Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2025. Vol. 4. No. 3; e-ISSN: 2808-4519

Implementation and Security Testing of Mikrotik Router Againts Cyber Attacks Using Firewall and Penetration Testing

Muhammad Afrian Rozan[1]*, Muhlis Tahir[2]

[1,2]*Universitas Trunojoyo Madura*
muhammadafrianrozan@gmail.com[1*], muhlis.tahir@trunojoyo.ac.id[2]

Abstract

Network security is a crucial aspect that must be considered, because without adequate security, the network becomes vulnerable to cyber attacks that can cause losses. Routers are one of the most vulnerable and easily attacked targets because of their very important role in computer network systems. One of the most common types of routers used in developing countries is Mikrotik. Mikrotik routers have several security holes, such as CVE-2018-14847 (Winbox Exploitation), Brute-Force Attacks, and Denial of Service (DoS), which can be exploited by attackers to cause disruption or loss. Therefore, efforts to prevent cyber attacks are very important. Preventive steps that can be taken are by implementing a strong security system on Mikrotik routers through firewall configuration and conducting penetration testing to ensure that the configuration applied is optimal. This study uses the SDLC (Security Development Life Cycle) model, using the waterfall model stages.

Keywords: *Network Security, Winbox Exploitation, Brute Force, Dos, Firewall, Penetration Testing*

1. Introduction

For an agency that uses a computer network system, network security is a crucial aspect that must be considered in maintaining data integrity, as well as ensuring the availability of system services for users [1]. Without adequate security, networks become vulnerable to various types of cyber attacks that can cause losses. Devices that are vulnerable to attacks on computer network systems are routers [2]. Routers are easy targets for attack because of their very important role in connecting local networks (LANs) to the internet.

In developing countries, the router devices commonly used are affordable routers, cost-effective routers that can function both as routers for home use and as the main router in an infrastructure network [3]. One type of router that has an affordable cost is Mikrotik. In 2018, a study was conducted by Schalton [3] which examines the characteristics of attacks on low-cost Mikrotik routers by utilizing honeypots and obtained data on attack patterns such as Mikrotik Common Vulnerabilities and Exposures (CVE), Denial of Service (DoS), and Brute-Force Attacks. In 2018, a security hole was discovered on Mikrotik devices named CVE 2018-14847 one of the most famous vulnerabilities ever found on Mikrotik. Winbox exploitation attacks exploit the CVE-2018-14847 security hole on Mikrotik routers [2]. Winbox exploit attacks allow attackers to gain unauthorized access to the router without requiring authentication, which can be used to change configuration and security settings. This attack allows access to files and directories and obtains Administrator account credentials [4].

The cvedetails.com site, a platform that records CVE (Common Vulnerability and Exposures) vulnerability data, provides data that the type of Mikrotik router attack that occurs most often from 2015 to 2024 is the Denial of Service (DoS) attack. This is because DoS attacks are very common attacks, therefore many researchers conduct simulations using this type of DoS attack, then carry out prevention or mitigation against DoS attacks on site hardware or servers [5]. Serangan DoS merupakan jenis serangan yang umum menargetkan perangkat seperti server, web dan termasuk juga router Mikrotik. This attack involves multiple devices simultaneously flooding a target with excessive traffic, rendering the system unable to accommodate it [6]. DoS (Denial of Service) attacks aim to make the router network down or not functioning. As a result of this attack, the router is unable to process services from parties that have valid authorization. This can disrupt operational activities and harm the organization, both materially such as loss of income, and non-materially such as damage to reputation or disruption to important business processes [7].

According to Bahri, many of our people are still not educated enough in creating strong usernames and passwords, making them very vulnerable to hacking [8]. Brute force attack is a persistent and detrimental threat that is often used by illegal parties to gain access to network devices, especially Mikrotik routers, by trying various combinations of usernames and passwords repeatedly [9]. This method relies on continuous trial and error until the right combination is found to enter the system. Brute force attacks result in unauthorized access to the network, theft of sensitive data, and damage to the integrity of the system as a whole. The impact of this attack can be very detrimental,

both in terms of data security and operations. Therefore, implementing proper network security is very important to keep the system safe from threats like this.

