ANALYSIS OF SOFTWARE SETS USED IN DETECTION OF ILLEGAL ACTIVITIES

Mahkamov Anvarjon Abdujabborovich
Uzbekistan International Academy of Islamic Studies
"Modern information and communication
Technologies" department, associate professor, PhD
mahkamovanvar2020@gmail.com

Abstract*. This article presents an analysis of software packages used to detect illegal actions in ensuring information security.*

At present, one of the most pressing problems today is to analyze each software package used to detect illegal actions, and then determine which one works best. Therefore, the statistics of the analysis of software packages used to detect illegal actions are presented below.

Keywords*: forensics, cybersecurity, law enforcement, cybercrime, fraud, hacking, illegal online behavior*

Introduction. Nowadays, many businesses use personal computers, networks, and servers to store their organization's critical data and manage their core operations. This emphasizes the importance of a good and reliable security system.

With the advent of advanced technologies, cybercriminals are also finding many ways to enter the systems of many organizations and are trying to solve the problem in an easy and convenient way. Therefore, it is necessary to use the best software package by analyzing the software packages used to detect illegal activities.

The analysis of software packages used to detect illegal activity is typically within the realm of digital forensics, cybersecurity, and law enforcement. These software packages are designed to detect and investigate various forms of illegal activity, such as cybercrime, fraud, hacking, and illegal online behavior. There are

several common types of software packages used for this purpose. We will list some of them below.

Firewalls. Firewalls work by inspecting and filtering network traffic based on predefined rules and policies.

An overview of how firewalls work:

Traffic inspection: A firewall examines network packets as they pass through a firewall device or software. They examine various attributes of the packets, such as source and destination IP addresses, ports, and protocols.

Rule-based filtering: Firewalls compare the attributes of each packet to a set of predefined rules or policies. These rules determine whether a packet should be allowed or blocked based on certain criteria. For example, a rule might allow incoming web traffic on port 80 (HTTP) but block traffic on port 22 (SSH).

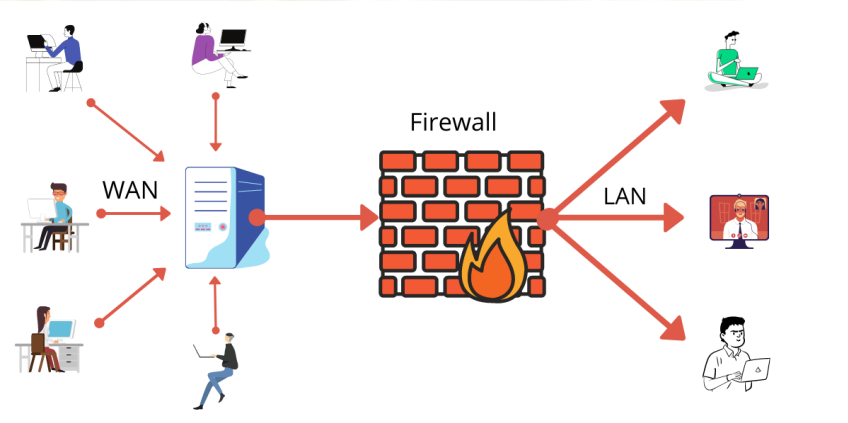

Figure 1. Firewall

Packet filtering: In packet filtering, firewalls examine individual packets individually, without considering the context of the overall network connection. They evaluate each packet independently based on rules and policies to determine whether to allow or deny.

Stateful inspection: Some firewalls perform stateful inspection that goes beyond simple packet filtering. These firewalls maintain information about the state of network connections. They analyze the context of the packet within an ongoing session, taking into account factors such as the session source, destination, and

connection state. This approach allows firewalls to make more intelligent decisions about which packets to allow or block.

Access Control: Firewalls enforce access control policies that determine which types of network traffic are allowed or blocked. Administrators configure these policies based on an organization's security requirements. Policies can be based on source and destination IP addresses, port numbers, protocols, and other criteria.

Network Address Translation (NAT): Many firewalls include Network Address Translation. NAT allows multiple devices on an internal network to share a single external IP address. It provides an additional layer of security by masking internal IP addresses from external networks.

