GENERAL STRUCTURE OF THE SOFTWARE PROTECTION SYSTEM NETWORK RESOURCES

Nebero K.I., *nebero.karina@gmail.com*
Institute of Special Communications and Information Security, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

The use of cyberspace expands the opportunities for people to communicate, promotes the development of information technology, research and innovation, stimulates business development, creates a global interactive market. At the same time, the benefits of modern cyberspace inevitably lead to new threats to people, society, national and international security. Along with incidents of natural (unintentional) origin, the number and power of cyberattacks motivated by the interests of individual states, associations of states, groups and individuals is growing [1].

Hacker groups are turning into cyber-terrorist organizations. Given that in recent years, information technology is increasingly used to achieve military-political goals, interference in the internal affairs of sovereign states and public order, acts of aggression against other states, the destructive impact on critical infrastructure, it allows against our state a number of cyberattacks and cyber operations, which can lead to problems related to the smooth operation of critical infrastructure.

It is known that information about the status of TCP / IP ports is the basis of network security. Building a network profile and creating tools for recognizing network traffic allows you to more effectively recognize unauthorized users. Network ports are the entry points to a machine connected to the Internet. The service that listens on the port can receive data from the client program, process it, and send a response back. Malicious clients can sometimes exploit server code vulnerabilities to gain access to sensitive data or remotely execute malicious code on a machine. That is why testing for all ports is necessary in order to achieve the highest level of security verification [2].

Port scans are usually performed at the initial stage of the penetration test to detect all network entry points.

Port scanners are one of the most useful tools for security in any remote or local network. There are the following five most popular port scanners:

– Nmap;
– Unicornscan;
– Angry IP Scan;
– Netcat;
– Zenmap .

Scanner ports are listed in order of popularity. Nmap is considered to be the most popular.

Nmap, "Network Mapper" - free open source software for research and audit of network security and detection of active network services. Since its publication in 1997, it has become the standard in the field of information security. The author of the program, Gordon Lyon, better known as Fyodor, after the release of version 5.0 called it the greatest

development of the application since 1997, when raw codes were first published in the journal Phrack.

Nmap uses many different scanning methods, such as UDP, TCP (connect), TCP SYN (semi-open), FTP -proxy (break through ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN- and NULL scan. Nmap also supports a wide range of advanced features.

Advanced Port Scanner is a free port scanner that allows you to quickly find all open ports on network computers and identify programs running on those ports. The program has a user-friendly interface and rich functionality [2].

Consider a software system for scanning available ports called "Scanner of ports availability", or "SPA" for short. The program scans ports using user-entered network addresses and implements the output in the form of a report stored in a .txt or .json file.

The algorithmic model of the software system is the following:

1. Specify a file with a finite number of network addresses. Also the lower threshold and the upper port scanning threshold are specified.
2. Use the API to create a connection for each of the addresses.
3. Check the availability of ports from the lower threshold to the upper for each of the network addresses.
4. The entire report is displayed in a file located in the current folder software system and is called "Ports.txt" or "Ports.json". Report file contains a table for recording data with mandatory fields "IP Address", "Number and condition of the port".

The main drawback that was identified when testing the software system, there is a vulnerability of open ports during scanning, and lack ability to close them during the operation of the software system.

Every open network port is connected to an application that listens to the network. Thus, everyone's attack surface server that is connected to the network can be reduced by disable optional network services and applications.

References

1. SecurityTrails. Access mode: https://securitytrails.com/blog/best-port scanners (access date: March 21, 2018)
2. Advanced Port Scanner. Access mode: https: //www.advanced-port scanner.com/ru/ (access date: 21.03.2018)
3. Scan the TCP port using Nmap. Access mode: https: // pentest tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap (date appeal: March 21, 2018)

Scientific adviser: *Zhylin A.V., Candidate of Technical Sciences, Associate Professor of the Special Department № 5, Institute of Special Communications and Information Security, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"*