SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 57, MAY 2019

A NOVEL ALGORITHM FOR DETECTING TCP/IP NETWORK ATTACKS USING HYBRID FIREWALL SCRIPT APPLIED IN LINUX OPERATING SYSTEM

Abstract: A novel algorithm for detecting TCP/IP network attacks using hybrid firewall script written in Linux operating system is made.

Author information:

Petar Kr. Boyanov
Associate Professor, PhD,
Lecturer in Department "Communication and Computer Technologies"
At Konstantin Preslavsky – University of Shumen
✉ peshoaikido@abv.bg
Bulgaria

Keywords:
Cyber attacks, Computer resources, Host, LAN, Network security, Protocols, Security, TCP/IP, Vulnerability, WAN

Introduction

The hybrid firewall is the most modern and effective means of combating unauthorized access to computer system and network resources. The hybrid firewall monitors the status of each incoming or outgoing network connection and checks for the presence of analytical web platforms that collect different user information in the Internet space [1], [2], [3], [4], [5], [6], [10], [11], [12], [13].

The built-in hybrid firewall consists of a firewall with packet filtering, a dynamic firewall with full inspection, a firewall with an attached gateway, a NAT network, a firewall and a host-based firewall. This ensures complete protection of the host from malicious network cyber attacks [7], [8], [9], [14], [15], [16], [17], [18], [19], [20], [29].

The Hybrid Firewall serves to protect the information resources of the web site of the Technology transfer center (ctt.shu.bg), the web site of annual of the Faculty of Technical Sciences (annuals.shu.bg) and the web site of the Faculty of Technical Sciences (ftn.shu.bg) at Konstantin Preslavsky University of Shumen [30], [31], [32], [33], [34], [35], [36], [40], [41], [42].

2. A Linear algorithm to build a hybrid firewall using script written in Linux

To protect against the TCP/IP network attack, a versatile scripting algorithm was developed to build a hybrid firewall to protect against unauthorized access to the resources of a particular host on a small private computer network.

11 scripts were used as the basis for the modified script. The script [] is characterized by the fact that it has secured blocking of the ECN field in IPv4 and TCP protocols, as well as security to block cyber attacks from file sharing and P2P. A major flaw in scripts [1] and [2] is the activation of the ICMP protocol. This Script [4] does not use security to block different types of port scanning cyber attacks on the input chain. The [3] shows basic firewall configurations, but without the implementation of detailed security policies against network scanning attacks [21], [22], [23], [24], [25], [26], [27], [28].

Only 6 command lines for blocking port scanning cyber attacks are used in Script [5], and this is not the most effective protection because it does not cover the full flags combination. A major flaw in the script [1] continues to be the use of the ICMP protocol, as well as the non-use of protection against various types of port scanning attacks. An advantage in this script is the activation of the IPv6 protocol. The Script [4] only provides basic protection against the major types of port scans of cyber attacks. Script [7] has a huge drawback by allowing all users to implement inbound network connections using the SSH, HTTP, and HTTPS protocols. The security script [6] is not configured to block the ECN field

in IPv4 and TCP protocols, as well as security to block cyber attacks from file sharing and P2P networking. The script [8] does not provide protection against cyber attacks targeting different countries and anonymous proxy IPs [34], [35], [36], [37], [38], [39], [40], [41], [42].

To remove all these shortcomings, a modified script that implements a hybrid firewall in a Linux-based operating system was created.

The hybrid firewall algorithm consists of basic 3 subsystems and 27 security solutions. Each of the algorithms, as well as the security solutions, are standalone software scripts designed to counteract various types of malicious cyber attacks.

The basic algorithm (Fig.1) of the hybrid firewall includes the following basic steps:

- Configure the logical IP addresses of all host network interfaces.
- Logical IP address of the firewall.
- Default gateway, whose role is to provide the host with access to the Internet space.
- Virtual Network Interface eth1:1, which acts as a router for the entire local computer network, thus all traffic passes and is processed through the dynamic firewall.
- Loading system firewall protection features in the kernel of the Ubuntu 18.04.2 LTS-desktop-i386 operating system kernel. In order to provide greater protection against malicious network cyber attacks, other non-kernel protections are being loaded, such as xtables extensions.

