Journal scientific and applied research, vol. 23, 2022
International Journal

Original Contribution

ISSN 1314-6289

IMPLEMENTATION OF MODIFIED NETWORK PORT SCANNER FOR WINDOWS BASED OPERATING SYSTEMS

Petar Boyanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,

E-MAIL: petar.boyanov@shu.bg

ABSTRACT: *In this paper a modified network port scanner for Windows based operating systems implementing a linear algorithm is developed.*

KEY WORDS: *Algorithm, Analysis, Connection, Libraries, Monitoring, Network, Ports, Processes, Scanning, Services, Traffic, Threads, Visual Studio, Windows.*

1. Introduction

Malicious attackers usually have motives and goals behind their information security cyberattacks. The motive stems from the idea that the target computer system is storing or processing something valuable, leading to the threat of an attack against the system. The goal of the attack may be to disrupt the business operations of the target organization, steal valuable information for curiosity or even revenge [2,3,6,9,10,11,14,24,25,26,28,29,32]. Therefore, these motives or goals depend on the state of mind of the malicious attacker, the reason for carrying out such activity, as well as his informational resources and capabilities. Once an attacker has identified their target, they can use a variety of software tools, cyberattack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls [1,4,5,7,8,11,13,27,26,27,29]. Therefore, the cyberattack is a collection of motives, targets, methods and exposed vulnerabilities.

The main motives for carrying out malicious cyberattacks are [19,20,23]:

- Disruption of business continuity [11,12,20,21,22,24,28,30,31,32].
- Committing information theft.
- Manipulation of electronic data.
- Creating fear and chaos to destroy certain critical infrastructure.

- Causing a financial loss to the respective company or corporation.
- Propaganda of certain religious or political beliefs.
- Achieving strict military objectives of the state.
- Damages the reputation of a chosen victim, which can be a host, corporation, government institution, etc [1,3,4,7,9,14,15,21,22,23,24,28,30,31].
- Taking revenge.
- Ransom and extortion.

In this scientific research, the main emphasis on the implementation of modified network port scanner using a linear algorithm in Windows based operating systems is placed.

2. Experiment

The experiment in a specialized computer network laboratory in the Faculty of Technical Sciences is made. In this paper a linear algorithm for network port scanning is suggested. This algorithm is respectively designed to operate on Windows based operating systems. In this regard, fundamentally new approaches for algorithmization of activities related to network port scanning is developed.

The modified port scanner in the Microsoft Visual Studio Ultimate 2012 version 11.0.50727.1 RTMREL software environment is developed. The used framework is .NET Framework 4 Client Profile. The applied programming language is Visual Basic and the project is a Microsoft Forms Application type in order to be created a graphical user interface of the port network scanner.

The operation of the modified port scanner implementing a linear algorithm for network port scanning for Windows based operating systems involves the following basic steps:

1. Loading the System.Net and System.Net.Sockets libraries. They allow programming and configuration of many network protocols for network communication.
2. Configuring the time to send and wait for a response from the host.
3. Entering the relevant global variables.
4. Defining the loopback (localhost) address - 127.0.0.1 as default address for initial port network scan.
5. Defining the start and end port fields for network scanning.
6. Defining the open ports field on the host.
7. Defining the field for the discovered closed ports on the host.
8. Configuring the button to start the network port scan.
9. Defining the rules and signaling when an IP address is incorrectly entered in the IPv4 address field or the start and end port numbers. The error message that appears is "Incorrectly configured IPv4 address or ports!!!".
10. Loading the Port Scanner graphical user interface (GUI).

The scientific research using the operating system Microsoft Windows 10 Pro x64 is carried out in order to scan and detect open ports on active hosts in

the local and wide computer networks. The network port scanner does not have any malware embedded in it, and thus a specialists or users can use it for performing host scan without having to worry about being infected with viruses and worms.

The flowchart of a modified network port scanner for Windows based operating systems implementing a linear algorithm on fig. 1 is presented.

