



**FORMAN
CHRISTIAN
COLLEGE**
(A CHARTERED UNIVERSITY)

Course Title:

COMP 421 – Information Security

Section: A

Instructor:

Dr Saad Bin Saleem

Instrument:

Project Proposal

Group members with roll numbers:

Sundas Javaid 19-10685

Mahad Rashid 22-11108

Sumera Shafi 231452028

Semester:

SP 22'

Submission Date:

May 2nd, 2022

ANTI-VIRUS EVADING PAYLOADS

By

Sundas Javaid,
Mahad Rashid &
Sumera Shafi

Submitted to:

Dr Saad Bin Saleem

Forman Christian College/ University, Lahore, Pakistan

REVISION HISTORY

| Version | Date | Description |
|---------|------|-------------|
| | | |
| | | |

TABLE OF CONTENTS

| | |
|---|----------|
| 1. Introduction | 5 |
| 1.1 Purpose | 5 |
| 1.2 Document Convention | 5 |
| 1.3 Intended Audience and Reading Suggestions | 5 |
| 1.4 Project Scope | 5 |
| 1.5 References | 5 |
| 2. Project Details | 6 |
| 2.1 Project Execution Plan | 6 |
| 2.2 Project Description | 6 |
| 2.3 Project Outcome | 6 |
| Appendix A | 7 |

1. Introduction

1.1 Purpose

The purpose of this study is to bring about a new concept of Anti-Virus-Evading-Payloads for exploring the significant field of ethical hacking in modern times. This paper contains the goal of this project which is to increase awareness of the reader about the vulnerabilities of an anti-virus. Specific tools will be used to test the vulnerabilities of the target system and then create payloads via backdoors and gain access of the target's system without consent. This will help increase the soundness of the anti-virus software.

1.2 Document Convention

The font used is Times New Roman of 12-size throughout the document except for the second project title page. There are multiple headings but not subheadings yet. These headings are bold and used in blue color. The tools mentioned for the first time in a section are written in italic style. The first page is the title page which shows the essential details. The proceeding page – which is the project title page – has the project name written in 28-size font and university's name in 20-size. The second page contains the table of revisions. The terms which have been defined in the Appendix A have been written in bold font.

1.3 Intended Audience and Reading Suggestions

The reading is intended for people having familiarity with the aspects of cybersecurity and information security in computer sciences. For convenience purposes, the verbiage used will be kept simple and the Appendix A will list down some important abbreviations and terms. It is recommended that the reader first reads the Appendix A and then start with the introduction so that the document is fully understood.

1.4 Project scope

Due to the increasing dependency of humans on digitalization and computerization of data and shifting everything peta-sized data to the internet, it is crucial that the organizations constantly work for the robustness of the antivirus software. The goal of this project is to provide an insight about the cyber risks and threats that are constantly active. Digital technology users are usually not aware about how their systems are at risk and how the hacker/ enemy can manipulate the user's system (also referred to as target system) for their own benefits and ultimately result in loss for the user or the organizations. This study explores how the anti-virus software are endangered. The results of this study can be used to further strengthen the anti-virus security software; and mitigate and prevent such fateful attacks so that cyber security can be guaranteed.

1.5 References

Saleem, S. (2022, March 29). *Anti-Virus-Evading-Payloads*. Github.
<https://github.com/sbinsaleem/Anti-Virus-Evading-Payloads>

2. Project Details

2.1 Project Description

The first task will be to try to get the payload to run on target system computers at the time of exploitation phase of a penetration test or ethical hacking engagement. Running code on target machines is a common aspect of most penetration testing, whether it's through phishing emails, exploits, or social engineering. For effective exploitation, it is imperative to get past the antivirus software or another host-based defense system. Creating a customized backdoor is the most efficient approach to escape the antivirus detection on target's PCs. Antivirus software have in-built hash keys of payloads so that when an external entity tries to gain access of the system, the antivirus software check if the hash keys match with the entries in their databases and block such unauthorized access. When constructing backdoors, focusing on payload's hash keys is an easy technique to get around antivirus software.

2.2 Project Execution Plan

The target system will be scanned for any vulnerabilities. This shall be accomplished via *Wireshark* or *Nikto* according to the requirement. After the vulnerability testing phase is complete, a payload will be made. The payloads and backdoors that are to be used shall be constructed by using *Metasploit*, *Veil*, *MSF Venom*, *The Fat Rat* or *Empire*. The idea behind using a particular payload of a backdoor is to smoothly bypass the antivirus software in the target system. One of these payloads will be used in accordance with the vulnerability result which has been obtained before. This will ensure that the payload enters the target's computer. At this stage, the payload will be activated so that it can work up-to the expected satisfaction level on the target computer. A code from *GitHub* will be used as a standard and changes shall be made in that code to investigate new strategies.

2.3 Project Outcome

After successful execution of payload, the backdoor will not be detectable by the target system's anti-virus. The generated code will allow the testing party to make changes to the target's system as if it were owned by the testing party itself. There will be easy access to the user's identity and relevant personal information. This process shall revolve around the concept of legal hacking. The outcome shall be recorded and analyzed via screenshots and explanations about how the target system is being manipulated via backdoor.

Appendix A

Digitalization – the conversion of text, pictures, or sound into a digital form that can be processed by a computer.

Manipulation – the act of changing/ modifying/ enhancing something skillfully

Vulnerability – the quality or state of being exposed to a possibility of being attacked or harmed