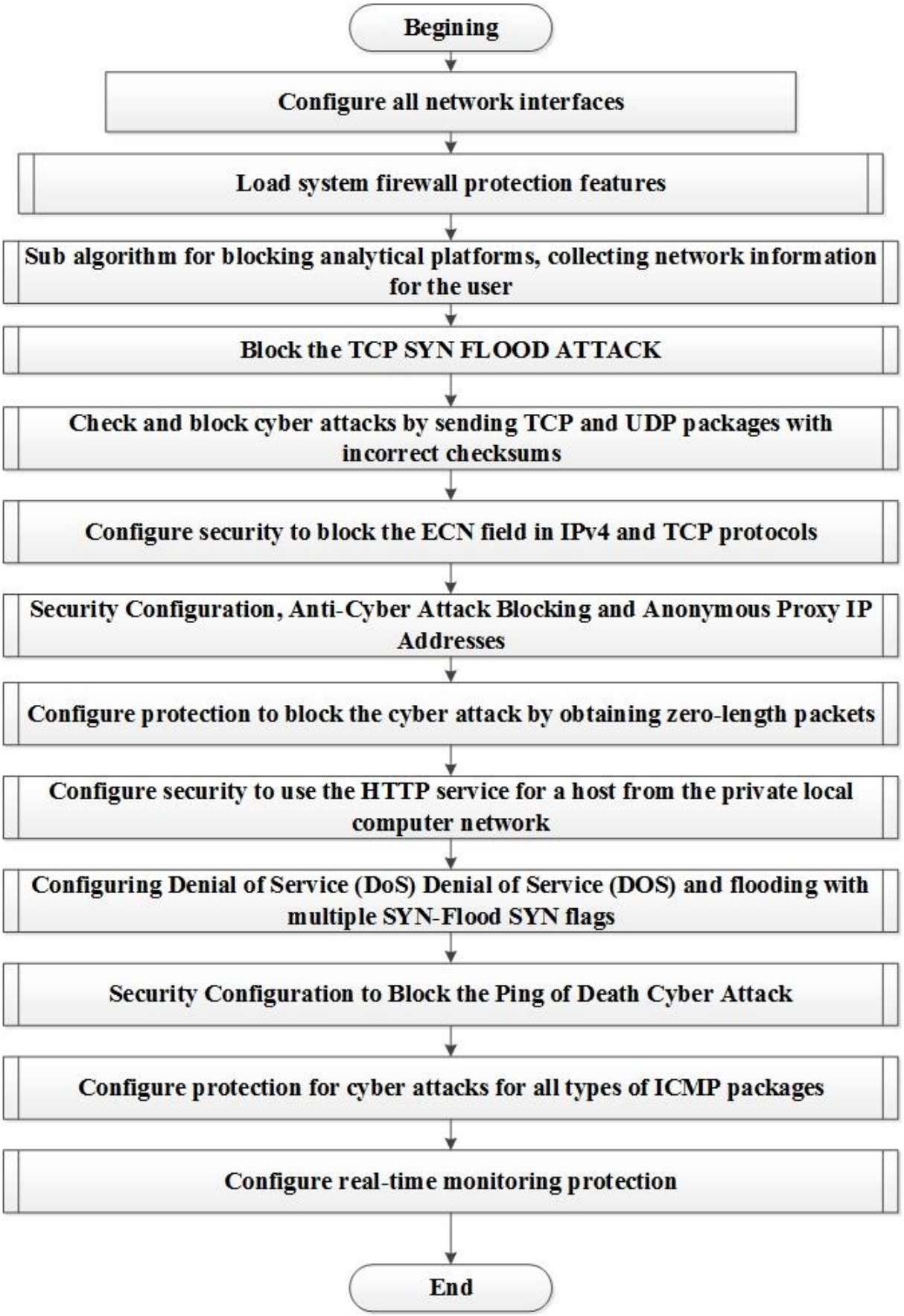

Fig.1. The basic algorithm of the built hybrid firewall

3. Experiment

The scientific research is realized in a real university local computer network, consisting of three hosts and one router. Fig.2 shows the way the hybrid firewall works in a local computer network at the Faculty of Technical Sciences.

