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

Original Contribution

ISSN 1314-6289

IMPLEMENTATION OF SOFTWARE APPLICATION FOR NETWORK PORT SCANNING IN ANDROID 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 implementation of software application using linear algorithm for network port scanning in android based operating systems is made.*

KEY WORDS: *Algorithm, Analysis, Android, Connection, Libraries, Monitoring, Network, Ports, Python, Scanning, Services, Traffic, Threads.*

1. Introduction

In order to stop hackers from illegally breaking into a computer network, it is necessary to understand the goals and mindset of the malicious perpetrators. Most of the computer systems [1,4,5,7,10,13,24] around the world systematically fall prey to wanton compromise and hacking. This unregulated process is not only widespread, but is executed so flawlessly that attackers compromise the system [2,3,6,8,9,10,11,12,13,15,19,20,21], steal everything of value, and completely erase their track.

In this regard, the main objective of an ethical hacker is to help the concerned organization to take and implement preventive defense measures against various types of modern malicious cyberattacks by attacking the computer network itself, all the while complying with all legal regulations for the proper functioning of all hosts. This philosophy is proven itself in computer practice, because in order to catch a computer thief or perpetrator, it is necessary that ethical hackers think exactly like them. As technological progress and organization become increasingly dependent on technology, information resources have become critical components for protection [1,2,5,9,14,16,21].

To ensure that organizations are applied all security mechanisms adequately to their information resources, it is necessary to adopt the approach of performing a thorough examination to detect weaknesses and vulnerabilities in host operating systems as well as network communication devices.

Therefore the certified ethical hacker is a person who normally works within the organization and who can be fully trusted to undertake and carry out planned intrusion attempts into computer networks and systems using the same methods as the malicious perpetrators - hackers. In this scientific research, the main emphasis on the implementation of software application using linear algorithm for network port scanning in android 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 Android based operating systems. In this regard, fundamentally new approaches for algorithmization of activities related to network port scanning is developed.

The Python programming language has various module libraries for network scanning of hosts and thus the performance of a modified script for Android based operating systems implementing a linear algorithm for network port scanning is showed.

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

1. Loading the required libraries and modules. The libraries and modules that are used in the port network scan script are several items.

2. Entering the relevant global variables.

3. Introducing the host scanning features.

4. Checking if the port is open or closed.

5. Getting the scope with ports from the graphical user interface (GUI).

6. Start recording the results to the log file.

7. Initialize the port scan process.

8. Showing the elapsed time since the scan.

9. Configuring the graphical user interface.

10. Define the color gamut of the GUI.

11. Configure the fields in the scanner.

12. Enter an IPv4 network address or domain. If a domain is entered, then the modified script, after performing the scan, prints the public IPv4 address of the domain.

13. Define the port scan range.

14. Viewing the list of found open ports.

15. Configuration of the buttons for starting the scan and saving the obtained results.

16. Launching the GUI.

The flowchart of a modified script for Android based operating systems implementing a linear network port scanning algorithm in fig. 1 is presented.

The scientific research using the smartphone Realme GT Master Edition with operating system Android 11 is carried out in order to scan and detect open ports on active hosts in the local computer network. In the generated log file the network scanner application shows how many ports are discovered and what their status is. It also shows how long it took the scanner to perform this network process. The network scanner does not have any malware embedded in it, and thus a specialist or user can use it for performing host scan.

