CyberSec Toolkit 2025 - Enhanced Edition

Submission for Project Competition 2025 by ThinkCyber

Project Overview

Author: ELVIN HUMURA
Student Code: S24
Class Code: RW-CODING-ACADEMY-I
Lecturer: CELESTIN NZEYIMANA
Institution: Rwanda Coding Academy

The **CyberSec Toolkit 2025 - Enhanced Edition** is a sophisticated Python-based cybersecurity suite designed for the ThinkCyber Project Competition 2025. It integrates twenty-five powerful tools with advanced features, providing capabilities for system monitoring, security testing, network analysis, forensics, and threat intelligence.

Features and Modules

1. System Monitoring & Security Testing

- Real-time system metrics with anomaly detection
- Security testing with packet crafting
- Remote reconnaissance with encrypted credentials
- Network scanning with vulnerability scoring
- Firewall rule auditing and optimization
- Intrusion Detection System (IDS) monitoring

2. Network & Web Security

- DNS enumeration and spoofing detection
- Wi-Fi security scanning and vulnerability analysis
- Web security scanner (SQLi, XSS, directory traversal detection)

- SSL/TLS auditor for certificate security
- Advanced protocol analyzer

3. Digital Forensics & Malware Analysis

- Memory forensics (RAM dump analysis)
- Static and dynamic malware analysis
- Binary analysis (reverse engineering)
- Packet forensics with deep PCAP inspection
- Auth log analyzer with threat intelligence integration

4. Offensive Security & Threat Intelligence

- Exploit framework for vulnerability assessment
- Dark web scanner for Onion network search
- OSINT collection (WHOIS, Shodan, web scraping)
- Phishing detection (email and URL analysis)
- Synthetic attack generator (DDoS, SYN flood, ICMP flood)

5. Reporting & Automation

- SOC automation dashboard for real-time threat monitoring
- GeoIP threat mapping and visualization
- Automated honeypot deployment
- PDF reporting for generated analysis

Technical Specifications

System Requirements

- **OS**: Linux (Ubuntu 20.04+), Windows 10/11 (WSL recommended)
- **Python**: 3.8 or higher
- **Memory**: 8GB RAM minimum (16GB+ recommended)
- **Storage**: 2GB free space
- **Network**: Stable internet connection required
- **Privileges**: Administrator/Root access required for full functionality

Dependencies

System Tools

sudo apt-get install -y nmap masscan hydra hping3 whois aircrack-ng tcpdump wireshark radare2 volatility tor git python3-dev

Python Libraries

pip install -r requirements.txt

Installation Guide

Step 1: Clone the Repository

git clone https://github.com/humuraelvin/Quantum-Lock.git

cd Quantum-Lock

Step 2: Set Up Environment

python -m venv venv

source venv/bin/activate # Linux/Mac

or

.\venv\Scripts\activate # Windows

Step 3: Install Dependencies

pip install -r requirements.txt

Step 4: Initialize Database and Configuration

python QuantumLockScript.py --init

Usage Guide

Launch the Toolkit

sudo ./QuantumLockScript.py # Linux/Mac

or

python QuantumLockScript.py # Windows (as Administrator)

Navigation

- Use number keys (0-25) to select tools
- Follow on-screen prompts
- Use `Ctrl+C` to exit any tool

Example Commands

python QuantumLockScript.py --scan 192.168.1.0/24 # Network scanning

python QuantumLockScript.py --osint example.com # OSINT collection

python QuantumLockScript.py --malware /path/to/file # Malware analysis

Reports and Logs

- Generated results are stored in `cybersec_output_YYYYMMDD_HHMMSS`.
- Detailed logs are saved in `cybersec_toolkit.log`.
- PDF reports can be exported after analysis.

Security Notice

This toolkit is designed for **educational and authorized testing purposes only**. Unauthorized use against systems without explicit permission is illegal and unethical.

License