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

Original Contribution

ISSN 1314-6289

A COMPREHENSIVE SCANNING FOR OPEN, CLOSED AND FILTERED PORTS IN THE COMPUTER SYSTEMS AND NETWORKS

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 comprehensive scanning for open, closed and filtered ports in the computer systems and networks is made.*

KEY WORDS: *Connection, Linux, Monitoring, Network, Ports, Processes, Scanning, Services, Traffic, Threads, Windows.*

1. Introduction

After identifying the target and performing initial reconnaissance, malicious attackers begin looking for a network entry point into the target computer system. Attackers need to determine whether target systems are active or inactive to reduce the time spent on network scanning. It should be noted that network scanning itself is not the actual penetration [4,5,6,11,20,24,25,26], but an advanced form of reconnaissance where the attacker learns more about his target, including information about operating systems, services and any other gaps in computer and system configuration. The information gathered from such intelligence helps the attacking host to choose cyberattack strategies on the target system or computer network [1,3,5,10,12,14,28,32].

The goal of network scanning is to discover exploitable communication channels, examine as many listeners as possible, and track down those that are responsive or useful to the hacker's particular needs. In the scanning phase of a cyberattack, the attacker tries to find different ways to penetrate the target system [26,27,28,29,31]. The attacker also tries to discover more information about the target system to determine the presence of configuration gaps. The attacker then uses the information obtained to develop a cyberattack strategy [1,3,7,8,9,11,27,30].

Port scanning is the process of checking services running on a target computer by sending a series of network messages in an intrusion attempt. Port scanning involves connecting or examining TCP and UDP ports on a target computer system to determine if services are running or listening. The listening state provides information about the version of the operating system and the application currently in use. Sometimes active listening services can allow unauthorized users to misconfigure systems or run software with vulnerabilities.

A burglar looking to break into a house looks for access points such as doors and windows. These are usually the vulnerable points of the house as they are easily accessible. When it comes to computer systems and networks [14,28], ports are the doors and windows of the respective computer system [2,4,7,13,21,22,23,24,27] that an attacker uses to gain unauthorized access. A general rule of thumb for computer systems is that the more open ports a computer system has, the more vulnerable it is. However, there are cases where a system with fewer open ports may be at a much higher level of vulnerability.

In this scientific research, the main emphasis on the comprehensive scanning for open ports in the computer systems and networks is placed.

2. Experiment

The network scanning is a process of gathering information about systems that are active and responsive on a computer network. Host discovery is considered the primary task in the network scanning process. In order to perform a full scan and identify open ports and services, it is necessary to perform a check for active computer systems. Active host detection provides an accurate state of the systems on the network, allowing an attacker to avoid scanning every port on every system in the IPv4 or IPv6 address space to identify whether the target host is running [19,21,22,23,27].

The network scanning tools are used to scan and identify active hosts, open ports, running services on the target computer network, location information, NetBIOS protocol information, and information about all TCP/IP and UDP open ports on the host. The information obtained from these tools will help the ethical hacker to create the profile of the target organization and scan the network for open ports on the connected network devices.

Nmap is a security scanner for network exploration and hacking. Through it, it is possible to discover hosts, ports and services in a computer network, thereby creating a map and topology of the computer network [3,4,6,10,11,13,22]. The scanner sends specially crafted network packets to the target host and then analyzes the received responses to achieve its goal. It scans huge computer networks of hundreds of thousands of machines. Nmap includes many mechanisms for scanning ports (TCP and UDP), detecting the operating system version, using ping sweep, and more [8,9,10,12,14].

A network administrator or attacker can use this tool for their specific needs. Network administrators can use Nmap to take inventory of the computer network, manage service upgrade schedules, and monitor the uptime of a host or service. Attackers use Nmap to extract information about live hosts on the network, open ports, services (application name and version), type of packet filters and firewalls, MAC details, and operating systems along with their versions [5,7,9,11,12,13].

Hping2/Hping3 is a command-oriented network scan and packet creation tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw IP protocols. This tool performs network security auditing, firewall testing, manual detection of the maximum transmitted packet unit - MTU path, advanced tracing, remote operating system printing, remote target uptime guessing, TCP/IP stack auditing, and other functions. It can send custom TCP/IP packets and display targeted responses similar to a ping program with ICMP responses. It handles fragmentation as well as arbitrary network packet body and size and can be used to transfer encapsulated files under the various supported protocols. It also supports scanning inactive hosts. This tool supports IP spoofing and network scanning to perform anonymous service probing. Hping2/Hping3 also has a Traceroute mode that allows attackers to send files between hidden channels. It also determines whether the host is working even when ICMP packets are being blocked. It supports a special feature that allows it to detect open ports behind firewalls [1,2,3,19,20,21,23,24]. Using Hping, an attacking host can examine the behavior of an idle host and obtain information about the target, such as the services the host offers, the ports supporting the services, and the operating system installed. This type of network scan is a precursor to either more serious probing or outright cyberattacks [4,6,7,10,11,26,27,28].

