Jurnal CoreIT, Vol.9, No.2, December 2023
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

DDoS Attack Using GoldenEye, DAVOSET, and PyLoris Tools

Kadek Sudewo Mahadiv Wikrama[1], Rangga Firdaus[1], Linda Zal Medes Mendrofa[1], Gede Arna Jude Saskara[1], I Made Edy Listartha[1]
[1]Sistem Informasi, Universitas Pendidikan Ganesha, Indonesia
sudewo@undiksha.ac.id, rangga@undiksha.ac.id, linda.zal@undiksha.ac.id, jude.saskara@undiksha.ac.id, listharta@undiksha.ac.id

Abstract. The development of computer networks is happening very rapidly, both in commercial installations, academics and homes of residents who now need and use internet access. Computer networks become a shared resource that is used by many applications representing different interests. With the ability and experience possessed by a hacker, he tries various kinds of computer network attacks with tools that are made independently or those that already exist are immediately used. A Distributed Denial of Service attack or what is often referred to as DDoS is a distributed attack with the aim of consuming the victim's bandwidth or resource availability by flooding servers, network links, and network devices with unauthorized traffic. Some of the DDoS tools used to carry out attacks include GoldenEye, DAVOSET, PyLoris. From the test results it was found that the GoldenEye tool was the most effective tool in causing the website to be inaccessible within 20 seconds and with 10,584 connections.
Purpose: The purpose of this research is to compare DDoS attacks from the GoldenEye, DAVOSET, and PyLoris tools..
Methods/Study design/approach: In this research, forensic research methods are used which aim to test system performance for analyzing file metadata in a digital evidence investigation process.
Result/Findings: The results found in this research are the effectiveness of time, number of attacks, and protocols used in the GoldenEye, DAVOSET, and PyLoris tools.
Novelty/Originality/Value: The novelty/originality/value used in this research provides documentation of the execution of attacks by the GoldenEye, DAVOSET, and PyLoris tools.

Keywords: DAVOSET, GoldenEye, and PyLoris.

Received November 2023 / **Revised** December 2023 / **Accepted** December 2023

INTRODUCTION

Computer networks become shared resources used by many applications representing different interests. The development of computer networks is occurring very rapidly, both in commercial, academic installations and in people's homes which now need and use internet access. Therefore, the internet is not only accessed by students, but hackers and crackers can also access the internet. For various special reasons, they carry out intrusions that will harm server and computer network owners. With the skills and experience possessed by a hacker, he tries various kinds of computer network attacks with tools that are created independently or that already exist and are used directly. The tools used and the sophistication of attacks on computer networks are inversely proportional to knowledge about infiltration of computer networks because the attacks that occur are more automatic and cause large numbers. Network attacks have a major effect on slow internet access, this is why if you access the internet sometimes it takes a long time to load because someone is trying to attack the server. Apart from that, malicious network attacks can result in data damage to the server. In general, attacks start by exploiting the host and computer network so that intruders come across the network, especially TCP/IP based networks

Denial of Service attacks or what are often called DDoS are distributed attacks with the aim of consuming the victim's bandwidth or resource availability by flooding servers, network links and network devices with unauthorized traffic {1]. Several DDoS tools used to carry out attacks include GoldenEye, DAVOSET, and PyLoris. GoldenEye is a tool used to carry out DDoS (Denial of Service) attacks against a website which aims to flood the server with too many connections so that the attacked server cannot serve a request [2]. DAVOSET is an at to carry out distributed denial of service attacks using execution on other sites [3]. DDoS attacks via another site execution tool (DAVOSET) – this is a command line tool to carry out DDoS attacks on sites via Abuse of Functionality and XML External Entity vulnerabilities on other sites [4]. Meanwhile, Pyloris is a script tool for testing server vulnerability against connection fatigue denial (DoS) attacks [5]. PyLoris can use SOCKS proxies and SSL connections, and can target protocols such as HTTP, FTP, SMTP, IMAP, and Telnet[6], these three tools have differences when carrying out attacks. This makes hackers have to choose which tools are more effective, faster and more profitable to use for hacking. Even though they are different, these three tools have their own advantages when hacking according to the object

DOI : 1024014/coreit.v9i2.20020

to be hacked. The research problem is which tool is the most effective to use to carry out a DDoS attack, from this problem it is found that the most effective tool is to carry out a DDoS attack on a late determined server.