It is very important to take preventive measures in dealing with these cyber attacks. Preventive measures that can be taken are by implementing a strong security system on the Mikrotik router through firewall configuration and Mikrotik operating system updates, so that the Mikrotik router is more protected from these various threats. Firewall is a cybersecurity technology that functions to protect computers connected to the network [10]. However, to ensure that the configuration applied is correct, testing is required. Penetration testing is a frequently implemented testing method, this method allows us to identify weaknesses and ensure that the router is well protected from potential attacks. Penetration testing is a series of techniques and steps applied to test the security of an organization's system [11]. This research aims to implement and test the security of Mikrotik routers against cyber attacks Winbox Exploitation, Brute Force, and Denial of Service using firewalls and penetration testing.

2. Research Methods

The model used in this study is the Security Development Life Cycle, with stages that follow the Waterfall method [12]. The Waterfall method is an approach to software development that is systematic and sequential, starting from the system development stage, analysis, design, implementation, testing, to maintenance [13]. The stages in the Waterfall model can be seen in Figure 1 below.

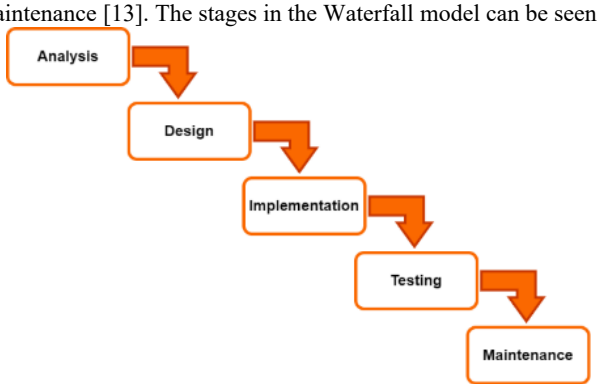

Fig. 1: Stages of Waterfall Research

2.1. Analysis

The analysis phase includes interviews with laboratory managers, computer network observations, vulnerability analysis against Winbox Exploitation, Brute Force, and Denial of Service attacks, and analysis of network security needs and strategies. Based on interviews with laboratory managers, it is known that the network has not used a network security system and only uses the hotspot feature on the Mikrotik router for basic authentication without special protection, making it vulnerable to Winbox exploitation, brute force, and Denial of Service (DoS) attacks. Observations and vulnerability analysis show a history of attacks and high network vulnerability to these three types of cyber attacks. Therefore, a security system is needed that is able to protect the network from these threats.

2.2. Design

Researchers designed a security configuration to protect Mikrotik routers from Winbox Exploitation, Brute Force, and Denial of Service attacks. For protection against Winbox Exploitation, RouterOS was updated to a stable version above 6.3, and access to user.dat was closed to prevent exploitation. In overcoming Brute Force attacks, a rate limiting firewall was applied to limit login attempts by temporarily blocking IPs if they exceed the limit. Meanwhile, protection against Denial Of Service attacks was carried out using a raw firewal.

3. Implementation

In the Implementation stage, the security design that has been designed is applied directly to the Mikrotik router. This stage includes the implementation of each security configuration to overcome Winbox exploitation, Brute force, and Denial of Service (DoS) attacks. Here are the implementation details:

a. Implementation of protection against Winbox exploitation

1) Upgrade Router OS to the latest version
   MikroTik has released an update that includes a security patch on versions above 6.42 to address the CVE-2018-14847 security vulnerability from the Winbox Exploitation attack.