The experiment in a specialized computer network laboratory in the Faculty of Technical Sciences is made. The scientific research using the operating system Kali Linux 2022.2 amd64 is carried out in order to scan and detect open ports on active hosts in the local and wide computer networks.

3. Results

Host discovery techniques can be adopted to discover the active or live hosts in the computer network. As a matter of practice, any ethical hacker should be aware of the different types of host discovery techniques. In fig. 1 the scan process on port 80 by sending a packet with enabled ACK flag is presented.

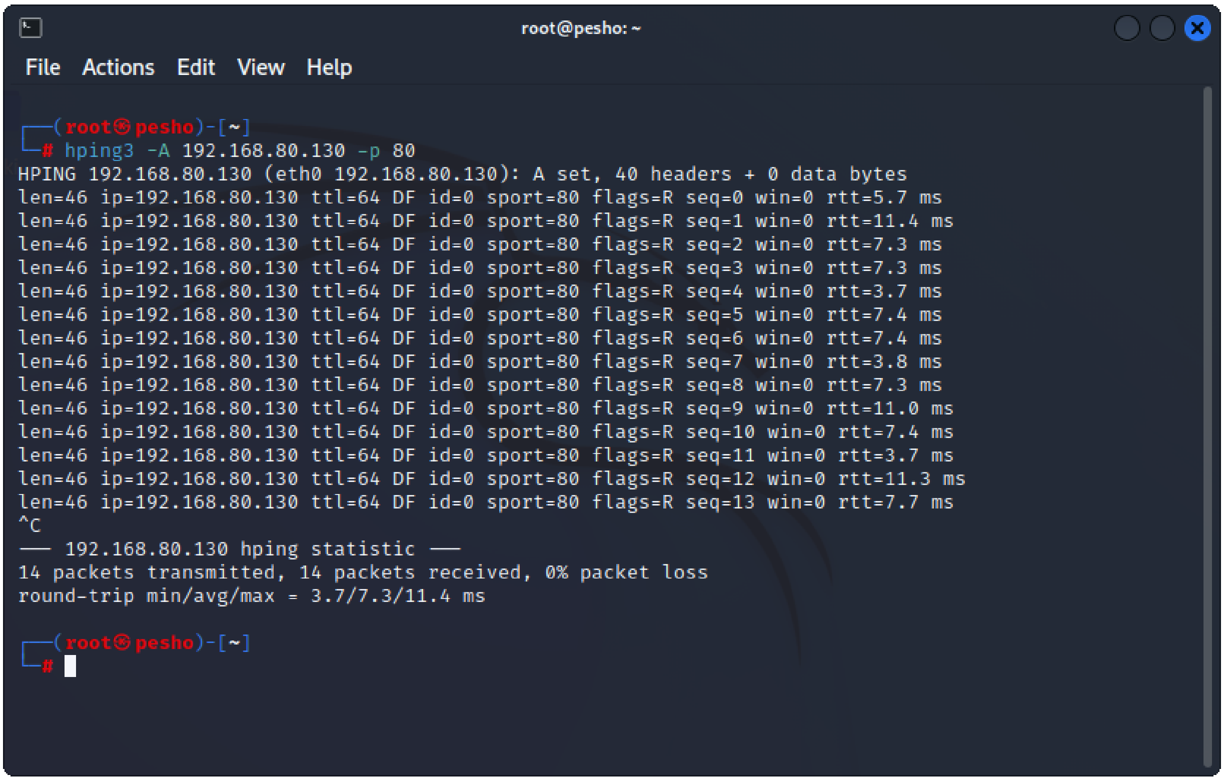

Fig. 1. Obtained results after ICMP scan on Windows 10 operating system

This network scanning technique can be used to investigate the existence of a firewall and its rule sets. The simple packet filtering allows the connection to be established, while a sophisticated stateful firewall prevents the connection from being established.

The network collection of initial serial number in fig. 2 is presented.

