

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

DIA

International Journal of Innovative Research in SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

 \bigcirc

🖂 ijirset@gmail.com





www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710

Volume 13, Issue 7, July 2024 |DOI: 10.15680/IJIRSET.2024.1307096|

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

Agustinus Noertjahyana¹, Dave Handoko Priatmojo², M. Zainal Arifin³

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

Department of Informatics, State University of Malang, Malang, Indonesia³

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 toolsage 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





www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307096|

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.

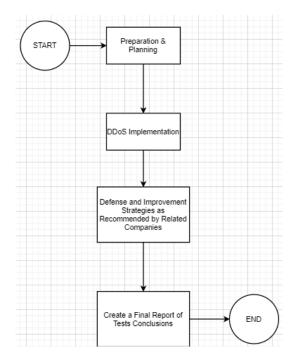


Fig. 1. Workflow of Research





www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024 |DOI: 10.15680/IJIRSET.2024.1307096|

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.

		53 6.29 Kbps	133.23 Kbytes	201 bytes		
Trash	HTTPS	443 0 bps	15.38 Mbytes	428 bytes	6" ago	
	ICMPV6	- 4.06 Kbps	24.87 Kbytes	76 bytes	0° ago	
0	MDNS	5353 0 bos	107 bytes	107 bytes	42" 300	
	TCP-UNKNOWN		1019.49 Kbytes	1.07 Kbytes	2° ago	
ile System	JDP-UNKNOWN	- 0 bps	2.13 Kbytes	199 bytes	8° ago	
kali@kali:-/GoldenEye						
File Actions Edit View Help						
kali@kali: ~/GoldenEye × kali@kali: ~ ×						
-hhelp Shows this help						
-\$ pythan3 goldeneye.py -w 3 -s 650 oldenEye v2.1 by Jan Seidl <jseidl@wroot.org></jseidl@wroot.org>	Protocols		reso -2880-2001-2	11 fe6d; 7bf5		
			e80::c189 2ebc d6bh1	Re-allopaes		
itting webserver in mode 'get' with 3 workers running 650 co	nnec UDP-UNKNOW			in6-anouter		
itting webserver in mode 'get' with 3 workers running 650 co ions each. Hit CTRL+C to cancel.			a09b:41c5:63ef.5ec6 ±481f.re50:1883	Ip6.abouter		
ions each. Hit CTRL+C to cancel. 50 GoldenEye strikes hit. (0 Failed)		fe80:: fe80::9c6i - fe80::8095: ¥	a096-44c5:63et5ec6 ±48m1e50:1883 #Tea5:12c8	106-30-outer 102- 102:	1518.daa6- 102-1162-10e3	
ions each. Hit CTRL+C to cancel. 50 GoldenEye strikes hit. (@ Failed) 300 GoldenEye strikes hit. (@ Failed) 300 GoldenEye strikes hit. (@ Failed)		fe80:: fe80::9c6i fe80::8095.1c fe80::7a4b:c807:i fe80::54cc:55ff:fe32	a09b.4bc5.63ef.5ec6 148ff.fe50.1883 ff.fe65.f2c8 88df.b9cc -731e	106-30-outer 102- 102:	10 1-518 daa6- 102-1-162-10e3 102-1-162-10e3	
ions each. Hit CTRL4. to căncel. 58 GoldenEye strikes hit. (0 Failed) 380 GoldenEye strikes hit. (0 Failed) 380 GoldenEye strikes hit. (0 Failed) 380 GoldenEye strikes hit. (0 Failed)		fe80:: fe80::9c6 - fe80::8095:3c fe80::7a4b:c807:4 fe80::54cc:56ff:fe32 fe80::502a.4ff.fe6;9	a09b.4bc5.63ef.5ec6 5.60ff.fe50.1883 mTea5.f2c8 68df.b9cc -731e 718	106-30-outer 102- 102:	1518.daa6- 102-1162-10e3	
ions sech. Hit CTEL-C to cancel. 58 Goldenfys strikes hit. (0 Failed) 380 Goldenfys strikes hit. (0 Failed)		fe80:: fe80::9c6i fe80::8095.1c fe80::7a4b:c807:i fe80::54cc:55ff:fe32	a09b.4%5.63e15ec6 2.68m.1e50.1883 mtea5.12c8 88dtb9cc -731e 718 116	106-30-outer 102- 102:	10 1018 daa6 02-1162 1003 02-1163 516 02-11651 02-11661 02-11661 02-11661 02-11661	9d 2692 Je
