

IJIRSET-Juli24.pdf

by Agustinus Noertjahyana

Submission date: 22-Jul-2024 08:50AM (UTC+0700)

Submission ID: 2420406344

File name: IJIRSET-Juli24.pdf (1.03M)

Word count: 2242

Character count: 12791

Analysis and Implementation of Distributed Denial of Service (DDoS) Attacks on the Website and Server

Agustinus Noertjahyana¹, Dave Handoko Priatmojo², M. Zainal Arifin³

^{1,2} Informatics Department, Petra Christian University, Surabaya, Indonesia

³ Informatics Department, State University of Malang, Malang, Indonesia

ABSTRACT: In today's digital era, maintaining the security of websites and server infrastructure is crucial to ensure data security and the smooth running of online services. This thesis explores the in-depth analysis and practical application of distributed DDoS attacks on websites and server infrastructures of relevant institutions. The aim of this thesis is to deepen the understanding of DDoS attack mechanisms and develop efficient mitigation methods. Through this research, frequent attack patterns were discovered, system vulnerabilities were evaluated, and systematic prevention and response strategies were proposed. Tests were conducted on the implementation of various defence strategies, including the use of more advanced firewalls, effective intrusion detection systems, and robust network architecture structures, to assess their ability to counteract DDoS attacks. During the research, various attacking and defensive strategies were evaluated, revealing interesting variations in the results. Some attack experiments yielded satisfactory outcomes, while others require further fine-tuning. The findings of this research are expected to provide new insights into the field of cybersecurity and serve as a guide for system administrators to protect their digital assets from ever-evolving threat.

KEYWORDS: DoS, Ddos, Goldeneye, Kali Linux, Slowloris.

I. INTRODUCTION

In today's digital age, ensuring the security of websites and servers is crucial. As websites continue to grow and cater to various user needs, including information access, shopping, and communication, the risk of cyber-attacks also increases. Protecting user data and ensuring smooth operations are the primary reasons why website and server security is of utmost importance[1-4]. Such attacks can result in severe consequences, including data breaches, financial loss, disruption of operations, loss of user trust, and more. Common types of attacks include malware attacks, SQL injection attacks, Denial of Service (DoS) attacks, cross-site scripting (XSS) attacks, among others [5]. One commonly utilized method to test the security of a website or server is through Distributed Denial of Service (DDoS) attacks. This method involves continuously sending fake traffic to overload the server or system being tested, thus assessing its resilience against such attacks [6-10]. This research focuses on testing the system's resilience to DDoS attacks.

This study will utilize GoldenEye and other tools to conduct DDoS attacks for the purpose of testing system or network security. GoldenEye is a freely available tool that can simulate DoS attacks on a targeted system or network, providing insights into the system's response. In addition to attacking the system, the research will also focus on implementing defensive solutions to protect against and prevent DDoS attacks. Known preventive measures include employing anti-DDoS hardware and software, configuring hardware to withstand DDoS attacks, and utilizing DDoS protection toolsets. inpainting is a method for repairing damaged pictures or removing unnecessary elements from pictures. It recovers the missing or corrupted parts of an image so that the reconstructed image looks natural. In real world, many people need a system to recover damaged photographs, designs, drawings, artworks etc. damage may be due to various reasons like scratches, overlaid text or graphics etc.

II. RELATED WORK

A Distributed Denial of Service (DDoS) Attack is a type of cyber-attack that overwhelms a network or system by flooding it with fake traffic, causing it to shut down [11-13]. Web security refers to measures taken to protect websites from such attacks [14]. This research focuses on other types of DDoS attacks, including Slowloris, TCP Syn Flood, and Ping Flood. Slowloris is a type of Denial of Service (DoS) attack that enables a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports. This attack was first introduced by hacker RSnake in 2009 and has since become a significant point of interest in cybersecurity research due to its unique method of operation, which involves sending partial HTTP requests to the target server, thereby holding the connections open and eventually exhausting the server's connection pool. Slowloris is a cyber-attack that gradually disables a website or server by sending numerous partial requests and keeping the connections open for as long as possible [15-17]. This eventually renders the website or server inaccessible to authorized users. TCP Syn Flood is a DDoS attack that exploits the TCP three-way handshake mechanism to overwhelm a network or system. This handshake is the foundation for establishing connections in TCP/IP networks [18-21]. Ping Flood, also known as ICMP Flood, is a denial-of-service attack where the attacker floods the target system with ping requests, overwhelming it with small data packets [22]. These attacks will be carried out on the target website, namely the XYZ website, which is one of the platforms used by Company XYZ to conduct business related to the automotive industry. Some of the services provided on the XYZ website include buying and selling used cars, swapping cars, and auctioning used cars.

