, untuk mengembangkan alat pentesting dengan file aplikasi menggunakan alat MSFvenom untuk mengekstrak maklumat mengenai peranti android sasaran, untuk menyiapkan pendengar untuk menerima sambungan dari sambungan TCP terbalik dari mensasarkan peranti mangsa untuk mendapatkan maklumat dari peranti tersebut, dan terakhir adalah menghasilkan laporan risiko untuk mendidik mangsa dengan pengetahuan tentang cara mengamankan peranti mereka agar tidak dieksploitasi oleh penyerang . Projek ini dirancang dengan menggabungkan semua 5 tahap pentesting yang merangkumi pengintaian, pengimbasan, akses, analisis risiko & cadangan dan penghasilan laporan. Terakhir, sebagai penguji penembusan, anda harus melihat perkara keselamatan bagi peranti android untuk membuat laporan risiko kepada mangsa dengan memasukkan semua maklumat dari proses pentesting untuk mengelakkan maklumat dieksploitasi oleh penyerang yang termasuk melumpuhkan pilihan aktif yang tidak diketahui sumber dengan memuat turun aplikasi dari aplikasi laman web pihak ketiga selain Google Play Store yang mengandungi tahap keselamatan yang tinggi dan juga dapat memasang anti-virus ke dalam peranti untuk mengesan virus aplikasi.

TABLE OF CONTENTS

PAGE

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

LIST OF ABBREVIATIONS

FYP	-	**Final Year Project**
ADB	-	**Android Debug Bridge**
API	-	**Application Programming Interface**
APK	-	**Android Package Kit**
CLI	-	**Command Line Interface**
GUI	-	**Graphical User Interface**
IP	-	**Internet Protocol**
MITM	-	**Man-In-The-Middle attack**
MSF	-	**Metasploit Framework**
OS	-	**Operating System**
SDK	-	**Software Development Kit**
SQL	-	**Structured Query Language**
TCP	-	**Transmission Control Protocol**
USB	-	**Universal Serial Bus**
VM	-	**Virtual Machine**
XSS	-	**Cross Site Scripting**

CHAPTER 1: INTRODUCTION

1.1 Introduction

Nowadays, many people use their smartphones in almost all aspects of their lives, social interactions, careers, finances, learning, and even health. According to (Statista, 2021), shown that the increasing number of mobile application that have installed from 2016 to 2020. This situation has attracted the attention of more hackers and not only increases the likelihood and number of smartphones that can be targeted by hackers, but it also increases the likelihood of hacking on any systems or devices that connect to the same network. Other than that, sometimes the application in Google Play Store has blocked the user's devices from installing the application compatible with the devices causes users take risks to install those applications from unknown sources in third-party which is not secure and could bring them to cybersecurity risk that are not easily to mitigate and manage. Hackers could design a malicious application that contain virus, payloads and worms and upload to the application websites once the user install the application inside their devices it will vulnerable to lead the user to leak their credentials such as bank account numbers, password, important documents and etc.

Besides, according to (BulletProof, 2019), in 2017 and 2018 stated that there are many victim or company is compromised by common attacks included Cross Site Scripting (XSS), poor passwords used, SQL injection, out of date software, etc. Therefore, the smartphone penetration test is one the most important type of security assessment that indicates what can be exploited, weaknesses that exist in the application and the level of damage that can occur if hacked. In general, penetration

testing or (ethical hacking) is a process discover security vulnerabilities and increase the security level of the system, network, or applications as performed by penetration testers or auditors. Also, it is important to show that penetration testing (often abbreviated as pentesting) is usually mistaken for vulnerability testing. Actually, vulnerability testing is to identify potential problems, where penetration testing aims to analyse those problems and attack the system into identify weaknesses.

In spite of that, the penetration testing process can be conducted by the help of the pentesting tools out there and available for pentester to be used to completing their task. According to (Howard Poston, 2021), it stated that the common pentesting tool that will be used on these days are Nmap, Nessus Vulnerability Scanner, John The Ripper, Social Engineering Toolkit, Wireshark, metasploit, etc. In this project, we use metasploit as process to hacking the android devices by generating a payload to the user purpose to extract information from the user's devices. Basically, the steps needed to run on an android application pentesting by using metasploit framework such as setting up the testbed environment, create an application file using msfvenom tool to generate a payload and save it as an application file and set up a listener to the Metasploit framework. Once the user downloads and install the malicious application file will give the permission access to the attacker by received the reverse back TCP connection to the listener and attacker able to extract the information from the victim devices.