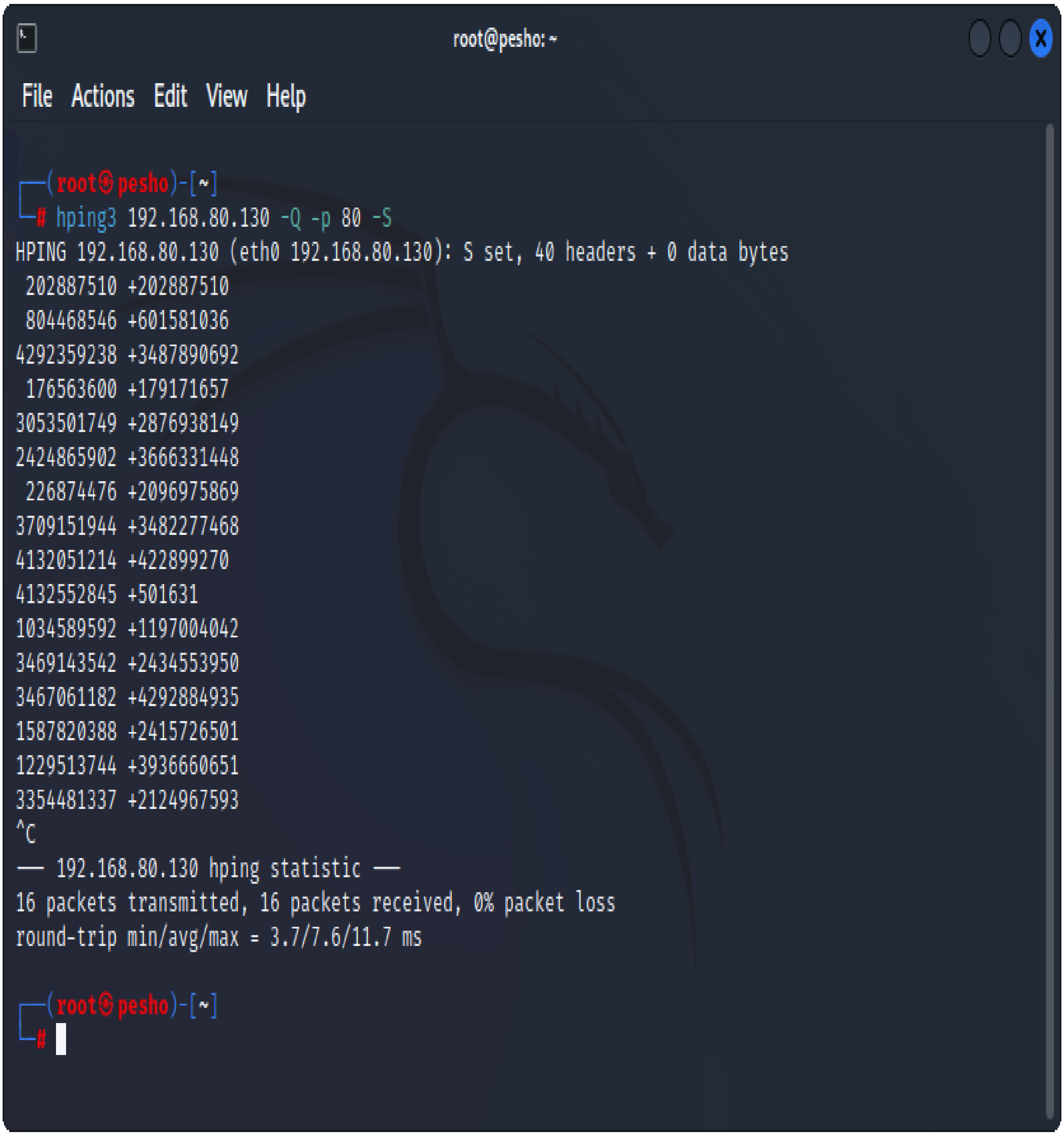

Fig. 2. Results obtained from network collecting initial sequence number for host 192.168.80.130

The firewalls and timestamps scan techniques in fig. 3 are illustrated. The following command "hping3 -S 192.168.80.129 -p 80 --tcp-timestamp" is used. Many firewalls drop those TCP packets that do not have the TCP timestamps option set. This is shown in fig. 3 and fig. 4.