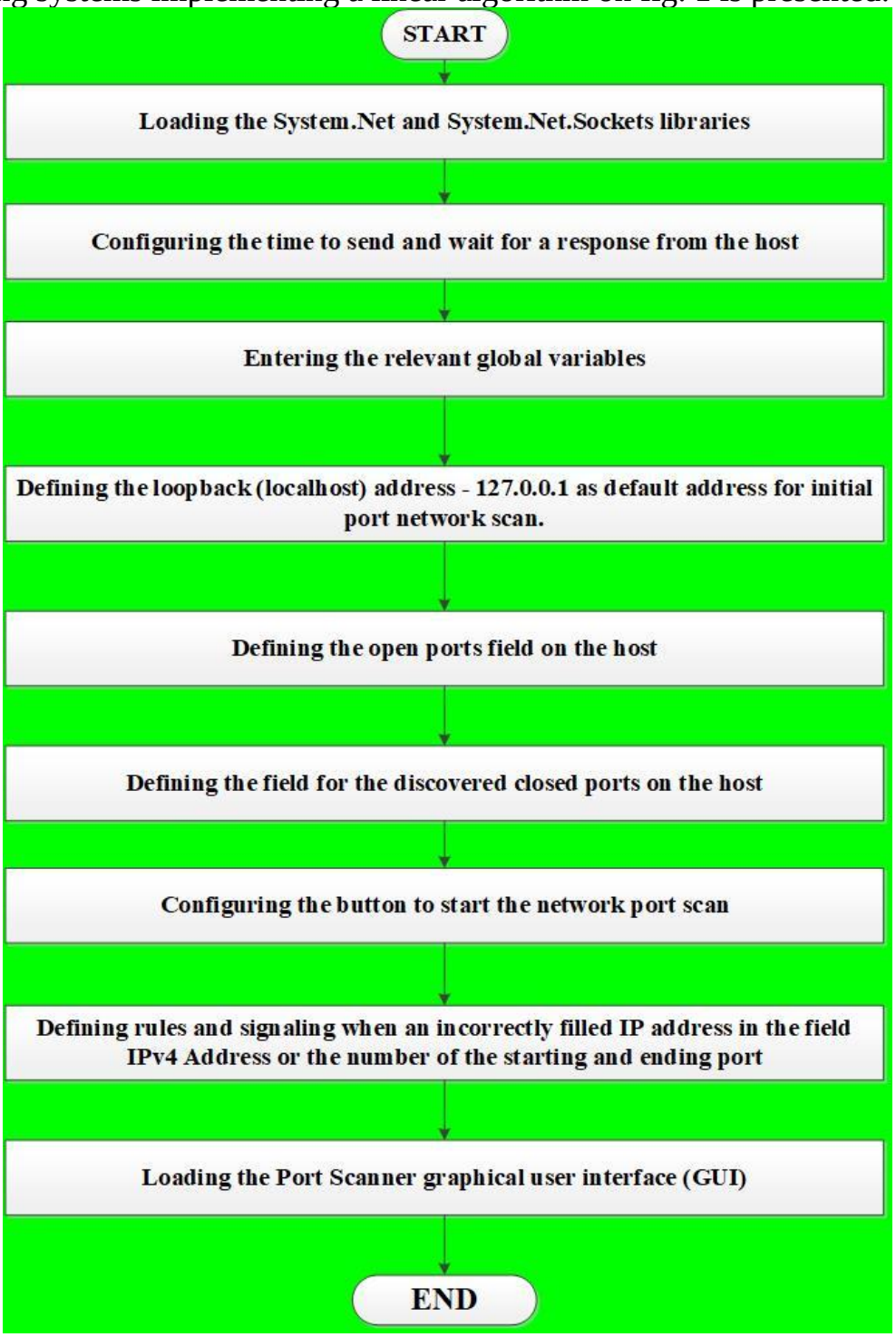

Fig. 1. Flowchart of a modified network port scanner for Windows based operating systems implementing a linear algorithm

3. Results

The loaded project of modified network port scanner in the Microsoft Visual Studio environment on fig. 2 is showed. The loaded files of the project in fig. 3 are presented.

