American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY

Publisher: Oscar Publishing Services

Journal Website: https://theusajournals.com/index.php/ajast

Research Article

ANALYSIS OF WEAKNESSES IN NETWORK PROTOCOLS AND SYSTEMS

Submission Date: October 12, 2024, Accepted Date: October 17, 2024,
Published Date: October 22, 2024
Crossref doi: https://doi.org/10.37547/ajast/Volume04Issue10-09

Sarvar Norboboyevich Tashev
Shakhrisabz Branch of Tashkent Institute of Chemical Technology
Address: 20 Shakhrisabz st.,181310, Shakhrisabz city, Republic of Uzbekistan

ABSTRACT

This article details the importance of assessing the vulnerabilities of network protocols and systems and the steps required to implement them. The article emphasizes that the main goal of vulnerability research is the timely identification of information security problems and their elimination. At the same time, the dependence of the main indicators of network efficiency on the protocols used in it is also scientifically substantiated. Information security issues were analyzed by integrating metrics obtained from assessing the impact of attacks in various areas of network packets into network monitoring systems. The article also provides an in-depth analysis of the advantages and disadvantages of network protocols, and also examines each of them from the point of view of information security.

KEYWORDS

Network protocols, vulnerability signatures, traffic filtering, systems pose, serious security threat, unauthorized access.

INTRODUCTION

Network protocols are the basis for data transmission in computer networks. They define the rules and data formats used for communication between computers. There are different network protocols, each of which is designed for a specific type of data transfer. For example, TCP/IP is one of the most common protocols used on the Internet.

However, although network protocols provide efficient communication between devices, they can be vulnerable to attacks.

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

Hackers can use various methods such as buffer overflow to infiltrate the system and gain unauthorized access to sensitive information.

To protect against such attacks, comprehensive security measures must be implemented. This includes using strong passwords, regularly updating software and operating systems, and using anti-virus software. It's also important to stay up-to-date on cybersecurity updates and stay up-to-date.

1.1 Vulnerabilities in network protocols and systems

Vulnerabilities in network protocols and systems pose a serious security threat. They can be used by attackers to gain unauthorized access to data, compromise systems, or perform other attacks.

Vulnerability research is an important task that allows you to identify and fix security problems in a timely manner. There are many ways to test for vulnerabilities, which can be divided into two main categories: static and dynamic.

Static methods Vulnerability research is based on the analysis of the program's source code and protocols. They allow you to detect potential security issues without having to execute programs or protocols in real-time.

The main static methods of vulnerability research are:

Source code analysis is a technique that involves manually or automatically analyzing the source code of programs and protocols for potential security problems.

Analysis of vulnerability signatures is a method based on the use of vulnerability signature databases. A vulnerability signature database contains information about known security issues that can be found in software code.

Analysis Static Analyzer is a tool that automatically analyzes the source code of programs and protocols for potential security issues [1].

Dynamic methods of vulnerability research are based on the real-time execution of programs and protocols. They allow you to identify security problems that may arise as a result of the interaction of various application components and protocols.

The main dynamic methods of vulnerability research are:

Penetration testing (Penetration testing) is a method that involves simulating the actions of an intruder to identify vulnerabilities in a system. Permissible attempts are made to bypass existing security measures from the position of a potential attacker, possible scenarios for entering the corporate network and achieving test goals are identified (for example, obtaining access rights, stealing confidential information, information making changes to the systems, breaking the system, the operation of individual network components and security systems or business processes). The main stages of the work are shown in Figure 1.1.

