Journal scientific and applied research, vol. 27, 2024
International Journal

Original Contribution

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

REVEALING ANOMALIES BY NETWORK PACKET FLOODING ON BUILT FTP AND OPENSSH SERVERS IN CONTROLLED LAB ENVIRONMENT

Petar Kr. Boyanov

COMMUNICATION AND COMPUTER TECHNOLOGIES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR., E-MAIL: petar.boyanov@shu.bg

ABSTRACT: *This scientific paper investigates the effects of network packet flooding on FTP (port 21) and SSH (port 22) protocols, aiming to reveal and document anomalies in server behavior under high-load conditions. By simulating packet flooding in a controlled lab environment, an analysis on vulnerabilities and anomalies unique to each protocol is conducted in order to the improve defensive capabilities. The results provide guidance on best practices to secure FTP and OpenSSH services against malicious traffic, such as Distributed Denial of Service (DDoS) attacks, supporting wider network security strategies.*

KEY WORDS: *Anomaly, DoS, DDoS, Detection, Flooding, FTP, OpenSSH, Packet, Privacy, Protocol, Revealing, Server, SSH.*

1. Introduction

In network security, understanding how servers respond to unusual or excessive traffic loads is essential for developing strong defensive measures. This scientific paper explores the effect of network packet flooding [5,6,8,36,40,41], which simulates scenarios that may occur in a DDoS attack or high-traffic environment, focusing on FTP and OpenSSH services. The FTP and OpenSSH protocols are commonly employed for transferring files and enabling secure remote access [1,2,5,6,7,8,20,25,33,34,35,40,41].

The scientific aims are to observe and record anomalies in FTP and OpenSSH server behavior under packet flooding and to detect how anomalies present in server responses to stress conditions, thereby revealing weak places, vulnerabilities and strengthening protective measures. Packet flooding is a technique involving the transmission of a large volume of packets to a target server to push its resources to their capacity. The network anomalies that arise from such flooding can include response delays, packet loss and service outages, all of which are important indicators of a server's resilience [12,16,21,22,23,24].

The conducted experiments in this scientific paper that aim to reveal some important and confidential information by network packet flooding without the host's permission is considered as a crime and, if proven, is punishable to the full extent of the law of the respective country [5,6]. Everything illustrated and explained in this scientific paper is for research work and educational purposes and the author is not responsible in cases of abuse.

2. Related work

This section reviews key concepts related to packet flooding and common anomalies in FTP and OpenSSH [1,2,3,5,6,7,8,10,11,12,16,17,18]. Relevant literature on DoS, DDoS cyber-attacks, FTP and SSH protocol vulnerabilities, and known protective measures will be approached [21,22,23,24,25,28,29,30].

These scientific works [32,33,34,35,36,37,40,41] collectively explore various aspects of revealing anomalies by network packet flooding on FTP and SSH protocols.

Revealing anomalies by network packet flooding is also used in application of electronic platforms [26], various types of instrumental equipment for cyberattack prevention [20], specific models for accessing information resources in a secure environment and other technologies [19], net model of command and control system [14], building data center system for defense and security [13], designing and implementation of software-defined systems [15], information exchange management in multimodule multi-position security systems [9], applications of Artificial Intelligence in e-Learning [27], information systems for crisis prevention [31], performance analysis of a mobile computer equipped with solid state disk [39], modeling and calculation of passive audio crossovers [38] and designing of stream ciphers based on random feedback shift registers [4].

3. Experiment

The scientific experiments in this paper in a specialized computer network laboratory in the Faculty of Technical Sciences of the Konstantin Preslavsky University of Shumen are made. The used operating systems are Windows 10 Pro x64 version 22H2, OS build: 19045.4355 and Kali Linux (Linux pesho 6.0.0-kali6-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.12-1kali1 x86_64 GNU/Linux) [5,6].

The study will be conducted in a controlled lab environment to avoid the risk of illegal activity and to maintain safe practices. The main setup includes building FTP and OpenSSH servers on Windows based operating system, platforms for observing network performance and controlled packet flooding simulating DDoS cyber-attack in the operating system Kali Linux [5,6].

The first step to create a ftp Server is to install the necessary packages from the menu - „Control Panel→All Control Panel Items→Programs and Features→Turn Windows features on or off". The necessary features that must be checked are "Internet Information Services" and "Internet Information Services Hostable Web Core". The following is a process of installing all necessary features. This is presented in fig. 1. The IPv4 address is set to 192.168.80.129 with ftp port 21 (shown in fig. 2). The site name of the FTP server is configured as "pesho_ftp" with the physical path is set to "C:\Users\pesho\Desktop\pesho_ftp" (shown in fig. 3). The authentication and authorization settings in fig. 4 are shown. Fig. 5 illustrates the already installed FTP server.