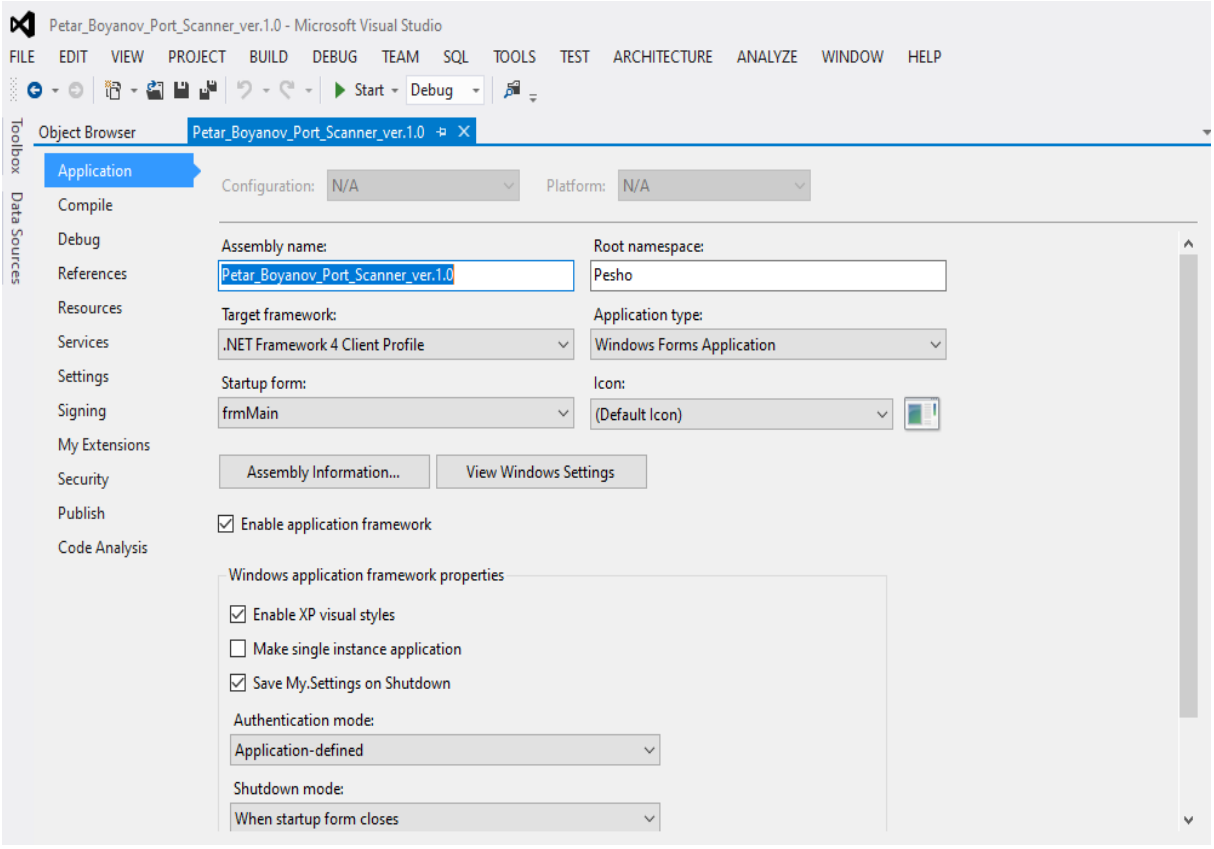

Fig. 2. The loaded project of modified network port scanner in the Microsoft Visual Studio environment

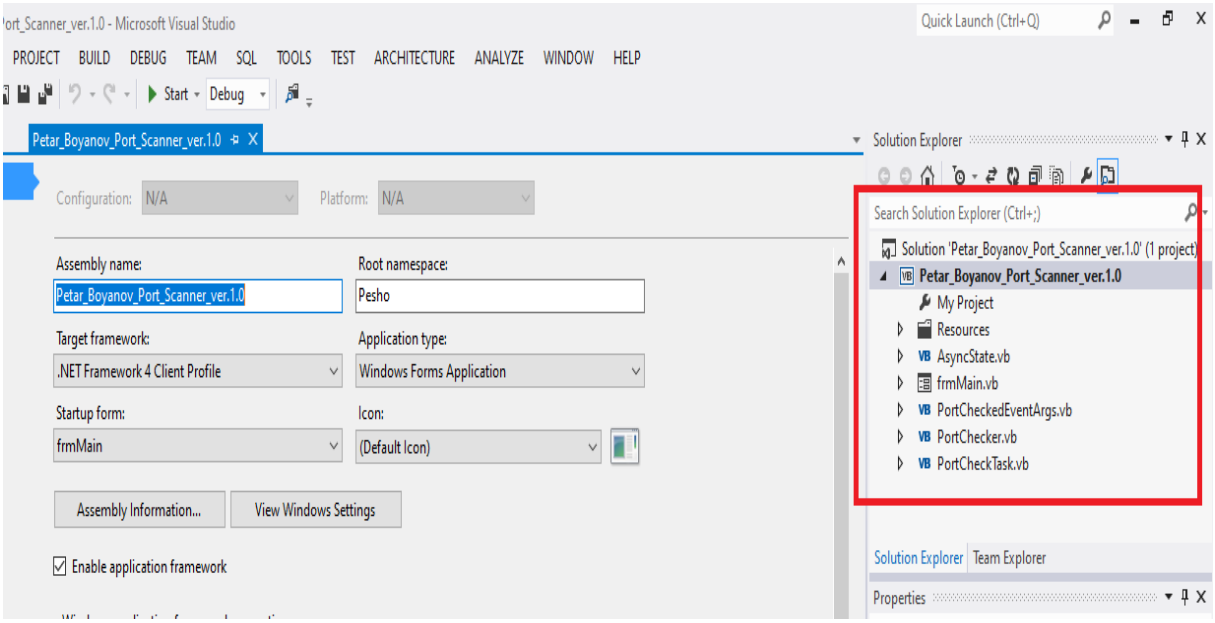

Fig. 3. The loaded files of the project for network port scanning

On fig. 4 the received results from the performed network port scan of the internal loopback address of the host are showed.