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Publisher: Oscar Publishing Services

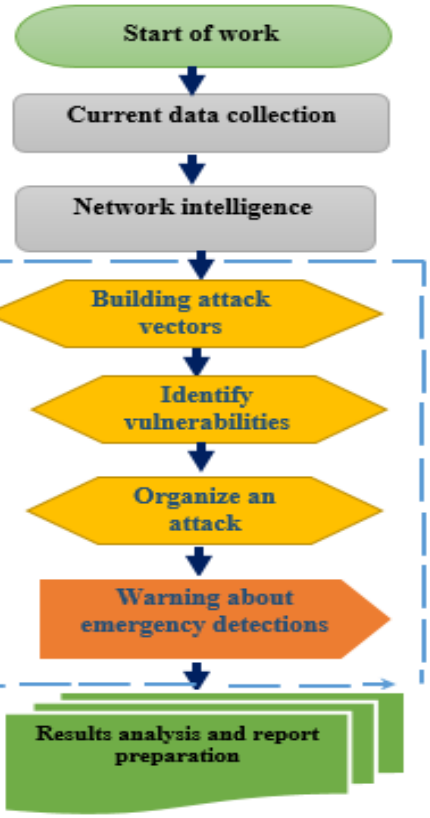

Figure 1.1. The main stages of work

A test direction based on sociotechnical methods is shown in Figure 1.2.

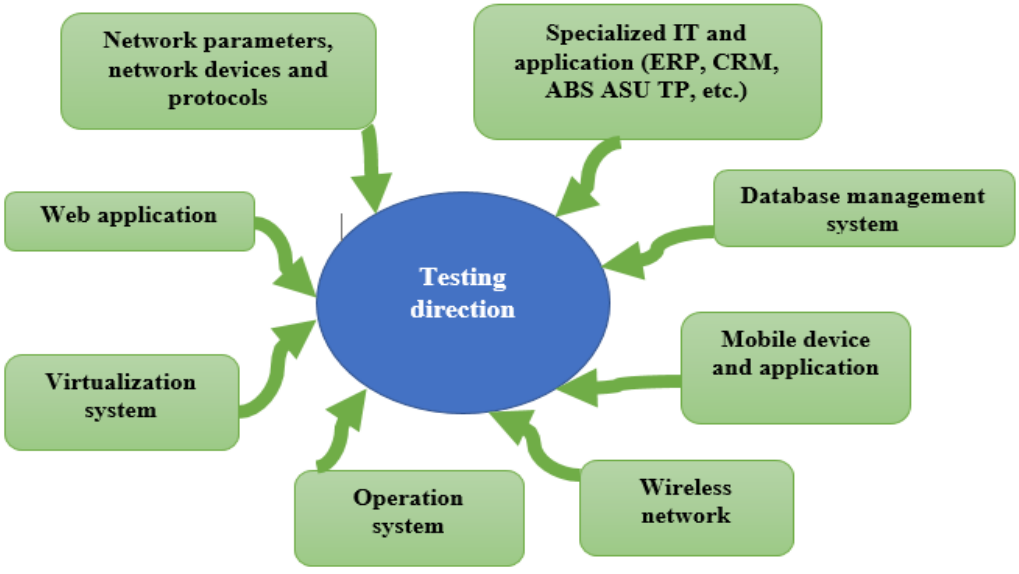

Figure 1.2. Test direction based on social technical methods

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

Attempts are made to allow unauthorized access to the target organization's corporate network and protected assets using social engineering techniques and the use of "human factors". The methods, as a rule, are aimed at users of the end systems, and allow to determine the reaction of employees in various normal and emergency situations, the level of awareness and knowledge of employees about security requirements [3].

Description of some examples of socio-technical methods:

Phishing. Creating a fake web page for a legitimate service (such as a remote mail access page) and encouraging users to enter sensitive information (such as passwords) into it.

Trojan horse. Sending emails to users with malicious attachments and encouraging them to open them through targeted cover letters, file names, callbacks, and other approaches

Pretexting. Modeling a specific scenario, which involves gaining the user's trust, in order to encourage the user to take a certain action (by gathering information in advance about the organization and individual employees and their areas of responsibility). For example, calling users under the guise of potential trusted individuals (external or internal) to obtain confidential information.

Don't go. Leaving infected media with logos/tags/filenames that encourage you to run them in public areas of the organization (elevator, kitchen, parking lot).

"Quid pro quo." Calls support service users with messages about problems with their PCs and helps them solve them.

'Reverse' Social Engineering'. Sending emails to users from trusted addresses with "support" contacts, causing problems with computers and waiting for calls / emails to solve problems, where necessary information can be obtained.