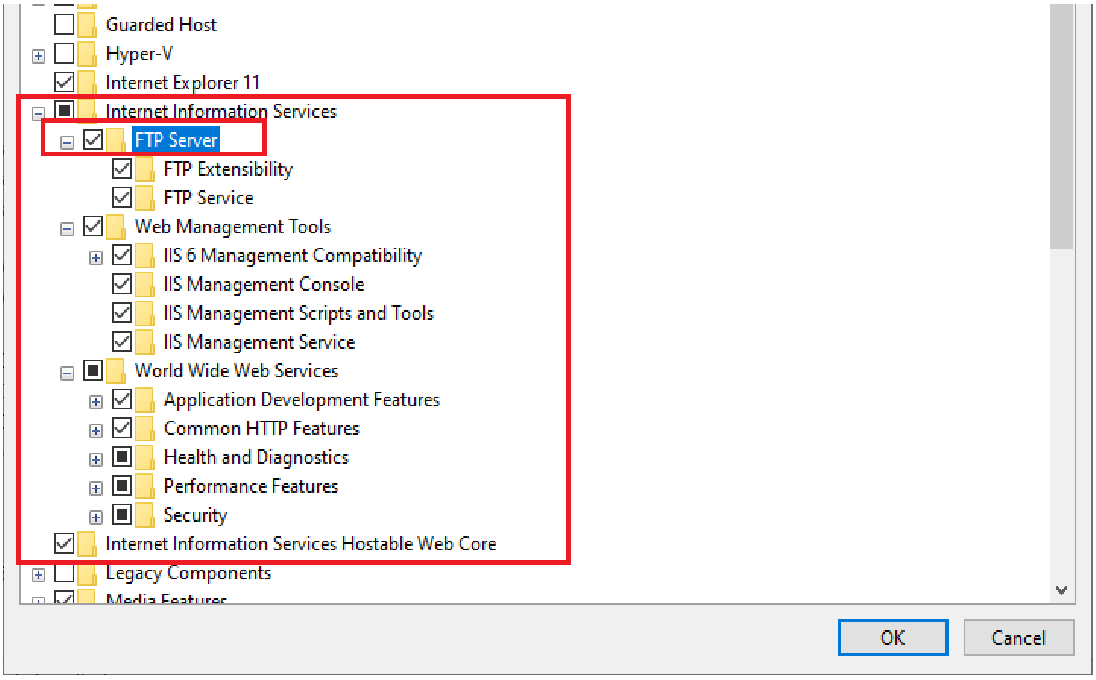

Fig. 1. The selected features for installing a FTP server

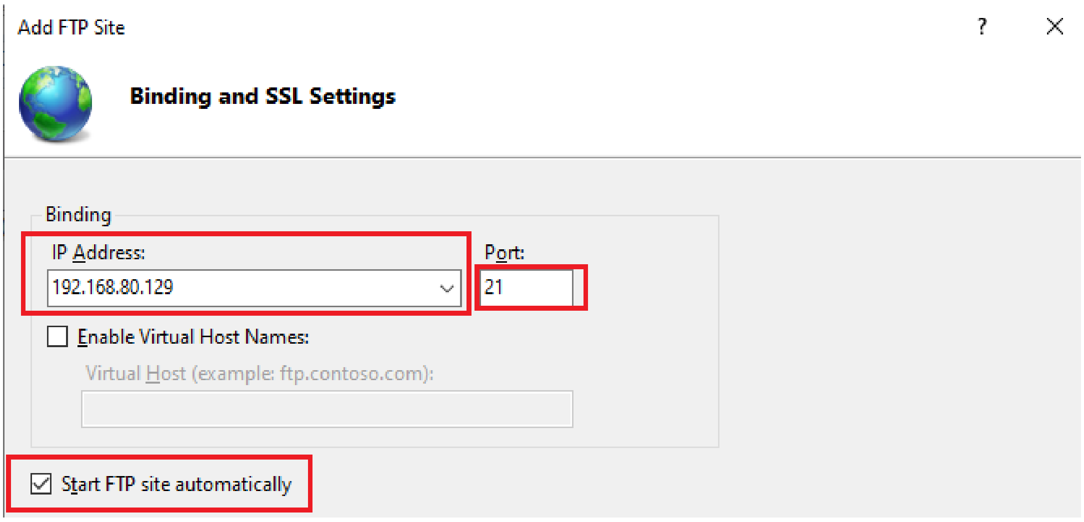

Fig. 2. The binding settings of the FTP server

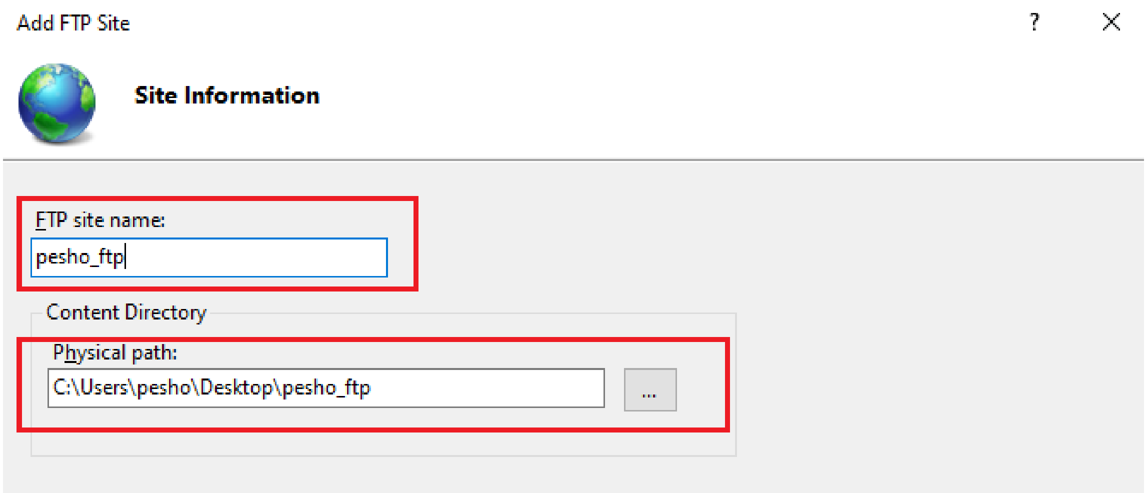

Fig. 3. Configured FTP site name and content directory

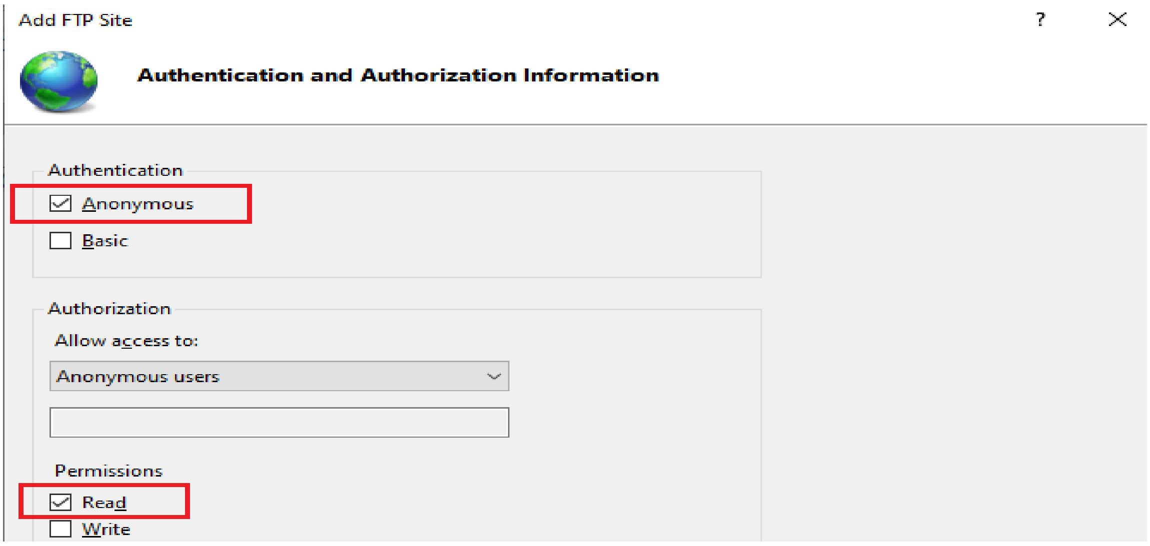

Fig. 4. Authentication and authorization settings

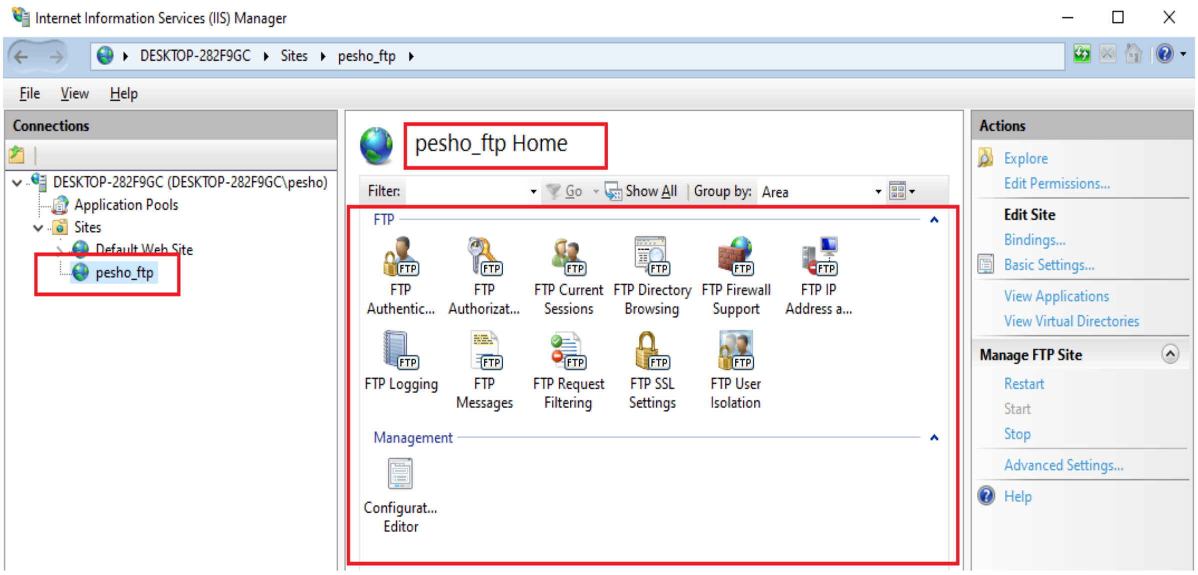

Fig. 5. The installed FTP server

The uploaded files to the FTP server in fig. 6 are shown.

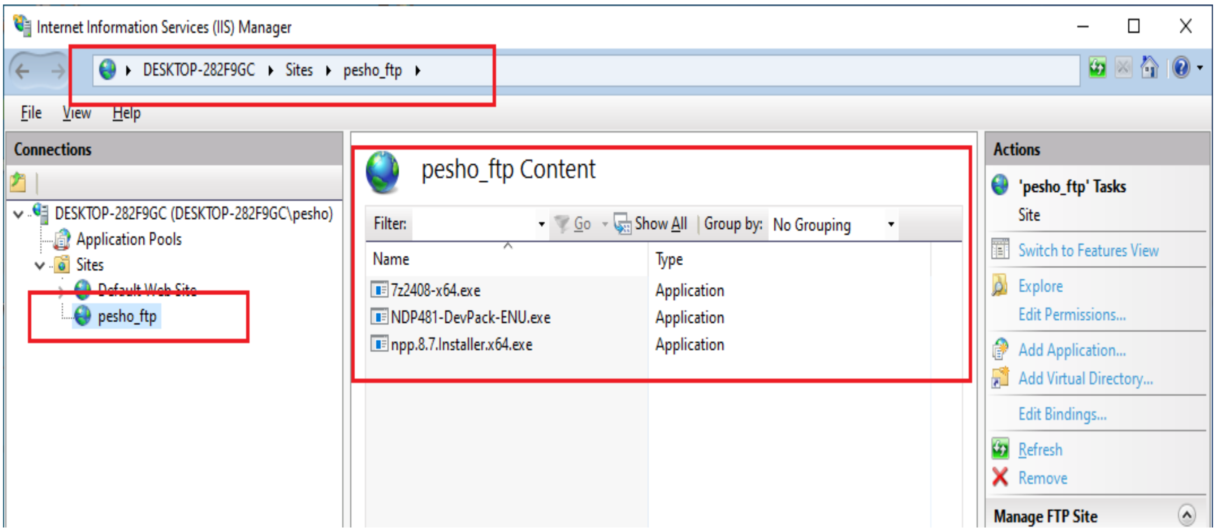

Fig. 6. The uploaded files to the FTP server

To verify that the FTP server is working, it is necessary to open a command-line terminal in Windows in which the “ftp” command must be entered in order to attempt a network connection to the FTP server. After that the IPv4 address 192.168.80.129 must be written to gain access to the server. Finally, the command “dir” shows the whole content of the FTP server. All these steps in fig. 7 are presented.