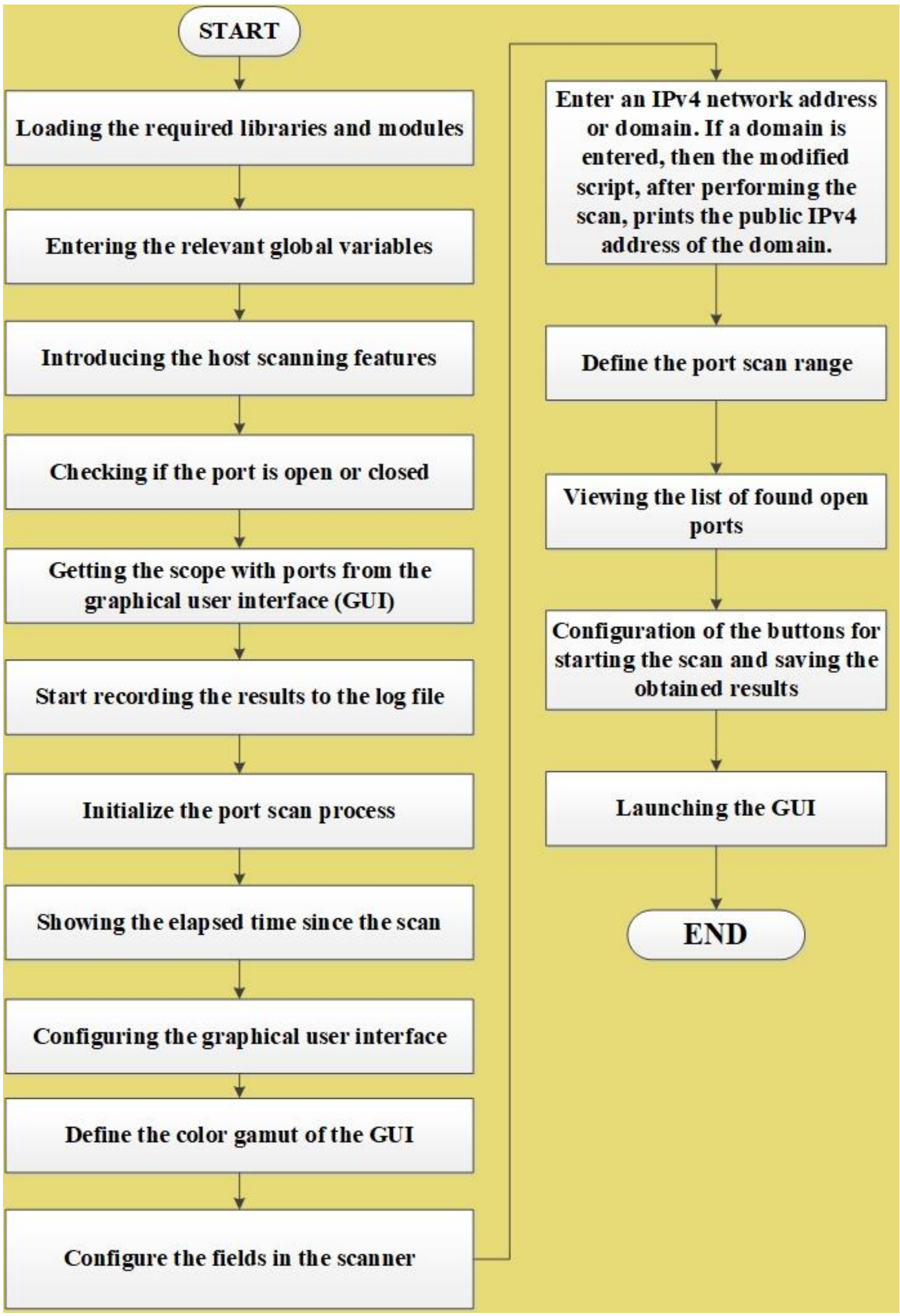