Additional security features: Some advanced firewalls offer additional security features such as intrusion detection and prevention, VPN support, deep packet inspection (DPI), application-level filtering, content filtering, and virus scanning. These features enhance the capabilities of the firewall and provide a more comprehensive security solution.

By implementing firewall technologies and effectively configuring rules and policies, organizations can monitor and secure their network traffic, protect sensitive data, prevent unauthorized access, and mitigate various types of cyber threats.

In today's digital age, where cyber threats continue to evolve, it is essential to protect your network from unauthorized access and malicious activity. One of the primary tools for protecting your network is a firewall. This article explores the importance of using a firewall as a proactive measure to strengthen network security. By understanding its functions, deployment options, and best practices, you can take full advantage of a firewall to increase the resilience of your network.

A firewall acts as a strong gatekeeper between your internal network and external entities, such as the Internet. It inspects incoming and outgoing network traffic, allowing or blocking access based on predefined security rules. By implementing a firewall, you establish a security perimeter that filters and manages traffic, protecting your network from unauthorized access attempts.

Firewalls play a vital role in mitigating external threats by blocking unauthorized access attempts and protecting against various cyberattacks. They monitor network traffic, detecting and blocking malicious packets that may contain viruses, malware, or attacks. With a properly configured firewall, you can significantly reduce the risk of network disruptions and potential data loss.

A firewall provides control over network traffic by defining access policies. You can configure rules to allow or deny traffic from specific IP addresses, protocols, ports, or at the application level. This control allows you to restrict access to sensitive resources and limit exposure to potential vulnerabilities. By implementing an effective firewall, you can align network traffic with your organization's security policies and compliance requirements.

Intrusion Detection Systems (IDS). Intrusion Detection Systems (IDS) are network security devices or software that monitor network traffic and systems for signs of unauthorized or malicious activity. IDS aims to detect and alert administrators to potential security incidents or attacks in real time. How IDS typically works:

Traffic monitoring: IDSs monitor network traffic, inspecting packets as they flow across the network. They can be strategically placed at various points in the network, such as at the network perimeter, in front of critical servers, or on specific network segments.

Signature-based detection: An IDS uses signature-based detection techniques to compare network traffic to a database of known attack patterns or signatures. The database contains predefined signatures for specific types of attacks or malicious actions. If the IDS detects a match between network traffic and the known signature, it generates an alert.

Anomaly-based detection: In addition to signature-based detection, an IDS can use anomaly-based detection techniques. Anomaly detection involves establishing a baseline of normal network behavior and detecting deviations from this baseline. The IDS analyzes network traffic, protocols, and other characteristics

to identify unusual or suspicious behavior. It then generates an alert when significant deviations are detected.

Network packet analysis: IDSs examine individual network packets to identify patterns or behaviors that may indicate an attack. They examine packet headers, payload content, and protocol behavior for specific attack indicators or anomalies.

Event Correlation: An IDS can perform event correlation by combining data from multiple sources, such as log files, network devices, and intrusion detection sensors. By correlating events, an IDS can provide a broader view of the security posture of a network and detect complex attacks that span multiple systems or stages.