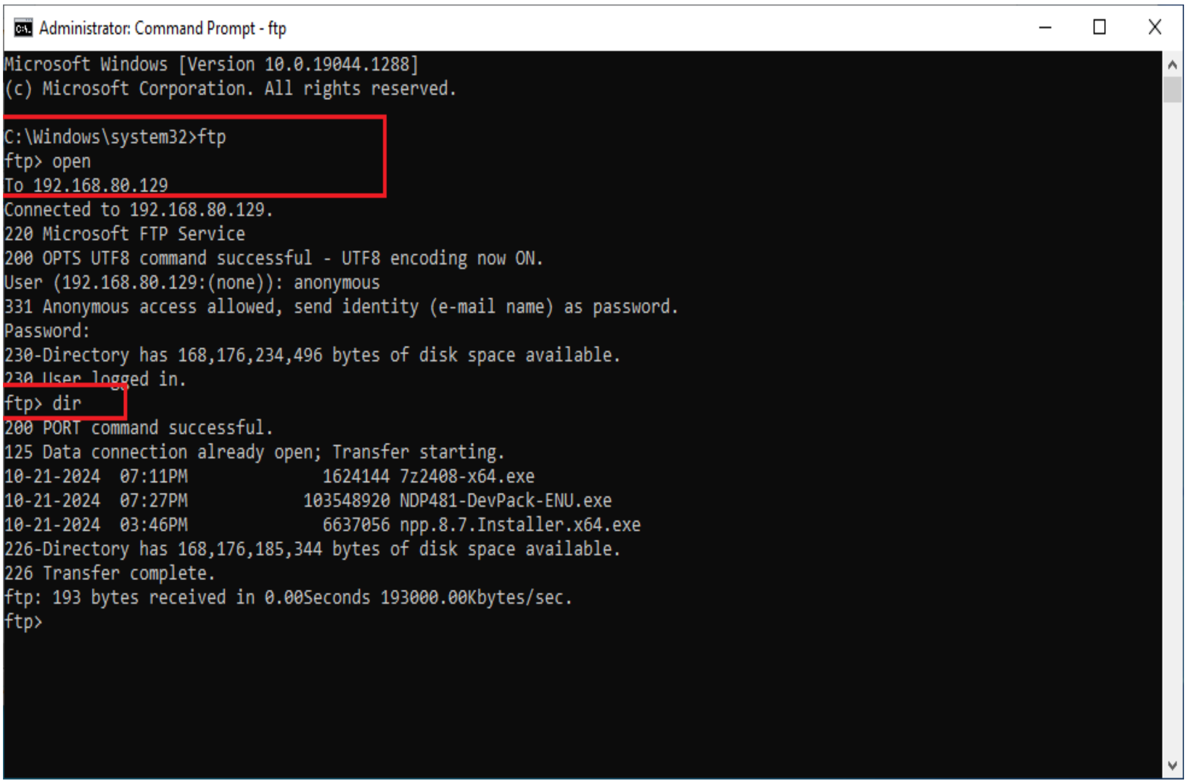

Fig. 7. Successfully login to the FTP server with IPv4 - 192.168.80.129

The installation configuration of the OpenSSH server from the following menu - “Apps and features”→”Optional features” is carried out. After the server is installed, it is necessary the command-line terminal again to be opened in order to be entered the following commands “cd OpenSSH” and “ssh 192.168.80.129”. The command “dir” shows the whole content of the OpenSSH server and the command “exit” serves to terminate the network session to this SSH server (showin in fig. 9).

Fig. 8. Successfully login to the OpenSSH server with IPv4 - 192.168.80.129

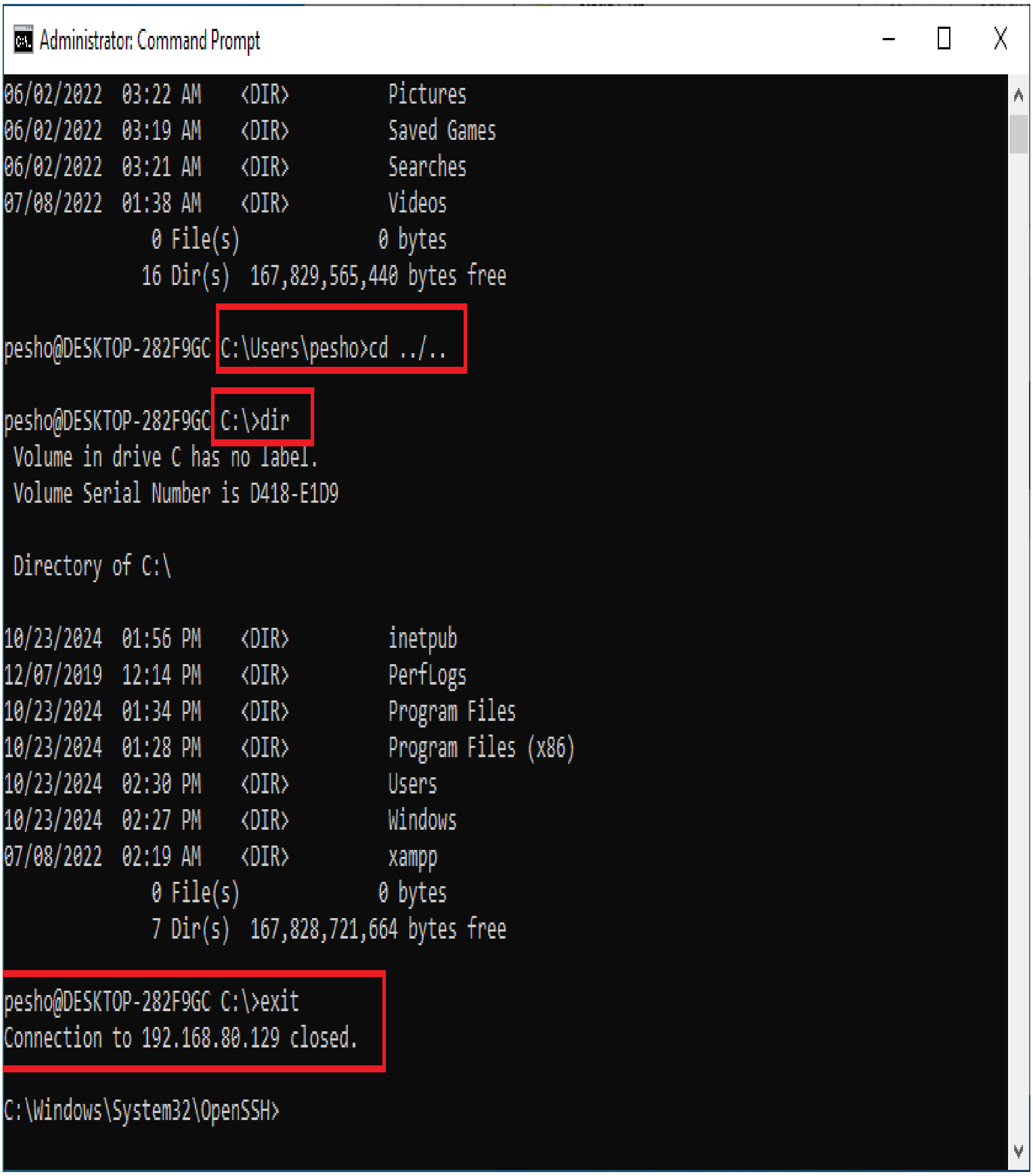

Fig. 9. Termination the network connection to the OpenSSH server

In this scientific paper, the attacking host is running the Kali Linux operating system and its IP address through the "ip addr" command is revealed. This is shown in fig. 10. The next task before simulating a packet network flood [1,2,5,6,33,35,8,36,39,40,41] is performing a port scan with the software network scanner Nmap on the victim host (192.168.80.129). The network scan by the command “nmap -p 21,22 192.168.80.129” is performed. After the network scan was done, it was found that two ports are open. Accordingly, port 21 is responsible for the FTP protocol, and port 22 by the SSH protocol is used. All these steps in fig. 11 are presented.