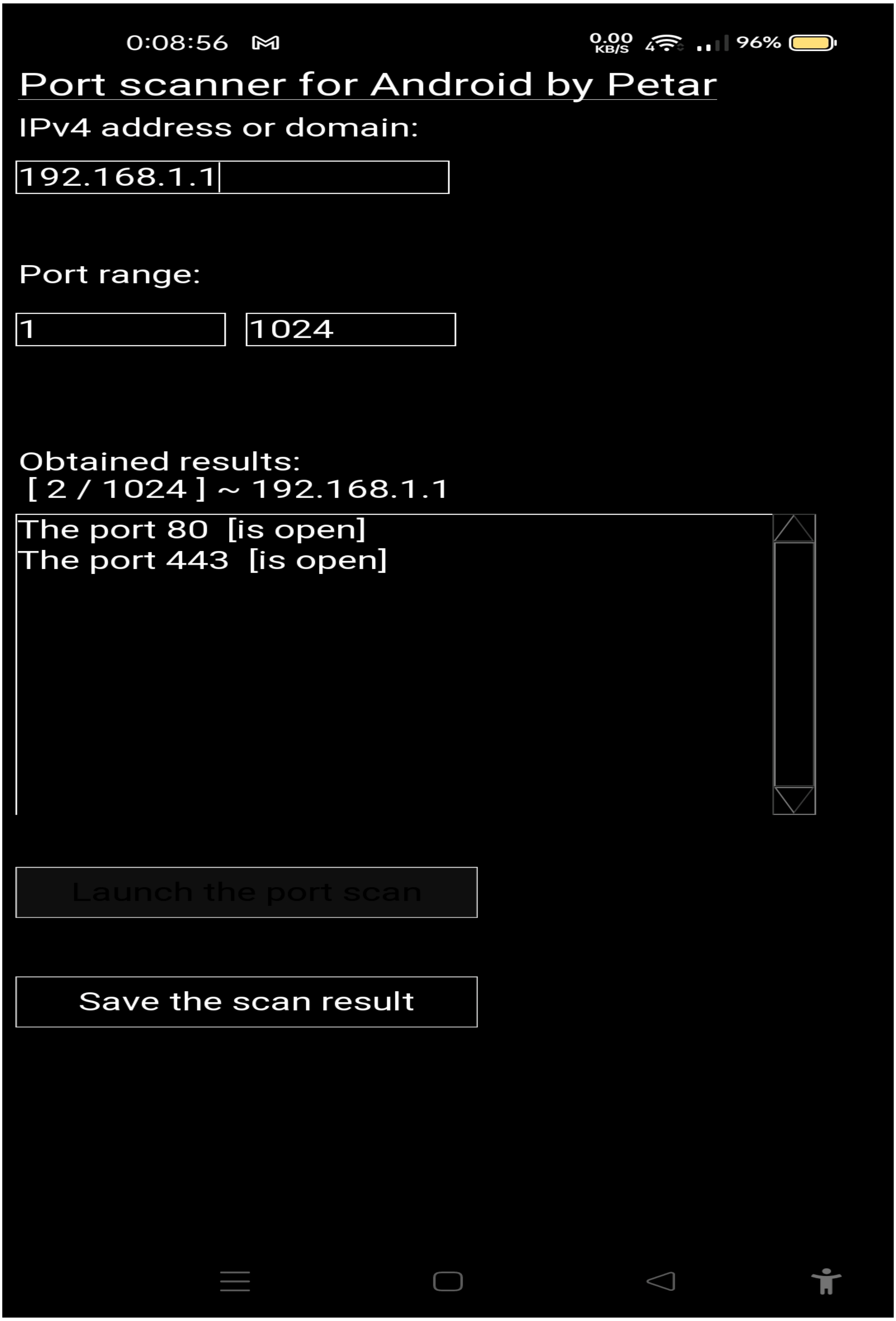