Jons Sach. HIL (TRu-C to Cancel. 306 Goldenies ettickes hit. (# Failed) 308 Goldenies ettickes hit. (# Failed) 308 Goldenies ettickes hit. (# Failed) 308 Goldenies ettickes hit. (# Failed) 508 Goldenies ettickes hit. (# Failed) 508 Goldenies ettickes hit. (# Failed)		1680- 1680-3095-10 1680-3095-10 1680-3746-16801 1680-5024-01166-39 1680-5024-01166-39 1680-4440-45517-11 1680-4440-45517-11 1680-4440-45511-11 1680-2235-11488-44	a09b;4bc5;63ef;5ec6 c4m;re50;1483 mfea5;12c8 s8db;9cc -731e 118 54	106-30-outer 102- 102:	rfb 1.508.daa6- 102-1.162:10e3 102-1.163:516 102-1.16e: 102-1.5ee: dnii boo 102-1.5ee:	9d 2692 ple ps.ov/h.us
June seck. Hit (TRu-t to cancel. 30 Goldenty strikes hit. (§ Failed) 30 Goldenty strikes hit. (§ Failed)		1680:: 1680::946 1680::946 1680::744::647 1680::544::547:647 1680::544::547:65 1680::542:547:642 1680::542:34 1665:10 1680::2235:1688-44 1680::1278:13:542:36	a096-44c5-63ef.5ec6 ±48mfe55-1883 mfte35-12c8 88drb9cc -731e 718 116 54 9-f148	196-39-004er 1902e 19002 19002 19002 10000 10000 10000 10000 10000 10000	190 1918:daa6- 1918:1062:1063 1917:1:1062:1063 1917:1:1062:1064 1917:1:1062: 191	9d 2692 ple ps.ovh.us 73 rcontent.c
Jons Sach. HIL (TRu-C to Cancel. 306 Goldenies ettickes hit. (# Failed) 308 Goldenies ettickes hit. (# Failed) 308 Goldenies ettickes hit. (# Failed) 308 Goldenies ettickes hit. (# Failed) 508 Goldenies ettickes hit. (# Failed) 508 Goldenies ettickes hit. (# Failed)	MONS CRANNIN FITTPS	fe80: fe80:3053 fe80:3055 fe80:34b:6805 fe80:34b:6805 fe80:34b:6805 fe80:34b:6805 fe80:34b:6805 fe80:34b:6805 fe80:34b:6805 fe80:1452:1684;280 fe80:1452:1684;280 fe80:1452:1684;280	a09b.44x5.63ef.5ec6 44077e50.1883 mtfe35.12e8 880f.99cc 7731e 773 116 54 9148 54 9148 54	196-350-4er 1002- 1022- 10 236-6 1111 static 218-159	10 10 10 10 10 10 10 10 10 10	9d 2692 ps.ovh.us 73 rcontent.c
Jone acds. Hit (TRA-to concel. 80 Goldenty strikes hit. (6 Failed) 80 Goldenty strikes hit. (6 Failed) 80 Goldenty strikes hit. (6 Failed) 90 Goldenty strikes hit. (6 Failed)		1680- 1680-5005-30 1680-540-540-540 1680-540-540-540-540 1680-540-540-540-540 1680-4440-656-640 1680-4440-656-640 1680-1693-1640-20 1680-1043-30 1680-1043-1040-1040-1040-1040-1040-1040-104	40%0.4%c5.63ef.5ec6 4.6%7e55.1883 %fei5.7c8 88tb9cc 7731e 778 116 54 9.148 9.148 9.57716.1194 5.57716.1194 6.577716.1194 6.577716.1194	196-39-004er 1902e 19002 19002 19002 10000 10000 10000 10000 10000 10000	10 11.12.8.daa6 102-11.02.10.03 102-11.03.516 102-11.03.516 102-11.04.51 102-11.04.51 102-11.04.51 104.51 104.55 104	9d 2692 ps.ovh.us 73 rcontent.c
June seck. Hit (TRu-t to cancel. 306 Goldenty strikes hit. (§ Failed) 308 Goldenty strikes hit. (§ Failed) 309 Goldenty strikes hit. (§ Failed)	MONS CRANNIN FITTPS	fe80: fe80:366 fe80:305 fe80:305 fe80:304:de805 fe80:302 fe80:302 fe80:302 fe80:440;e35rd2 fe80:402 fe80:2235 fe80:2235 fe80:1218 fe80:122 fe80:1041 fe80:c55 fe80 fe80 fe80 fe80 fe80 fe80 fe80 fe80	4590-48c5-63et5ec6 1-4877-520-1683 1-4877-520-1683 1-4877-520-1683 1-4876-52-128 1-4876-52-128-128 1-4876-52-128-128 1-4876-52-128-128 1-4876-52-128-128-128 1-4876-52-128-128	196-3360.4er 1902: 1902: 1902: 1902: 1902: 1902: 1903: 1904: 1905: 1905: 1905: 1905: 1905: 1905: 1905: 1906: 1906: 1906: 1906: 1906: 1906: 1906: 1906: 1907:	10 11 318 daa6 1021106211083 1021106211083 102110841 102110841 102110841 102110841 102110845 10211085 10211085 10211085 10211085 10211085 10211085 10211085 10211085 10211085 10211085 10211085 10211085 10211085 10211000000000000000000000000000000000	9d 2692 ps.ovh.us 73 rcontent.c