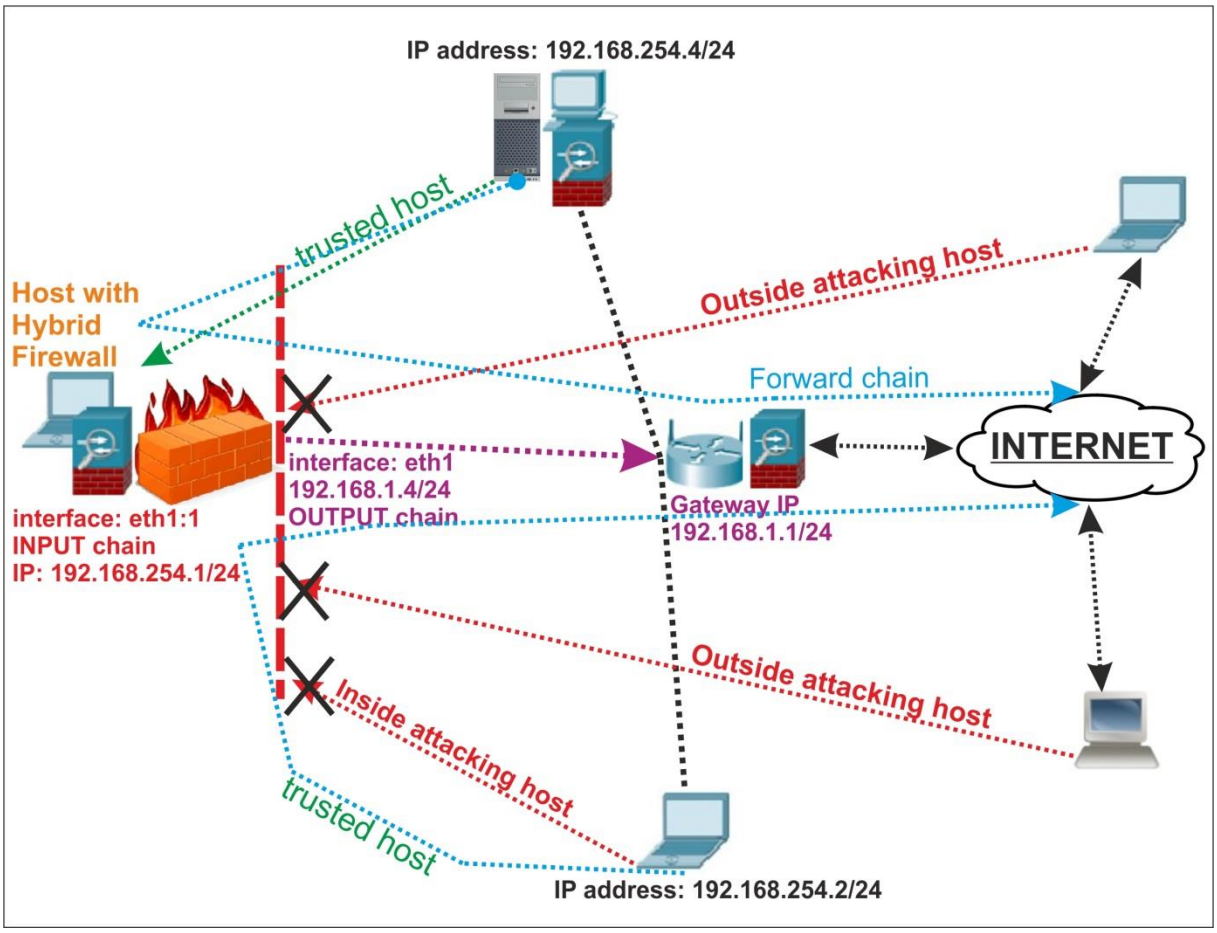

Fig.2. Implementation of hybrid firewall against modern types of cyber attacks

The research is realized in a real local computer network consisting of three hosts and one router. The devices are configured as follows:

- The logical IP address of the real network interface eth1 of a hybrid firewall is set to a logical IP address 192.168.1.4 and a network mask 255.255.255.0. HP ProBook 4540s laptop with Intel® Core ™ i3-3110M 2.40 GHz dual-core processor and 4.00 GB of RAM is used in the research. The installed operating system is Linux Ubuntu 18.04.2 LTS-desktop-i386.
- Configured the virtual network interface eth1:1 of the hybrid firewall with a logical IP address 192.168.254.1 and a network mask 255.255.255.0. This interface acts as a router for the entire local computer network, thus all network traffic passes and is processed through the hybrid firewall.
- A default firewall gateway is configured with a logical IP address of 192.168.1.1 and a network mask of 255.255.255.0. The role of this gateway is to provide access to the hybrid firewall to the Internet space.
- The logical IP address of the trusted host real network eth1 interface is set to logical IP address 192.168.254.4 and network mask 255.255.255.0. A desktop computer with a Gigabyte 7N400-L motherboard and a AMD ATHLON XP2500 + single core processor AMD ATXLON XP2500 + was used. The installed operating system is Linux Ubuntu 3.19.0-26-generic 14.04.2-desktop-i386. A default gateway host is configured with a trusted host with logical IP address 192.168.254.1. The role of this gateway is to provide trusted host access to the Internet space through detailed inspection and filtration by the hybrid firewall.
- The logical IP address of the attacking host's real network interface is set to logical IP address 192.168.254.2 and network mask 255.255.255.0. Asus x52j laptop with Intel® Core ™ i5 CPU M460 2.53 GHz dual-core processor and 4.00 GB of RAM is used. The installed operating system is Microsoft Windows 7 Professional 64 bit. A default gateway host is configured for the attack host with logical IP address 192.168.254.1. The role of this gateway is to provide access to the attacking host to the Internet space through detailed inspection and filtration from the hybrid firewall.
- The Huawei HG532e wireless router with four FastEthernet (100 Mbps) connections was used in the research. Access to router settings is disabled by the BTC Broadband Service Internet provider (Vivacom) with dynamic IP address range 79.100.0.0 - 79.100.127.255. Despite the prohibition applied, the hybrid firewall successfully operates on the small local computer network.