START
Loading the required libraries and modules
Entering the relevant global variables
Introducing the host scanning features
Checking if the port is open or closed
Getting the scope with ports from the graphical user interface (GUI)
Start recording the results to the log file
Initialize the port scan process
Showing the elapsed time since the scan
Configuring the graphical user interface
Define the color gamut of the GUI
Configure the fields in the scanner
Enter an IPv4 network address or domain. If a domain is entered, then the modified script, after performing the scan, prints the public IPv4 address of the domain.
Define the port scan range
Viewing the list of found open ports
Configuration of the buttons for starting the scan and saving the obtained results
Launching the GUI
END

Fig. 1. Flowchart of a modified script for Android based operating systems implementing a linear network port scanning algorithm

3. Results



Port scanner for Android by Petar

IPv4 address or domain:

192.168.1.1

Port range:

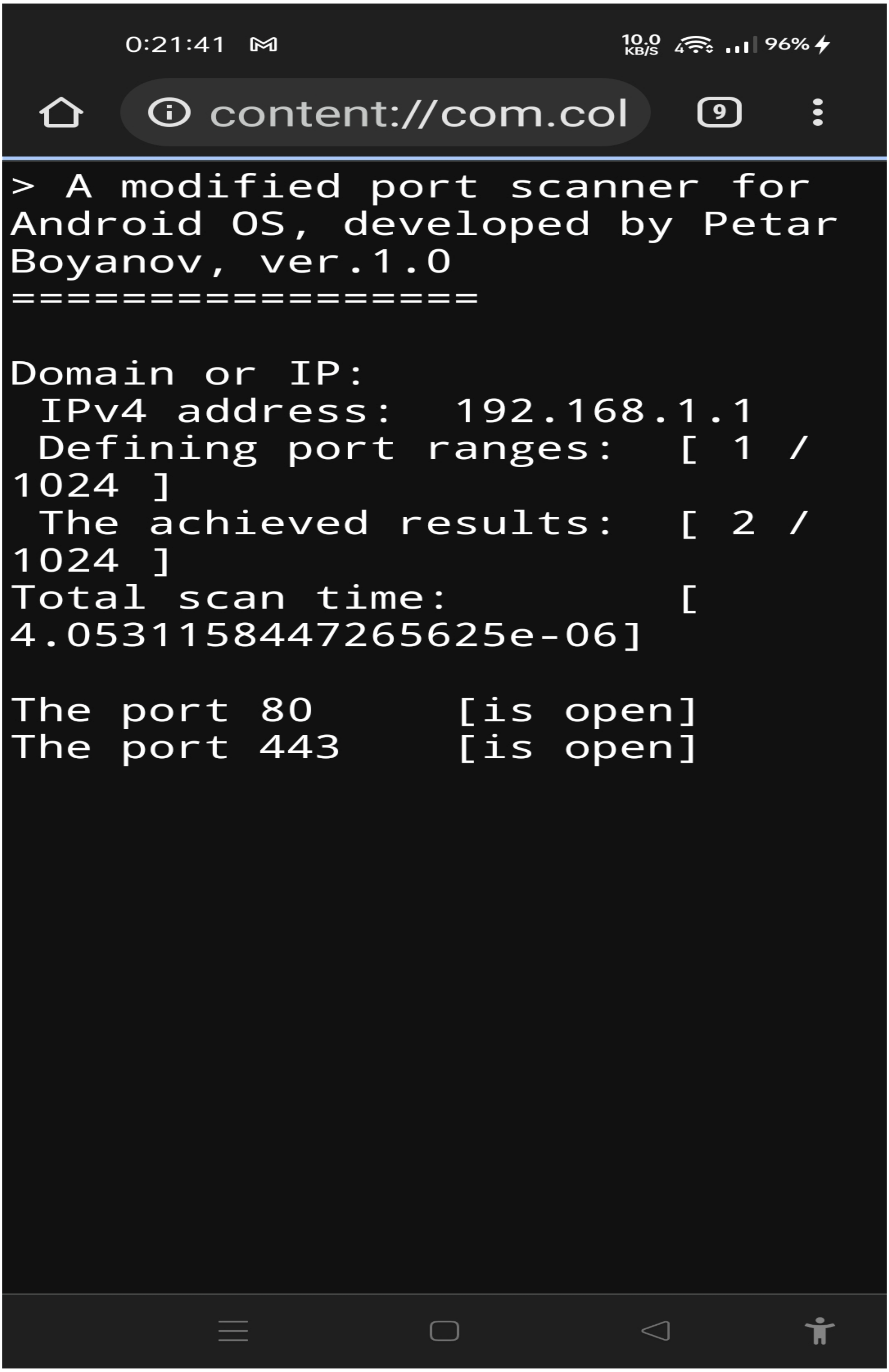
1

1024

Obtained results:
[2 / 1024] ~ 192.168.1.1

```
The port 80  [is open]
The port 443  [is open]
```

Fig. 2. Port scan of host with IPv4 address – 192.168.1.1 for the first 1024 ports

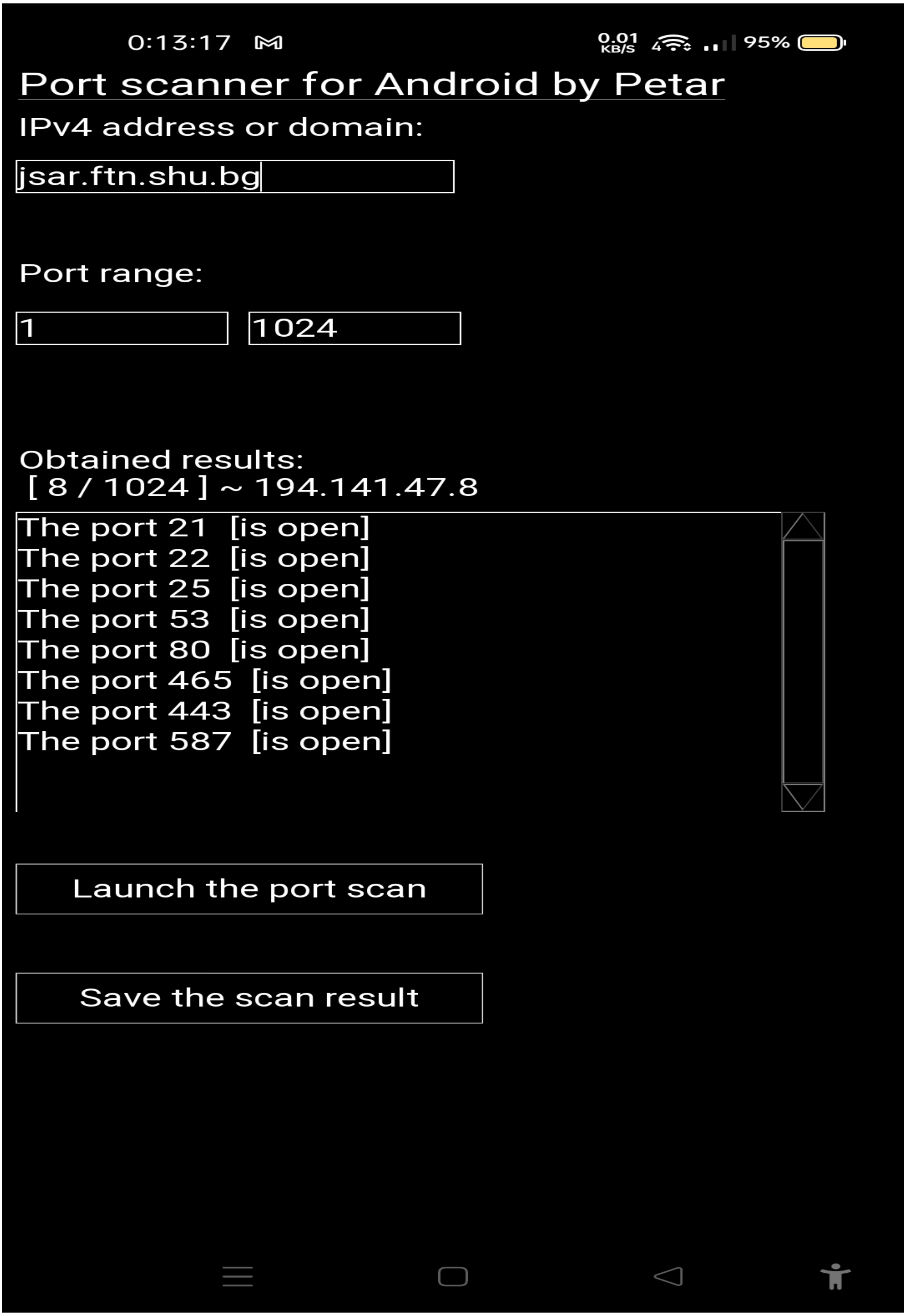


```
> A modified port scanner for
Android OS, developed by Petar
Boyanov, ver.1.0
==================

Domain or IP:
 IPv4 address:   192.168.1.1
 Defining port ranges:   [ 1 /
1024 ]
 The achieved results:   [ 2 /
1024 ]
Total scan time:         [
4.0531158447265625e-06]

The port 80      [is open]
The port 443     [is open]
```