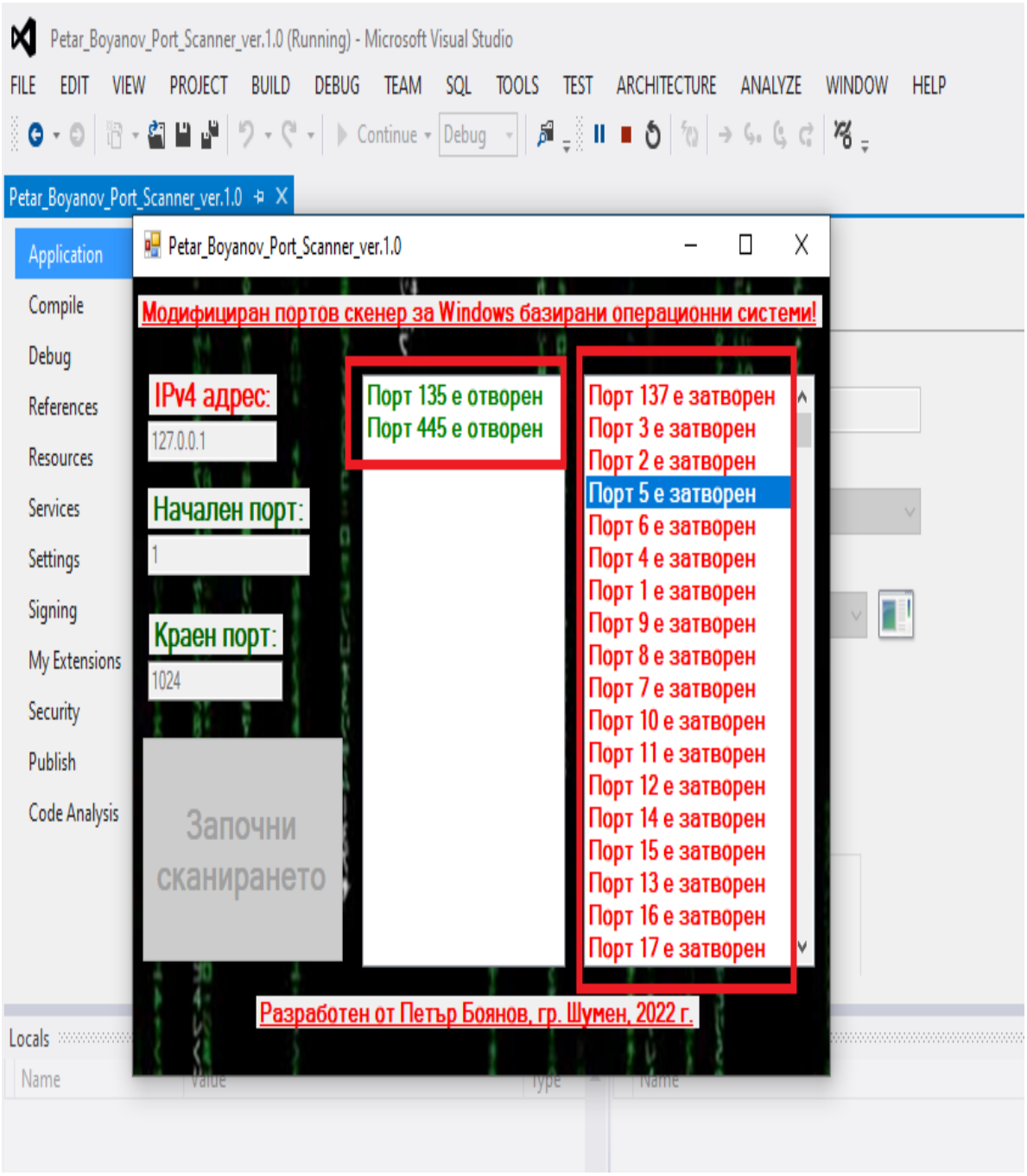

Fig. 4. The received results from the performed network port scan of the internal loopback address of the host

From the obtained results from fig. 4 it is found that 2 open ports are found on the Windows 10 Pro x64 operating system on the scanning host. The rightmost column lists all closed ports and leftmost column lists all found open ports. The total number of the scanned ports is 1024. It should be noted that this

network scanner only works with IPv4 addresses, and the ability to scan domains will be added in the next scientific future research and development.

