JINTEKS (Jurnal Informatika Teknologi dan Sains) ISSN 2686-3359 (Online)
Vol. 4 No. 4, November 2022, hlm. 467 – 471

PERBANDINGAN DDOS *ATTACK* MENGGUNAKAN *TOOLS* LOIC, HOIC DAN HULK DALAM MELAKUKAN PENYERANGAN PADA SUATU WEBSITE

Made Alit Juniska[1*], Ni Made Gita Ayu Padmasari[2], Ni Ketut Rika Suryani[3], Komang Widhi Dharma Pratiwi[4], Gede Arna Jude Saskara[5], I Made Edy Listartha[6]
[1,2,3,4,5,6]Sistem Informasi, Universitas Pendidikan Ganesha
email: alit.juniska@undiksha.ac.id*

Abstrak: DDoS Attack merupakan bentuk serangan yang dilakukan dengan mengirim paket secara terus-menerus kepada suatu sistem atau website dengan cara melakukan serangan pengiriman permintaan kepada website dengan tujuan memberatkan suatu penyimpanan layanan yang dipunyai oleh suatu website. Metode yang digunakan adalah penelitian terapan, dengan tujuan memberikan informasi terkait efektivitas penggunaan perangkat lunak LOIC, HOIC, dan HULK. Secara pembuktian, studi ini akan dilakukan tahapan serangan dan hasil pengujian atau evaluasi dari perangkat lunak LOIC, HOIC, dan HULK dengan melakukan perbandingan penggunaan protokol dan efektivitas waktu. LOIC menggunakan protokol TCP dengan efektivitas waktu 15 detik, HOIC menggunakan protokol HTTP GET dengan efektivitas waktu 60 detik, dan HOIC menggunakan protokol HTTP dengan efektivitas waktu 600 detik.

Kata Kunci : Serangan, LOIC, HOIC, HULK

Abstract: DDoS Attack is a form of attack that is carried out by sending packets continuously to a system or website by carrying out an attack on sending requests to the website with the aim of burdening a service storage owned by a website.The method used is applied research, with the aim of providing information related to the effectiveness of using LOIC, HOIC, and HULK software. Evidentially, this study will be carried out in the attack stage and the results of testing or evaluation of LOIC, HOIC, and HULK software by comparing the use of the protocol and time effectiveness. LOIC uses the TCP protocol with a time effectiveness of 15 seconds, HOIC uses the HTTP GET protocol with a time effectiveness of 60 seconds, and HOIC uses the HTTP protocol with a time effectiveness of 600 seconds.

Keywords **:** *Attack, LOIC, HOIC, HULK*

PENDAHULUAN

Dalam dunia teknologi informasi, keamanan merupakan salah satu hal yang sangat penting. Banyak serangan yang kerap diberikan oleh pihak-pihak tertentu untuk meretas keamanan dari sistem tersebut. Serangan merupakan usaha yang dilakukan untuk dapat melumpuhkan suatu sistem. Dalam dunia Cyber, serangan yang kerap dilakukan oleh para peretas adalah serangan DDoS atau DDoS Attack. DDoS Attack merupakan bentuk serangan yang dilakukan dengan mengirim paket secara terus-menerus kepada suatu sistem atau jaringan komputer. Serangan DDoS ini, akan mengakibatkan sistem atau jaringan komputer tidak dapat diakses dan digunakan oleh pengguna. Serangan DDoS ini sekarang sudah menargetkan layanan tertentu, yang menyebabkan aplikasi yang ditargetkan gagal, sementara komponen jaringan lainnya (link, switch, router) baik- baik saja. Metode ini memungkinkan serangan untuk menyamar sebagai lalu lintas normal karena memiliki kekuatan tinggi. Ini berbeda dengan serangan DDoS, yang biasanya menghasilkan traffic yang tinggi.

Mengingat banyaknya serangan yang terjadi, mekanisme serangan DDOS serta cara mengatasinya dapat terjadi. Tidak banyak orang yang memahaminya, tetapi tidak ada salahnya untuk memperluas pengetahuan pengguna tentang serangan mematikan semacam ini. Menarik juga untuk mengangkat cara mengatasinya, sebagai pertimbangan penting, jika suatu saat, tanpa sepengetahuan kita, serangan ini dapat mengincar Skita. Ada beberapa cara untuk menghadapi serangan cyber, yang pertama adalah dengan menggunakan sistem deteksi intrusi "IDS". Kedua menggunakan server firewall router. IDS adalah salah satu dari komponen keamanan jaringan yang melindungi data dan informasi keamanan dengan memantau lalu lintas paket data dan mendeteksi penyusup. IDS dirancang untuk melindungi sistem komputer dengan mendeteksi dan mendiagnosis semua aktivitas berupa integritas sistem dan pelanggaran izin. Firewall router adalah sistem yang menyaring dan menganalisis semua paket lalu lintas dengan mengizinkan atau memblokir lalu lintas berbahaya dari port atau aplikasi.