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



Volume 13, Issue 7, July 2024



www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Def: full: fu

Fig. 4. DDoS Attack Second Results Using Goldeney 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.

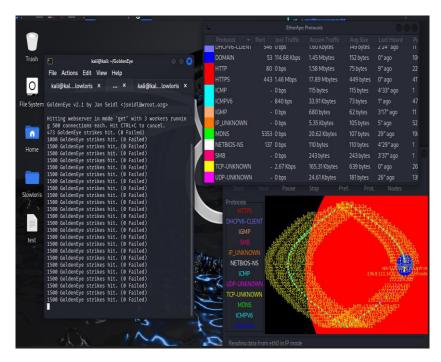


Fig. 5. DDoS Attack First Results Using Slowloris, Goldeneye, and Etherape on Kali Linux





www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

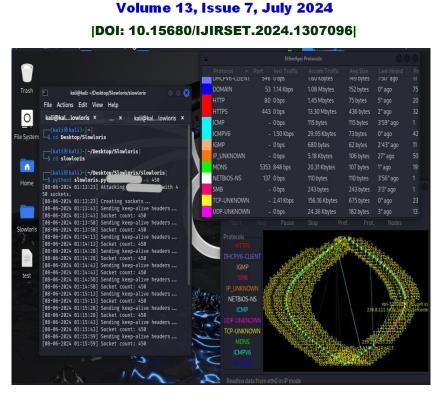


Fig. 6. DDoS Attack Second Results Using Slowloris, Goldeneye, and Etherape on Kali Linux

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.

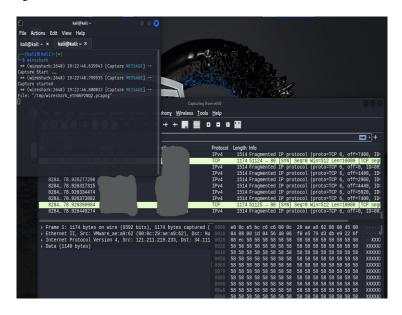


Fig. 7. TCP Syn Flood Attack First Results Using Hping3 and Wireshark on Kali Linux



Volume 13, Issue 7, July 2024



www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

<complex-block>

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.

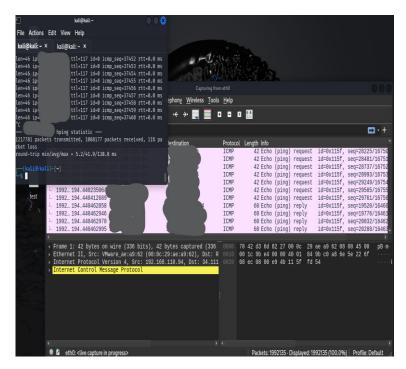


Fig. 9. Ping Flood Attack First Results Using Hping3 and Wireshark on Kali Linux



Volume 13, Issue 7, July 2024



www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

<complex-block>

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.
- Mirkovic, J., & Reiher, P. (2004). "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review, 34(2), 39-53.
- 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.





www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307096|

- 8. Douligeris, C., & Mitrokotsa, A. (2004). "DDoS attacks and defense mechanisms: classification and state-of-theart." 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. Douligeris, C., & Mitrokotsa, A. (2004). "DDoS attacks and defense mechanisms: classification and state-of-theart." 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).
- 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.
- 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.
- 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.

INTERNATIONAL Standard Serial Number India







INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY





www.ijirset.com