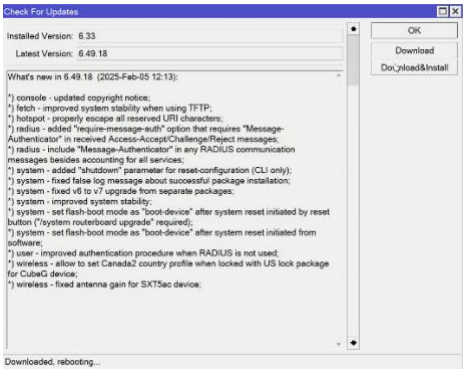

Fig. 2: Upgrade Router OS

RouterOS is updated to version 6.49.18 to address the security holes exploited in Winbox Exploitation attacks, so the risk of attacks can be minimized.

2) Closing access to the user.dat file with firewall configuration

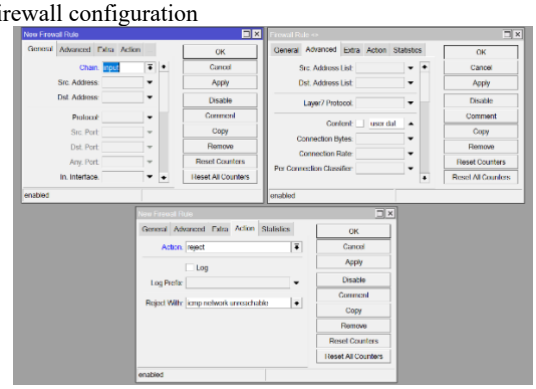

Fig. 3: Configure Firewall to block access to user.dat file

The firewall will set all incoming packets to the Mikrotik router to be rejected, so that attackers cannot access sensitive user.dat files used for authentication. This step is very effective in protecting important information from attacks. Thus, access from Winbox Exploitation attackers can be prevented.

b. Implementation of protection against Brute force

Brute Force prevention is done by implementing a rate limiting firewall that limits login attempts, if the limit is exceeded, the system automatically blocks the IP temporarily.

```
/ip firewall filter add chain=input protocol=tcp dst-port=22 src-address-list=black_list action=drop \ comment="drop ssh brute forcers" disabled=no add chain=input protocol=tcp dst-port=22 connection-state=new \ src-address-list=ssh_stage3 action=add-src-to-address-list address-list=black_list address-list-timeout=1d \ comment="" disabled=no add chain=input protocol=tcp dst-port=22 connection-state=new \ src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=1m \ comment="" disabled=no add chain=input protocol=tcp dst-port=22 connection-state=new \ src-address-list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m \ comment="" disabled=no add chain=input protocol=tcp dst-port=22 connection-state=new \ action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m comment="" \ disabled=no
```

Fig. 4: Script firewall rate limiting brute force

The above rate limiting firewall script is used to prevent brute force attacks on SSH (port 22) on MikroTik with a gradual monitoring mechanism. If an IP has been blacklisted, all connections to port 22 from that IP will be immediately blocked. To detect suspicious login attempts, the firewall implements a tiered system. In the initial stage, the IP that tries a new connection will be included in the ssh_stage1 list for 1 minute. If the IP tries again within the same time, it will be moved to the ssh_stage2 list, and if attempts continue, it will enter ssh_stage3. If the IP continues to try to login, it will be blacklisted for 10 days, so that its access to the SSH server is completely cut off. With this method, the firewall can automatically identify and block brute force attempts before they pose further threats.

c. Implementation of protection against Denial of Service (DoS)

This RAW firewall configuration is used to detect and block SYN flood-based DoS (Denial of Service) attacks on MikroTik. The following is the raw firewall configuration used:

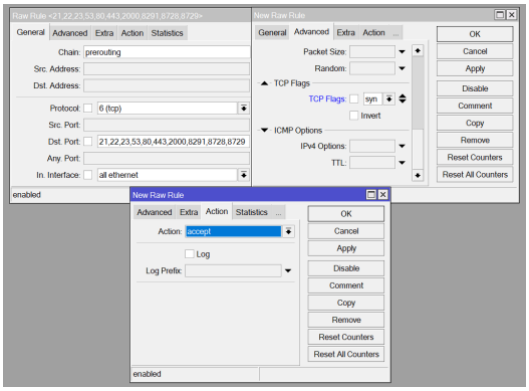

Fig. 5: Raw DoS Firewall Configuration

The first configuration allows a maximum of 6000 SYN packets per second. If the number of packets exceeds 6000 per second, this rule no longer accepts packets and the next rule will handle the excess traffic.