Fuzzing is a technique that involves passing random or specially selected data to program input to detect security problems. In network protocols, ambiguity is an effective way to identify vulnerabilities due to errors in the code, interactions between different protocol components, or mishandling with incorrect data. Fuzzing can be used to test software, network protocols, systems, and devices.

Log analysis is a technique that involves analyzing system event logs to identify security issues.

Selection of methods of vulnerability study. The choice of vulnerability scanning methods depends on various factors, such as the complexity of the system, the type of vulnerabilities to be detected, and the available resources.

In general, static vulnerability scanning techniques are more effective at identifying security problems that involve bugs in code. Dynamic vulnerability scanning methods are more effective in identifying security issues related to the interaction of different system components.

II. Analysis of traffic filtering and application efficiency approaches

The black and white list system is one of the most promising and widespread methods of automatically identifying the type of content in incoming traffic. Blacklists and whitelists are a set of rules for classifying data as "trusted" or "untrusted" within data packets, by which incoming content is filtered. Due to the development of inappropriate content, blacklists and

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

whitelists must be updated, modified and/or deleted on an ongoing basis. A content filter is defined as a program that blocks access to websites with prohibited content. Content filtering allows you to comply with the requirements of applicable laws and easily protect users from unwanted information such as extremist sites and resources [2].

Traditionally, content filters can be divided into two types: products installed on the protected devices themselves (host devices) and products that filter network gateways and traffic passing through them.

The first type of product is mainly used in home and personal devices. The second type of product is used in Internet gateways with content filtering functions. They help reduce the risks associated with Internet browsing by filtering out dangerous or unwanted content, malicious files, social media and other web threats, as well as monitor users' web pages and optimize the use of communication channels.

III. Formation of lists

The standard that describes the technical aspects of blocking and filtering Internet services is called RFC7754. This paper examines several technical approaches to Internet blocking and filtering as they relate to the overall Internet architecture.

Filtering is done in two ways:

– work according to the "black" list: ALLOW everything else;

– work according to the "white" list: PROHIBIT everything else.

Whitelists block all but permitted content. Blacklists allow access to all content except what is expressly prohibited. Custom blacklists deny access and whitelists allow access to websites. Maintaining a blacklist requires constant updating. You must manually update records and remove records when removing unwanted content. When using a whitelist, you must monitor the availability of allowed resources and add new ones. Often, whitelist updates do not keep up with the needs of network users for new resources. Using whitelists and blacklists, you can specify which resources are queried and which resources affect the performance and status of application tests. Whitelists and blacklists are only available for web and script tests. The blacklist always overrides the whitelist when determining allowed or blocked positions. Table 1.1 describes the filtering and blocking mode for all scenarios, including whitelists and blacklists.

Table

Filtering and blocking mode for whitelists and blacklists

6	White list	Mode	Code
Empty	Empty	Allow access	Filtering rules are not specified
Empty	The URL does not match an entry in the list	Block access	The URL is not whitelisted
Empty	The URL matches the list entry	Allow access	The URL is whitelisted. There are no entries in the blacklist

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

			to block access.
The URL does not match an entry in the list	Empty	Allow access	The URL is not blacklisted. There are no whitelist entries to deny access to non-whitelisted URLs.
The URL matches the list entry	Empty	Block access	The URL is blacklisted
The URL does not match an entry in the list	The URL does not match an entry in the list	Block access	The URL is not whitelisted
The URL does not match an entry in the list	The URL matches the list entry	Allow access	The URL is whitelisted. The URL is not blacklisted
The URL matches the list entry	The URL does not match an entry in the list	Block access	The URL is not whitelisted. The URL is blacklisted
The URL matches the list entry	The URL matches the list entry	Block access	The URL is blacklisted. A blacklist entry overrides a whitelist entry.