Fig. 3. Detailed information about the results of the performed port scan for the host with IPv4 address - 192.168.1.1



jsar.ftn.shu.bg

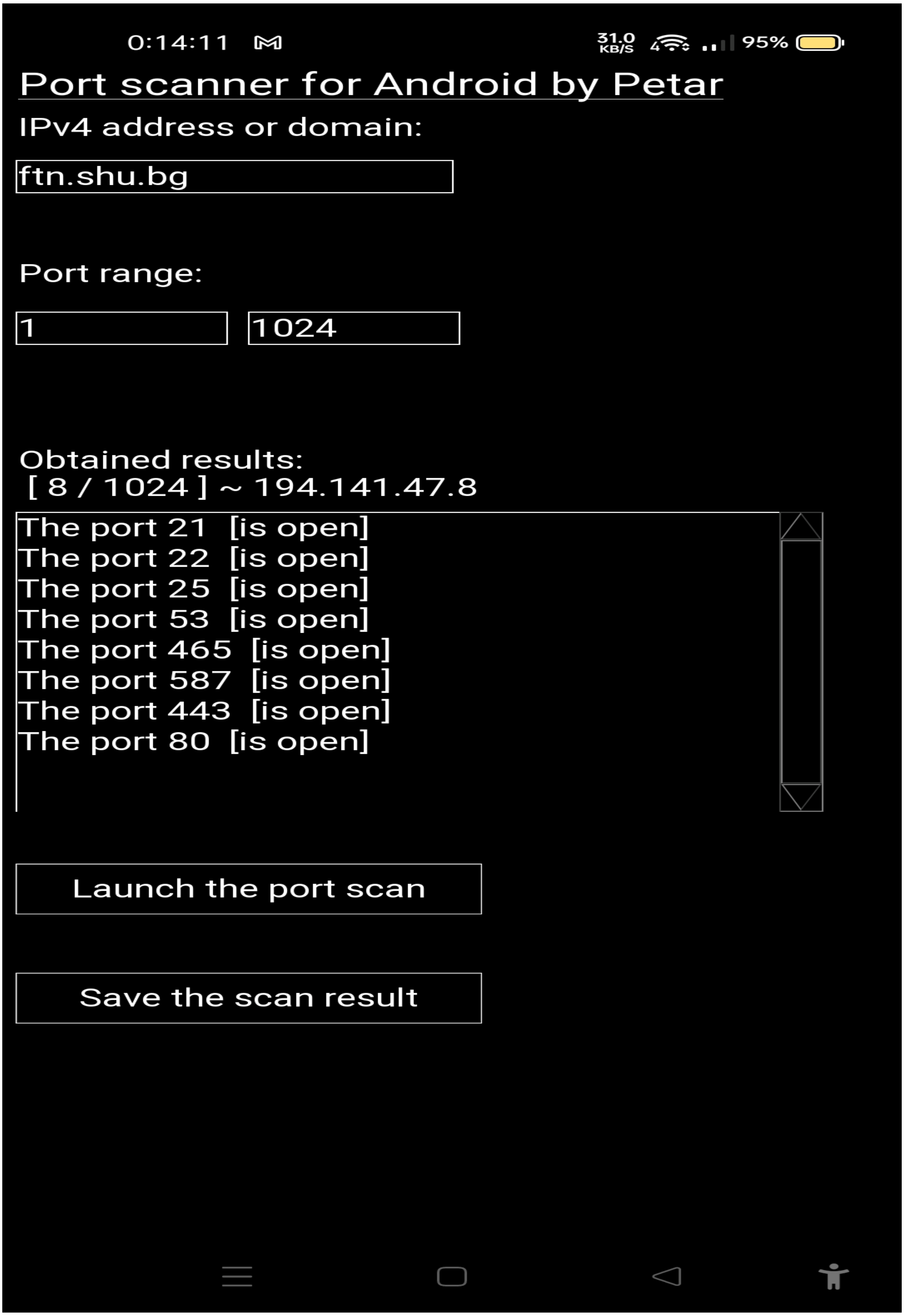
1

1024

[8 / 1024] ~ 194.141.47.8

```
The port 21  [is open]
The port 22  [is open]
The port 25  [is open]
The port 53  [is open]
The port 80  [is open]
The port 465  [is open]
The port 443  [is open]
The port 587  [is open]
```

