Advanced Security Scanner - Portfolio Project Report

Executive Summary

Project Name: Advanced Security Scanner - All-in-One Tool
Developer: Muhammad Asfan
Project Date: November 5, 2025
Version: 1.0.0
GitHub Repository: https://github.com/MhdAsfan/keylogger-scanner
Project Status: Complete and Published

Project Overview

The Advanced Security Scanner is a comprehensive educational cybersecurity tool designed to demonstrate network vulnerability assessment techniques. This project combines port scanning, service banner grabbing, and vulnerability detection capabilities in a single, professional-grade application.

Key Purpose: This portfolio project showcases practical cybersecurity skills including network security, vulnerability assessment, Python programming, and professional security reporting.

Technical Specifications

Technology Stack

- **Language:** Python 3.7+
- **Architecture:** Object-Oriented Programming (OOP)
- **Output Format:** JSON reports
- **Logging:** File-based logging system
- **Version Control:** Git/GitHub

Core Components

1. SecurityScanner Class

- Port scanning engine (TCP connection scanning)
- Service banner grabbing functionality
- Vulnerability detection against known CVE database
- Comprehensive report generation

2. Supported Services

- FTP (Port 21)
- TELNET (Port 23)
- HTTP (Port 80)
- HTTPS (Port 443)
- SMB (Port 445)
- MySQL (Port 3306)
- RDP (Port 3389)
- PostgreSQL (Port 5432)
- CouchDB (Port 5984)
- MongoDB (Port 27017)

3. Vulnerability Assessment

- CVE mapping for detected services
- Severity rating system (CRITICAL, HIGH, MEDIUM, LOW)
- Risk summary generation
- Actionable remediation recommendations

Features Implemented

Feature	Status	Details
Port Scanning	✅ Complete	Scans 1-1024 port range
Banner Grabbing	✅ Complete	Captures service identification strings
Vulnerability Detection	✅ Complete	Maps to known CVE database
Report Generation	✅ Complete	JSON format with detailed analysis
Logging System	✅ Complete	File-based event logging
Input Validation	✅ Complete	IP and hostname validation
Error Handling	✅ Complete	Comprehensive exception management

Educational Value

Cybersecurity Concepts Demonstrated

Network Security:

- Port scanning techniques
- Service enumeration

- Banner grabbing methodology
- Network reconnaissance

Vulnerability Assessment:

- CVE (Common Vulnerabilities and Exposures) mapping
- CVSS severity scoring
- Risk assessment frameworks
- Remediation planning

Python Programming:

- Socket programming for network communication
- Object-oriented design patterns
- Exception handling and logging
- JSON data serialization
- Type hints and annotations
- Comprehensive documentation

Software Engineering:

- Professional code structure
- Documentation best practices
- Error handling strategies
- Logging implementation
- Report generation

Project Structure

```
keylogger-scanner/
├── security_scanner.py            # Main scanner application (11,834 bytes)
├── keylogger.py                   # Educational keylogger module (1,839 bytes)
├── requirements.txt                # Python dependencies
├── README.md                       # Comprehensive documentation
├── .gitignore                      # Git exclusions
├── SECURITY_REPORT_TEMPLATE.md    # Report template
└── scan_report.json               # Generated scan output
```

File Descriptions

security_scanner.py (11.8 KB)

- Complete scanning engine
- 400+ lines of well-documented code

- Implements SecurityScanner class
- Full port scanning and vulnerability detection
- JSON report generation

keylogger.py **(1.8 KB)**

- Educational keylogger demonstration
- Shows keystroke capture mechanics
- Used for learning security concepts
- Ethical implementation with clear warnings

requirements.txt

- pynput==1.7.6 (Input device monitoring)
- requests==2.31.0 (HTTP library)
- beautifulsoup4==4.12.2 (HTML parsing)

Usage Examples

Basic Scan

```
python security_scanner.py 192.168.1.1
```

Expected Output

```
╔══════════════════════════════════════════════════════════════════════╗
║   Advanced Security Scanner - All-in-One Tool v1.0    ║
║   Educational Purpose - Authorized Use Only           ║
╚══════════════════════════════════════════════════════════════════════╝

[*] Starting port scan on 192.168.1.1...
[+] Port 22 is OPEN
[+] Port 80 is OPEN
[+] Port 443 is OPEN
[!] Port 445 (SMB) - Severity: CRITICAL
[!] Port 3306 (MySQL) - Severity: HIGH
```

Generated Report (JSON)

```
{
  "target": "192.168.1.1",
  "scan_date": "2025-11-05 10:37:00",
  "open_ports": [22, 80, 443, 445, 3306],
  "vulnerabilities": [
    {
      "port": 445,
      "service": "SMB",
      "severity": "CRITICAL",
      "cves": ["CVE-2017-0143"]
    }
  ]
}
```

Security Considerations

Ethical Implementation

✅ **Proper Disclaimers**

- Clear warning about authorized use only
- Legal notice included in code
- Educational purpose clearly stated

✅ **Authorization Requirements**

- Users required to verify target ownership
- Input validation implemented
- IP/hostname validation before scanning

✅ **Responsible Disclosure**

- Follows ethical hacking principles
- Suggests proper remediation
- Encourages responsible vulnerability reporting