METHODS

The flow of the research starts from conducting a literature study, then preparing a test plan, followed by carrying out tests and compiling a report. An overview of the research flow can be seen in Figure 1.

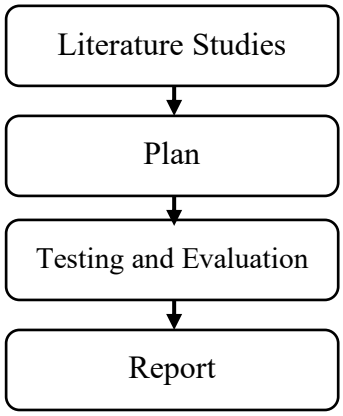

Figure 1. Research Flow

1. Literature Studies

The first stage in this research is a literature study, at this stage we carry out a literature study as support or reference for the studies and theories that we use in compiling DDoS attack reports, while to analyze the tools used and website security, forensic methods are used to carry out calculation and security tests.

2. Plan

The second stage is to prepare a test plan. Developing a test plan is divided into 2, namely, determining the testing environment, and also the testing stages. An adequate environment for this research is 2 laptops with 4GB RAM, WiFi with an average speed of 25 mbps, using VirtualBox software with Kali Linux. The tools used to carry out the attack are GoldenEye, DAVOSET, and PyLoris. The target for testing the tool is a vulnerable website with the address http://testphp.vulnweb.com/index.php. Testing in this research was carried out on the protocol used, number of attacks and effectiveness.

3. Testing and Evaluation

At the testing and evaluation stage, researchers carried out tests with 3 applications, namely GoldenEye, DAVOSET and PyLoris. These three tools are used to carry out Denial of Service attacks on predetermined addresses.

a. GoldenEye

GoldenEye is a tool used to carry out DDoS (Denial of Service) attacks against a website which aims to flood the server with too many connections so that the attacked server cannot serve a request. GoldenEye is written in python..

DOI : 1024014/coreit.v9i2.20020

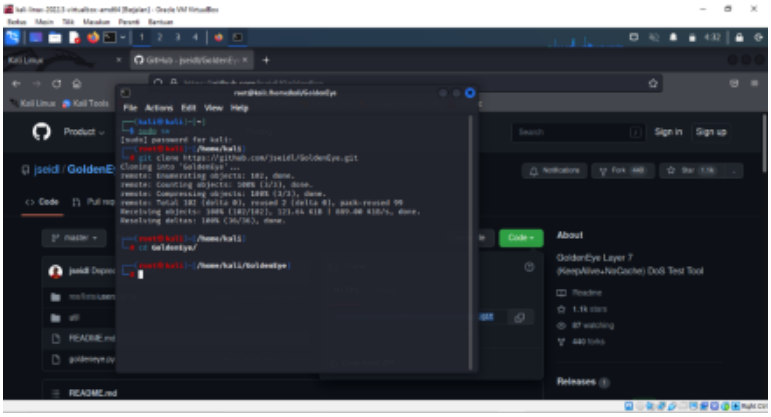

Figure 2. GoldenEye Initial View

GoldenEye Test Tool is HTTP DoS. This tool can be used to test whether a site is vulnerable to Denial of Service (DoS) attacks. It is possible to open multiple parallel connections against a URL to check whether the web server can be compromised. The program tests security on the network and uses 'HTTP Keep Alive. GoldenEye's changes generate requests dynamically – it randomizes user agents, referrers, and almost all the various parameters used. GoldenEye tries to keep the connection alive and also adds a suffix to the end of the URL that will allow requests to bypass many CDN systems (Also known as "Cacheless"). When a server's concurrent connections limit is reached, the server can no longer respond to valid requests from other users.

b. DAVOSET

DAVOSET is a tool for conducting distributed denial of service attacks using execution on other sites. DDoS attacks via another site execution tool (DAVOSET) this is a command line tool to perform DDoS attacks on sites via Abuse of Functionality and XML External Entity vulnerabilities on other sites. Davoset is a PERL based attack tool and has the ability to create many zombies to generate botnets to launch DDoS attacks