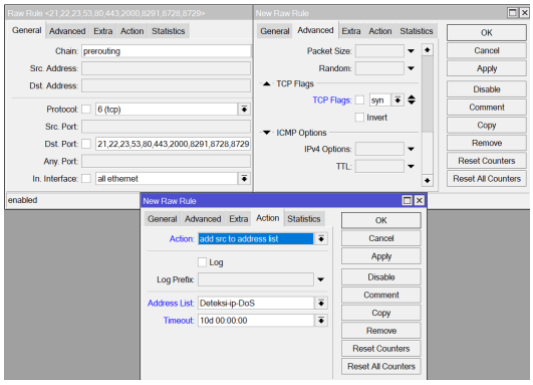

Fig. 6: Advanced Raw DoS Firewall Configuration

In the second configuration, if an IP sends too many SYN packets (more than 6000/s), that IP is added to the "detect ip dos" address list for 10 days.

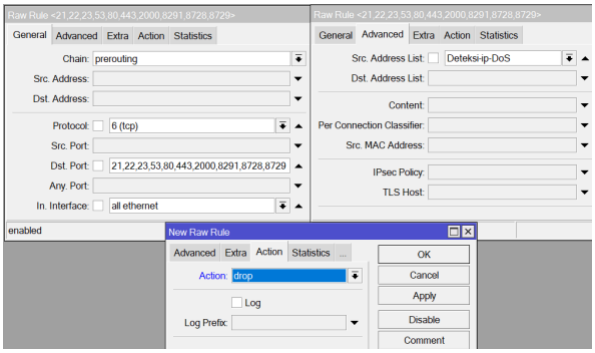

Fig. 7: Advanced Raw DoS Firewall Configuration

The third configuration, if the IP is already included in the "DoS-ip-detection" list, then the packet from that IP will be immediately blocked, the packet will not be processed further, thus reducing the CPU load.

3. Results and Discussion

3.1. Testing

In the testing phase, Penetration testing is carried out using the white box method to test whether the implemented configuration is able to ward off Winbox exploitation, Brute force, and Denial of Service (DoS) attacks. The following are the stages in the white box Penetration testing that are carried out:

a. Reconnaissance
   At this stage, collect data related to the network that will be tested, such as IP address addressing and firewall configuration on the network system. In this test using Mikrotik Router RB951Ui-2HnD with OS version 6.49.18.
   The IP address address used in this test is as in table 1 below.

Table 1: Reconnaissance

Interface	Address	Gateway	Network	Information
Ether 1	192.168.235.247/24	192.168.235.1	192.168.235.0	Automatic IP address from the internet
Ether 2	192.168.6.1/24	192.168.6.1	192.168.6.0	Function for LAN connection
Ether 3	192.168.1.1/22	192.168.1.1	192.168.0.0	Function for Hotspot connection

The firewall configuration used in this test is as shown in Figure 8 and Figure 9 below