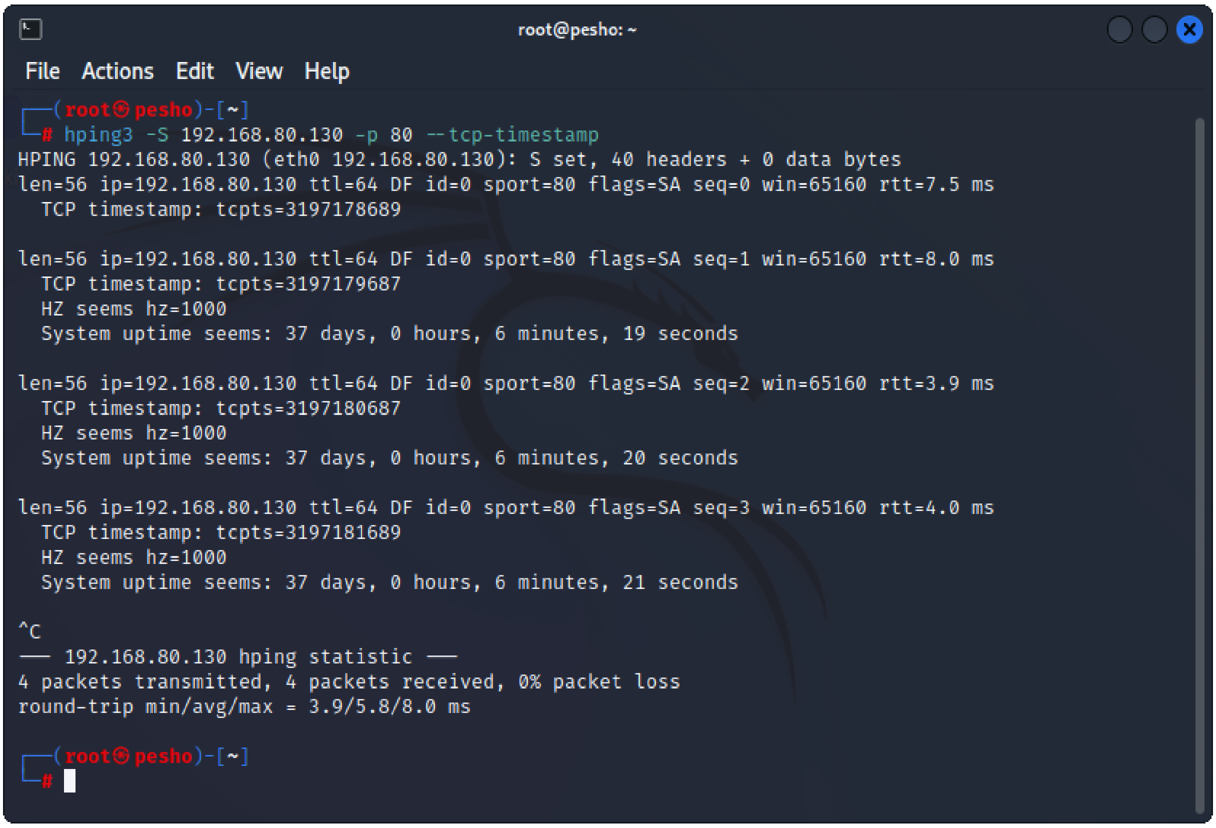

Fig. 3. Obtained scan results bypassing firewalls and obtaining timestamps for the host with IPv4 address – 192.168.80.130

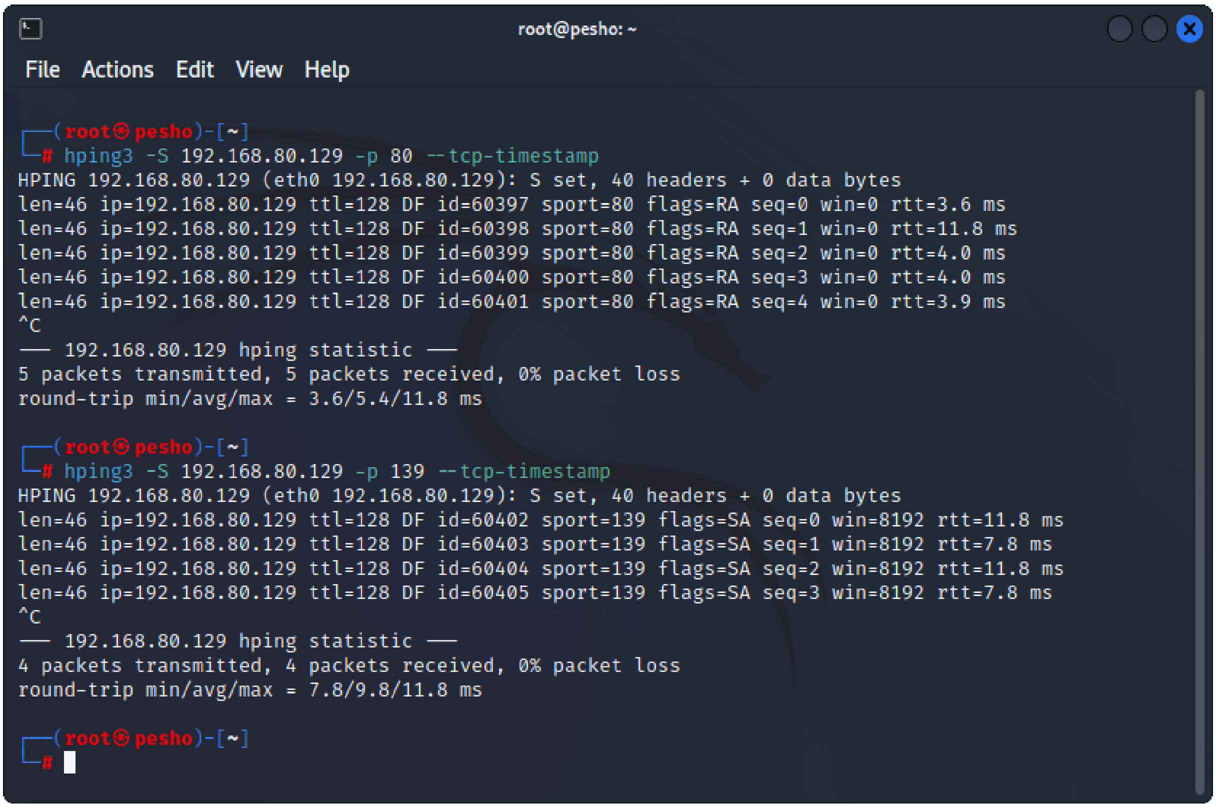

Fig. 4. Obtained scan results bypassing firewalls and obtaining timestamps for the host with IPv4 address – 192.168.80.129

In fig. 5 the scanning of the entire subnet for live hosts is presented.