4. Results

Results obtained from the real-time hybrid firewall monitoring module in the presence of the cyber attacks on figures 3, 4, 5 and 6 are illustrated.

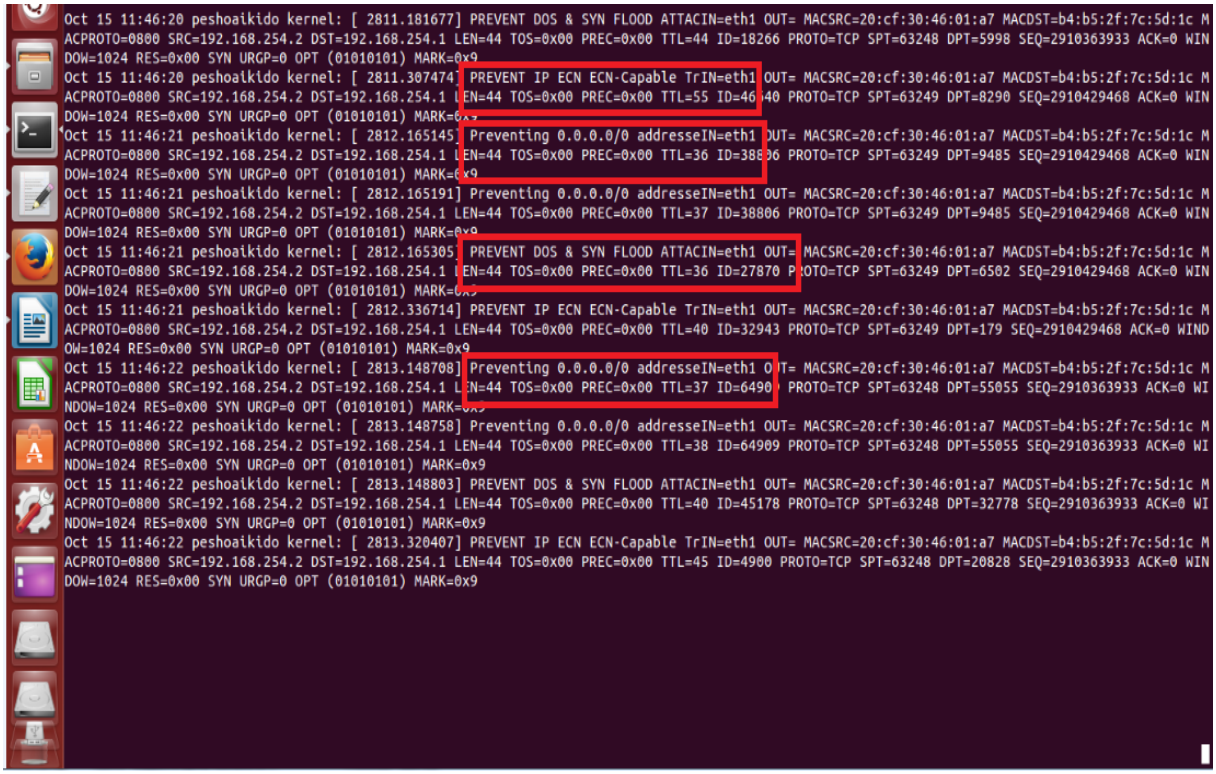

Fig.3. The results obtained from the real-time hybrid firewall monitoring module

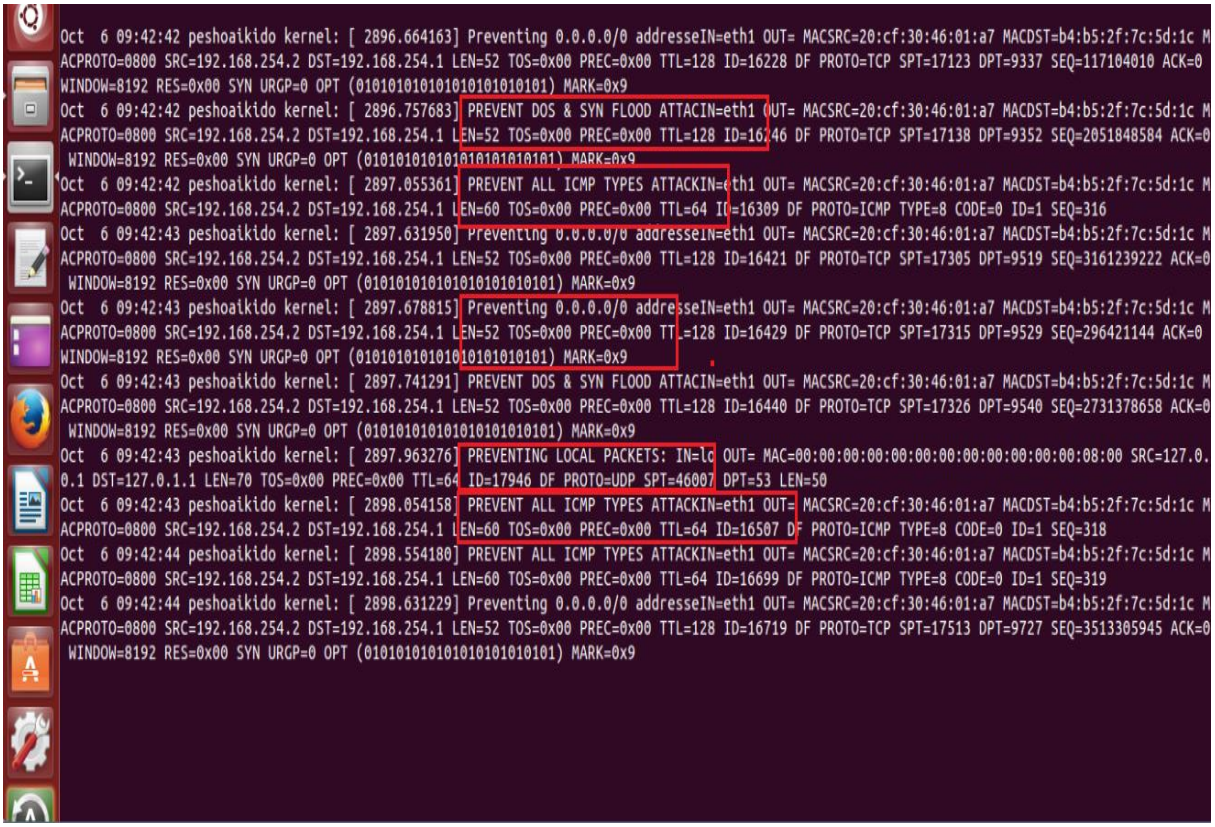

Fig.4. The results obtained from the real-time hybrid firewall monitoring module

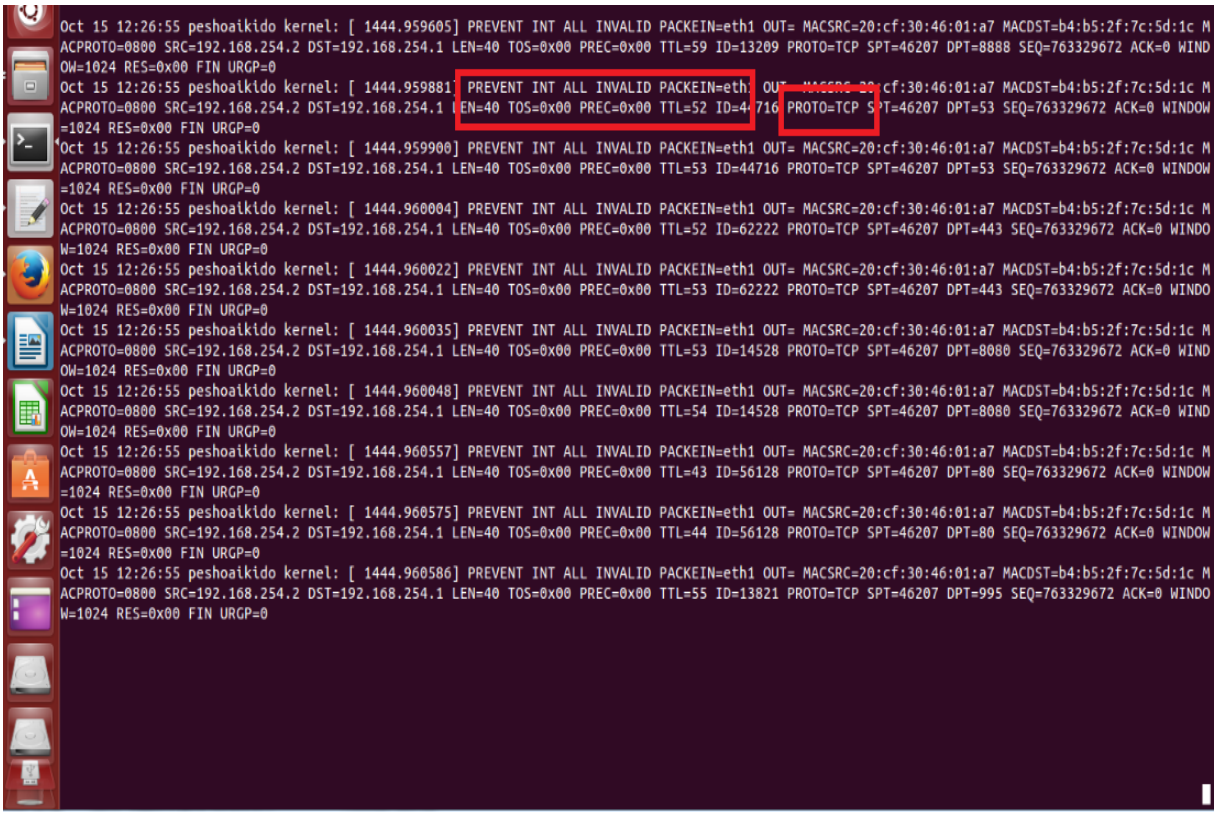

Fig.5. The results obtained from the real-time hybrid firewall monitoring module

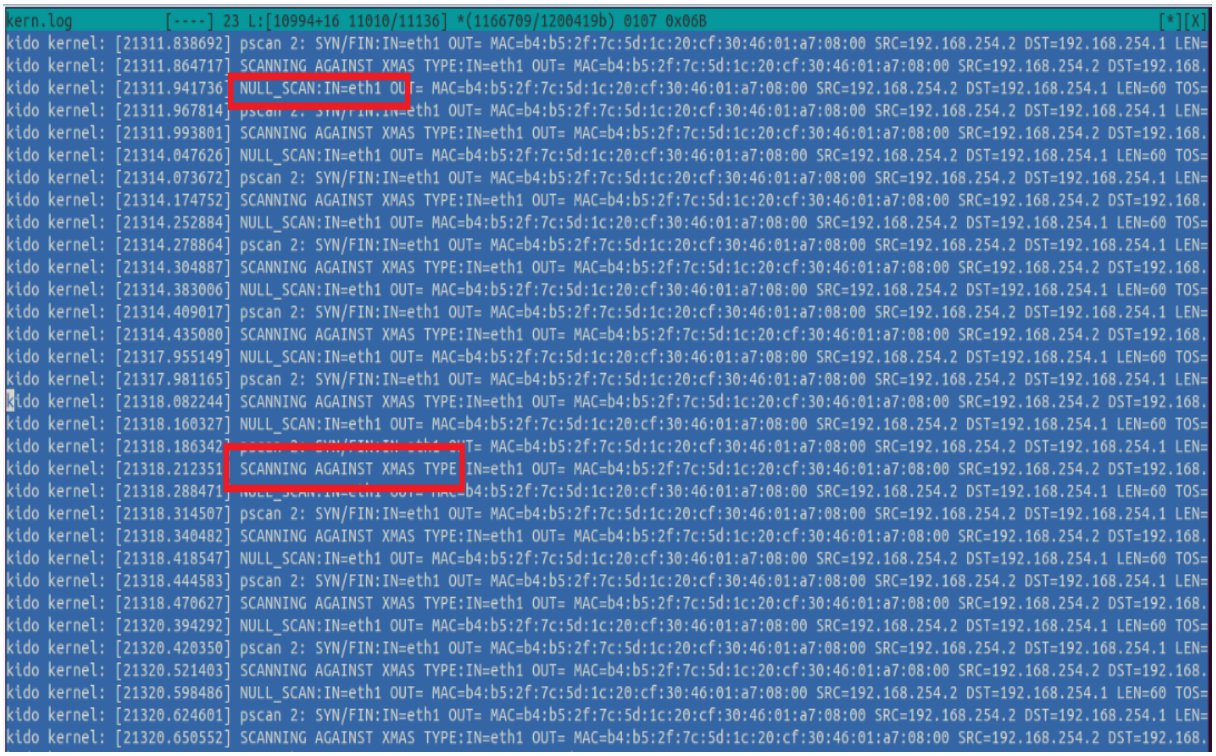

Fig.6. The results obtained from the real-time hybrid firewall monitoring module

ATTENTION: All the experiments and research in this paper are made in a specialized computer laboratory at the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen, consisting of several hosts and a home-based local computer network consisting of five hosts. Everything illustrated and explained in this paper is for research purposes and the authors are not responsible in cases of abuse.

5. Conclusion

As a result of the research it is concluded that an algorithm has been developed for blocking different types of port scanning cyber attacks for the input chain, which is practically realized with a

modified script in a Linux based operating system. The developed hybrid firewall can be used to train students from the Faculty of Technical Sciences in the subjects "Data transmission and computer communications", "Computer networks" and "Network administration", "Cybersecurity", "Technical means in the security sector", "Computer and network security", "Countering cyber attacks against information systems handling classified information and personal data", "Detection and Intrusion Prevention Systems", "Cybersecurity of information resources in the organization" and etc. The future scientific work will be related to the synthesis of an algorithm for detecting anomalies when transmitting network packets to local and global computer networks

References:

1. Barry B. I., Chan H. A., Intrusion detection systems, Handbook of Information and Communication Security, Springer Berlin Heidelberg, ISBN: 978-3-642-04117-4, pp. 193 – 205.
2. Beale J., Foster J. C., Snort 2.0 Intrusion Detection, Syngress Publishing, 2003, ISBN: 1-931836-74-4, pp. 650.
3. Bejtlich R., The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013, ISBN-13: 978-1593275099, pp.376.
4. Berenjkoub, Mehdi S. H. F. H., A Taxonomy for Network Vulnerabilities, International Journal of Information & Communication Technology, May 2010, Vol.2, №1, pp. 29-44.
5. Fry C., Nystrom M., Security Monitoring, O'Reilly Media, 2009, ISBN: 978-0-596-51816-5, pp. 248.
6. Hekmat S, "Communication Networks", "PragSoft Corporation", USA, 2005 г.
7. Helmer, Guy, et al. "A software fault tree approach to requirements analysis of an intrusion detection system", Requirements Engineering 7.4 (2002): 207-220.
8. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Informatsionnые tehnologii i bezopasnosty, Zhurnal Akad. nauk Ukrainы., Spets. vыpusk, Kiev, 2013, Str. 79-86.
9. Nachev A.I., G. Zhablyanova, Analitichen model na efektivnost na sistema za zashtita na informatsiyata, Voenni tehnologii i sistemi za osiguryavane na otbranata, Sofia, 2014.
10. Nachev A. I., St. Zhelezov, G. Zhablyanova, Sintez na sistemi za zashtita na informatsiyata pri zadadeno nivo na efektivnost, Voenni tehnologii i sistemi za osiguryavane na otbranata, sofia, 2014.
11. Ogletree, Terry William, ed. Upgrading and repairing networks. Que Publishing, 2004.
12. Stanev St., Szczypiorski Krzysztof., Steganography Training: a Case Study from University of Shumen in Bulgaria, Intl Journal Of Electronics And Telecommunications, 2016, Vol. 62, No. 3, Pp. 315-318, Manuscript received September 7, 2016; revised September, 2016, DOI: 10.1515/eletel-2016-0043.
13. Savov, I., Edin pogled varhu protivodeystvieto na hibridnite zaplahi v Evropeyskia sayuz, mezhdunarodna konferentsia „Asimetrichni zaplahi, hibridni voyni i vliyanieto im varhu natsionalnata sigurnost", Nov Balgarski universitet, mart 2018 g., ISBN 978-619-7383-09-6, s. 179-185.
14. Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost", VUSI, 2017, ISSN 2535-0358, s. 36-47.
15. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
16. Neykova, M., Vavezhdaneto na vtoro nivo na mestno samoupravlenie – osnovna antikrizisna myarka, godishnik BSU, tom XXVII str. 161.
17. Neykova, M., Protsesat na detsentralizatsia na Republika Bulgaria, godishnik na BSU, str.161.
18. Neykova, M., Prilaganeto na printsipa na subsidiranostta – osnoven instrument za regionalizatsia i detsentralizatsia , Yuridicheski sbornik na TsYuN pri BSU, str. 161.
19. Sotirov, Ch., Preventsia na uchilishtnoto nasilie chrez elektronni sredstva, Nauchni trudove tom 50, seria 6,2 RU - 2011. ISSN 1311-3321.