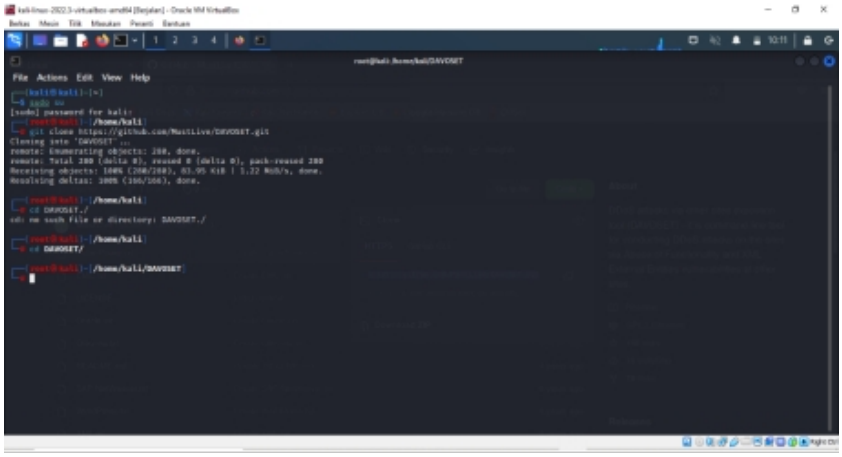

Figure 3. DAVOSET Initial Display

A DDoS attack tool that uses a zombie system to distribute attacks to various systems, this software works by using the Abuse of Functionality and XML External vulnerabilities.

c. PyLoris

PyLoris is a slow HTTP DDoS tool that allows attackers to create their own HTTP request headers, this includes packet headers, cookies, packet size, timeout and CRLF options. The goal of PyLoris is to keep the TCP connection open as long as possible between the attacker and the victim server. This results in Exhaustion of server connection table resources, once the server connection table

DOI : 1024014/coreit.v9i2.20020

is exhausted, it will not be able to handle new connections from legitimate users, resulting in denial of service.

Figure 4. PyLoris Initial View

PyLoris is software for DDoS attacks that allows you to build your own HTML request header structure. This software works to keep the TCP path open as long as possible to drain server bandwidth usage. Pyloris is a script-based tool and is used to test service level vulnerabilities for certain classes of Denial of Service attacks. It uses the built-in Slowloris operating system method and is used to test the server's readiness to withstand Botnet-based DDoS attacks. It is written in Python and has an IRC-based attack model

4. Reporting

The final stage in the research flow is compiling a report, which is a comprehensive synthesis of the entire research process. At this stage, researchers combine findings from literature studies, research plans, as well as results from trials and evaluations. The process of preparing a report involves in-depth analysis of the data that has been collected, choosing a logical information structure, and clear and concise writing.

RESULT AND DISCUSSION

In this section, the results and discussion of the planned stages are elucidated. The system testing is conducted alternately using the designated tools, namely GoldenEye, DAVOSET, and PyLoris. The following are the testing outcomes of these three tools.

1. GoldenEye

a. Attack Stages

The attack begins by installing GoldenEye on Kali Linux. Perform installation on the terminal. After the installation is complete, the initial display of GoldenEye will appear. The attack was carried out with the target website http://testphp.vulnweb.com/index.php using the GoldenEye tool, researchers succeeded in causing the target website to experience network traffic congestion and a large number of connections accessing the web page. Due to network traffic congestion, the target website cannot be accessed.

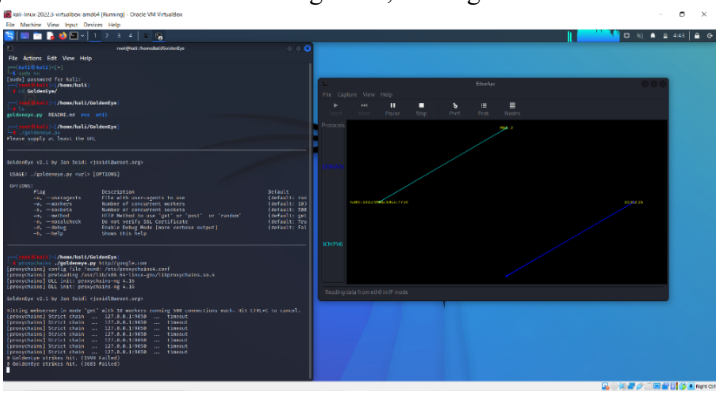

Figure 5. GoldenEye testing and measurements

The CPU load can suddenly increase even though there are no processes running, this results in not being able to see the system using the CPU, so the website goes down and cannot be accessed by users.