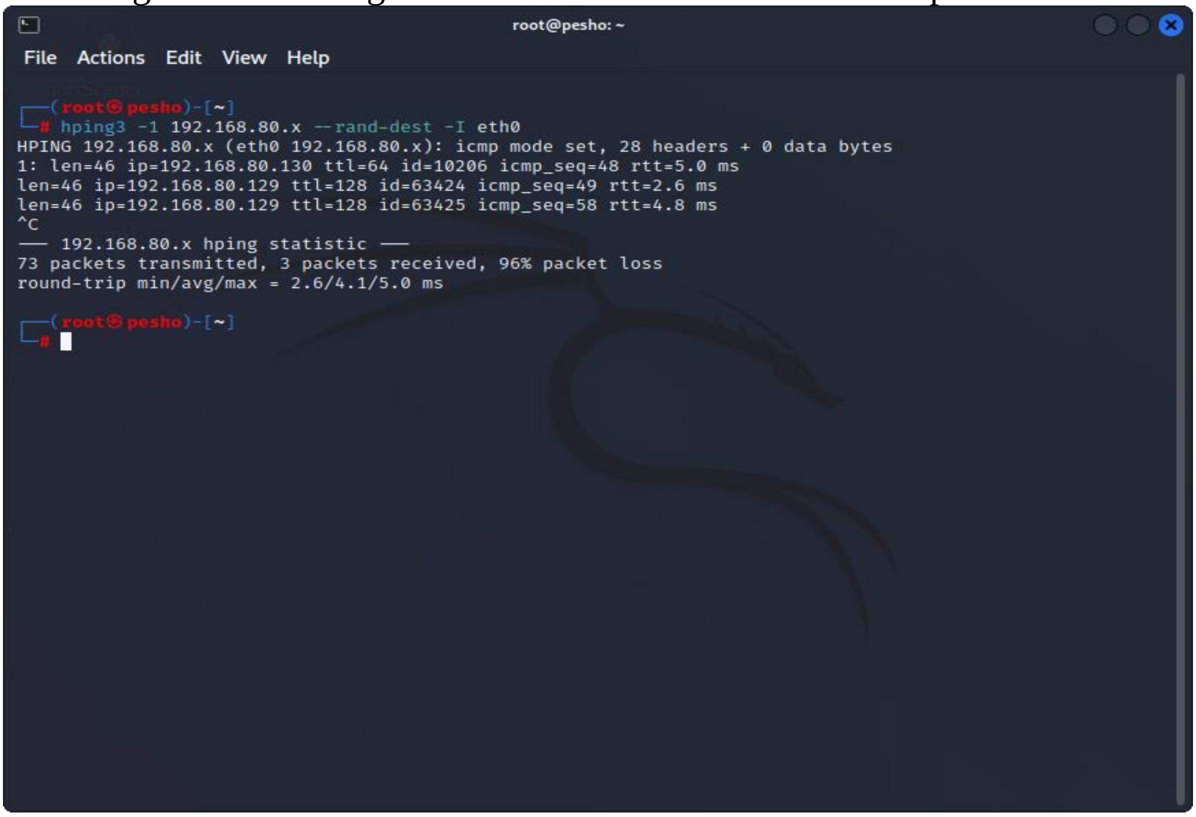

Fig. 5. Scanning the entire subnet for live hosts - 192.168.80.0/24

Scanning with enabled SYN flag on ports 133-140 in fig. 6 is shown.

