PENETRATION TESTING TOOL BASED ON SINGLE-BOARD COMPUTERS PIRat

Authors: Grushka M.O., Skarga-Bandurova I.S.

Basic characteristics, essence of the development
Penetration testing tool PIRat is a hardware and software tool that implements modelling methods of external malicious acts, as well as allows making combined attacks and displaying the status of attacks. Testing process management is carried out via existing mobile devices using single-board computers.

Patentable and competitive results
The developed software of the PIRat system allows using single-board computers for penetration testing under conditions similar to real.
The main advantage of such development is that it does not require any additional installation or deployment system for testing, such as, e.g. Cyber Ranges.
To begin testing it is necessary to connect the attacking single-board computer managed via a mobile device with a pre-prepared Linux distribution.

Comparison with world analogues
Penetration testing uses the most popular specially optimized Linux distributions (Kali Linux, BlackArch Linux), which contain many individual software pentest tools.
The developed software is a graphical environment of Linux. It allows its installation on the pentest distribution, and usage of tools included into the distribution in addition to its own techniques of detection and usage of vulnerabilities. One of the key advantages is a common interface for various software pentest tools.

Economic attractiveness of the development for market promotion, implementation, parameters, price
PIRat is an effective automated tool for security testing that simulates real attacks and hacking techniques and allows performing comprehensive analysis of local networks.
Usage of PIRat enables to check reliability of each element of the network within the organization and qualitatively assess the security policy without additional investment in software and personnel.
The tool is equipped with a specially designed graphical shell that provides convenient management of testing programmes.
Although the development is mainly focused on single-board computers, used cross-platform tools enable to use the developed software not only for single-board computers, but for any devices under Linux: desktop computers, laptops, workstations, servers.

Branches, ministries, departments, enterprises and organizations where the development results are going to be implemented
The product is designed for organizations and professionals involved in auditing security of computer systems and networks.

Development readiness level - (100%)
The system is at the stage of beta testing.

Implementation results

A simplified block diagram of software to manage the testing process of computer systems' and networks' security on single-board computers using available mobile devices is shown in Fig. 1.

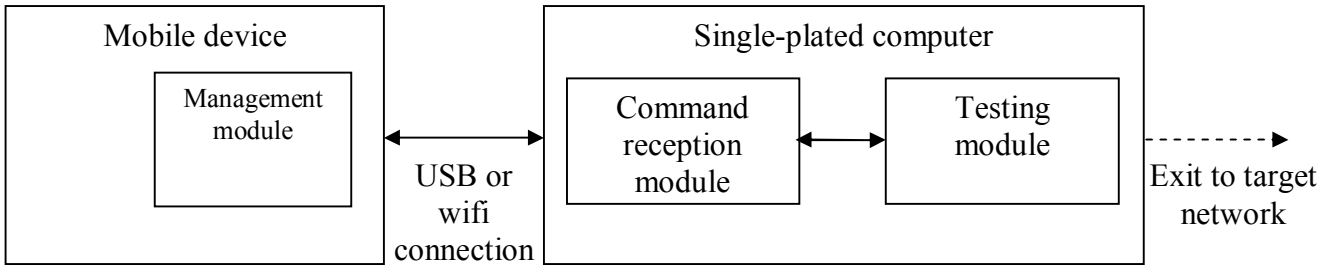

Figure 1 - Block diagram of PIRat tool

Graphical shell is developed using Qt framework. Implementation of penetration testing techniques uses the programming languages: C, C ++, Python 3, Bash script.

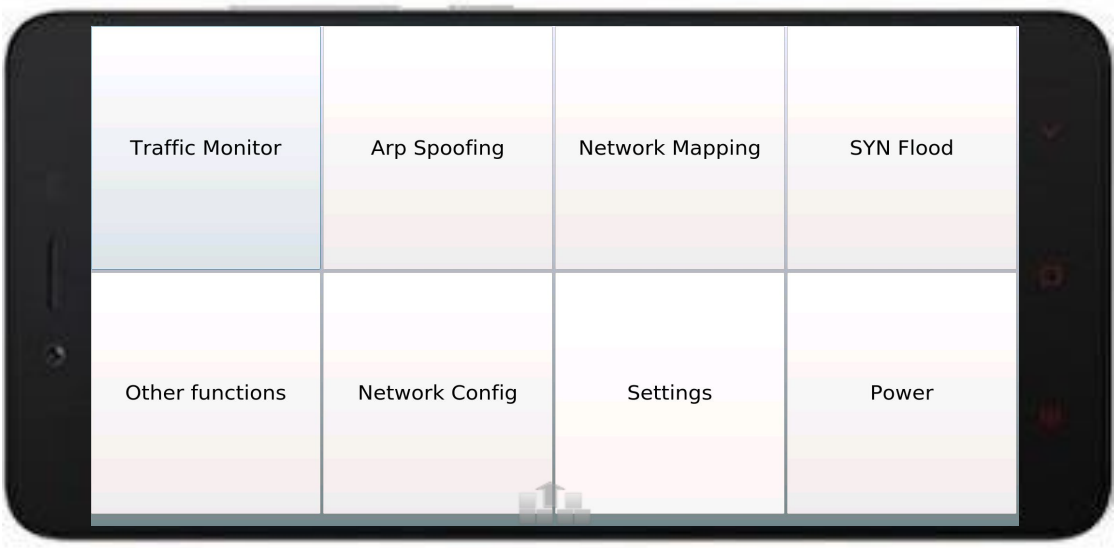

Figure 2 - Main window of the programme of penetr