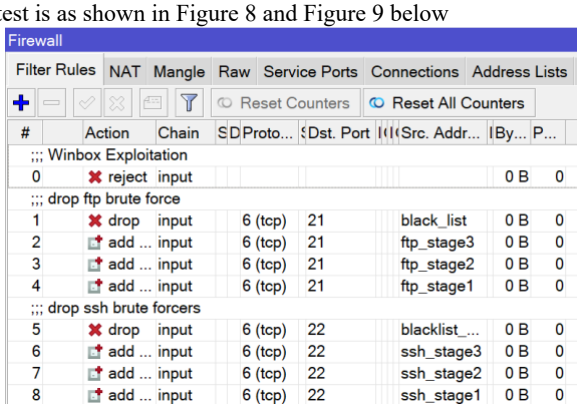

Fig. 8: Firewall Filter Configuration

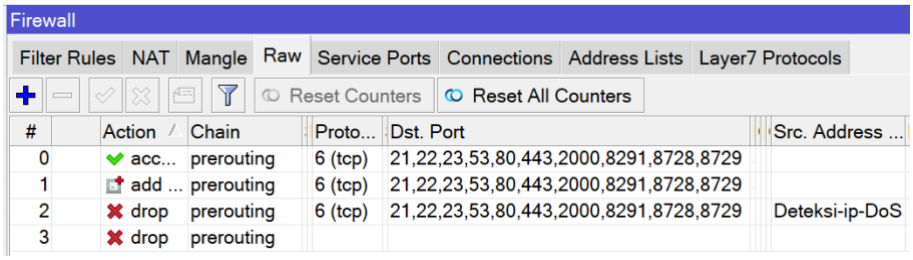

Fig. 9: Firewall RAW Configuration

b. Scanning

This process uses Nmap to scan Mikrotik routers, so that it can evaluate existing vulnerabilities.

Fig. 10: Scanning

From the scan results on the Mikrotik router, four ports were found to have open status, namely 21/tcp (FTP), 22/tcp (SSH), 2000/tcp (Bandwidth Test), and 8291/tcp (Winbox).

c. Exploitation

1) Winbox Exploitation

Fig. 11: Winbox exploitation attack

In the image above, a Winbox Exploitation attack is seen using a Python3 exploit script to the MikroTik gateway IP address. The attack failed, marked by the appearance of the message "Connection error: timeout", so that hackers cannot obtain the MikroTik username and password.

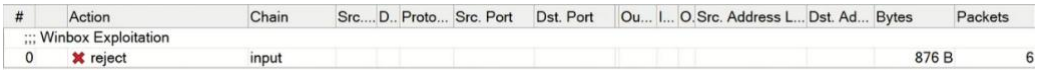

Fig. 12: Firewall winbox exploitation

In Figure 12, it can be seen that the firewall that was created to overcome the Winbox Exploitation attack by rejecting user.dat successfully ran and thwarted the attack. This success can be observed from the movement of bytes and packets.

2) Brute Force

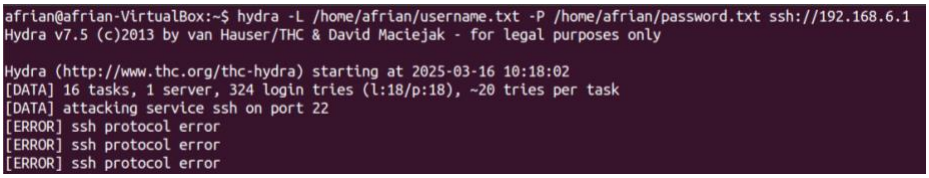

Fig. 13: Brute force attack

In Figure 13, a Brute Force attack using the Hydra tool is seen towards the MikroTik gateway IP address via the SSH service. The attack failed, marked by the appearance of the message "Error: SSH protocol error", so that the hacker could not obtain the MikroTik username and password via the Brute Force technique.

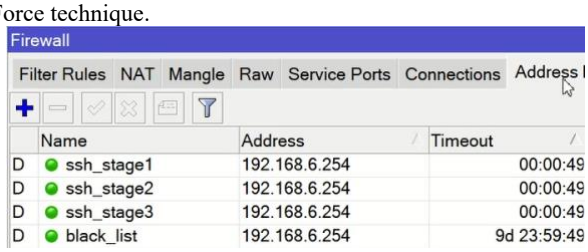

Fig. 14: Address list brute force attack

Figure 14 shows the success of the rate limiting firewall in overcoming Brute Force attacks through the SSH service. This firewall works according to the rules that have been created, namely by entering the attacker's IP address into a list such as ssh_stage1, ssh_stage2, and ssh_stage3, until finally it is blacklisted. As a result, connections to port 22 from the attacker's IP are blocked for 10 days, so that the Brute force attack is successfully thwarted.