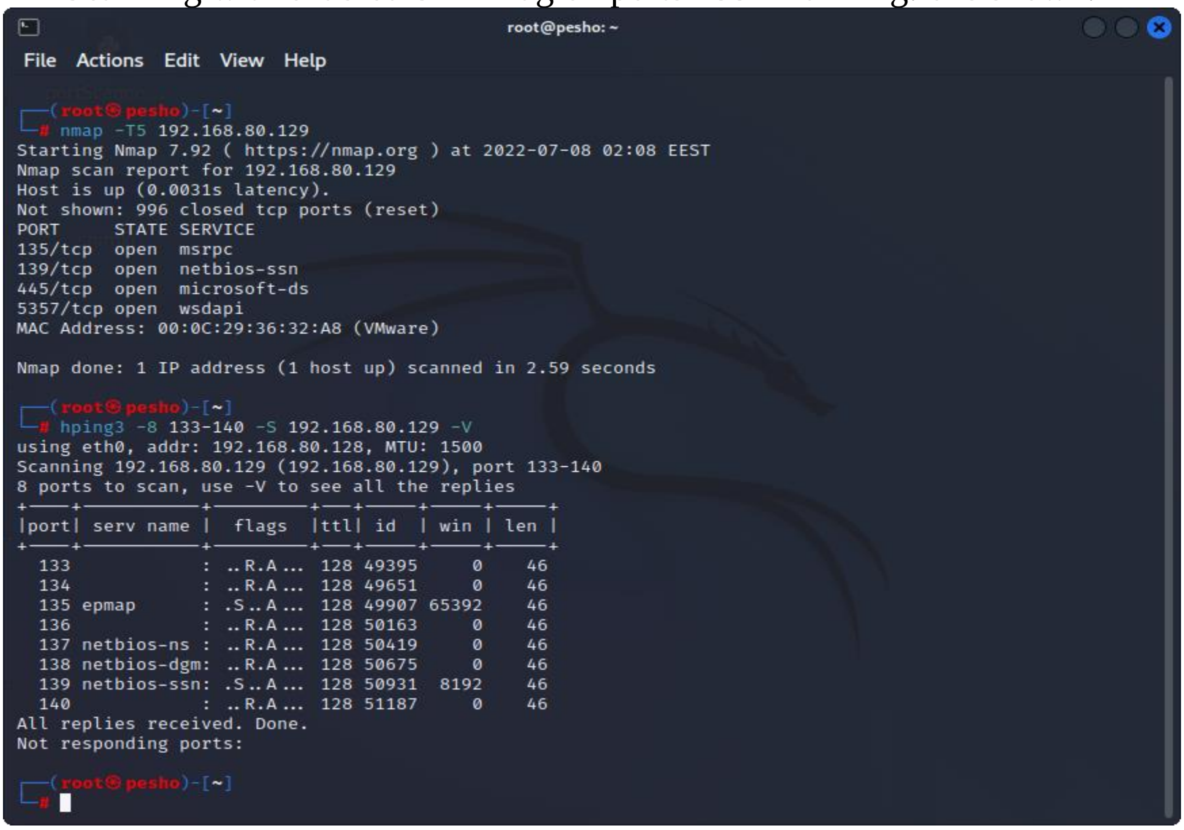

Fig. 6. Obtained results after scanning with enabled SYN flag on ports 133-140

Both the SYN and the ACK packet can be used to increase the chances of bypassing the implemented firewall. However, firewalls are mostly configured to block ping SYN packets as they are the most common ping technique. In such cases, the ACK probe can effectively be used to easily bypass these firewall rule sets. In fig. 7 and fig. 8 the obtained results of the TCP ACK ping scan with a detailed illustration of the communication processes of sending and receiving requests is presented.