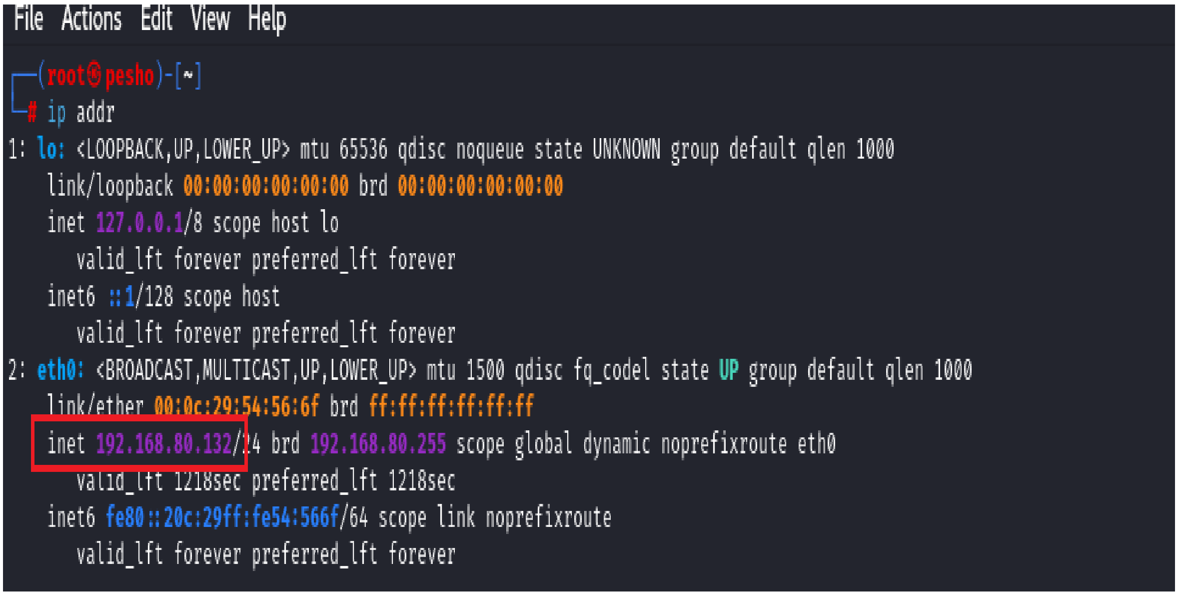

Fig. 10. The IPv4 address of the attacking host (192.168.80.132)

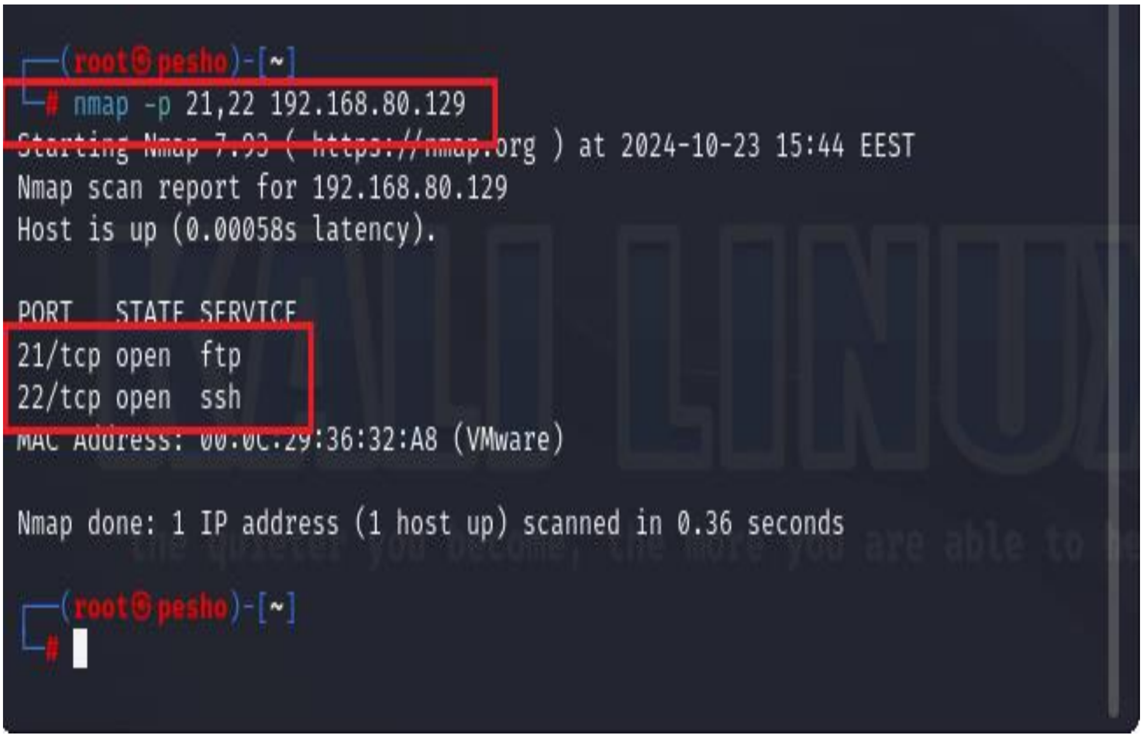

Fig. 11. The detected two open network ports

One of the most popular platforms for generating network packet is Metasploit. For the purposes of the scientific research the auxiliary module “dos/tcp/synflood” [11,12,29,40,41] is used. This aims to flood [1,5,8,21,25,29,32,33,36,40,41] only with activated TCP SYN flag the other host. Accordingly, the network packet flood settings are the following:

- The IPv4 address of the victim host is set to 192.168.80.129 (Windows machine).

- The IPv4 address of the attacking host is set to 192.168.80.132 (Linux machine).
- The network port that will be flooded with packets is set to 21 (FTP).

After all the settings are done, the „exploit" command is written to start the packet flooding on port 21 (FTP protocol). All these steps in fig. 12 are shown.

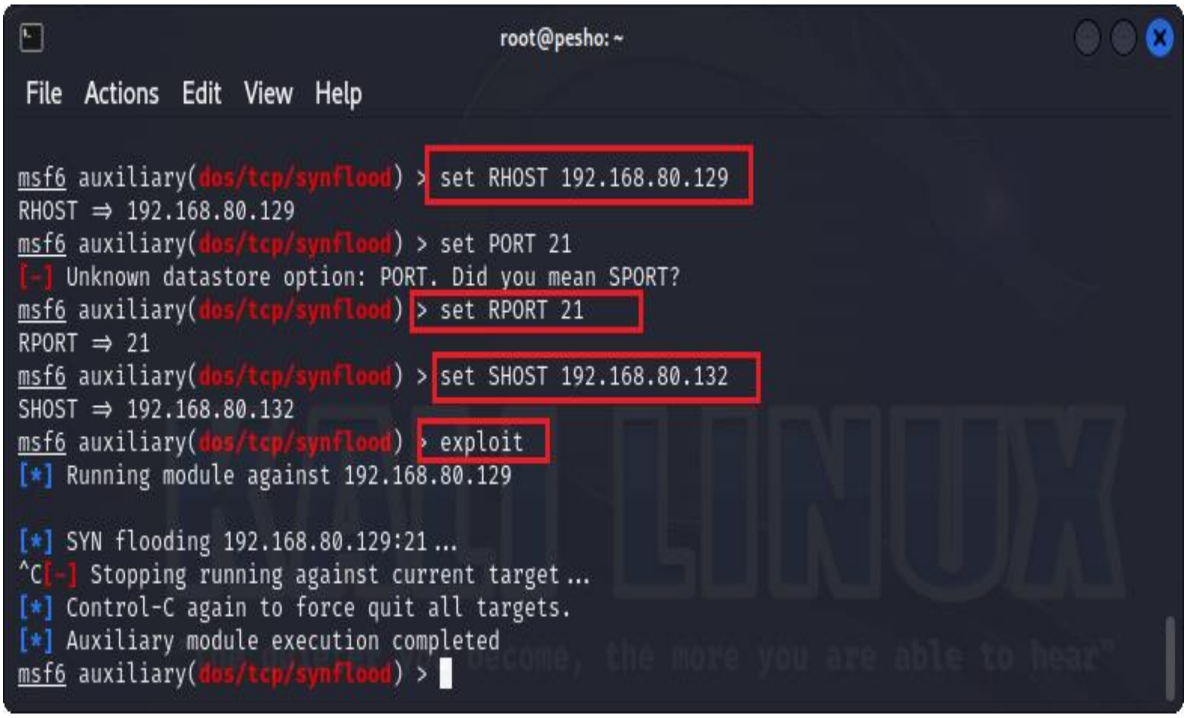

Fig. 12. The network packet flood settings

The other packet emulation utility is Hping3 [5,11,12,29,35,36,37,40]. It is a command-line utility and the command used for generating a packet flooding is "hping3 -S 192.168.80.129 -a 192.168.80.132 -p 22 --flood -V". This time the traffic will be directed to port 22 (SSH protocol). This is shown in fig. 13.