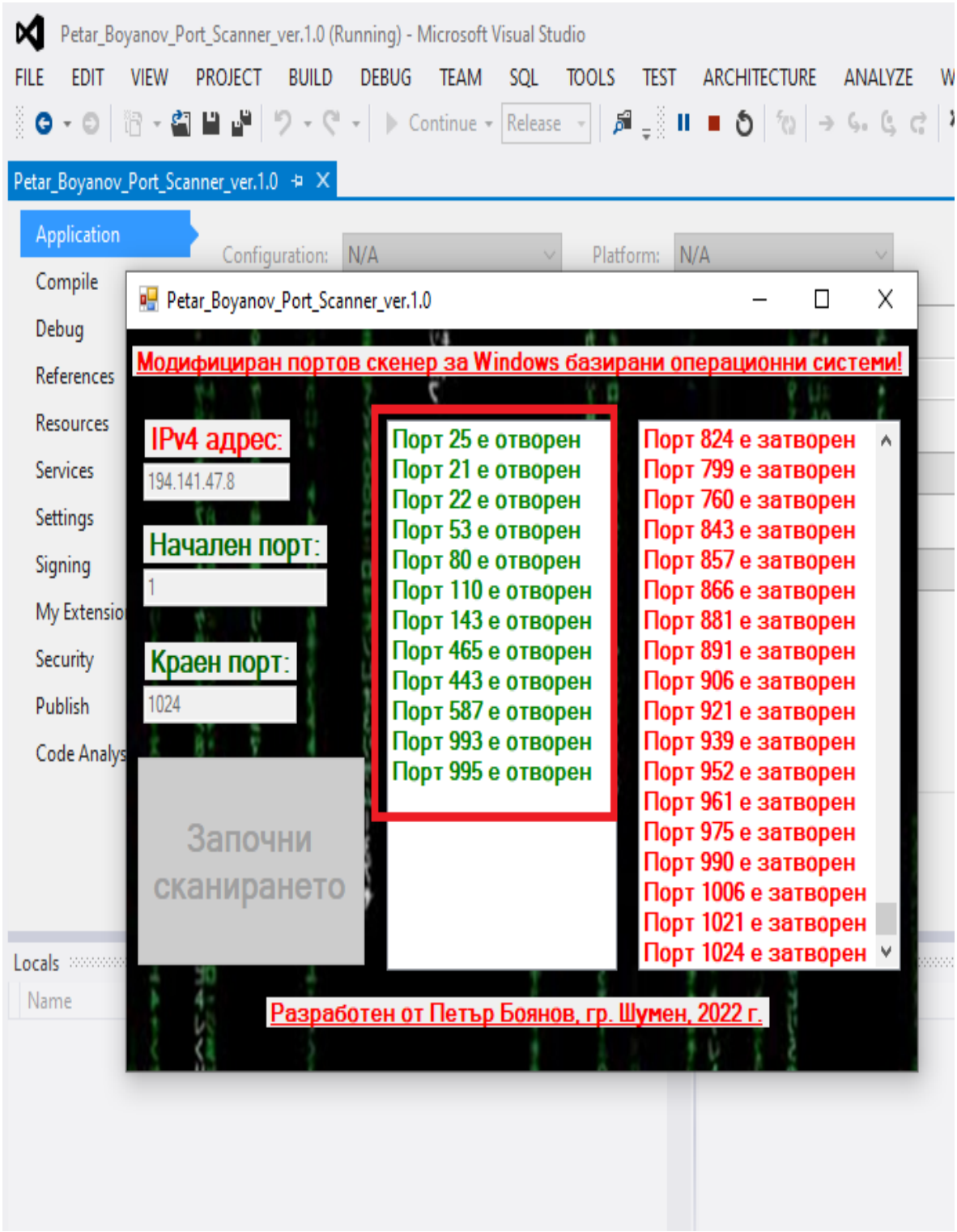

Fig. 5. The detailed information about the results of the performed port scan for host with the IP address 194.141.47.8

The obtained results from fig. 5 show that 12 open ports are found out of a total of 1024 ports scanned. As in the previous figure above, closed ports are colored red and in the rightmost column of the port scanner are located. The found open port numbers are accordingly 21, 22, 25, 53, 80, 110, 443, 443, 465, 587, 993 and 995. Actually, the public IPv4 address 194.141.47.8 is the address of the subdomains jsar.ftn.shu.bg and ftn.shu.bg and this software application does not reveal the fully qualified domain name (FQDN) of the scanned subdomain. The obtained detailed information about the started services and protocols on the detected open ports is the following:

- Open port 21 - File Transfer Protocol (FTP).
- Open port 22 - The Secure Shell (SSH) Protocol.
- Open port 25 - Simple Mail Transfer Protocol (SMTP).
- Open port 53 - Domain Name Server (DNS).
- Open port 80 - World Wide Web, Hypertext Transfer Protocol (HTTP).
- Open port 110 - Post Office Protocol - Version 3.
- Open port 143 - Internet Message Access Protocol (IMAP).
- Open port 443 - World Wide Web, Hypertext Transfer Protocol Secure (HTTPS).
- Open port 465 - URL Rendezvous Directory for Source Specific Multicast (SSM).
- Open port 587 - Message Submission.
- Open port 993 - IMAP over Transport Layer Security (TLS) protocol
- Open port 995 - Post Office Protocol 3 (POP3) over TLS protocol.

