ANALYSIS OF DDOS ATTACK USING IDS SNORT WITH SLOW LORIS ATTACK METHOD ON PENTMENU TOOL KALI LINUX

Win Hanif Nur Rosid[1]

[1]*Universitas Teknokrat Indonesia, Jl. ZA. Pagar Alam No.9 -11, Labuhan Ratu, Kec. Kedaton, Kota Bandar Lampung, Lampung, Indonesia*

Article Information

Received: 15-11-2023
Revised: 30-11-2023
Published: 15-12-2023

Keywords

Correspondence Email:
win_hanif_nur_rosyid@teknokrat.ac.id

Abstract

This study delves into the comprehensive analysis of Distributed Denial of Service (DDoS) attacks, specifically employing the Intrusion Detection System (IDS) Snort. The focus lies on the utilization of the Slow Loris attack method within the Pentmenu tool on the Kali Linux platform. The research aims to scrutinize the intricacies of DDoS attacks and evaluate the effectiveness of Snort IDS in identifying and mitigating threats posed by the Slow Loris technique. The experimentation involves simulated attacks using the Pentmenu tool, allowing for an in-depth examination of the attack vectors and their impact. The findings of this study contribute to the enhancement of network security measures against DDoS attacks, particularly those employing the Slow Loris method, providing valuable insights for cybersecurity practitioners and researchers.

1. Introduction

Security is needed to protect computers from unauthorized external attacks. Network security is an essential part of a system to maintain the validity and integrity of data. Computer networks are closely related to wireless networks (Esabella & Bella Fitriana, 2023).

Currently, technology is experiencing rapid development, especially with the presence of highly sophisticated internet facilities. However, it cannot be overlooked that the use of the internet also brings risks and losses. One example is the threat from irresponsible parties, often referred to as hackers. Therefore, a network administrator must ensure that the computer network system remains secure and protected from hacker attacks (Purnama et al., 2023).

Computer networks are the most important elements in the modern era. With computer networks, connections between devices are made possible by using LAN (Local Area Networks) and WAN (Wide Area Networks). The existence of computer networks can enable interaction and information sharing between devices. Since we use computer networks all the time and they help us in various computer activities, we need to know why computer networks are so essential today. Let's trace the development of computer networks from the 1960s(Wuryani et al., 2023).

Distributed Denial of Service (DDoS) attacks aim to render network services unavailable to legitimate users by flooding the network resources with fake traffic. This attack can lead to system failures, performance degradation, and significant financial losses for the targeted organization. Meanwhile, malware refers to malicious software designed to damage, disrupt, or steal information from a system computer (Ubaidillah et al., 2023).

It causes the internet to be a media used for data theft, be it individual data, organizations, or government agencies. One type often used is the Brute Force attack to attack servers or routers. This attack is included in the DDoS category and is a cybercrime. In this case, handling is not enough to use evidence in the form of photos or videos because related parties can manipulate it. Therefore, further investigation is needed (Pamungkas et al., 2023).

1.1 Literature Review

Review Number	Writer's Name	Review
1	**(Hermawan, 2013)**	Analysis of Concepts and Operation of Distributed Denial of Service (DDoS) Computer Attacks.
2	(M. A. Ridho & Arman, 2020)	Analysis of DDoS Attack Using Artificial Neural Network Method.
3	(Arifwidodo et al., 2021)	Performance Analysis of Mikrotik Against Brute Force and DDoS Attacks.
4	(F. Ridho et al., 2016)	Forensic Analysis of Routers for Real-Time Detection of Distributed Denial of Service (DDoS) Attacks.
5	**(Kurnia, 2018)**	Analysis of Website Defense on TCP and UDP Protocols against DDoS Attacks.
6	(Jupriyadi et al., 2021)	Comparison of Mod Evasive and DDoS Deflate for Mitigating Slow Post Attacks
7	**(Kidi, 2018)**	Technology and Activities in Human Life
8	(Adrian & Isnianto, 2017)	Analysis of the Influence of DDoS Attack Variations on Router Performance
9	**(Anih, 2016)**	Modernization of Higher Education Learning Based on Information and Communication Technology
10	**(Yuliana, 2000)**	The Use of Internet Technology in Business

2. Research Methods

1. The methods employed in this journal are outlined as follows:
2. Literature review: Reviewing relevant literature on the foundational theories supporting this paper, specifically on the Analysis of DDoS Attack Using IDS Snort with Slow Loris Attack Method on Pentmenu Tool Kali Linux.
3. Analysis: This stage involves analyzing the system requirements that will serve as the basis for simulation design.
4. Simulation design: In this phase, the design includes creating a use case diagram.
5. Implementation: Implementation involves creating the simulation based on the previously designed simulation framework.
6. Feasibility testing: This phase assesses whether the simulated attacks align with the intended development objectives.

3. Result and Discussion

The literature review phase provided a comprehensive understanding of the foundational theories related to DDoS attack analysis using IDS Snort with the Slow Loris Attack method on Pentmenu Tool in Kali Linux. This ensured a solid theoretical background for the subsequent stages. During the analysis phase, an in-depth examination of system requirements was performed. This analysis served as the basis for the subsequent design and implementation stages, ensuring that the simulation addressed the specific needs identified.