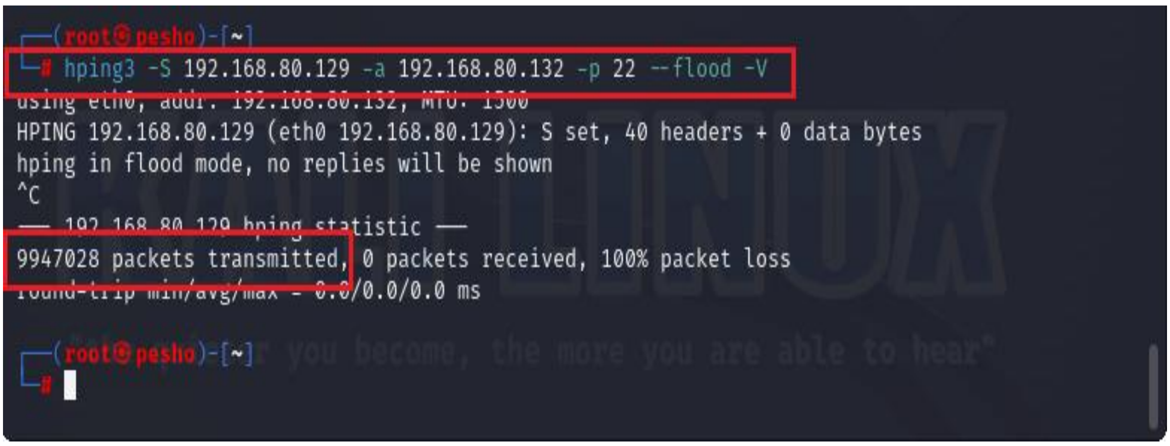

Fig. 13. Performing a packet flooding with Hping3 on port 22

The third network port which will be scanned is 139 (SMB). This port is responsible for the file sharing. The command “nmap -p 139 192.168.80.129” is used [1,5,6,11,12,29,40,41] and the opened port in fig. 14 is presented. For generating a packet flooding the following command “hping3 -2 -p 139 --flood 192.168.80.129 -V” is used. This is illustrated in fig. 15.

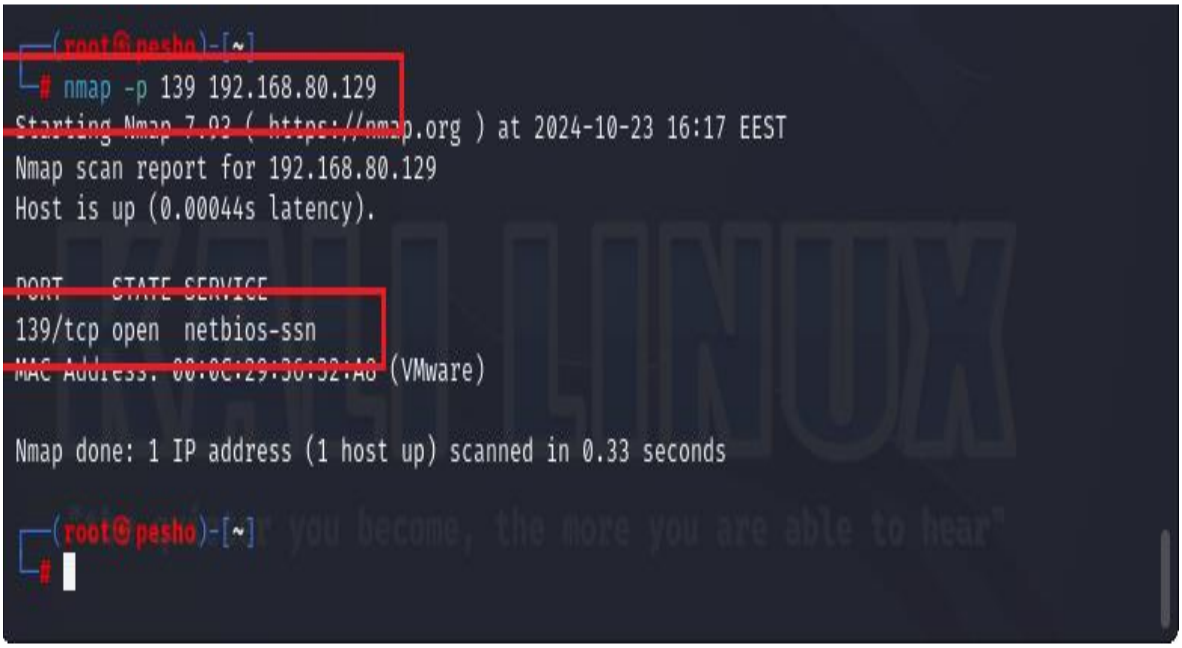

Fig. 14. Performed Nmap scan on port 139

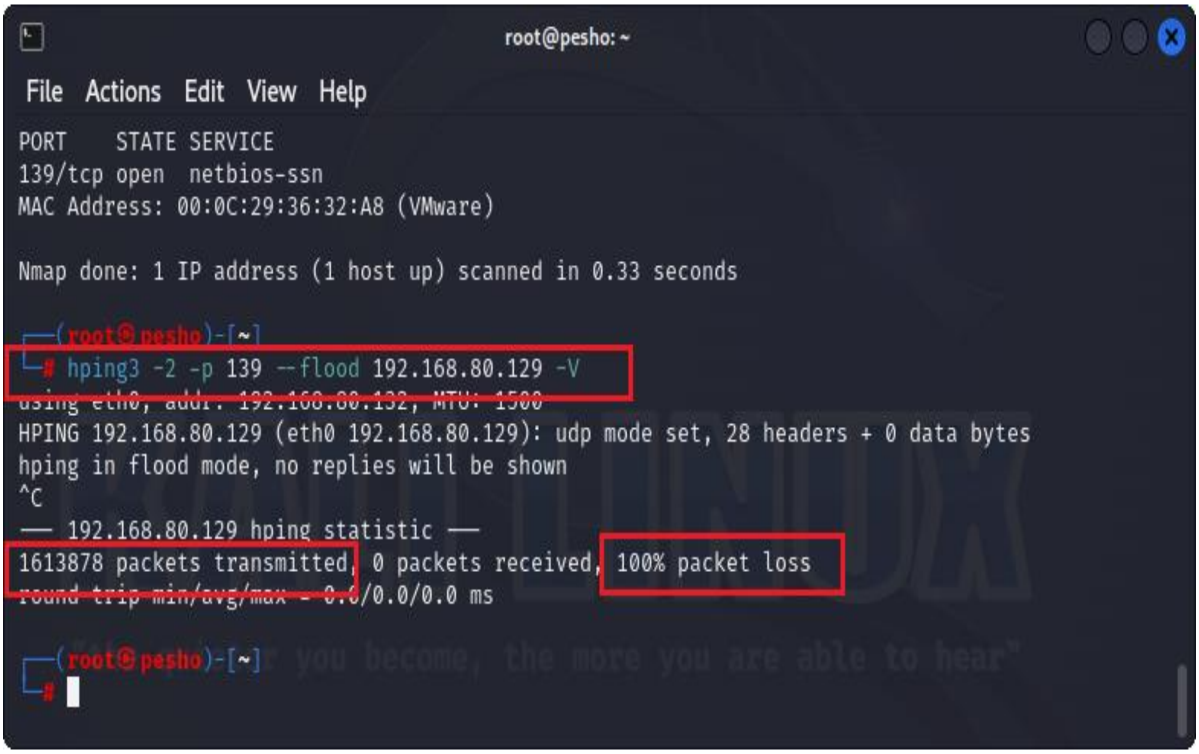

Fig. 15. Performing a packet flooding with Hping3 on port 139

4. Results

The network packet flooding on the victim host via the free of charge network monitoring tool [5,6,11,12,29,40,41] Wireshark version 4.4.1 is intercepted. The main purpose of the research is to reveal the anomaly network traffic directed to ports 21, 22 and 139. Fig. 16 shows the successfully detected packet flooding on port 21 generated from the attacking host 192.168.80.132. Fig. 17 illustrates the detected packet flooding on port 22 and fig. 18 presents the detected packed flooding on port 139.

