Automated\_security\_framework is a penetration testing toolkit. The goal is to simplify and enhance the footprinting and scanning steps for testing purposes. It gives various features such as footprinting websites (Ping, whois, traceroute, dns enumeration, etc), or footprinting machines in your private network.

This tool also allows port scanning and scanning for known vulnerabilities using nmap.

**Features:**

1. Whois
2. Traceroute
3. Domain / IP Age
4. DNS Enumeration
5. NS Lookup
6. Dig
7. Port Scanning
8. Different types of nmap scans (as per user requirement)
9. Nmap scripting engine
10. Option to save outputs seperately for various users

**Usage:**

cd /opt/

git clone https://github.com/73pp31in/Pentesting-Framework.git

chmod 777 framework.sh

./framework.sh

Important: For best usage, run the script in an empty folder, as all the outputs (if chosen to save) will be stored in the "outputs" folder that will be created in the root folder of the application.

**Supported OS:**

Kali Linux

**Coming Soon:**

1. More NSE Scripts
2. Python implementation (for multiple Platform support)
3. Exploit Techniques and various attacks used for testing.