RIPHAH INTERNATIONAL UNIVERSITY

Faculty of Computing

FINAL YEAR PROJECT INITIAL PROPOSAL

Automated Reverse Shell through undetectable and obfuscated techniques

Project Team

Full Name of Student	SAP Id	Program	Contact Number	Email Address
Muneeb-Ur-Rehman	32575	BSCY	0310-6161831	32575@students.riphah.edu.pk
Abdul Wahab	36676	BSCY	0311-1912045	36676@students.riphah.edu.pk
Hamid	35415	BSCY	0341-5117009	35415@students.riphah.edu.pk

Sir Humayun Raza
Lecturer at Riphah International University

Project Proposal

Project Title: Automated Reverse Shell through undetectable and obfuscated techniques.

Introduction

In the world of cybersecurity, penetration testing, and red teaming are critical processes that help organizations identify vulnerabilities before malicious actors can exploit them. This project focuses on automating the creation and deployment of reverse shell connections, making payloads undetectable through advanced obfuscation techniques, and enhancing post-exploitation processes. The goal is to streamline and simplify these tasks for pentesters, reducing both time and complexity while maintaining adherence to ethical hacking guidelines.

Problem Statement

The manual execution of reverse shell creation, payload obfuscation, and post-exploitation tasks is not only time-consuming but also prone to frequent errors. Pentesters often encounter challenges and setbacks when performing these tasks, leading to inefficiencies and the need for extensive manual intervention. There is a clear need for a tool or framework that can automate these processes, ensuring that payloads remain undetectable by advanced security defenses e.g. antiviruses. This project aims to overcome the limitations of current methodologies by automating these tasks, ultimately improving the effectiveness and efficiency of penetration testing.

Objectives

1. Automate the process of establishing reverse shell connections with target systems.
2. Develop techniques to make reverse shell payloads undetectable by utilizing methods like obfuscation to alter the signature or behavior of exploits.

3. Automate post-exploitation tasks, including persistence, installing keyloggers, webcam access, access to sensitive files, and reporting.
4. Ensure all processes adhere to ethical hacking guidelines and contribute to the advancement of cybersecurity practices for penetration testers.

Scope of the Project

- **In-Scope**:
  - The project will focus on automating the establishment of reverse shell connections with target systems, reducing manual intervention.
  - Techniques like obfuscation will be employed to alter the signature or behavior of reverse shell payloads, ensuring they remain undetectable by antiviruses.
  - Automation of post-exploitation activities.
- **Out-of-Scope**:
  - Any actions or techniques that fall outside the bounds of ethical hacking.
  - The project will not involve testing or exploiting non-consenting individuals or organizations. All testing and development will be conducted in controlled, simulated environments.
  - The project will not create tools intended for malicious activities, focusing instead on enhancing the capabilities of penetration testers within legal and ethical boundaries.

Literature Review

The project builds on established methodologies in offensive security, particularly in the areas of reverse shell creation and payload obfuscation. Frameworks and tools like Metasploit, Veil-Evasion, and Hoax Shell have been extensively used by pentesters to create reverse shells and obfuscate payloads. However, these tools often require manual configuration and execution, which can be challenging and time-consuming. Research on obfuscation techniques and fileless malware samples demonstrates their effectiveness in evading detection but underscores the need for automation to enhance usability and efficiency.

Expected Outcomes

- A fully automated tool, bypassing antiviruses that simplifies the process of establishing reverse shell connections.
- Development of undetectable reverse shell payloads that can bypass advanced security measures.
- A comprehensive post-exploitation framework that automates key tasks, reducing the manual effort required by pentesters.

Conclusion

This project addresses critical inefficiencies in the current practices of reverse shell creation, payload obfuscation, and post-exploitation techniques. By automating these processes, pentesters can perform their tasks more effectively and efficiently, ultimately contributing to the improvement of cybersecurity practices.