20. Sotirov, Ch., Relationship between the social development and motor activity of the child. SocioBrains - international scientific online journal publisher: www.sociobrains.com., Issue 24, August 2016, ISSN 2367-5721.
21. Sotirov, Ch., Stoyanova, I., Savremenni tehnologii v preduchilishtnoto obrazovanie. Godishnik na ShU „Ep. K. Preslavski", tom XX D,2016 ISSN 1314-6769.
22. Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6 (available at: http://varepsilon.com/), indexed in Russian Science Citation Index, (RINTs: Nauchnaya эlektronnaya biblioteka eLIBRARY.RU), VINITI RAN Эlektronnыy katalog nauchno-tehnicheskoy literaturы VINITI.RU, National Centre for Information and Documentation (Bulgaria), Google Scholar, OpenAIRE, Polish Scholarly Bibliography (PBN), Index Copernicus International, ROAD, the Directory of Open Access scholarly Resources, DOAJ, Directory of Open Access Journals.
23. Kantardzhiev, I., Stanev, S., Hristov, H.,Otnosno finansovoto osiguryavane na deynostta na firmeno kontrarazuznavatelno zveno. Sbornik nauchni trudove - Nauchna konferentsia s mezhdunarodno uchastie "MATTEH 2018" - 25-27 oktomvri 2018, ISSN: 1314-3921, t.2, ch.1, 2018, s. 96-108.
24. Hristov, L., Stanev, S., Hristov, H., Sredstva za zashtita na chuvstvitelnata informatsia na firmata ot vatreshni zlozhelateli (insayderi). Sbornik nauchni trudove - Nauchna konferentsia s mezhdunarodno uchastie "MATTEH 2018" - 25-27 oktomvri 2018, ISSN: 1314-3921, t.2, ch.1, 2018, s. 109-115.
25. Trifonov T., Bateriite na prenosimite kompyutri - problemi i reshenia, Sbornik nauchni trudove MATTEH 2018, tom 2, chast 2, str. 37-45, Universitetsko izdatelstvo ShU, 2018, ISSN: 1314-3921.
26. S. Kazakov, T. Trifonov, I. Tzonev, Probabilistic-temporal characteristics in a three level centralized computer structure, Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, 2014, Liepaya, Latvia, Riga.
27. Zh. Zhivkov, T. Trifonov, Meditsinskie mikrokommunikatsionnыe sistemы maloy moshtnosti, ispolyzuyushtie slozhnыe signalы, Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, 2014, Liepaya, Latvia.
28. Trifonov T., Analiz na proizvoditelnostta na prenosim kompyutar, oborudvan s poluprovodnikovo ustroystvo za sahranenie na danni, Godishnik na ShU „Ep. K. Preslavski", Tehnicheski nauki, Universitetsko izdatelstvo, Shumen, 2014 str. 27-42, ISSN 1311-834X.
29. Dimitrova, N., 2014: The motivation for effective study of technical and technological information assimilation. International Scientific Online Journal – ISSN 2367-5721 Issue 4, December 2014, www.sociobrains.com, pp 94-99.
30. Dimitrova, N., 2015: Operationalize the aims of technological education International Scientific Online Journal. Issue 16, December 2015, www.sociobrains.com pp. 48 –53.
31. Dimitrova, N., 2014: Role of informatization in technological education and information culture of students International Scientific Online Journal, Issue 2, October 2014, www.sociobrains.com pp. 26-30.
32. Dimitrova, N. Prinosat na tehnologichnoto obuchenie za sahranyavane na balgarskite natsionalni traditsii. – Godishnik na Shumenskia universitet „Episkop Konstantin Preslavski", T. HH D, Nauchni trudove ot konferentsia „Inovatsii v obrazovanieto", 30 septemvri – 02 oktomvri 2016, Pedagogicheski fakultet, Shumen, Episkop Konstantin Preslavski, 2016, 686 – 690.
33. Ilieva, V., Social Change and Historical Reality, SocioBrains, Issue 52, December 2018, pp. 179-186, ISSN 2367-5721 (online), www.sociobrains.com, Publ.: Veselina Nikolaeva Ilieva., Bulgaria, 2018, (SJIF = 5.536).
34. Ilieva, V., Main Personal Orientations of Identity, SocioBrains, Issue 43, March 2018, pp. 383-392, ISSN 2367-5721 (online), www.sociobrains.com, Publ.: Veselina Nikolaeva Ilieva., Bulgaria, 2018, (SJIF = 5.536).

35. Ilieva, V., The Protection of Individual and Group Identities as Human Rights, SocioBrains, Issue 48, August 2018, pp. 128-131, ISSN 2367-5721 (online), www.sociobrains.com, Publ.: Veselina Nikolaeva Ilieva., Bulgaria, 2018, (SJIF = 5.536).
36. Ilieva, V., The social administration as specialized administration for social work , SocioBrains, Issue 29, January 2017, pp. 61-67, ISSN 2367-5721 (online), www.sociobrains.com, Publ.: Veselina Nikolaeva Ilieva., Bulgaria, 2017.
37. Chalakov, R., Iliev, K., Kibersurnostta v „neobyatnoto" informatsionno prostranstvo, Mezhdunarodna nauchna konferentsia Kibersigurnostta v informatsionnoto obshtestvo. Sbornik nauchni trudove. Shumen 2017. ISBN 978-954-9681-82-6.
38. Chalakov, R., Iliev, K., „Internet" – neobhodimost i zaplaha, Mezhdunarodna nauchna konferentsia Kibersigurnostta v informatsionnoto obshtestvo. Sbornik nauchni trudove. Shumen 2017. ISBN 978-954-9681-82-6.
39. Iliev, K., Petrov, V., Savremenni zaplahi za natsionalnata sigurnost ot voenen harakter, Nauchna konferentsia, s mezhdunarodno uchastie v katedra „Informatsionna sigurnost" gr. Shumen may 2016 g. ISBN 978-954-9681-73-4.
40. Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Pyce, 2017, c.19-27, http://jei.uni-ruse.bg/Issue-2016/02.%20Zagorcheva%20-%20Pavlov.pdf.
41. Zagorcheva, D., Stages in the systems for financial management and control in the Bulgaria's public sector, The XIV International Scientific Conference Information Technologies and Management, 2016, Riga, Latvia.
42. Zagorcheva, D, Velcheva, Y., Byudzhetnata detsentralizatsia kato faktor za ednovremenno razvitie na obshtinite i industrialnia biznes, Narodnostopanski arhiv, godina LXX, kniga 3 – 2017, ISSN 0323-9004, str. 46-59, https://www.uni-svishtov.bg/NSArhiv/title.asp?title=981.