1.2 Problem Statement (PS)

Table 1.1: List of problem statement

PS	Problem Statements
PS_1	According to (Statista, 2021), the chart has shown that the increasing number of mobile application downloads worldwide in year 2020 which consumers downloaded 218 billion mobile apps to their devices and this situation has attracted more hackers. Some of the application in the Google Play Store which is not suitable to installed into devices compatible to the devices and user that **lack of security knowledge** about the risk to installed application in other websites different from Google Play Store and running those application has given vulnerabilities to the hackers to exploit those devices to extract the information from the target devices. Besides that, users who lack of security knowledge do not how to secure their data on the devices.

1.3 Project Question (PQ)

Table 1.2: List of project question

PS	PQ	Project Question
PS_1	PQ_1	How to develop an pentesting tool with apk file?
	PQ_2	How to receive the connection from the victim's devices to obtain the permission to control the devices.
	PQ_3	How to test the developed pentesting tool in the pre-setup testbed?
	PQ_4	How to educate victim about the knowledge on how to secure their devices from being exploit by the attackers.

1.4 Project Objective (PO)

Table 1.3: List of project objective

PS	PQ	PO	Project Objective

PS_1	PQ_1	PO_1	To develop an pentesting tool with apk file using MSFvenom tool to extract information about the targeting android devices
	PQ_2	PO_2	To set up a listener to receive the connection from the reverse TCP connection from targeting victim's devices in order to obtain the information from the devices
	PQ_3	PO_3	To test the developed pentesting tool and secure the target device in the pre-setup testbed.
	PQ_4	PO_4	To generate a risk report to educate victim about the knowledge on how to secure their devices from being exploit by the attackers.

1.5 Project Scope

- This project will be executed on a pre-setup testbed on a virtual platform that involve tester machine installed with Kali Linux OS and victim machine installed with android OS.

- This apk file that created by pentesting tools should be signed and aligned with the appropriately signed certificate tools like apktool as successfully created and allowed for installing this apk file into android devices.

- The developed pentesting tool will integrate with other pentesting tools to extract information from the target device by transfer the apk file that contain payload to the victim's devices through the vulnerabilities that found to successfully gaining access to the victim devices.

- This project conducts a risk report to educate victim on how to secure their devices from being exploit by the attackers.

1.6 Project Contribution (PC)

Table 1.4: List of project contribution

PS	PQ	PO	PC	Project Contribution
PS_1	PQ_1	PO_1	PC_1	User could understand how the apk file with malicious payload be created and signed using some tools to allow installed into android devices.
	PQ_2	PO_2	PC_2	User would understand better how the attacker receive the information and gain control to victim's devices.
	PQ_3	PO_3	PC_3	Pentester can secure the target device to conduct the penetration testing in the pre-setup testbed by being damaged to the real devices
	PQ_4	PO_4	PC_4	This risk report educate victim to look into some security points in order to secure their devices

1.7 Report Organisation

Chapter 1: Introduction

This chapter discuss about introduction of this project, problem statement, project question, project objective, project scope and project contribution.

Chapter 2: Literature Review

This chapter discuss about the previous work that are related to this project, critical review to previous project and proposed solution.

Chapter 3: Project Methodology

This chapter discuss about each stage of the selected methodology and technique that will used to develop in every stage in this project.

Chapter 4: Design

This chapter describe about the result of the analysis and project design of this project.

Chapter 5: Implementation

This chapter provide how the testbed and system environment to be setup.

Chapter 6: Testing

This chapter will test the developed project tool on testbed.

Chapter 7: Project Conclusion

This chapter describe the summarization of all the project contribution and project limitation.

1.8 Summary

In this chapter will give reader brief outline about what this project does. The project objective in this project is to develop an pentesting tool with apk file using MSFvenom tool to extract information about the targeting android devices, to setup a listener to receive the connection from the reverse TCP connection from targeting victim's devices in order to obtain the information from the devices, to test the develop pentesting tool in the pre-setup testbed, to generate a risk report to educate victim about the knowledge on how to secure their devices from being exploit by the attackers. The project scope that will be involved is the pre-setup testbed on a virtual platform that involve tester machine installed with Kali Linux OS and victim machine installed with android OS and the application file that created should be signed and aligned by the appropriately signed certificate using some tools. The next chapter is about literature review.

CHAPTER 2: LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

This chapter is about literature review, where focusing on previous study of another researcher works or study about other related work to the project. This literature review is required to gather, analyze and synthesis the collected data from various source such as journal, book, website, E-book and etc. On previous chapter, briefly discussed about the pentesting technique and tools. In this chapter will explained more detail about the pentesting stage and the pentesting methodology involved. This chapter cover literature review to previous study and related work, provide taxonomy of penetration testing phase, critical review of current problem and summary.