III. METHODOLOGY

Every website has its own issues, such as a company website that conducts car buying and selling transactions, which faces several potential security problems, particularly related to Distributed Denial of Service (DDoS) attacks. One example of an attack by an attacker/hacker can be observed when the website is unable to handle many requests from users, leading to a DDoS attack. This attack is executed by sending an overwhelming number of requests to the website server, causing the server to become burdened or overloaded and unable to handle any more requests from other users. This can render the website inaccessible to other users. Additionally, DDoS attacks will vary according to the strategy that has been designed.

Based on Figure 1, it can also be seen that in addition to the attack strategies, methods for defending and protecting the system from DDoS attacks will also be explained.

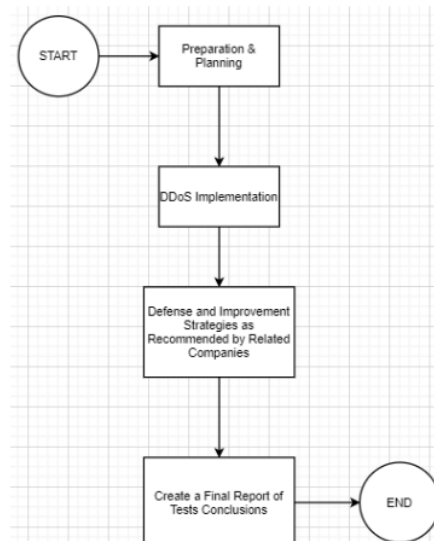


Fig. 1. Workflow of Research

IV. EXPERIMENTAL RESULTS

Fig. 2 depicts the website that will be the target of the DDoS attack. Each DDoS attack experiment will be conducted using different tools and various types of DDoS attacks, such as Slowloris, TCP Syn Flood, and Ping Flood. Before carrying out the attack, researchers conducted a reconnaissance and scanning stage on the target website using Nmap and Zenmap. This was done to obtain information about the target system and to identify vulnerabilities in the target's security system.



Fig.2. Targeted Website

Figs. 3 and 4 are the results of DDoS attack experiments that have been carried out using Goldeneye and Etherape on 2 operating systems, namely Kali Linux and Linux Ubuntu. Both have quite similar results, where the target security system has not been penetrated and the target security system has detected the attack while giving a false alarm to the system used by researchers.

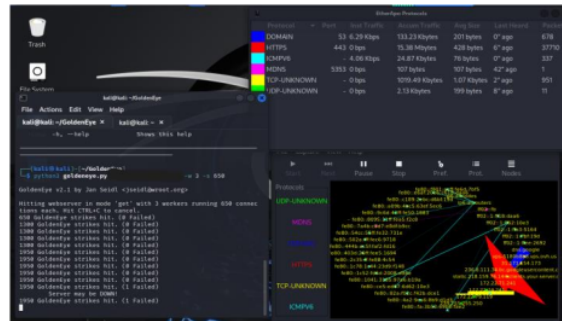


Fig. 3. DDoS Attack First Results Using Goldeneye and Etherape on Kali Linux

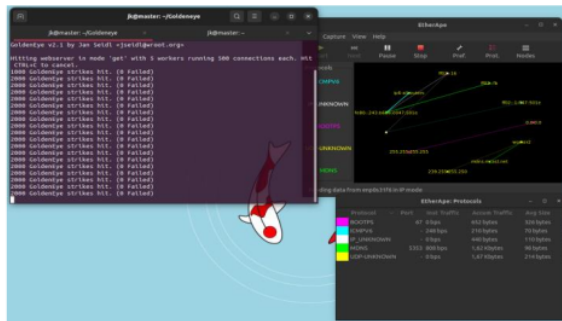


Fig. 4. DDoS Attack Second Results Using Goldeneye and Etherape on Linux Ubuntu

Figures 5 and 6 depict two attack experiments that have been previously conducted, yielding satisfactory results. This was determined through monitoring the target website, where it was observed that the target website experienced side effects or negative impacts from the attacks.