DOI : 1024014/coreit.v9i2.20020

b. Attack Result

The result of the attack carried out on the targeted website was that a website was successfully hacked, losing content and being inaccessible to users. The following is the initial appearance of the website http://testphp.vulnweb.com/index.php

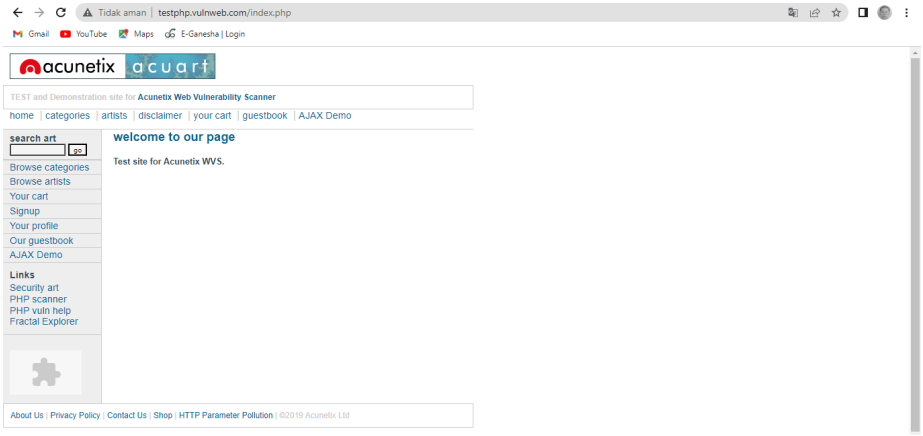

Figure 6. Initial appearance of the website

After a DoS attack was carried out using Golden Eye, the website was no longer accessible. The following is what the website looks like after hacking:

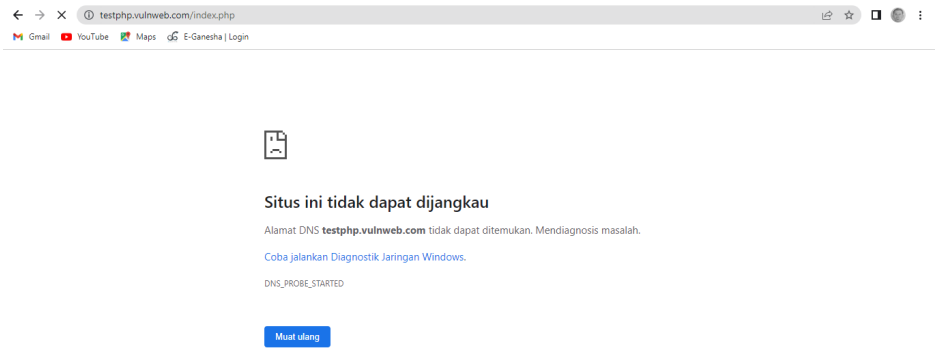

Figure 7. Website Appearance After Hacking

2. DAVOSET

a. Attack Stages

The attack begins by installing DAVOSET on Kali Linux. Perform installation on the terminal. After the installation is complete, the initial DAVOSET display will appear. The attack was carried out targeting the website http://testphp.vulnweb.com/index.php using the DAVOSET tool, the website was slow.

DOI : 1024014/coreit.v9i2.20020

Figure 8. DAVOSET Testing and Measurement

Even though there is no significant increase in traffic, website performance can be slow due to DDoS attacks. Understanding that the goal of DDoS is to overload the hosting server then, the solution is to store data on several servers around the world, this CDN serves websites to users from servers close to them for faster performance. By using a CDN you don't need to worry about attacks because if one server is overloaded then there are still other servers that can be used.

b. Attack Result

The result of the attack carried out on the targeted website was that a website was successfully hacked, losing content and being inaccessible to users. The following is the initial appearance of the website http://testphp.vulnweb.com/index.php

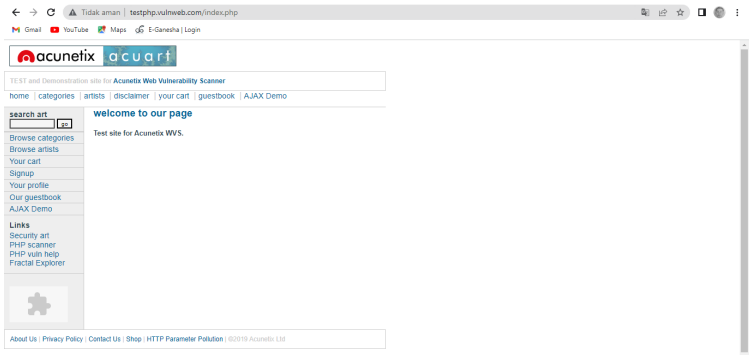

Figure 9. Initial appearance of the website

After a DoS attack was carried out using DAVOSET, the website was no longer accessible. The following is what the website looks like after hacking:

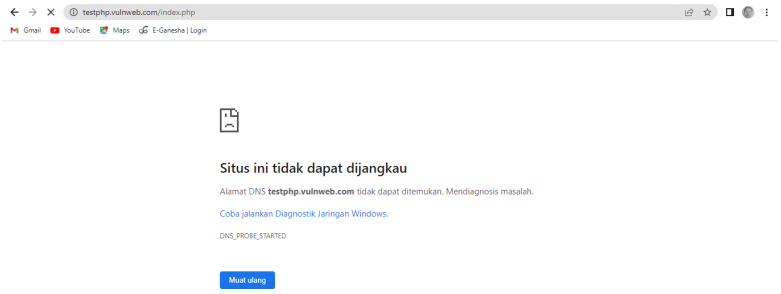

Figure 10. Website Appearance After Hacking

DOI : 1024014/coreit.v9i2.20020

3. PyLoris

a. Attack Stages

The attack begins by installing PyLoris on Kali Linux. Perform installation on the terminal. After the installation is complete, the initial screen of PyLoris will appear. The attack was carried out with the target website http://testphp.vulnweb.com/index.php using the Pyloris tool, that is, we succeeded in hacking a website so that the website experienced a lack of bandwidth because this attack used up a lot of bandwidth..

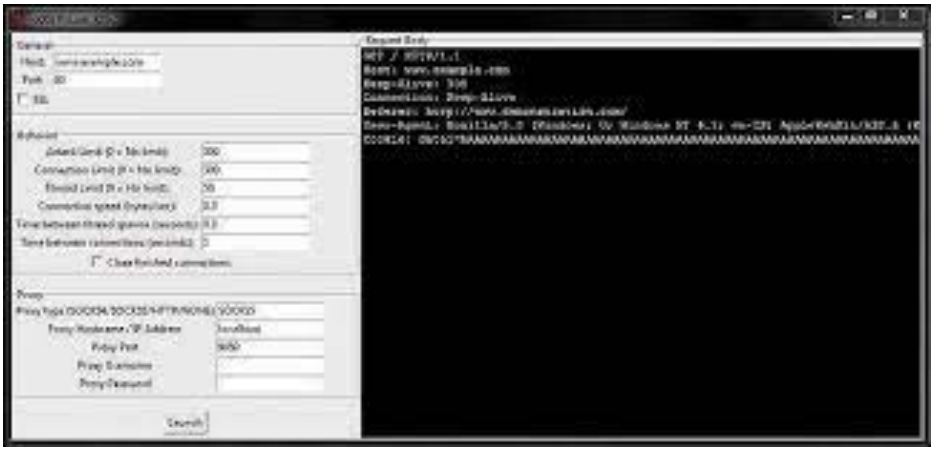

Figure 11. PyLoris Testing and Measurement

Bandwidth traffic is experiencing drastic congestion because too many requests mean the internet requires more bandwidth, so it is necessary to monitor bandwidth to stay alert and immediately take preventative steps.

b. Attack Result

The result of the attack carried out on the targeted website was that a website was successfully hacked, losing content and being inaccessible to users. The following is the initial appearance of the website http://testphp.vulnweb.com/index.php/.