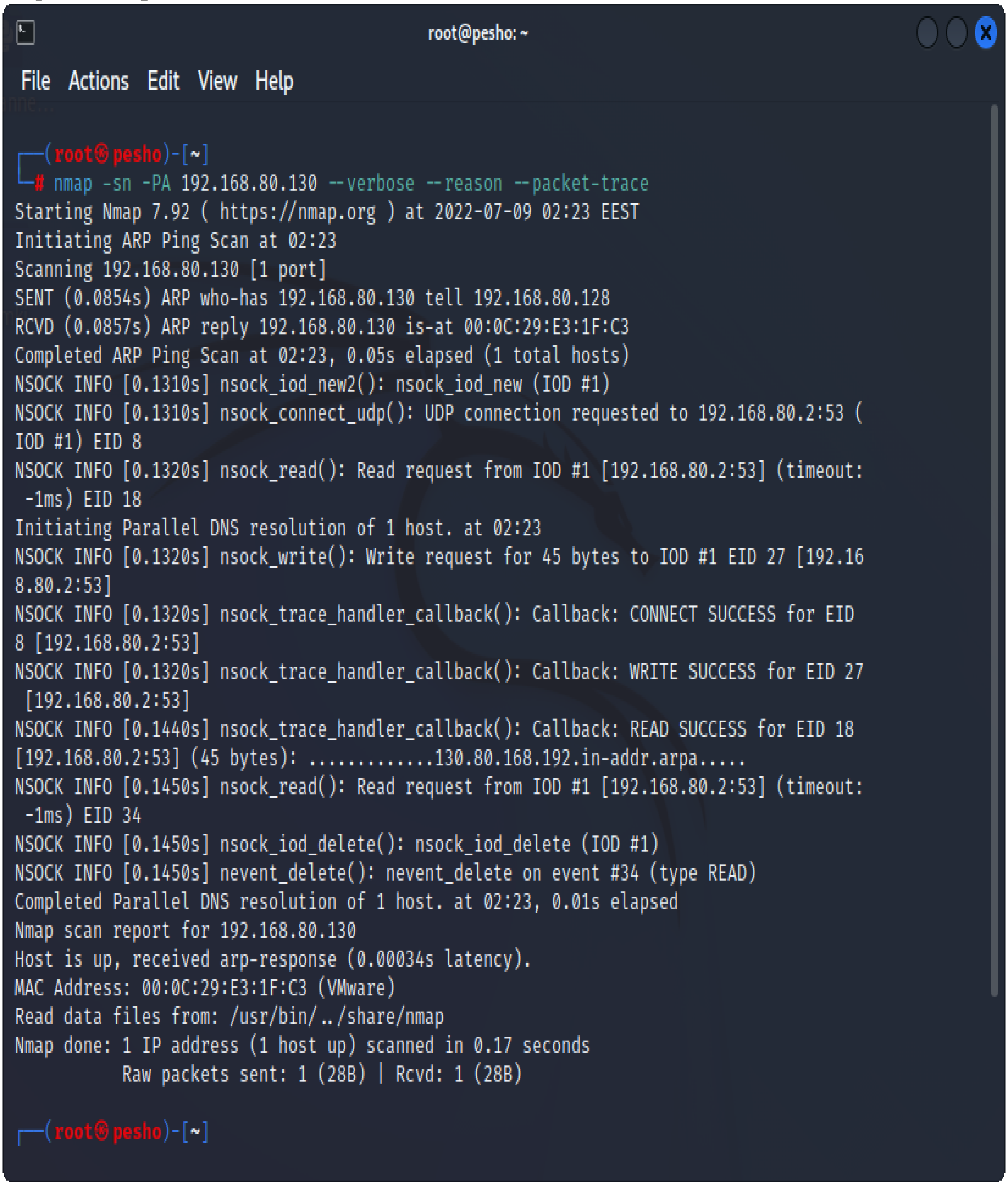

Fig. 7. Received TCP SYN Ping scan results for host with IPv4 address - 192.168.80.130