The presented modified network port scanner for Windows based operating systems in Bulgarian Defense Institute can be used in order to be detected open unprotected network ports. In relation to this the chief information security officers will be able to take timely measures to implement protective mechanisms and policies for the protection of the information resources containing critical and confidential information about data centers in defense and security, jamming devices, bullets, ammunitions, projectiles, rocket motors and ballistic materials [1,2,15,16,17,18,19,20,21,22,27,31,32].

Thanks to this information, the malicious perpetrator can use the most correct exploit to perform unauthorized and unsanctioned access to the resources of the victim host. At the same time, the system administrator's goal is to apply security mechanisms to each of the found open ports.

The results of the conducted scientific research show that this modified network port scanner for Windows based operating systems is able to find ports with open state in a relatively short time. In this scientific research, it is shown that the maximum number of scanned ports is configured to be up to 1024. As is accepted in practice, the total number of ports is 65535. In the next further scientific research a time will be added that counts the elapsed seconds of the network port scan.

The statistical processing between the sent network packets in bytes and the found open ports from the scientific research visually in fig. 6 are presented.

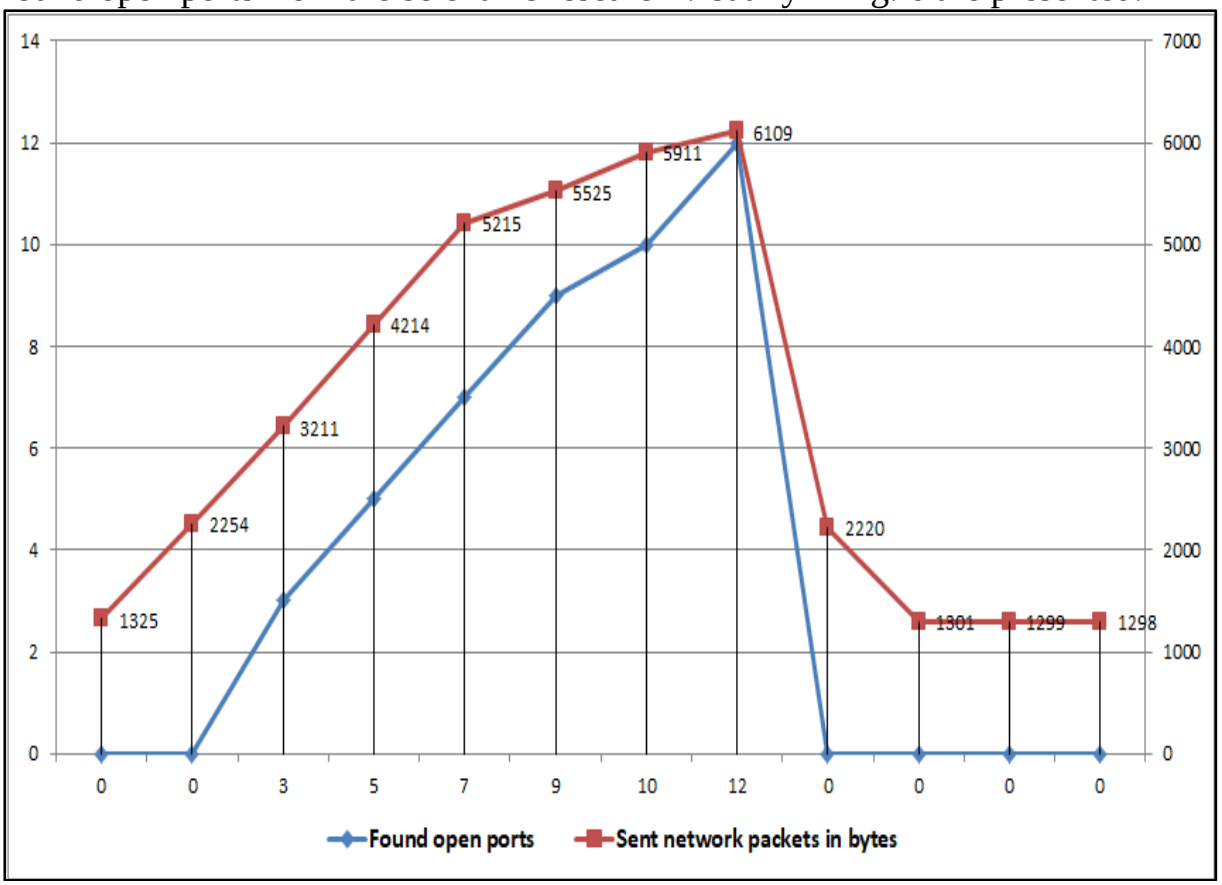

Fig. 6. The statistical processing of the obtained results of the conducted scientific research