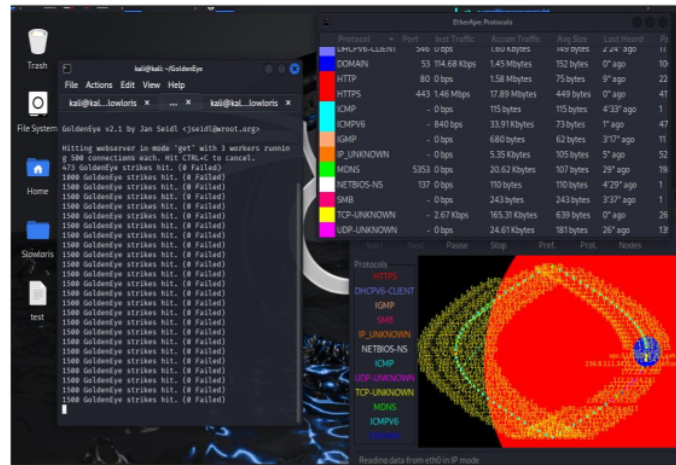


Fig. 5. DDoS Attack First Results Using Slowloris, Goldeneye, and Etherape on Kali Linux

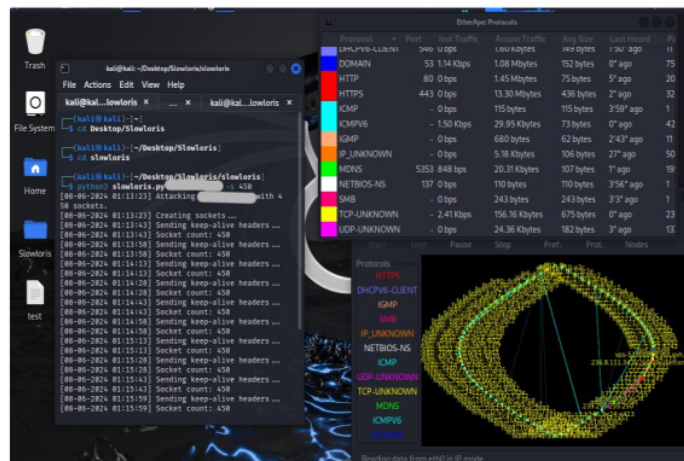


Fig. 6. DDoS Attack Second Results Using Slowloris, Goldeneye, and Etherape on Kali Linux

Figs. 7 and 8 show the results of attack experiments using the TCP Syn Flood method, which is a type of DDoS attack. Both experiments yielded quite good results as the side effects or negative impacts of the attack were visible on the target website during monitoring. However, the side effects experienced by the target website were only temporary; after a while, the attack began to be detected and became ineffective over time.

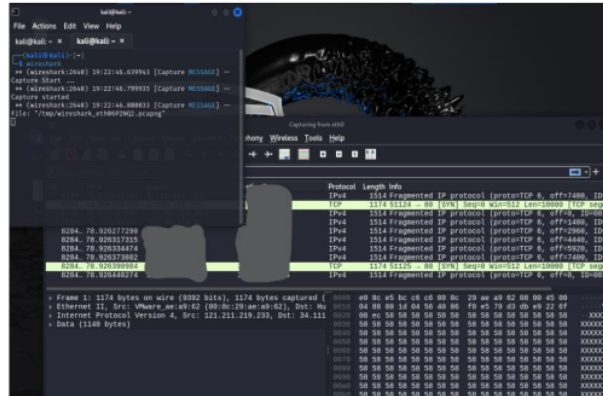


Fig. 7. TCP Syn Flood Attack First Results Using Hping3 and Wireshark on Kali Linux