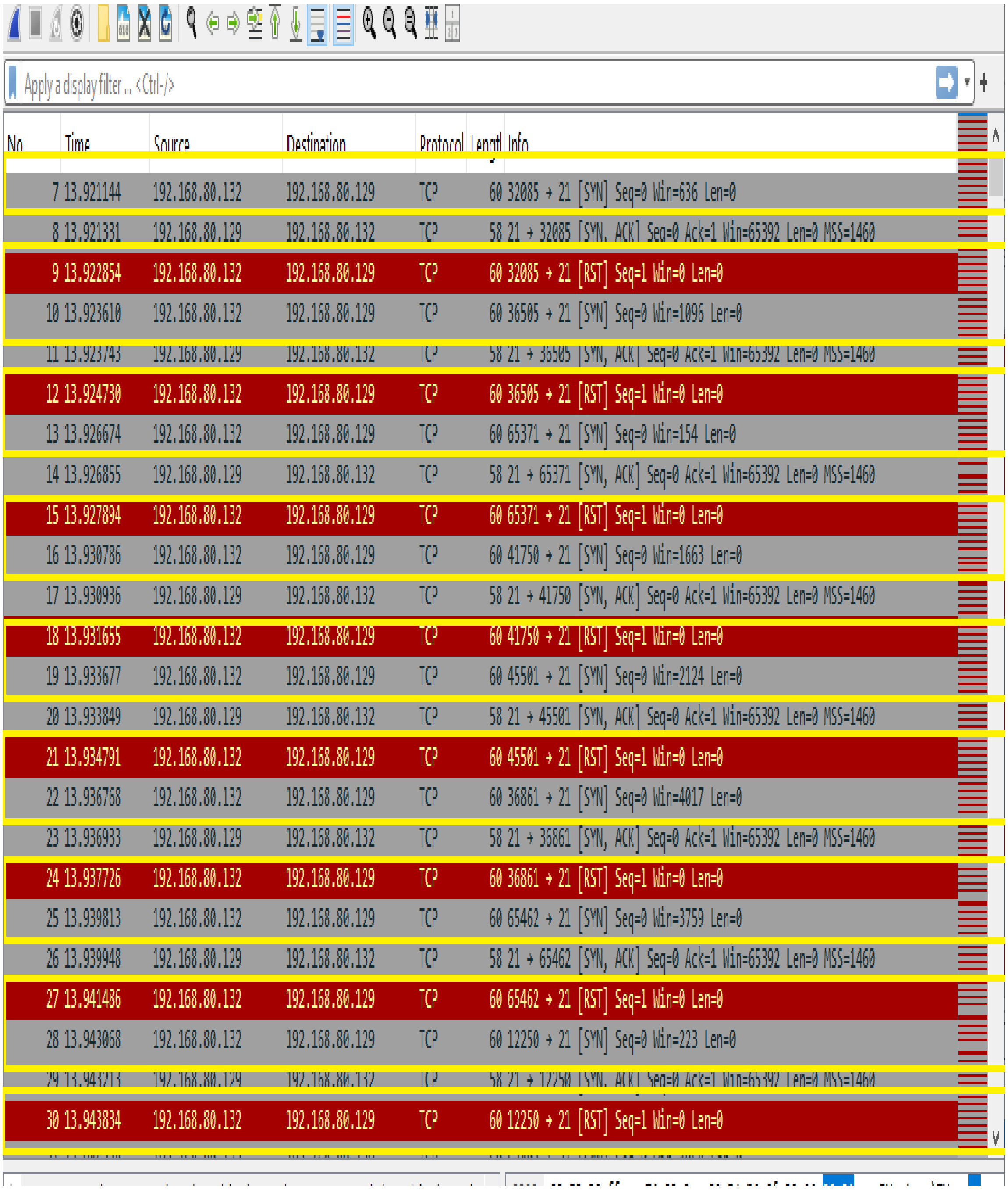

Fig. 16. Detected packet flooding on port 21

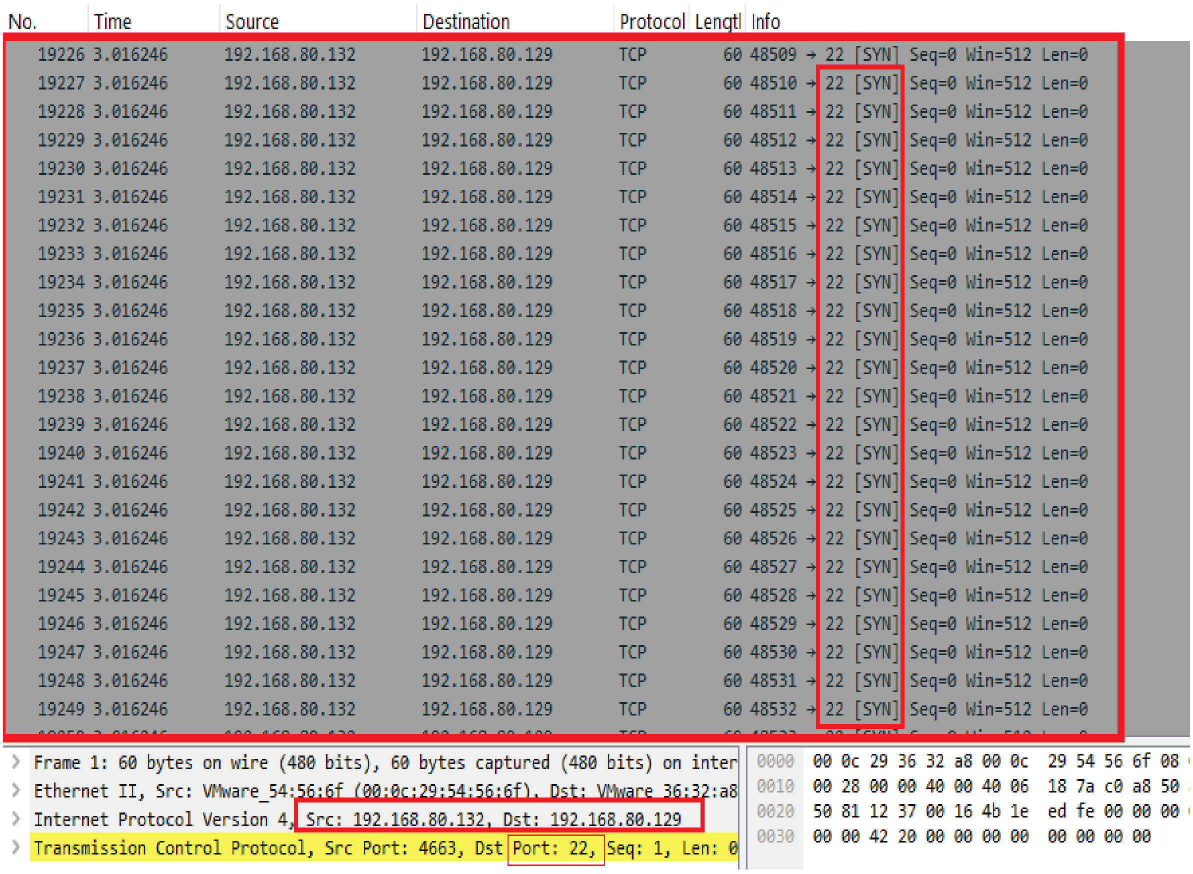

Fig. 17. Detected packet flooding on port 22

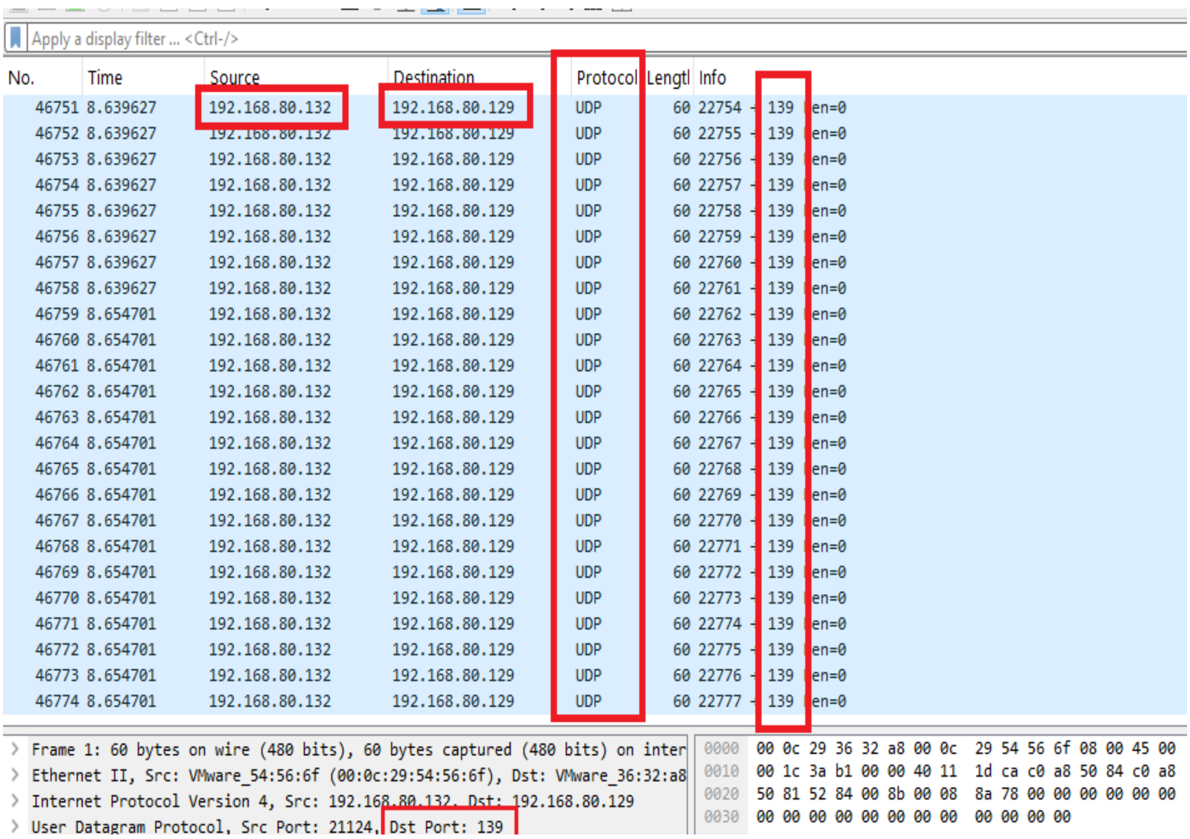

Fig. 18. Detected packet flooding on port 139

As a result of the performed packet flooding in controlled lab environment, the CPU, Memory and Disk resources are totally overloaded which causes a denial of service on the FTP and SSH services. This is shown in fig. 19.