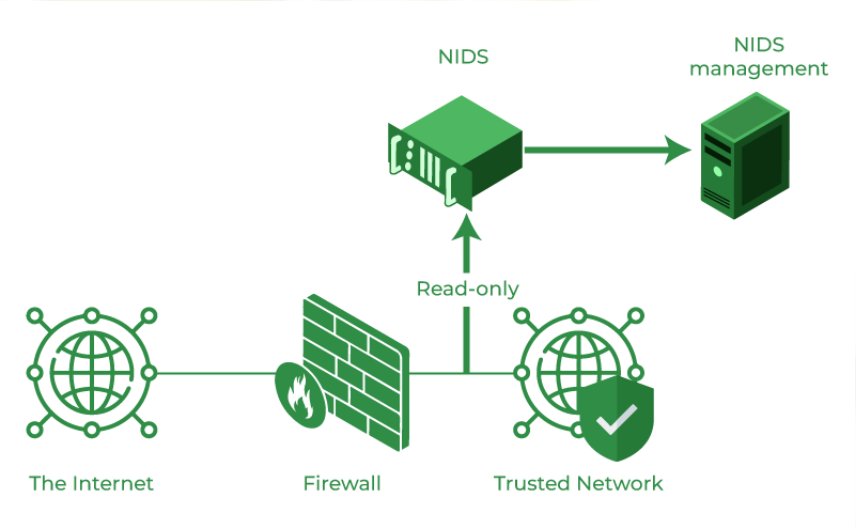

Figure 2. Intrusion detection systems

Generate an alert: When an IDS detects a potential security incident or attack, it generates an alert or notification. The alert can be sent to security administrators, network administrators, or the Security Operations Center (SOC) for further investigation and response.

Response and Mitigation: IDSs primarily focus on detecting and alerting on security incidents rather than actively blocking or preventing them. However, some IDSs may have limited response capabilities, such as triggering automated actions, sending alerts to firewalls or other security devices, or initiating incident response procedures.

Logging and Reporting: An IDS maintains logs of detected events, alerts, and other relevant information. These logs are valuable for forensic analysis, compliance auditing, and ongoing network security monitoring.

Conclusion. Information technology security software offers a number of advantages to the user. It is worth noting that even the most professional users can download some forms of malware or become victims of online fraud and identity theft. Preventing viruses, spyware, and identity theft is a serious matter. Professional hackers are finding sophisticated methods and algorithms to create viruses.

Once these viruses have taken root on a computer, they can dramatically slow down processing speed, delete important data, and damage computer or network systems. Identity theft and spyware can also be prevented by using software to protect sensitive personal information, such as passwords, financial information, credit card numbers, and the social security numbers of your system users. In fact, 80% of cyberattacks are caused by weak, stolen passwords, so they need to be carefully protected.

USED LITERATURE

1. Fazilov, S. X., Mahkamov, A. A., & Jumayev, T. S. (2018). Algorithm for extraction of identification features in ear recognition. Информатика: проблемы, методология, технологии, 3-7.

2. Mahkamov, A. A., Jumayev, T. S., Tuhtanazarov, D. S., & Dadamuxamedov, A. I. (2024). Using AdaBoost to improve the performance of simple classifiers. In Artificial Intelligence, Blockchain, Computing and Security Volume 2 (pp. 755-760). CRC Press.

3. Zhumaev, T.S., Mirzaev, N.S., & Makhkamov, A.S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27),

4. Маҳкамов, А. А., & Инадуллаев, Х.Ў.Ў. (2021). Сравнительный анализ биометрических систем в обеспечении информационной безопасности. Universum: технические науки, (12-1 (93)), 32-37.

5. Махкамов А. А. Алгоритмы идентификации личности человека по изображению ушных раковин //Исследования технических наук. – 2015. – №. 4. – С. 28-32.

6. Tuhtanazarov, D., Xodjayeva, M., Jumayev, T., & Mahkamov, A. (2022, June). Computational algorithm and program for determining the indicators of wells based on processing of information of oil fields. In AIP Conference Proceedings (Vol. 2432, No. 1, p. 060021). AIP Publishing LLC.

7. Zhumaev, T. S., Mirzaev, N. S., & Makhkamov, A. S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27), 4.

8. Жумаев, Т. С., Мирзаев, Н. С., & Махкамов, А. С. (2015). Алгоритмы сегментации цветных изображений, основанные на выделение сильносвязанных элементов. Исследования технических наук, (4), 22-27.

9. Махкамов, А. А., & Дадамухамедов, А. И. (2022). Алгоритм выделения области ушных раковин при распознавании личности. Universum: технические науки, (5-1 (98)), 14-17.

10. Махкамов, А. А. (2015). Алгоритмы идентификации личности человека по изображению ушных раковин. Исследования технических наук, (4), 28-32.

11. Е.А.Степанов, И.К.Корнеев, Информационная безопасность и защита информации. – М.: Инфра, 2002.