METHODS

A traffic filtering system is usually a set of rules - a set of entries (URL addresses, IP addresses, TCP ports, etc. When the next packet arrives from the external network, the filtering system intercepts this packet, checks its metadata and content for a match with one of the entries in the rule set, and if a match is found, forwards the packet to the local network or drops, the local network does not even know about the existence of such a packet. At the same time, so that the user understands that the traffic is blocked, the filtering system sends to the local network, for example, a web page with information about the reason for the block (if the requested website if blocked) can transmit [5].

Threats are prevented with content filters

Phishing attacks are becoming more sophisticated and social engineering techniques are being used. Phishing sites usually have a short lifespan (5 days on average).

Modern browsers use several types of phishing protection:

 blacklists: when each new connection is opened, the address of the resource being opened is passed to servers with blacklists, where it is checked to see if the address being opened is on the blacklist. If the address is blacklisted, the browser will display an appropriate error message.

 white lists: the addresses opened from the white lists are considered reliable, the remaining addresses are checked using the black list.

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

Both blacklists and whitelists contain a large number of entries, which primarily causes additional problems with the performance of user computers. In fact, you cannot download the entire blacklist to the user's computer. First, it contains a lot of records and downloading it will load the user's Internet channel a lot. Second, lists are updated regularly - it's very difficult to keep lists updated on remote computers.

Third, even if the user's computer has an up-to-date blacklist, searching for an address in it takes an unacceptably long time.

In addition to phishing, the concept of MITM is also widespread. The term refers to a type of cyberattack in which attackers intercept a conversation or data transmission by eavesdropping or pretending to be a legitimate participant. The goal of a MITM attack is to obtain sensitive information such as bank account details, bank card numbers or login details that can be used to commit further crimes such as identity theft or money laundering. A successful MITM attack involves two distinct steps: capture and decryption [6].

Modern browsers solve the problems of completeness, relevance and responsiveness using two approaches:

1. Whitelists, which are very small in size, are stored on the user's computer as chunks of website address hashes, which saves hard disk space and allows for quick searches for matching addresses. Whitelists are also easy to update due to their relatively small size.

2. Large blacklists are stored on specialized cloud servers, which are designed for fast, uniform processing of large amounts of data. Such systems are called reputable.

Filter traffic by IP addresses

IP addresses of the fourth and sixth versions have a hierarchical structure, that is, a node's address is written in blocks of numbers that each specific network administrator can use to group nodes according to logical or physical criteria.

To filter traffic by IP address, the filtering system first receives the packet and reads the information from the IP packet header. This header always contains the Source address and the destination address in an unencrypted form, which always point to the original source of the packet (unless a VPN or other tunnel is used - in this case it is impossible to filter traffic using standard means and the only way to limit. in this case access to hosts is to restrict access to the VPN servers themselves) [7].

A VPN connection is called a "tunnel" between the user's computer and the server's computer. Each node encrypts the data before entering the "tunnel". When you connect to a VPN, the system detects the network and initiates authentication.

Next, the server gives permission, that is, gives the right to perform certain actions: read mail, surf the Internet, etc. Once the connection is established, all traffic is encrypted between the computer and the server. The computer has an IP address provided by the Internet service provider. This IP blocks access to some sites. The VPN server changes the IP to itself. Already, all data from the VPN server is transmitted to external resources requested by the user, VPN opens access to blocked resources, and as a result, many are willing to put up with low Internet speed and possible application logs. Although VPN uses very strong encryption algorithms, running a VPN client on a PC does not guarantee 100% security of confidential data, so you should choose a VPN provider carefully.

Filter traffic by TCP ports

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

The principle of filtering by TCP ports is similar to filtering by IP addresses, the difference is that TCP ports are used to identify traffic carried in the transport layer of the network model - application identifiers. Accordingly, for this, the traffic filtering system must also read the Destination port from the header.

A TCP packet enclosed in an IP packet. TCP packets are also transmitted over the network in an unencrypted form, which ensures the reliability of this filtering method.

Filter traffic by URL

To implement this component, the device on which the traffic filter is located must access a DNS server - a server for converting domain names to IP addresses - or be installed directly on a DNS server. This is because packets on the Internet are identified only by IP addresses, and URLs have precise translations to such addresses and are created solely for the convenience of the user.

