YoInspector

BSCS2309753

About

YoInspector is an advanced penetration testing automation tool.
Built using Python, it integrates seamlessly with the Metasploit framework to automate the exploitation of Android and Windows vulnerabilities.
By simplifying complex attack configurations, YoInspector reduces manual effort and increases testing efficiency.

Supported Attacks

Android Exploitation:

Uses Meterpreter Reverse_TCP to gain remote access to Android devices.

Windows Exploitation:

Utilizes SMB MS17-010 (EternalBlue) to exploit unpatched Windows machines.

Integration with Metasploit

Automates Metasploit commands for efficient exploitation.
Uses Python subprocess calls to execute related modules.
Saves time by eliminating manual Metasploit setup.

Automation Scheme

1. User Input: The user selects the target (Android/Windows) and provides network details (HOST, PORT).
2. Payload Generation: The tool automatically creates a reverse shell payload using Metasploit's msfvenom.
3. Payload Deployment: The user installs or delivers the payload to the target system.
4. Listener Setup: YoInspector configures and launches a Metasploit listener to await connections.
5. Exploitation & Access: Once executed, the payload establishes a reverse shell, granting the tester remote access to the target system.

Advantages

- Fully Automated: Users only provide minimal input (HOST, PORT), and the tool handles the rest.
- Simplifies Metasploit Usage: Reduces complexity in penetration testing for Android and Windows systems.
- Command-Line Interface (CLI): Lightweight and optimized for Linux-based penetration testing environments.
- Scalable & Modular: Can be expanded to include additional exploits and attack techniques.

UNIVERSITY OF PLYMOUTH