Fig. 4. Port scan of subdomain jsar.ftn.shu.bg for the first 1024 ports



Port scanner for Android by Petar

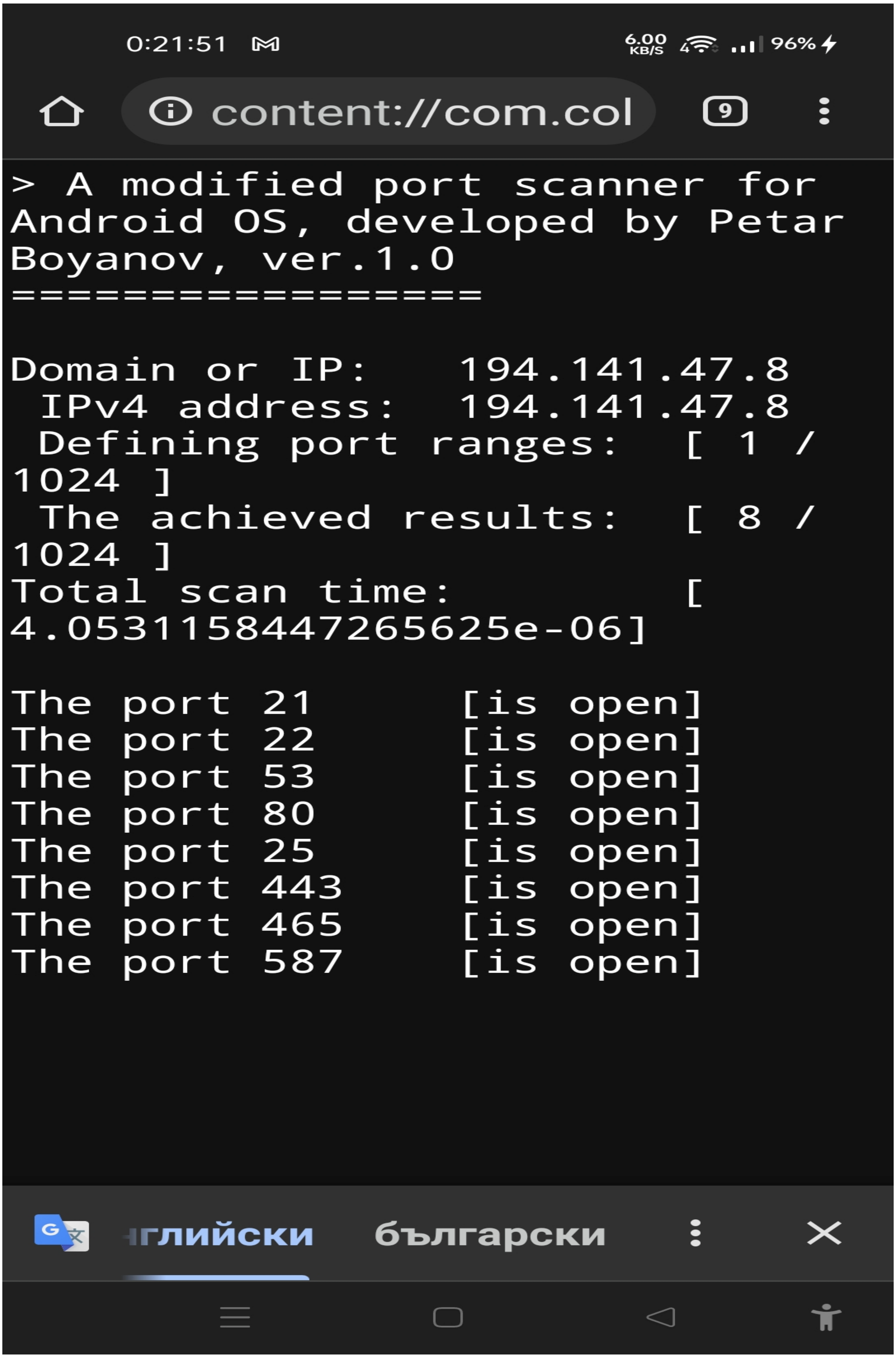
IPv4 address or domain: ftn.shu.bg

Port range: 1 1024

Obtained results:
[8 / 1024] ~ 194.141.47.8

```
The port 21  [is open]
The port 22  [is open]
The port 25  [is open]
The port 53  [is open]
The port 465  [is open]
The port 587  [is open]
The port 443  [is open]
The port 80  [is open]
```

Fig. 5. Port scan of subdomain jsar.ftn.shu.bg for the first 1024 ports



```
> A modified port scanner for
Android OS, developed by Petar
Boyanov, ver.1.0
==================

Domain or IP:    194.141.47.8
 IPv4 address:   194.141.47.8
 Defining port ranges:   [ 1 /
1024 ]
 The achieved results:   [ 8 /
1024 ]
Total scan time:         [
4.0531158447265625e-06]

The port 21      [is open]
The port 22      [is open]
The port 53      [is open]
The port 80      [is open]
The port 25      [is open]
The port 443     [is open]
The port 465     [is open]
The port 587     [is open]
```

Fig. 6. Detailed information about the results of the performed port scan for both subdomains jsar.ftn.shu.bg and ftn.shu.bg

Fig. 2 shows the direct network scan by IP address and in this case the IPv4 address of the host is 192.168.1.1. From the obtained results in fig. 3, it is found that a total of 2 open ports are detected out of a total of 100 scanned network ports. From figures 4, 5 and 6 it can be seen that the public IPv4 address of the subdomains jsar.ftn.shu.bg and ftn.shu.bg is the same for both - 194.141.47.8. This application actually reveals the fully qualified domain name (FQDN) of the scanned subdomain. The subdomain jsar.ftn.shu.bg is the official web site of the scientific journal – Journal Scientific and Applied Research and the subdomain ftn.shu.bg is the official web site of the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen. As a result of the performed scientific research 8 open ports are found out of a total of 1024 ports scanned and the total elapsed time to complete the scan is 4.053 seconds. The found open port numbers are accordingly 21, 22, 25, 53, 80, 443, 465 and 587. 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 obtained detailed information about the started services 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 443 - World Wide Web, Hypertext Transfer Protocol Secure (HTTPS).
- Open port 465 - URL Rendezvous Directory for SSM.
- Open port 587 - Message Submission.

The presented modified script for Android 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 [15,16,17,18,19,20,21,22,23,25].

The results of the conducted scientific research show that this Android application can find ports with open state very fast. 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, and in this case, when is performed a scanning the subdomain edu.shu.bg, it was found that all ports were scanned in a record 3.576 seconds and 4 open ports were found.

All this really shows high performance and port scanning in extremely negative time. This is shown on fig. 7.