Accordingly, when receiving a packet, the network filter must determine the domain name from the source IP address of the packet. After receiving a domain name, the system can proceed by comparing the received domain against a list of rules.

However, in general, the working principle of URL filtering is more complicated than its predecessors. This is because IP addresses do not always correspond to actual domain names and vice versa. When a request is sent to a website, there are virtual servers that redirect the user to another server with a different domain name [8]. This is usually done for load balancing, but it complicates the work of the transport filter

USING MACHINE LEARNING TO CLASSIFY TRAFFIC

The changing trends of network traffic, the widespread use of encryption, the increase in the speed of data transfer and, accordingly, the required speed of their processing, the constant appearance of new classes of traffic - all this required the emergence of new methods of classification . For this purpose, the creation of a set of distinguishing characteristics of classes, based on the analysis of many examples of these classes, machine learning methods were proposed, which can significantly simplify work with the automation of this process. In addition, most of the proposed methods work with general properties of streams rather than packet payloads, which solves the problems of encryption and protection of user data. It also gives an advantage in classification speed and reduces the amount of memory required for decision making. Next, machine learning techniques for network traffic classification are discussed in detail: the types of classification, the models and features used, and the datasets on which the models are trained and tested [1].

TYPES OF NETWORK TRAFFIC CLASSIFICATION

Network traffic can be segmented into individual packets, and port-based and DPI-based classification techniques can do the job, but most work is currently done based on flow-based classification. There are approaches where sender requests and receiver responses are interpreted as two different counter-flows, but a common solution is to combine these flows into a single bi-directional flow. Since an Internet stream usually contains a single complete session of interaction between a sender and a receiver (client and server), problems with classifying the entire stream as a whole into a single class usually arise. does not come. Since streams differ in their duration and the amount of data transferred, the smallest and largest streams are sometimes distinguished. Because of the

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Publisher: Oscar Publishing Services

significant difference in the size of these streams, the classification results are sometimes examined separately for the percentage of correctly classified streams and the percentage of bytes classified. The length of the stream is also of great importance. Streams or stream fragments consisting of a small number of packets may not contain enough information to determine the class and therefore require special treatment or are ignored. Traffic classification can be done online, i.e. in real time, or offline after the fact. The order of classification is determined by the problem being solved. For example, collecting network usage statistics for global redistribution of resources, receiving information about user activity for billing for Internet services and recalculating these prices - all this does not require an urgent response and is free of charge in any amount mode can be processed. available information and resources. Other tasks, such as ensuring the quality of service to the user, detecting attacks and threats, and immediately reallocating resources, require the fastest response. In such cases, the classifier does not have the opportunity to wait for the end of the flow and work with the complete information about it, but is forced to limit itself to only a part of the data, for example, only the first N packets. flow the current classifier model is also limited in that it must use system resources sparingly and make flow decisions as quickly as possible [9]. Also, in these cases, the decision is usually made in parallel for multiple/multiple data streams at the same time, so there are also limits on the amount of RAM allocated for stream processing. The choice of a set of classes for traffic classification depends on the problem being solved. Figure 1.3 shows the types of network traffic classification.

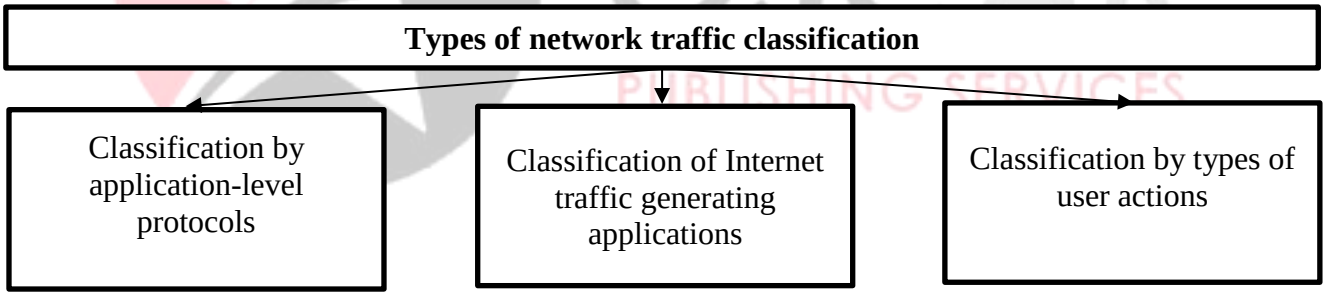

Figure 1.3. Types of network traffic classification

Classification by application-level protocols is preferred by application-level protocols because such classification is the most practically valuable.