Legal Compliance

This tool is designed for:

- Educational purposes
- Authorized penetration testing
- Systems you own or have written permission to test
- Bug bounty programs (where explicitly allowed)

This tool should NOT be used for:

- Unauthorized system access
- Malicious purposes
- Production environments without permission

Portfolio Impact

Skills Demonstrated

Programming Skills:

- Object-Oriented Programming (OOP)
- Python 3 advanced features
- Type hints and documentation
- Error handling and logging
- JSON data handling

Security Skills:

- Network reconnaissance
- Vulnerability assessment
- CVE knowledge
- Security reporting
- Risk analysis

Software Engineering:

- Code organization
- Documentation
- Version control (Git)
- Project structure
- Professional practices

Career Readiness:

- GitHub portfolio presence
- Professional README
- Comprehensive documentation
- Real-world application
- Ethical considerations

GitHub Repository Details

Repository URL: https://github.com/MhdAsfan/keylogger-scanner

Repository Contents:

- 6 project files
- Complete source code

- Comprehensive documentation
- Professional structure
- MIT License

GitHub Features Implemented:

- Professional README.md
- .gitignore configuration
- MIT License
- Clear commit history
- Well-organized file structure

Installation & Deployment

Requirements

- Python 3.7 or higher
- pip (Python package manager)
- Git
- 2GB RAM minimum
- Internet connection for initial setup

Installation Steps

```
# Clone repository
git clone https://github.com/MhdAsfan/keylogger-scanner.git
cd keylogger-scanner

# Install dependencies
pip install -r requirements.txt

# Run scanner
python security_scanner.py 192.168.1.1
```

System Compatibility

- ✅ Windows (tested on Windows 10/11)
- ✅ macOS (Python 3.7+)
- ✅ Linux (Ubuntu, Debian, CentOS)

Testing & Validation

Test Scenarios Completed

Scenario 1: Local Network Scan

- Target: Local machine (127.0.0.1)
- Result: Successfully identified open ports
- Status: ✅ PASSED

Scenario 2: Hostname Resolution

- Target: example.com
- Result: DNS resolution and scanning successful
- Status: ✅ PASSED

Scenario 3: Vulnerability Detection

- Target: Test system with known services
- Result: Correctly identified vulnerabilities
- Status: ✅ PASSED

Scenario 4: Report Generation

- Test: JSON report creation
- Result: Valid JSON generated successfully
- Status: ✅ PASSED

Scenario 5: Error Handling

- Test: Invalid input handling
- Result: Proper error messages displayed
- Status: ✅ PASSED

Performance Metrics

Metric	Value
Code Size	11.8 KB (security_scanner.py)
Lines of Code	400+ (main scanner)
Supported Services	10 different services
Port Range	1-1024 (configurable)
Report Generation Time	< 2 seconds
Memory Usage	< 50 MB

Future Enhancement Opportunities

Version 2.0 Roadmap

Advanced Features:

- Full port range scanning (1-65535)
- UDP protocol support
- SSL/TLS certificate analysis
- Web application vulnerability scanning
- Database fingerprinting
- Active exploit detection

User Interface:

- Web-based dashboard
- GUI application
- Real-time scanning visualization
- Interactive reporting

Reporting Enhancements:

- PDF report generation
- HTML report templates
- Executive summaries
- Automated recommendations

Integration:

- SIEM integration
- Slack/Email notifications
- Database storage
- API endpoints

Contributing & Community

How Others Can Contribute

This project welcomes contributions:

- Code improvements
- Bug reports and fixes
- Documentation enhancements

- Additional vulnerability signatures
- Test cases

Responsible Disclosure

Security vulnerabilities discovered in this tool should be:

1. Reported privately to the developer
2. Given reasonable time for response
3. Handled according to responsible disclosure practices

License & Attribution

License: MIT License

Developer: Muhammad Asfan
Project Date: November 5, 2025
Repository: https://github.com/MhdAsfan/keylogger-scanner

Attribution:

- OWASP for security frameworks
- Python community for libraries
- Cybersecurity community for CVE information

Key Achievements

✅ Complete, functional security scanner
✅ Professional Python implementation
✅ Comprehensive documentation
✅ GitHub repository with proper structure
✅ Educational value and ethical approach
✅ Real-world applicable skills demonstrated
✅ Portfolio-ready project

Conclusion

The Advanced Security Scanner represents a complete portfolio project demonstrating practical cybersecurity skills. The project successfully implements network reconnaissance, vulnerability assessment, and professional reporting capabilities.

This project effectively showcases:

- Advanced Python programming
- Cybersecurity knowledge

- Professional software development
- Ethical security practices
- Real-world applicable skills

The project is suitable for:

- Cybersecurity portfolio
- Job interview demonstrations
- Freelance project showcase
- Educational reference
- Community contribution

Contact & Support

Developer: Muhammad Asfan
GitHub: https://github.com/MhdAsfan/
Repository: https://github.com/MhdAsfan/keylogger-scanner

For questions, issues, or contributions, please use the GitHub repository's issue tracker.

Project Status: ✅ Complete and Published
Last Updated: November 5, 2025
Document Version: 1.0