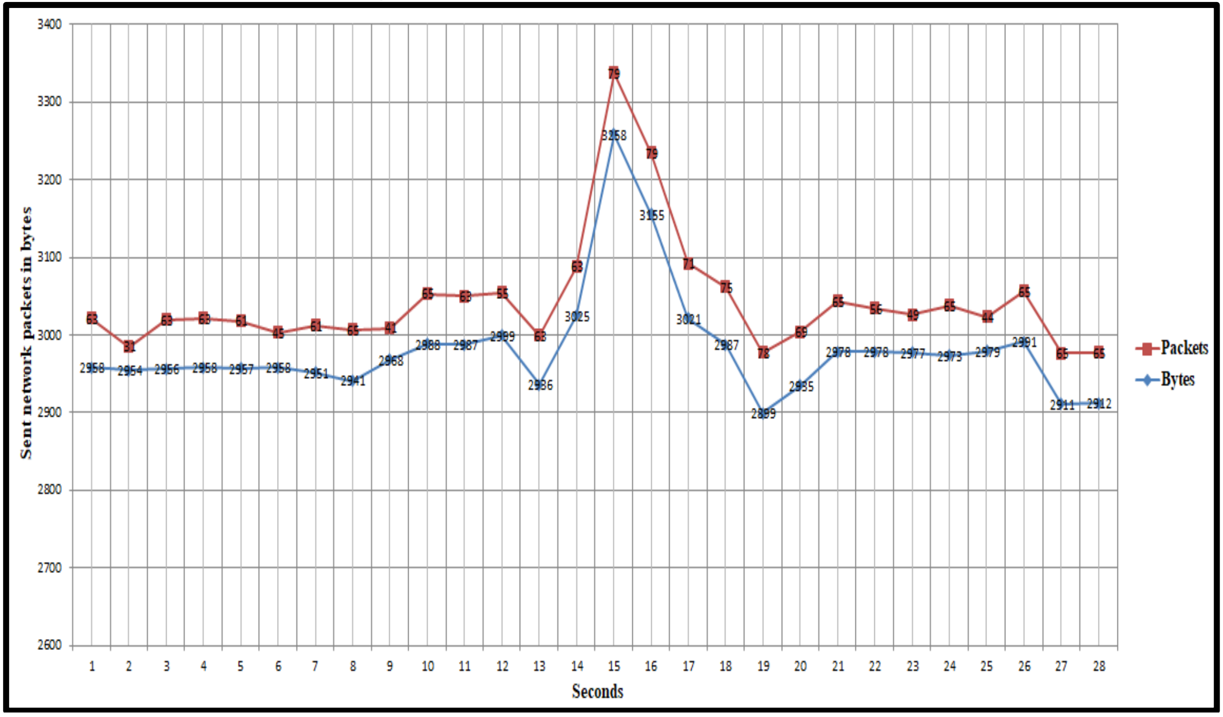


Fig. 7. The statistical processing of the obtained results of the conducted scientific research

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

There are a number of different methods of doing the actual network port scan by setting different TCP (Transmission Control Protocol) flags or sending different types of TCP packets. The port scanning finds open, closed and filtered ports. For example, a SYN network scan shows port scanners which ports are listening and which are not, depending on the type of response which is generated. A FIN scan will generate a response from closed ports, but ports that are open and listening will not send a response, so the port scanner will be able to determine which ports are open and which are not. Network port scanning software, basically sends a serial connection request to the target host on each port and notes which ports are responded or appear open for further investigation and exploitation.

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 software applications created for the Android based operating systems.

References:

[1] Arkamburge, Python Quick Basics and Advacnced programming Guide for Dummies and beginners on coding in computer science design using tricks with javascipt along learning to network and hack quickly: Guide 2 code. Independently published, ISBN-13 2021, 979-8768745837, p. 193.

[2] Ballmann, B., Understanding Network Hacks: Attack and Defense with Python 3 2nd ed. Springer, ISBN-10 3662621592, ISBN-13 978-3662621592, 2022, p. 236.

[3] Ballmann, B., Network Hacks - Intensivkurs: Angriff und Verteidigung mit Python 3 (German Edition). Springer, ISBN-10 3662616351, ISBN-13 2020, 978-3662616352, p. 237.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Choi, B., Introduction to Python Network Automation: The First Journey 1st ed. Edition. Apress, ISBN-10 1484268059, ISBN-13 978-1484268056, 2021, p. 896.

[10] Chou, E., Kennedy, M., Whaley, M., Mastering Python Networking: Your one-stop solution to using Python for network automation, programmability, and DevOps, 3rd Edition. Packt Publishing, ISBN-10 1839214678, ISBN-13 2020, 978-1839214677, p. 576.

[11] Codings, Z., Python Machine Learning: A Beginner's Guide to Python Programming for Machine Learning and Deep Learning, Data Analysis, Algorithms and Data Science With Scikit Learn, TensorFlow, PyTorch and Keras. Independently published, ISBN-10 1696563119, ISBN-13 978-1696563116, 2019, p. 147.

[12] Codings, Z., Computer Programming And Cyber Security for Beginners: This Book Includes: Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking. Coding and Cybersecurity Fundamentals. Independently published, ISBN-10 1671532902, ISBN-13 978-1671532908, 2019, p. 408.

[13] David, M., Mastering Python Network Programming: learn Network programming in simple and easy steps using Python as a programming language. Independently published, ISBN-13 2021, 979-8758780589, p. 103.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[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] 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.

[25] 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.