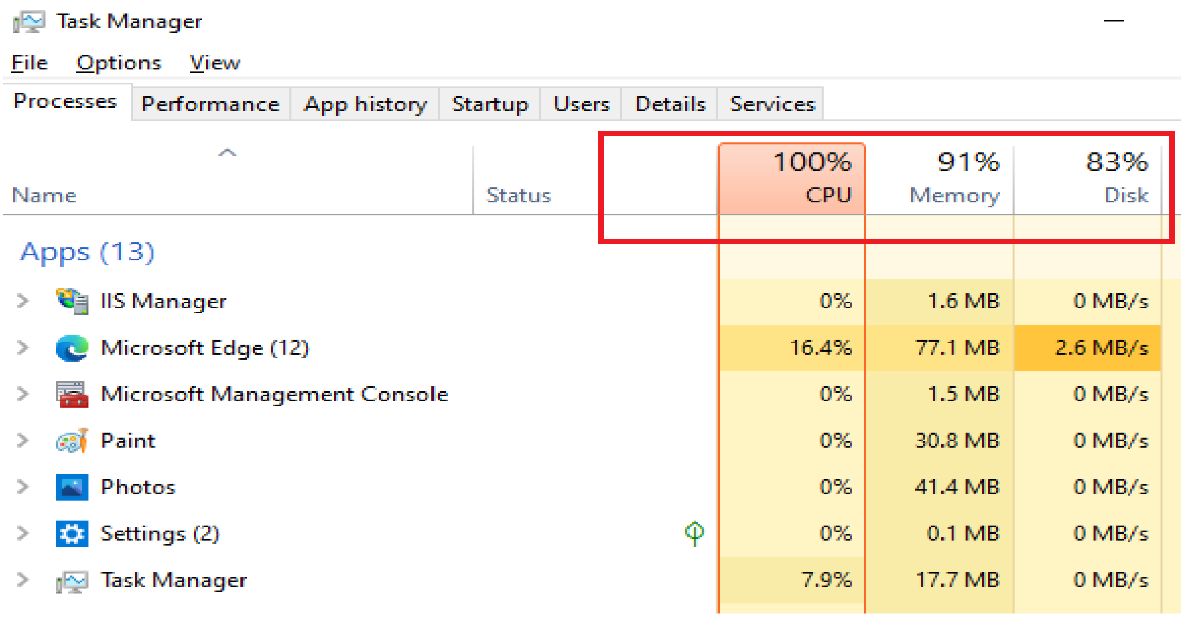

Fig. 19. The overloaded resources

Fig. 20 shows statistics for the detected TCP error packets in 200 ms time intervals. Fig. 21 shows the conversation settings between the hosts - 192.168.80.129 and 192.168.80.132 on port 22.

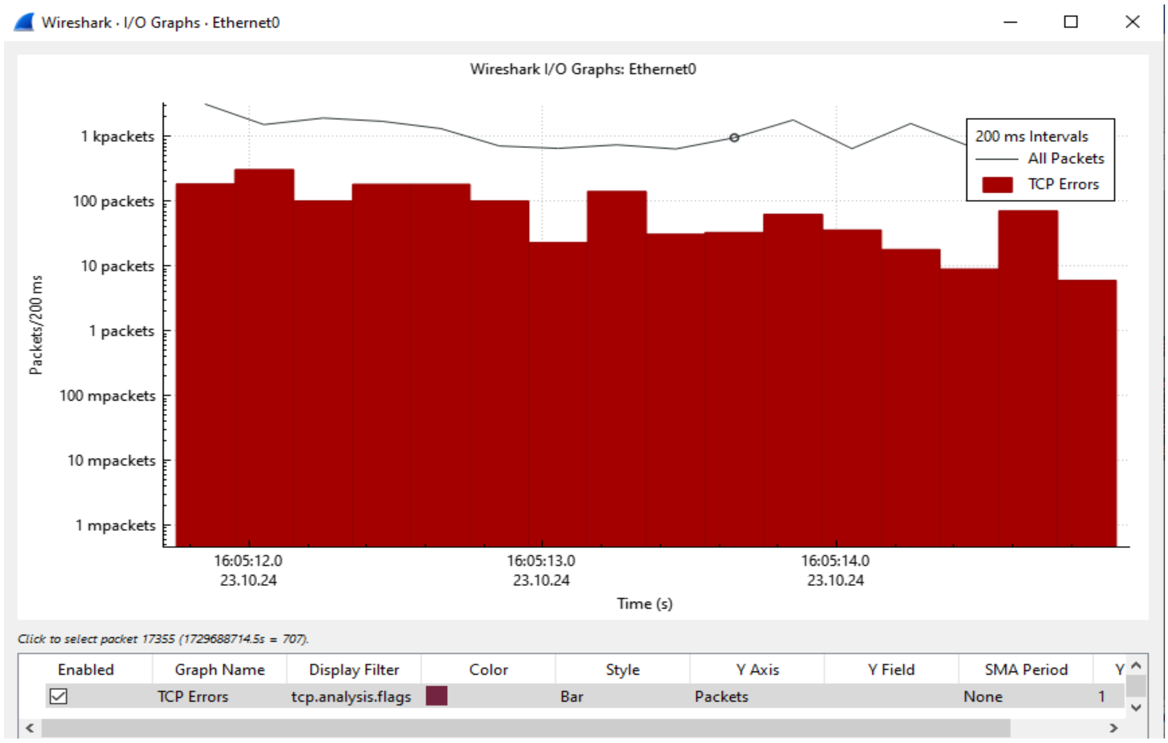

Fig. 20. Statistics for the detected TCP error packets

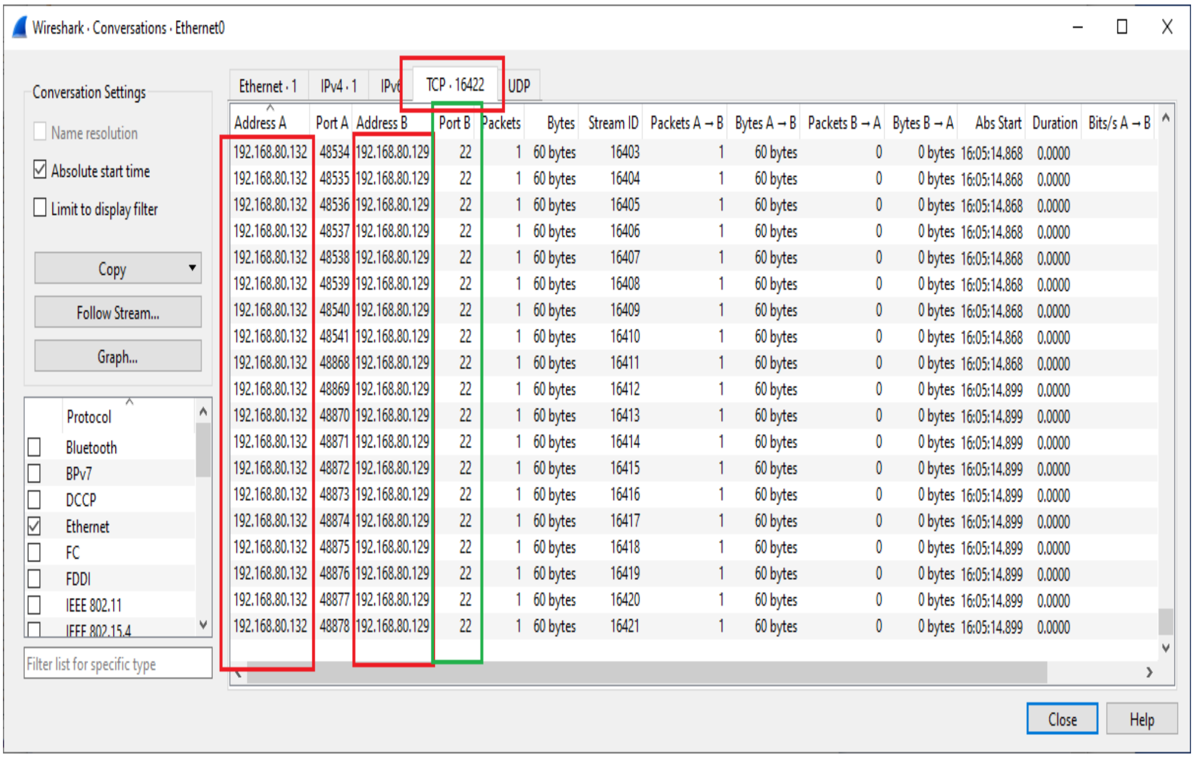

Fig. 21. The conversation settings on port 22

The Recommendations for defending FTP and SSH services from network packet flooding and similar network-based attacks may include the following suggestions [1,2,16,17,22,28,5,6,11,12,29,40,41]:

- Implementing thresholds to manage incoming network traffic and filtering abnormal traffic patterns.
- Deploying IDS and IPS solutions to detect and mitigate suspicious traffic based on predefined rules and machine learning models.
- Strategies for optimizing resource allocation and using load balancers to distribute traffic.