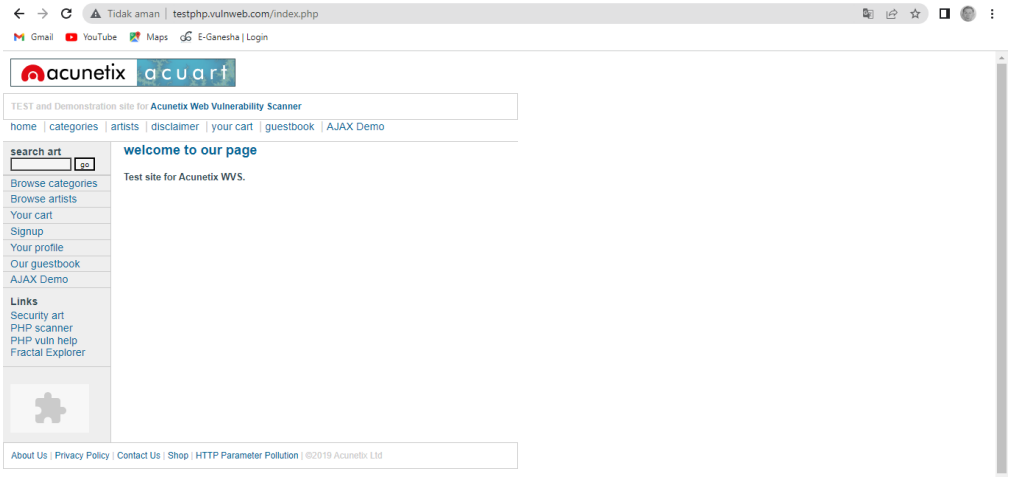

Figure 12. Initial appearance of the website

After a DoS attack was carried out using PyLoris, the website was no longer accessible. The following is what the website looks like after hacking

DOI : 1024014/coreit.v9i2.20020

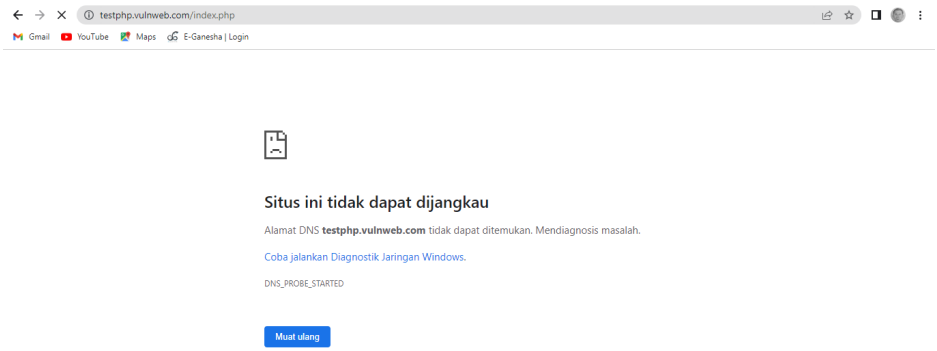

Figure 13. Website Appearance After Hacking

4 Pembahasan

Tools	Protocol	Amount Attack	Time	Result
GoldenEye	HTTP GET	18 workers 588 connection, 10.584 connection	20 Second	The CPU load can suddenly increase even though there are no processes running, this results in not being able to see the system using the CPU, so the website goes down and cannot be accessed by users.
DAVOSET	HTTP	80 port 400 limit connection 32.000 connection	40 Second	Even though there is no significant increase in traffic, website performance can be slow due to DDoS attacks
PyLoris	HTTP	80 port 500 limit connection 40.000 connection	60 Second	Bandwidth traffic is experiencing drastic congestion because too many requests mean the internet requires more bandwidth, so it is necessary to monitor bandwidth to stay

DOI : 1024014/coreit.v9i2.20020

				alert and immediately take preventative steps.

CONCLUSION

Distributed Denial of Service attacks or what are often referred to as DDoS are distributed attacks with the aim of consuming the victim's bandwidth or resource availability by flooding servers, network links and network devices with unauthorized traffic. Several DDoS tools used to carry out attacks include GoldenEye, DAVOSET, and PyLoris. GoldenEye is a tool used to carry out DDoS (Denial of Service) attacks against a website which aims to flood the server with too many connections so that the attacked server cannot serve a request. DAVOSET is a tool for conducting distributed denial of service attacks using execution on other sites. DDoS attacks via other site execution tools and PyLoris is a slow HTTP DDoS tool that allows attackers to create their own HTTP request headers, this includes packet headers, cookies, packet size, timeout and CRLF options. Based on the test results, based on time, it was found that GoldenEye was the fastest to make a website inaccessible in 20 seconds, then DAVOSET 40 seconds, and PyLoris 60 seconds. GoldenEye can make websites go down faster because it reduces CPU load and also increases traffic significantly compared to other tools. As for suggestions for further research, you can compare other tools in carrying out DoS attacks and also other attacks.