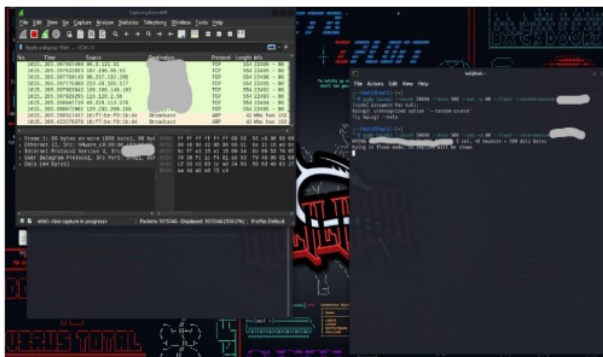


Fig. 8 . TCP Syn Flood Attack Second Results Using Hping3 and Wireshark on Kali Linux

Figs 9 and 10 are the results of the Ping Flood experiment conducted using Hping3 and Wireshark. The results of the attack did not produce satisfactory results and it can be said that the attack was not effective enough to penetrate the security system owned by the target. When monitoring the target website, no side effects, or negative impacts of the attack were found at all and the target website can run smoothly.

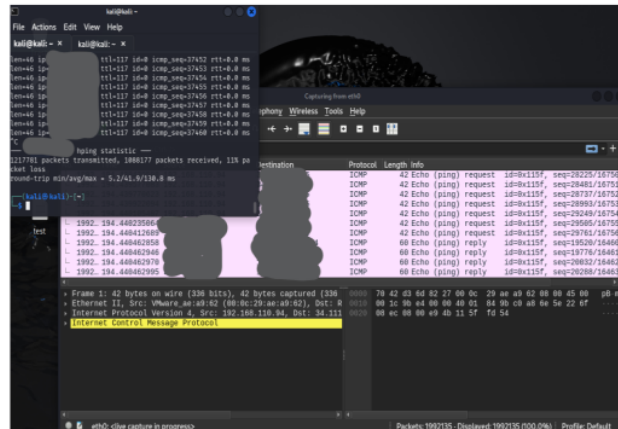


Fig. 9. Ping Flood Attack First Results Using Hping3 and Wireshark on Kali Linux

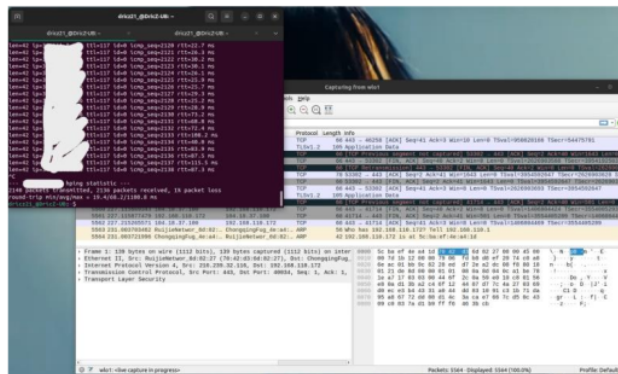


Fig. 10. Ping Flood Attack Second Results Using Hping3 and Wireshark on Linux Ubuntu

V. CONCLUSION

The study concludes that DDoS attacks on XYZ websites and servers fail to achieve their desired goals due to the robust security systems in place. The research utilized Goldeneye on Kali Linux, running through a Virtual Machine, and found that the performance of the attack was affected by the hardware specifications of the device used. Factors such as memory and processor greatly influenced the performance of the Virtual Machine and Goldeneye. While it cannot be entirely ruled out that there are no vulnerabilities to DDoS attacks, the study suggests that potential vulnerabilities in XYZ websites and servers are almost non-existent. However, it acknowledges that no security system can provide a 100% guarantee against all types of attacks conducted by hackers.

Moreover, the security system of the XYZ website and server is quite strong, as it can withstand prolonged DDoS attacks carried out by researchers through continuous efforts. Additionally, despite the varied nature of some attacks, the impact of these attacks was minimal, and the XYZ website and server remained secure. Furthermore, related to several other strategies that researchers employed during the study, such as experimenting with TCP Syn Flood and Ping Flood (ICMP Flood) attacks, the desired results were still not achieved.