5. Conclusion

This scientific work illustrates the detection of network packet flooding on ports 21, 22 and 139. The observations obtained from studying anomalies during network packet flooding [8,36,40,41] can be applied to protect these specific TCP network protocols. The early and rapid revealing anomalies by network packet flooding on built FTP and SSH servers can protect some important and confidential information of various organizations. In this context, the highly advanced laboratories at the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen provide significant opportunities for students studying [5,6] "Communication and Information Systems", "Computer Technologies in Automated Manufacturing" and "Signal Security Systems and Technologies" in order to acquire substantial theoretical and practical experience in process the revealing anomalies by network packet flooding on built FTP and SSH servers in controlled lab environment [5,6].

References:

[1] Ahda, A., Wulandari, C., Husellvi, H. P., Alhuda, M. Y., Reda, M., Zahwa, P., & Ananda, S. (2023). Information security implementation of DDoS attack using hping3 tools. JComce-Journal of Computer Science, 1(4).

[2] Ajayan, A. C., Prabaharan, P., Krishnan, M. R., & Pal, S. (2016, September). Hiper-ping: Data plane based high performance packet generation bypassing kernel on× 86 based commodity systems. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 478-483). IEEE.

[3] Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arabian Journal for Science and Engineering, 42, 425-441.

[4] Bedzhev, B., Trıfonov, T., & Nıkolov, N. (2010). A multicore computer system for design of stream ciphers based on random feedback shift registers. İstanbul Aydın Üniversitesi Dergisi, Turkey, 2(7), 1-15., https://dergipark.org.tr/en/download/article-file/319309. [Last accessed on 25 September 2024]

[5] Boyanov, P., Using modified sniffer scripts, implementing linear algorithms for detection of network port scan attacks in Linux based operating systems. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 24, Shumen, 2023, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 78-88, DOI: https://doi.org/10.46687/jsar.v24i1.371.

[6] Boyanov, P., Investigating the network traffic using the command-line packets sniffer Tcpdump in Kali Linux. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 25, Shumen, 2023, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 31-44, DOI: https://doi.org/10.46687/jsar.v25i1.378.

[7] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer networks, 44(5), 643-666.

[8] Ghanti, S. R., & Naik, G. M. (2015). Design of system on chip for generating syn flood attack to test the performance of the security system.

[9] Gueorguiev N.L., Nesterov K.N., Minev S., An approach to information exchange management in multimodule multi-position security systems. International Scientific Journal "Security & Future", Vol. 6, Issue 1, pp: 28-31, STUME, 2022, WEB ISSN 2535-082X; PRINT ISSN 2535-0668,https://stumejournals.com/journals/confsec/2022/1/28.full.pdf. [Last accessed on 21 September 2024]

[10] Happe, Andreas, and Jürgen Cito. "Understanding Hackers' Work: An Empirical Study of Offensive Security Practitioners." In Proceedings of ESEC/FSE '23: San Francisco CA USA December 3-9, publisher: Association for Computing Machinery, New York, NY, United States, 2023, pp. 1669-1680. 2023, ISBN: 979-8-4007-0327-0, https://doi.org/10.1145/3611643.3613900.

[11] Haniyah, W., Hidayat, M. C., Putra, Z. F. I., Pertama, V. A., & Setiawan, A. (2024). A Simulasi Serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux. Journal of Internet and Software Engineering, 1(2), 8-8.

[12] Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials, 17(4), 2242-2270.

[13] 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.

[14] Iliev, R., Kochankov, M., A Generalized Net Model of Command and Control System. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 127-131, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8035.

[15] Ivanov, I., & Aleksandrova, K. (2024, June). Design and Implementation of Software-Defined Doppler Radar. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume III, pp. 105-108, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol3.8159.

[16] Islam, M. M., Shahid, S., Awar, K. B., Khan, R., & Sohail, M. (2021). Cyber-Security: Dos Attack Outcomes are Dangerous. European Journal of Electrical Engineering and Computer Science, 5(3), 54-59.

[17] Kamerling, E. J. (2012). The Hping2 Idle Host Scan.
[18] Khare, N., & Bhutad, S. (2023, October). Intrusion Detection System for Live Anomaly-Based Network Packets. In 2023 IEEE International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.
[19] Kochankov, M., & Iliev, R. (2024, June). A Generalized Net Model for Accessing Information Resources in a Secure Environment. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 175-178, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8034.
[20] Kolev, Alexander, Nikolova, Pavlina. Instrumental Equipment for Cyberattack Prevention. Information & Security: An International Journal 47, no. 3 (2020):285-299. https://doi.org/10.11610/isij.4720.
[21] Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security, 127, 103096.
[22] Lee, K., Kim, J., Kwon, K. H., Han, Y., & Kim, S. (2008). DDoS attack detection method using cluster analysis. Expert systems with applications, 34(3), 1659-1665.
[23] Liang, L., Zheng, K., Sheng, Q., & Huang, X. (2016, December). A denial of service attack method for an iot system. In 2016 8th international conference on Information Technology in Medicine and Education (ITME) (pp. 360-364). IEEE.
[24] Liu, R. (2023, October). Study limitations of DoS attackers due to computer resources. In Third International Conference on Signal Image Processing and Communication (ICSIPC 2023) (Vol. 12916, pp. 447-451). SPIE.
[25] Mirkovic, J., Prier, G., & Reiher, P. (2002, November). Attacking DDoS at the source. In 10th IEEE International Conference on Network Protocols, 2002. Proceedings. (pp. 312-321), IEEE.
[26] Mirtcheva-Ivanova, Daniela, Application of electronic platforms to increase the knowledge of learners. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 448-452, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8090.
[27] Mirtcheva-Ivanova, D., Application of Artificial Intelligence in E-Learning. In Proceedings of the 15th International Scientific and Practical

Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 208-211, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8053.

[28] Nazario, J. (2008). DDoS attack evolution. Network Security, 2008(7), 7-10.

[29] Nedyalkov, I., & Georgiev, G. Kali Linux - a simple and effective way to study the level of cyber security and penetration testing of power electronic devices, International Journal on Information Technologies & Security, 16(2):103-114, 2024, doi:10.59035/JMFY4876.

[30] Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications, 67, 147-165.

[31] Pavlov, G., Kolev. Al., A place of GIS technologies in information Systems for crisis prevention, 6th International Conference on Application of Information and Communication Technology and Statistics In Economy and Education (ICAICTSEE – 2016), December 2-3rd, 2016, UNWE, Sofia, Bulgaria, ISSN 2367-7635 (print), ISSN 2367-7643 (online), pp. 452-457.

[32] Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 39(1), 3-es.

[33] Qureshi, M. A., Ahmed, S., Mehmood, A., Shaheen, R., & Dildar, M. S. (2024). Vulnerability assessment of operating systems in healthcare: exploitation implications techniques and security. Health Sciences Journal, 2(2), 104-111, ISSN (Online): 2959-2259, ISSN (Print): 2959-2240, https://doi.org/10.59365/hsj.2(2).2024.98.

[34] Rao, G. S., & Subbarao, P. K. (2024). Exploring a novel framework for DOS/DDOS attack detection and simulation in contemporary networks. i-manager's Journal on Software Engineering, 18(3).

[35] Servanda, Y. (2024). Analisis Serangan Forensik Terhadap Serangan Ddos Ping of Death Menggunakan Tools NMAP dan HPING3. Jurnal Sains dan Teknologi (JSIT), 4(2), 209-216.

[36] Singh, N., Sharma, D., & Rawat, V. (2023, April). Evaluation of the efficiency of honeypots in opposing flooding attack. In 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) (pp. 365-370). IEEE.

[37] Tampati, I. F., Setyawan, F. G., Sejati, W. W., & Kardian, A. R. Comparative analysis of CPU performance on freebsd 64-bit and redhat 64-bit operating system against denial of service (DoS) using hping3. CESS (Journal of Computer Engineering, System and Science), 8(1), 209-219.
[38] Trifonov T., 2019, Modeling and Calculation of Passive Audio Crossovers, Annual of Konstantin Preslavsky University of Shumen, Vol IX E Technical Sciences, ISSN 1311-834X, pp. 182-189.
[39] Trifonov, T., Performance analysis of a mobile computer equipped with solid state disk. Annual of Konstantin Preslavsky University of Shumen, Shumen, Konstantin Preslavsky University Press, ISSN 1311-834X, Vol. IV E, 2014, pp. 27–42.
[40] Vuletić, D. V., & Nojković, N. D. (2018). Realization of A TCP Syn Flood Attack using Kali Linux. Vojnotehnicki glasnik/Military Technical Courier, 66(3), 640-649.
[41] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 15(4), 2046-2069.