3) Denial Of Service

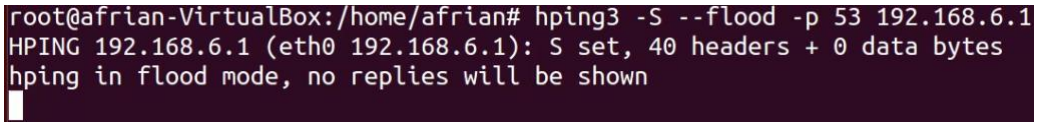

Fig. 15: DoS attack

Figure 15 shows a Denial of Service (DoS) attack of the DNS TCP flood attack type using the hping3 tool on Linux Ubuntu, which targets the Mikrotik router gateway IP address via the DNS port (53).

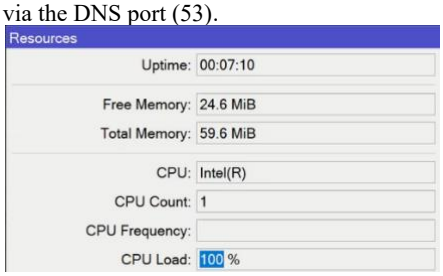

Fig. 16: Mikrotik CPU load before firewall implementation

Figure 16 shows the CPU load resource on the Mikrotik router when hit by a DoS attack before the firewall implementation, where the CPU load reached 100%.

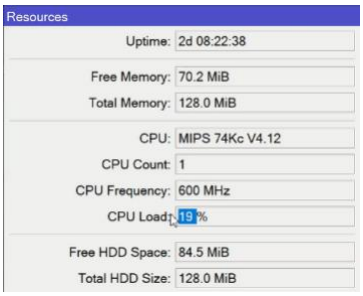

Fig. 17: Mikrotik CPU load after firewall implementation

Figure 17 shows the CPU load resource on the Mikrotik router when hit by a DoS attack after implementing the firewall, where the CPU load dropped to 19%.

Fig. 18: DoS attack address list

Figure 18 shows the attacker's IP address that is included in the "Detect-IP-DoS" address list, where the IP is detected as carrying out a DoS attack. As a result, packets from the IP are immediately blocked and not processed further, thus reducing the CPU load. This shows the success of the firewall configuration that has been implemented previously.

d. Reporting

Based on the attacks that have been carried out on the Mikrotik RB-750 Gr3 router (OS version 6.49.18) against Winbox Exploitation, Brute Force, and DoS cyber attacks, the author obtained the results presented in the following table.

Table. 2 Reporting

No	Attack Type	Attack Status	Description
1	Winbox Exploitation	Unsuccessful	Hackers failed to obtain Mikrotik router username and password after the device was updated to version 6.49.18 (above version 6.42) and a firewall was applied to block access to the user.dat file. Thus, hackers were unable to access data in user.dat, so the username and password remained protected.
2	Brute Force	Unsuccessful	Hackers failed to obtain the Mikrotik router username and password. The implementation of rate limiting firewall has proven effective in preventing Brute Force attacks. The IP address of the attacker that is detected making repeated login attempts is automatically blacklisted, so that hacking attempts using the Brute Force technique fail to obtain the Mikrotik username and password.
3	Denial Of Service	Unsuccessful	RAW firewall implementation can reduce processor resource usage by up to 81% against DoS attacks (DNS tcp flood attack)

3.2. Maintenance

At this stage, ongoing maintenance is essential to ensure the effectiveness and reliability of the developed system in the long term. Researchers work closely with the computer laboratory to maintain both hardware and software components, by conducting routine inspections, updates, and periodic monitoring.