Categorizing Internet traffic by applications determines user activity and allows profiling, limiting the activity of certain applications, and solving marketing problems.

Classification according to the type of user action is determined by the type of user activity, not by the specific application used. In a sense, this is a generalization of the previous type of classification.

CONCLUSION

It should be noted in this paper that weaknesses in network protocols and systems. Filtering and blocking

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 55-64
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

mode for whitelists and blacklists, using machine learning to classify traffic and types of network traffic classification, types of network traffic classification are considered as well.

REFERENCES

1. Gulomov Sh.R. Tarmoqdagi zararli trafik turlari va ularni aniqlash. Multidisciplinary Scientific Journal. December, Issue 24 | 2023, -B.424-432 https://doi.org/10.5281/zenodo.10445437
2. SN Tashev, AG Ganiev The Role of "Imagination" in the Process of "Creative Thinking" Developing Students'"Imagination" and "Creative Thinking" Skills in Teaching Physics. Annals of the Romanian Society for Cell Biology, 2021/3/6, 633-642 DOI:10.17762/pae.v58i1.1309
3. SN Tashev THE ROLE OF "IMAGINATION" IN THE PROCESS OF "CREATIVE THINKING", DEVELOPING STUDENTS' "IMAGINATION" AND "CREATIVE THINKING" SKILLS IN TEACHING PHYSICS PSYCHOLOGY AND EDUCATION, 3569-3575 DOI:10.17762/pae.v58i1.1309 License CC BY 4.0
4. Y.B. Karamatovich, T.S. Norboboevich, N.I. Ibrohimovich. Verification of the pocket filtering based on method of verification on the model. 2019 International Conference on Information Science and Communications Technologies (ICISCT) DOI:10.1109/ICISCT47635.2019.9011901
5. J. Ning et al., "Pine: Enabling privacy-preserving deep packet inspection on TLS with rule-hiding and fast connection establishment," in Proc. Eur. Symp. Res. Comput. Secur., 2020, pp. 3–22 DOI:10.1007/978-3-030-58951-6_1
6. J. Kim, S. Camtepe, J. Baek, W. Susilo, J. Pieprzyk, and S. Nepal, "P2DPI: Practical and privacy-preserving deep packet inspection," in Proc. ACM Asia Conf. Comput. Commun. Secur., 2021, pp. 135–146. https://doi.org/10.1145/3433210.3437525
7. Kim, S.; Yoon, S.; Narantuya, J.; Lim, H. Secure collecting, optimizing, and deploying of firewall rules in software-defined networks. IEEE Access 2020, 8, 15166–15177. DOI:10.1109/ACCESS.2020.2967503
8. Hakani, D. A Survey on Firewall for cloud security with Anomaly detection in Firewall Policy. In Proceedings of the International Conference on Artificial Intelligence and Smart Communication, Greater Noida, India, 27–29 January 2023; pp. 825–830. DOI:10.1109/AISC56616.2023.10085419
9. Rajaboevich, G.; Dilbar, K.; Azatovna, A.; Ismoilovna, Q. Comparative Analysis of Methods Content Filtering Network Traffic. Int. J. Emerg. Trends Eng. Res. 2020, 8, 1561–1569 DOI:10.30534/ijeter/2020/15852020
10. Islam, M.; Uddin, M.; Hossain, D.; Dulal, M.; Ahmed, D.; Shakil, M.; Moazzam, D.; Golam, M. Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall. Int. J. Comput. Digit. Syst. 2023, 13, 193–202 DOI:10.3390/molecules26082297