REFERENCES

- [1] Schneier, B. (2003). "Beyond Fear: Thinking Sensibly About Security in an Uncertain World." Springer.
- [2] Mirkovic, J., & Reiher, P. (2004). "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review, 34(2), 39-53.
- [3] Beitollahi, H., & Deconinck, G. (2012). "Analyzing well-known countermeasures against distributed denial of service attacks." Computer Communications, 35(11), 1312-1332.
- [4] Puketza, N., Chung, K., Olsson, R., & Mukherjee, B. (1997). "A software platform for testing intrusion detection systems." IEEE Software, 14(5), 43-51.
- [5] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection." Pattern Recognition Letters, 51, 1-7.
- [6] Yu, S., Thapngam, T., Zhou, W., Jiankun, H., & Doss, R. (2010). "An efficient DDoS attack detection mechanism based on entropy estimation." Proceedings of the 7th IEEE International Conference on Service-Oriented Computing and Applications (SOCA), 1-8.
- [7] Moore, D., Voelker, G. M., & Savage, S. (2001). "Inferring internet denial-of-service activity." Proceedings of the 10th USENIX Security Symposium, 9-22.
- [8] Douligieris, C., & Mitrokotsa, A. (2004). "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer Networks, 44(5), 643-666.
- [9] Peng, T., Leckie, C., & Ramamohanarao, K. (2007). "Survey of network-based defense mechanisms countering the DoS and DDoS problems." ACM Computing Surveys (CSUR), 39(1), 1.
- [10] Meadows, C. (1999). "A formal framework and evaluation method for network denial of service." Proceedings of the 12th IEEE Computer Security Foundations Workshop, 4-13.
- [11] Murdoch, S. J., & Zieliński, P. (2004). "Low-cost traffic analysis of Tor." Proceedings of the IEEE Symposium on Security and Privacy, 183-195.
- [12] Wang, H., Zhang, D., & Shin, K. G. (2002). "Detecting SYN flooding attacks." Proceedings of the IEEE INFOCOM, 3, 1530-1539.
- [13] Li, J., Mirkovic, J., Wang, M., Reiher, P., & Zhang, L. (2002). "SAVE: Source address validity enforcement protocol." Proceedings of the IEEE INFOCOM, 3, 1557-1566.
- [14] Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidis, J., Paxson, V., & Shenker, S. (2002). "Controlling high bandwidth aggregates in the network." ACM SIGCOMM Computer Communication Review, 32(3), 62-73.
- [15] Beitollahi, H., & Deconinck, G. (2012). "Analyzing well-known countermeasures against distributed denial of service attacks." Computer Communications, 35(11), 1312-1332.
- [16] Douligieris, C., & Mitrokotsa, A. (2004). "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer Networks, 44(5), 643-666.
- [17] Kumar, R., et al. (2015). "Vulnerability analysis of web servers against Slowloris attack." International Journal of Computer Applications, 112(9).
- [18] Kaur, K., & Kaur, P. (2014). "DDoS attack prevention and mitigation techniques: A review." International Journal of Computer Applications, 94(4).
- [19] Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). "A framework for classifying denial of service attacks." Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, 99-110.
- [20] Karami, M., & McCoy, D. (2013). "Understanding the emerging threat of DDoS-as-a-service." Proceedings of the 2013 ACM SIGCOMM Conference on Internet Measurement Conference, 349-354.
- [21] He, J., Chan, K., & Guizani, M. (2007). "Network-based detection and defense for DDoS attacks: a review." IEEE Systems Journal, 3(4), 503-513.
- [22] Li, Z., Yuan, Y., Chen, X., & Li, Y. (2008). "Tunable parameters in QoS metrics for DDoS attack detection." International Journal of Security and Its Applications, 2(3), 17-28.

ORIGINALITY REPORT

16%
SIMILARITY INDEX

12%
INTERNET SOURCES

8%
PUBLICATIONS

10%
STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

3%
★ **ijritcc.org**
Internet Source

Exclude quotes On
Exclude bibliography On

Exclude matches < 5 words