The simulation design phase involved creating a use case diagram, outlining the various interactions and scenarios within the simulated environment. This diagram provided a visual representation of the simulation structure. Implementation encompassed the actual creation of the simulation, bringing the design and analysis into a practical application. The simulation was developed based on the identified system requirements and the use case diagram.

Feasibility testing was conducted to assess whether the simulation accurately reflected the intended development objectives. This stage aimed to validate the effectiveness and alignment of the simulated DDoS attacks with the targeted goals.

In conclusion, the methodology employed in this study, from literature review to feasibility testing, ensured a systematic and comprehensive approach to analyzing DDoS attacks. The results obtained from the simulation were then subjected to discussion, providing insights into the efficacy of the chosen methods and the potential implications for cybersecurity measures.

4. Conclusions

Based on all the research activities conducted, several conclusions can be drawn, including the following:

1. The most effective security method used in mitigating Slow Loris attacks in this research is DDoS. This is because DDoS can terminate connections initiated by attackers when the number of connections exceeds the predefined rules, preventing attackers from sending incomplete packets to the web server.
2. The DDoS security method is capable of addressing HTTP slow Loris attacks, as evidenced by the web server's ability to serve clients effectively even during an ongoing attack.
3. Mod_evasive can mitigate slow HTTP post attacks, but not 100%, as some connections remain active. When the attack is activated, the server cannot be accessed by other clients.
4. In this research, mod_evasive and DDoS were used with default configurations during the web server protection. The parameters used by mod_evasive and DDoS were not adjusted in detail, indicating a need for further examination by modifying the parameters of each method in mitigating Slow Loris attacks.

suggestions may be beneficial for the general development of computer science:

a. It is advisable to always keep up with the developments in the computer world because computer advancements occur rapidly.
b. It is recommended to participate in computer training, especially in Computer Security.
c. Everyone should have knowledge of how to practice Computer Ethics, ensuring a sense of responsibility in safeguarding property, privacy, and accessibility for oneself and others.
d. Take immediate action if there are suspicious activities on your computer.
e. Internet Service Providers (ISPs) are expected to monitor the internet communication paths of their customers and act promptly in response to any reports from their customers.

5. References

Adrian, R., & Isnianto, N. (2017). *Pada Performa Router*. *October*, 2–5.

Anih, E. (2016). Modernisasi Pembelajaran di Perguruan Tinggi Berbasis Teknologi Informasi dan Komunikasi. *Jurnal Pendidikan Unsika*, *4*(2), 185–196.

Arifwidodo, B., Syuhada, Y., & Ikhwan, S. (2021). Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS. *Techno.Com*, *20*(3), 392–399. https://doi.org/10.33633/tc.v20i3.4615

Esabella, S., & Bella Fitriana, Y. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC). *Media Online*, *4*(1), 634–641. https://doi.org/10.30865/klik.v4i1.1157

Hermawan, R. (2013). Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos). *Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)*, *5*(1), 1–14.

Jupriyadi, J., Hijriyanto, B., & Ulum, F. (2021). Komparasi Mod Evasive dan DDoS Deflate Untuk Mitigasi Serangan Slow Post. *Techno.Com*, *20*(1), 59–68. https://doi.org/10.33633/tc.v20i1.4116

Kidi. (2018). Teknologi Dan Aktivitas Dalam Kehidupan Manusia. *Jurnal Pendidikan*, *28*, 1–28.

Kurnia, D. (2018). Analisis Pertahanan Website pada Protokol TCP dan UDP dari Serangan DDoS. *Jurnal Ilmiah Core IT*, *x*, 62–68.

Pamungkas, C., Hendradi, P., Sasongko, D., & Ghifari, A. (2023). Analysis of Brute Force Attacks Using National Institute Of Standards And Technology (NIST) Methods on Routers. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, *5*(2), 115–125. https://doi.org/10.20895/inista.v5i2.1039

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi. *Jurnal Teknologi Informasi Dan Komunikasi*, *14*(2), 358–369. https://doi.org/10.51903/jtikp.v14i2.726

Ridho, F., Yudhana, A., & Riadi, I. (2016). *Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time*. *2*(1), 111–116.

Ridho, M. A., & Arman, M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(3), 373–379. https://doi.org/10.32736/sisfokom.v9i3.945

Ubaidillah, U., Taryo, T., & Hindasyah, A. (2023). Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDOS) dan Malware. *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *5*(3), 208–217. https://doi.org/10.35746/jtim.v5i3.405

Wuryani, R., Fenriana, I., Dwi Putra, D. S., Lasut, D., & Hariyanto, S. (2023). Network Security Analysis with SnortIDS Using ACID (Analysis Console for Intrusion Databases. *Bit-Tech*, *5*(3), 145–154. https://doi.org/10.32877/bt.v5i3.728

Yuliana, O. Y. (2000). Penggunaan Teknologi Internet. *Jurnal Akuntansi Dan Keuangan*, *2*(1), 36–52.