REFERENCES

[1] Xie, Y., & Yu, S. Z. (2009). Monitoring the application-layer DDoS sttacks for popular websites. *IEEE/ACM Transactions on Networking*, *17*(1), 15–25. https://doi.org/10.1109/TNET.2008.925628 *(diakses 18 November 2022)*

[2] Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. In *Computer Communications* (Vol. 107, pp. 30–48). Elsevier B.V. https://doi.org/10.1016/j.comcom.2017.03.010 *(diakses 18 November 2022)*

[3] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. In *Computer Communication Review* (Vol. 34, Issue 2, pp. 39–53). https://doi.org/10.1145/997150.997156 *(diakses 18 November 2022)*

[4] Sriram, B., & Santhosh Kumar, M. P. (2018). Distributed Denial of Service (DDOS) Attacks Detection Mechanism. In *IJSTE-International Journal of Science Technology & Engineering* | (Vol. 4, Issue 10). www.ijste.org *(diakses 19 November 2022)*

[5] Gill, S. S., & Buyya, R. (2018). SECURE: Self-Protection Approach in Cloud Resource Management. *IEEE Cloud Computing*, *5*(1), 60–72. https://doi.org/10.1109/MCC.2018.011791715 *(diakses 19 November 2022)*

[6] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666. https://doi.org/10.1016/j.comnet.2003.10.003 *(diakses 19 November 2022)*

[7] Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. In *Arabian Journal for Science and Engineering* (Vol. 42, Issue 2, pp. 425–441). Springer Verlag. https://doi.org/10.1007/s13369-017-2414-5 *(diakses 19 November 2022)*

DOI : 1024014/coreit.v9i2.20020

[8] Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of Recent Detection Methods for HTTP DDoS Attack. In *Journal of Computer Networks and Communications* (Vol. 2019). Hindawi Limited. https://doi.org/10.1155/2019/1283472 *(diakses 20 November 2022)*

[9] Behal, S., & Kumar, K. (2017). Characterization and comparison of DDoS attack tools and traffic generators - a review. *International Journal of Network Security*, *19*(3), 383–393. https://doi.org/10.6633/IJNS.201703.19(3).07 *(diakses 20 November 2022)*

[10] Jones, N. L., Sherman, P., Fallone, C. A., Flook, N., Ccfp, M. D., Smaill, F., Cb, M. B., Frcpc, F., Veldhuyzen Van Zanten, S., Rrcpc, M., Hunt, R., Frcp, M. B., Facg, F., & Thomson, A. (2005). Jones_H.qxd. In *Can J Gastroenterol* (Vol. 19, Issue 7). *(diakses 21 November 2022)*

[11] Kaur, H., Behal, S., & Kumar, K. (2016). Characterization and comparison of Distributed Denial of Service attack tools. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, 1139–1145. https://doi.org/10.1109/ICGCIoT.2015.7380634 *(diakses 21 November 2022)*

[12] Fadlil, A., Riadi, I., & Aji, S. (2017). Pengembangan sistem pengaman jaringan komputer berdasarkan analisis forensik jaringan. *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)*, *3*(1), 11-19.https://www.researchgate.net/profile/Imam-Riadi-2/publication/318670501_Pengembangan_Sistem_Pengaman_Jaringan_Komputer_Berdasarkan_Analisis_Forensik_Jaringan/links/5976a94baca2728d02706ac8/Pengembangan-Sistem-Pengaman-Jaringan-Komputer-Berdasarkan-Analisis-Forensik-Jaringan.pdf. *(diakses 22 November 2022)*

[13] Muttaqin, M., Halid, A., Resha, M., Andryanto, A., Firdian, F., Syamsu, S., ... & Sasongko, D. (2022). *Teknologi Jaringan Komputer.* Yayasan Kita Menulis. https://scholar.google.com/citations?user=ytBGmuEAAAAJ&hl=id&oi=sra. (*diakses 22 November 2022)*

[14] Shorey, T., Subbaiah, D., Goyal, A., Sakxena, A., & Mishra, A. K. (2018, September). Performance comparison and analysis of slowloris, goldeneye and xerxes ddos attack tools. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 318-322). IEEE. https://ieeexplore.ieee.org/abstract/document/8554590/ *(diakses 22 November 2022)*

[15] Sihombing, J. C. J., Kartikasari, D. P., & Bhawiyuga, A. (2019). Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, 964X. http://download.garuda.kemdikbud.go.id/article.php?article=1479208&val=10384&title=Implementasi%20Sistem%20Deteksi%20dan%20Mitigasi%20Serangan%20Distributed%20Denial%20of%20Service%20DDoS%20menggunakan%20SVM%20Classifier%20pada%20Arsitektur%20Software-Defined%20Network%20SDN. *(diakses 22 November 2022)*

DOI : 1024014/coreit.v9i2.20020