ATTENTION: The scientific experiments and research works in this paper in a specialized computer laboratories at the Faculty of Technical Sciences of the Konstantin Preslavsky University of Shumen are made. Everything illustrated and explained in this paper is for research work and educational purposes and the authors are not responsible in cases of abuse.

3. Conclusion

One of the main tasks of any ethical hacker is to perform a network scan of the computer network in order to detect unprotected open ports. With the help of the modified network scanner, these tasks can be completed in a relatively short time. One of the most important advantages of the modified network scanner is that it does not contain agents, backdoors, viruses or worms, and thus it can be quite safely used by any ordinary user or chief information security officer. Thus the exceptionally well-equipped laboratories at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen give great opportunities to students majoring in "Communication and Information Systems", "Computer Technologies in Automated Manufacturing" and "Signal

Security Systems and Technologies" to perform network scanning of hosts using modified port scanner, created for the Windows based operating system. On the other hand, it will allow students to upgrade the current network scanner with additional new functionalities in its code.

References:

[1] Bravo, C., Mastering Defensive Security: Effective techniques to secure your Windows, Linux, IoT, and cloud infrastructure. Packt Publishing, ISBN-10 1800208162, ISBN-13 978-1800208162, 2022, p. 528.

[2] Bryant, T., PTFM: Purple Team Field Manual. Independently published, ISBN-13 2020, 979-8682974061, p. 215.

[3] Calderon, P., Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips, 3rd Edition, Packt Publishing, ISBN-10 1838649352, ISBN-13 978-1838649357, 2021, p. 436.

[4] Candel, J., Mastering Python for Networking and Security: Leverage the scripts and libraries of Python version 3.7 and beyond to overcome networking and security issues, 2nd Edition. Packt Publishing, ISBN-10 1839217162, ISBN-13 2021, 978-1839217166, p. 538.

[5] Candel, J., Sarker, M., Washington, S., Learning Python Networking: A complete guide to build and deploy strong networking capabilities using Python 3.7 and Ansible , 2nd Edition. Packt Publishing, ASIN B07Q4SDBGZ, 2019, p. 492.

[6] Candel, J., Mastering Python for Networking and Security: Leverage Python scripts and libraries to overcome networking and security issues. Packt Publishing, ISBN-10 1788992512, ISBN-13 978-1788992510, 2018, p. 426.

[7] Candel, J., Hacking ético con herramientas Python (Colecciones ABG - Informática y Computación) (Spanish Edition). American Book Group, ISBN-10 168165699X, ISBN-13 978-1681656991, 2020, p. 290.

[8] Codings, Z., Ethical Hacking: A Beginner's Guide to Computer and Wireless Networks Defense Strategies, Penetration Testing and Information Security Risk Assessment. Independently published, ISBN-10 1694041565, ISBN-13 2019, 978-1694041562, p. 140.

[9] Cole, E., Advanced persistent threat: understanding the danger and how to protect your organization, Syngress, 2013, ISBN: 978-1-59749-949-1, p. 309.

[10] Diogenes, Y., Ozkaya, E., Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition. Packt Publishing, ISBN-10 183882779X, ISBN-13 2019, 978-1838827793, p. 634.
[11] El-Hajj W., Aloul F., Trabelsi Z., Zaki N., On detecting port scanning using fuzzy based intrusion detection system, IEEE Wireless Communications and Mobile Computing Conference, 2008, IWCMC'08, ISBN: 978-1-4244-2201-2, pp. 105–110.
[12] Elghaly, Y., Learn Penetration Testing with Python 3.x: Perform Offensive Pentesting and Prepare Red Teaming to Prevent Network Attacks and Web Vulnerabilities (English Edition). BPB Publications, ISBN-10 9390684919, ISBN-13 2021, 978-9390684915, p. 344.
[13] Friedman, J., Hoffman, D. V., Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses, Information, Knowledge, Systems Management 7, №. 1, 2008, pp. 159–180.
[14] Friedman, A., Singer, P., Cybersecurity and Cyberwar: what everyone needs to know. Oxford University Press, UK, 2014, ISBN 978-0-19-991809-6, p. 320.
[15] Genov, B., Nedelchev, D., Mihovski, M., Mirchev, Y., Comprehensive approach for service life assessment of solid-propellant rocket motors. International Journal "NDT Days", Volume II, Issue 4, 2019, ISSN: 2603-4018 (print), 2603-4646 (online), pp. 467-475.
[16] Genov, B., NDT Assessment Model for Missile Motors. International Journal "NDT Days", Volume I, Issue 4, 2018, ISSN: 2603-4018 (print), 2603-4646 (online), pp. 484-493.
[17] Genov, B., Criteria for Selection of NDT in the Ammunition Life Cycle. International Journal "NDT Days", Volume I, Issue 4, 2018, ISSN: 2603-4018 (print), 2603-4646 (online), pp. 494-503.
[18] Genov, B., Kirkov, D., Mihovski, M., Mirchev, Y., Ageing of Solid Rocket Propellants Investigated by Ultrasound Technique. International Journal "NDT Days", Volume I, Issue 5, 2018, ISSN: 2603-4018 (print), 2603-4646 (online), pp. 577-582.
[19] Grubb, S., How Cybersecurity Really Works: A Hands-On Guide for Total Beginners. No Starch Press, ISBN-10 1718501285, ISBN-13 978-1718501287, 2021, p. 216.