4. Conclusion

Based on the test results using the penetration testing method to evaluate the effectiveness of the firewall that has been implemented on the MikroTik router in dealing with Winbox Exploitation, Brute Force, and Denial of Service cyber attacks, the following conclusions were obtained:

1. Winbox Exploitation attack was successfully thwarted by updating MikroTik router to version 6.49.18 (above version 6.42) and implementing firewall to block access to user.dat file. Thus, hackers cannot access data in user.dat, so username and password are not successfully obtained.
2. Implementation of firewall with rate limiting technique is effective in preventing Brute Force attacks. The attacker's IP address is detected to make repeated login attempts and is automatically blacklisted, so that hacking attempts using brute force techniques fail to obtain the MikroTik username and password.
3. The implementation of the RAW firewall has proven effective in preventing Denial of Service attacks (DNS TCP Flood Attack) by reducing the CPU load on the MikroTik router by 81%.

References

[1] D. H. Gutama, A. K. A. Estetikha, and R. A. Setiawan, "Penanganan Serangan Brute Force dan Port Scanning Pada Router Mikrotik," *J. Sist. Informasi, dan Teknol. Inf.*, vol. 1, no. 2, pp. 1–13, 2022, [Online]. Available: https://journal-siti.org/index.php/siti/PublishedByHPTAI

[2] Haeruddin, "Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS," *J. Media Inform. Budidarma*, vol. 5, no. 3, pp. 848–855, 2021, doi: 10.30865/mib.v5i3.2979.

[3] C. P. B. Scholten, "Hacking the router: characterizing attacks targeting low-cost routers using a honeypot router," (Bachelor's thesis, University of Twente)., 2019.

[4] J. M. Ceron, C. Scholten, A. Pras, and J. Santanna, "MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification," in *Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020*, 2020. doi: 10.1109/NOMS47738.2020.9110336.

[5] Rosihan and Y. Muin, "MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method," *Int. J. Comput. Appl.*, vol. 183, no. 47, pp. 975–8887, 2022, doi: 10.5120/ijca2022921878.

[6] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, no. 4, pp. 115–123, 2020, doi: 10.37034/jsisfotek.v2i4.32.

[7] B. Jagad, G. Putra, T. Musri, M. Kom, and L. M. Gultom, "Pemanfaatan Mikrotik Routerboard Sebagai Keamanan Jaringan Dari Udp Flood Dengan Menggunakan Firewall Di Dinas Pendidikan Bengkalis," *SNIT Semin. Nas. Ind. dan Teknol.*, vol. 2, no. 1, pp. 260–292, 2020, [Online]. Available: https://snit-polbeng.org/eprosiding/index.php/snit/article/view/136/138

[8] S. Bahri, "Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 136–147, 2023, doi: 10.60076/indotech.v1i3.239.

[9] R. A. Febrian, Y. Muhyidin, and D. Singasatia, "Analisis Penyerangan Bruteforce Terhadap Secure Shell (Ssh) Menggunakan Metode Penetration Testing," *Sci. J. Ilm. Sain dan Teknol. Anal.*, vol. 2, no. 11, pp. 151–162, 2024.

[10] B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, "Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan," *JOCOTIS-Journal Sci. Inform. Robot.*, vol. 1, no. 2, pp. 63–80, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[11] Rafay Baloch, *Ethical hacking and penetration testing guide*. Auerbach Publications, 2017.

[12] B. S. Anggoro and W. Sulistyo, "Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi," *Semin. Nas. APTIKOM*, pp. 1–9, 2019.

[13] D. Syafriani, R. T. Amanda, S. M. Rambe, and U. K. Siregar, "Pelatihan Perancangan Jaringan LAN Pada Ruangan SMK Telkom-2 Menggunakan Cisco Packet Tracer," *J. Has. Pengabdi. Masy.*, vol. 1, no. 1, pp. 8–15, 2022, doi: 10.62712/juribmas.v1i1.4.