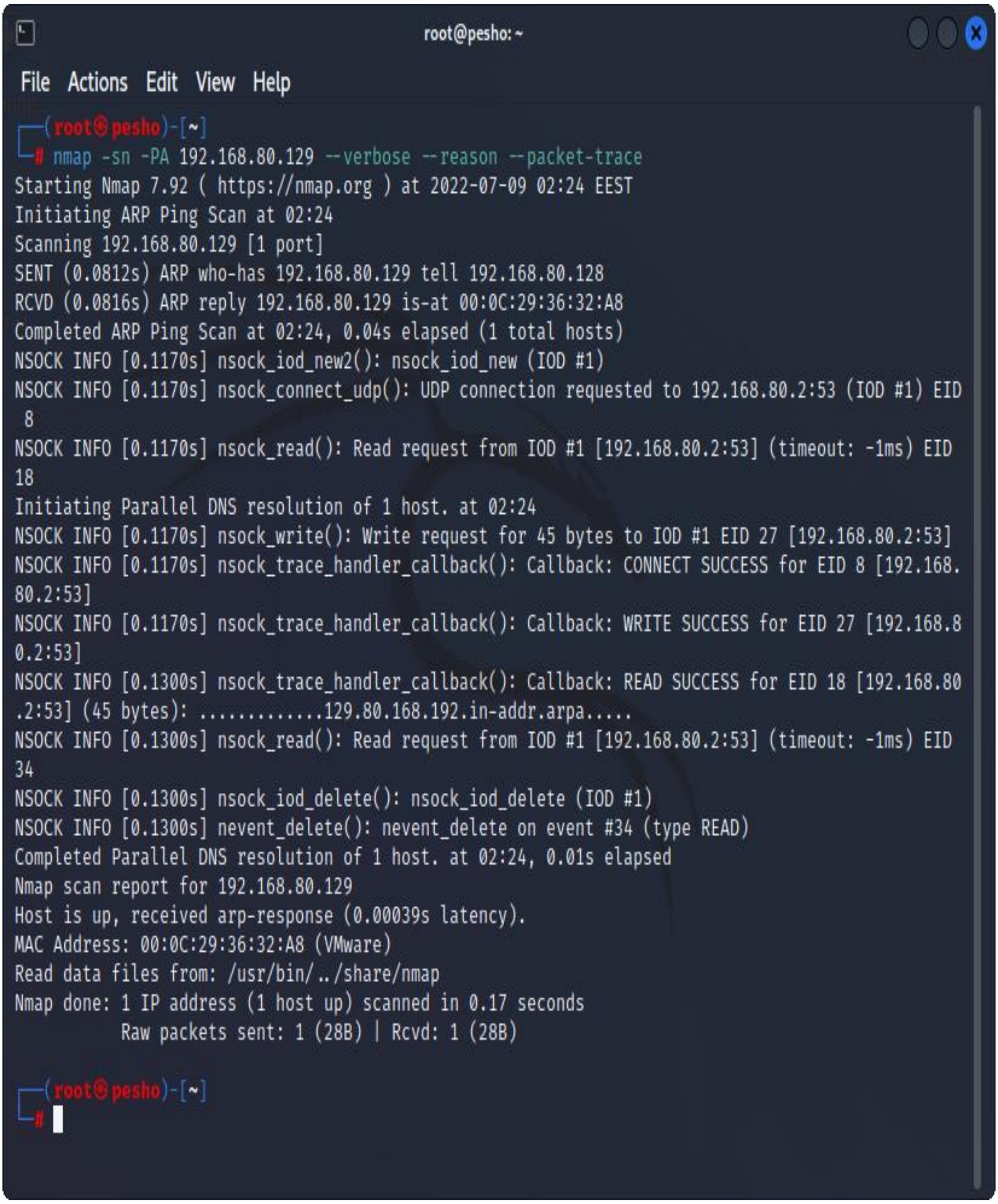

Fig. 8. Received TCP SYN Ping scan results for host with IPv4 address - 192.168.80.129

The presented network scan techniques 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 [2,14,15,16,17,18,21,22,23,31].

Thanks to this information, the malicious hackers can use the most correct exploit to perform unauthorized and unsanctioned access to the information resources of the victim host. At the same time, the chief information security officers must quickly apply security mechanisms and policies to each of the found open ports.

The results of the conducted scientific research present that these network scan techniques are able to find ports with open, closed or filtered state in a relatively short time with detailed obtained information for the scanned host.

The statistical processing between the network packets and bytes from the conducted scientific research visually in fig. 9 is presented.

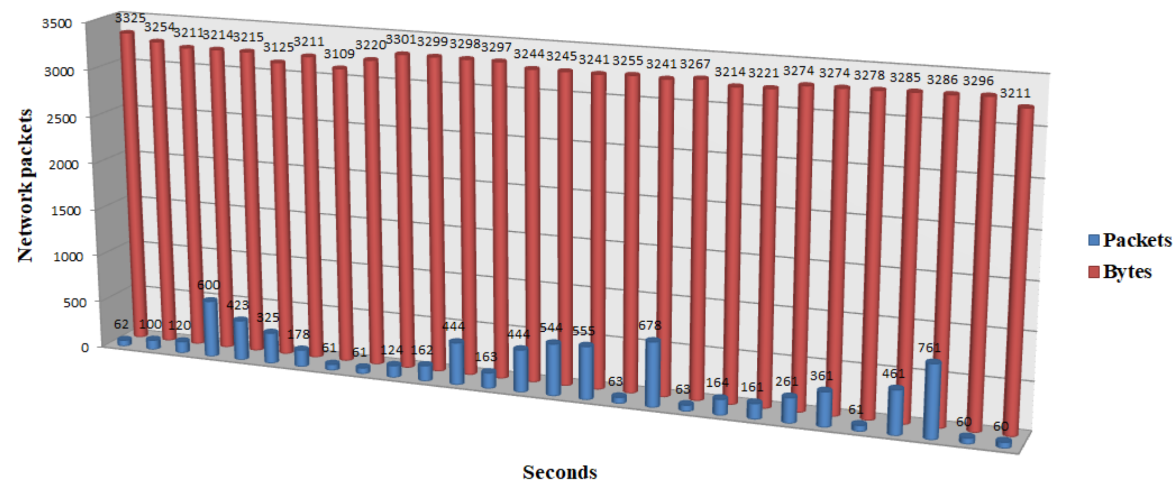

Fig. 9. The statistical processing of the obtained results of the conducted scientific research

<u>**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.</u>

3. Conclusion

Cyber threat intelligence is the collection and analysis of threat and adversary information and the production of models that enable informed decisions to be made about preparedness, prevention, and response to the various types of modern cyberattacks. It is the process of recognizing or detecting any unknown threats that an organization may face so that the necessary protective mechanisms can be implemented to avoid such occurrences. This term includes collecting, researching and analyzing trends and technical developments in the field of cyber threats, including cybercrime, hacktivism and espionage.

Any knowledge of threats that leads to planning and decision-making by the organization to address them is part of threat intelligence. The main purpose of cyber threat intelligence is to make an organization aware of existing or emerging threats and to prepare it to develop a proactive pre-exploitation cybersecurity posture. This process of converting unknown threats into potentially known ones helps to predict cyberattack before it happens and ultimately leads to a better and more secure computer system. Threat intelligence is useful for achieving secure data sharing and global transactions between organizations. 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 use various types of network scan techniques in order to find which ports are in open, closed and filtered network state.

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.