[20] Hadnagy, Ch., Social Engineering: The Science of Human Hacking 2nd Edition. Wiley, ISBN-10 111943338X, ISBN-13 2018, 978-1119433385, p. 320.
[21] Iliev, R., K. Ignatova. Implementation of cloud technologies for building data centers in defence and security. Information & Security: An International Journal 43, No. 1. 2019, ISSN 0861-5160, pp. 89-97., https://doi.org/10.11610/isij.4308.
[22] Iliev, R., K. Ignatova. Cloud technologies for building data center system for defense and security. T. Tagarev et al. (eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies, Studies in Big Data 84, , ISBN 978-3-030-65721-5, Springer 2020, pp. 13-24, https://doi.org/10.1007/978-3-030-65722-2.
[23] Kaur, R., Singh, G. Analysing, Port Scanning Tools and Security Techniques, International Journal of Electrical Electronics & Computer Science Engineering, Volume 1, Issue 5, October 2014, ISSN 2348 2273, pp. 58–64.
[24] Lyon, G., F., Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Nmap Project, ISBN-13: 978-0979958717, 2009, p. 464.
[25] Orebaugh, A., Pinkard, B., Nmap in the Enterprise: Your Guide to Network Scanning, Syngress Publishing, ISBN 13: 978-1-59749-241-6, 2008, p. 259.
[26] Orebaugh, A., Ramirez, G., Beale J., Wright J., Wireshark & Ethereal Network Protocol Analyzer Toolkit (Jay Beale's Open Source Security), Syngress, ISBN-13: 978-1597490733, 2007, p. 448.
[27] Pavlova. D., Gindev, P. Designing an intelligent system for knowledge and process management in a university information environment. INTED2020 Proceedings. 14th International Technology, Education and Development Conference, Valencia, Spain, 2nd-4th March 2020, pp. 2743-2747. ISBN: 978-84-09-17939-8 doi: 10.21125/inted.2020.0818.
[28] Pavlova, D., Dzhelepov, V., Gindev, P., Effectiveness of information security in computer systems for object and process management. 13th International traveling seminar, Modern dimensions in European education and research area. Bulgarian-Austrian cultural dialogue, 26-31 May 2019, Sofia, “ZA BUKVITE – O Pismeneh” Publishing House, vol. 7, 2019, pp. 241-249. ISSN 2367-7988.

[29] Pavlova, D., Gindev, P., System synthesis approach for intelligent knowledge management. 13th International traveling seminar, Modern dimensions in European education and research area. Bulgarian-Austrian cultural dialogue, 26-31 May 2019, Sofia, "ZA BUKVITE – O Pismeneh" Publishing House, vol. 7, 2019, pp. 250-257. ISSN 2367-7988.
[30] Pavlova, D., Gindev, P., A System for Intelligent Electronic Management of Knowledge and Business Processes in a University Information Environment. Proceedings of Seventh National Seminar with international participation - Intellectual property and digital people, 24 April 2019, Sofia, "ZA BUKVITE – O Pismeneh" Publishing House, vol. 7, 2019, pp. 221-234. ISBN 978-619-185-379-3.
[31] Radoeva, N., Iliev, R., A measurement process model implemented by generalized net. IEEE 8th International Conference on Intelligent Systems (IS), September 3-6, 2016, pp. 574-578, ISBN:978-1-5090-1355-5, DOI: 10.1109/IS.2016.7737482.
[32] Sanders, Ch., Practical Packet Analysis, 2nd Edition, No Starch Press, San Francisco, USA, ISBN: 978-1-59327-266-1, 2011, p. 280.