University of Plymouth

School of Engineering,

Computing, and Mathematics

MAL3018

Computing Project

2024/2025

YoInspector

An Automation Pentesting tool

MUHAMMAD SAHIF AS SANI BIN MOHAMAD

BSCS2309753

Supervisor: Ts. Nafisah Misriya Shahul Hamid

BSc (Hons) Computer Science (Cyber Security)

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Ts. Nafisah Misriya Shahul Hamid, for their invaluable guidance, support, and encouragement throughout the course of this project. Their expertise and insights were instrumental in shaping the direction and depth of this project.

I am also thankful to Peninsula College for providing the necessary resources and facilities that enabled the successful completion of this study.

Special thanks to my colleagues and peers who offered constructive feedback and assistance during various stages of the project.

Lastly, I extend my heartfelt appreciation to my family and friends for their unwavering support and motivation throughout this endeavor.

Abstract

This project, titled YoInspector, focuses on developing a command-line-based penetration testing automation tool using Python. It specifically targets two widely exploited vulnerabilities: Android Meterpreter Reverse_TCP and Windows SMB MS17-010 (EternalBlue). Both vulnerabilities are critical due to their widespread impact on Android devices and Windows systems, respectively. YoInspector aims to automate the processes of payload generation and exploitation through the integration of the Metasploit framework, a leading platform in penetration testing.

Android Meterpreter Reverse_TCP is a commonly used attack vector, enabling unauthorized access to Android devices by establishing a reverse TCP connection. The exploit is significant in cybersecurity research and real-world attack simulations due to its versatility in testing mobile device vulnerabilities. Windows SMB MS17-010, known as EternalBlue, was famously used in the WannaCry ransomware attack in 2017. It exploits a critical flaw in the Windows SMB protocol, enabling remote code execution on vulnerable systems. Automating these attacks allows for a deeper understanding of their mechanisms and provides a streamlined method for cybersecurity practitioners to test their systems against these threats.

The project leverages a Linux CLI to provide a lightweight and user-friendly interface for users. Unlike GUI-based tools like Armitage, which can be overly complex for targeted tasks, YoInspector focuses on simplicity and efficiency. Users can select either Android or Windows exploitation tasks through a menu-driven CLI, requiring minimal technical expertise. The integration with Metasploit automates steps such as payload generation, listener setup, and exploit execution, significantly reducing manual configuration.

The tool is designed with several objectives in mind:

1. Automation of Payload Generation: For Android, it automates the creation of APK files for reverse TCP connections. For Windows, it automates the EternalBlue exploitation process, generating payloads that enable remote code execution.
2. Simplification of Metasploit Integration: By using Python scripts to handle complex Metasploit commands, the tool ensures that users do not need advanced knowledge of the framework.
3. Accessibility via Linux CLI: The lightweight command-line interface makes the tool suitable for environments with limited resources, ensuring wide usability across academic, professional, and small business settings.

The primary audience for YoInspector includes:

- Cybersecurity Students: Those looking to gain hands-on experience with penetration testing concepts and tools without requiring advanced technical expertise.
- Penetration Testers: Professionals who need a quick and efficient way to conduct targeted penetration tests on Android and Windows systems.
- Small Businesses: Organizations that lack the resources for comprehensive penetration testing services but want to ensure the security of their systems.

This project builds on the foundation of existing penetration testing tools but fills a critical gap by focusing on lightweight automation for specific vulnerabilities. Tools like AutoSploit and Cobalt Strike offer broader automation but are either limited to generalized attack scenarios or are prohibitively expensive. YoInspector, in contrast, is open-source and caters specifically to Android and Windows vulnerabilities, ensuring cost-effectiveness and precision.

The significance of this project lies in its ability to balance technical functionality with accessibility, making penetration testing more approachable for a diverse range of users. The inclusion of ethical guidelines and disclaimers further ensures that the tool aligns with responsible cybersecurity practices. As the threat landscape continues to evolve, tools like YoInspector play a vital role in equipping individuals and organizations to proactively address vulnerabilities in their systems.

By integrating the Metasploit framework, the project provides users with a powerful and flexible toolset for ethical hacking. Its emphasis on automation not only simplifies the testing process but also highlights the importance of innovation in cybersecurity education and practice. With its focus on Android and Windows platforms, YoInspector demonstrates the potential to bridge the gap between complex penetration testing frameworks and accessible, targeted solutions for cybersecurity challenges.

Contents

Github link: https://github.com/Sahif02/Computing-Project-1.git