TINJAUAN PUSTAKA

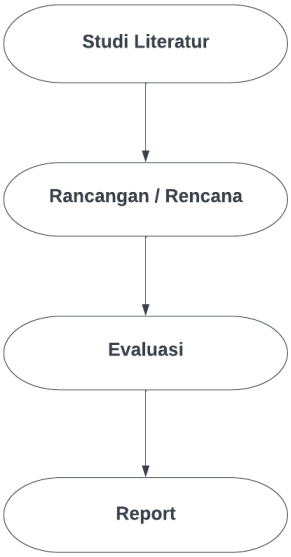
DDoS (*Distributed Denial of Service*) merupakan jenis serangan yang bertujuan mengganggu hak akses pengguna jaringan yang dilakukan secara massif [11]. Secara umum serangan

 ISSN 2686-3359 (Online)

DDoS terdiri dari beberapa jenis, serangan dengan basis bandwidth, serangan dengan basis lalu lintas jaringan, dan serangan dengan basis aplikasi.

Pengujian kerentanan bertujuan untuk mengetahui keamanan yang dimiliki oleh website tersebut dengan menggunakan metode penelitian terapan, dengan berfokus pada analisis evaluasi untuk bisa mendapatkan informasi sebagai masukan dan kritik serta mengambil keputusan tergantung tujuan urgensi. Pada pengujian kerentanan banyak serangan yang dilakukan untuk bisa masuk dan merusak sistem di dalamnyaserta mengambil informasi agar nantinya bisa mengetahui kerentanan pada website dan dapat mengatasi serangan yang masuk ke sistem dan dapat merusak sistem website. Dengan menggunakan metode penelitian terapan ini dapat membantu keamanan website tanpa membahayakan website yang di analisis.

METODE



Gambar 1. Diagram *Flowchart* Metode Penelitian

Dapat dilihat pada gambar 1, diagram flowchart yang digunakan pada penelitian ini. Pada penelitian ini metodologi yang digunakan secara garis besar menggunakan dua pendekatan, yaitu pendekatan proses forensik untuk menganalisa teknis keamanan website, menganalisa *tools* yang akan digunakan dan studi pustaka sebagai referensi kajian dan teori dalam melakukan terhadap tema penelitian yakni serangan DDoS.

Pada penelitian ini lingkungan yang ada adalah dua laptop dengan ram 4 GB , wifi dengan kecepatan 20 Mbps, menggunakan software VirtualBox dengan kali linux, dan dengan stopwatch. Dengan *tools* untuk melakukan serangan DDoS yaitu LOIC, HOIC, dan HULK pada kali linux.

Pada penelitian ini pengujian yang dilakukan adalah protokol yang digunakan, efektivitas, dan jumlah serangan.

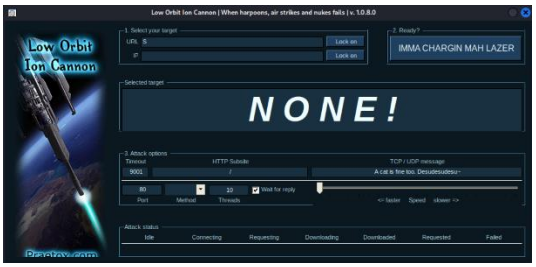
HASIL DAN PEMBAHASAN

Hasil penelitian ini berfokus pada perbandingan dari ketiga *tools* dari protokol yang digunakan untuk menyerang website dan efektivitas waktu yang dibutuhkan dalam proses serangan berhasil dilakukan.

A. LOIC

Tahapan Serangan

Serangan diawali dengan menginstall LOIC pada kali linux. Lakukan instalasi pada terminal. Setelah instalasi selesai dilakukan, maka akan muncul tampilan awal dari LOIC. Setelah itu masukkan alamat ip dari website yang dituju, atur port, treads, time out lalu simpan dengan klik Lock on, dan lakukan serangan dengan menekan "*IMMA CHARGIN MAH LAZER*".



Gambar 2. Tampilan Setelan LOIC

Pengujian atau Evaluasi

1. Melakukan Serangan

Serangan dilakukan dengan target website https://www.herminahospitalgroup.com dengan menggunakan *port* 80, *threads* 1000, dan *time out* sebanyak 9001. Simpan dengan menekan "Lock On" lalu lakukan serangan dengan menekan "IMMA CHARGIN MAH LAZER".

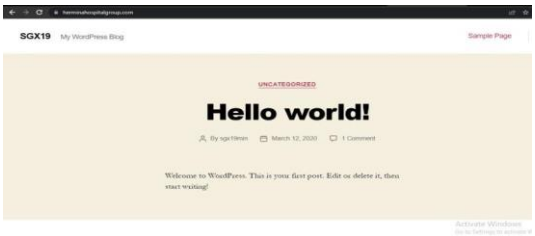
Gambar 3. Tampilan Proses Serangan LOIC

2. Hasil Serangan

Hasil dari serangan yang dilakukan terhadap website yang dituju adalah berhasil membuat website menjadi error dengan faktor utama yaitu permintaan spam (*requested*) yang berhasil dikirim sebanyak 24269880 *requested*. Banyaknya *requested* yang diterima oleh website membuat website tidak dapat diakses oleh pengguna. Berikut adalah tampilan awal website

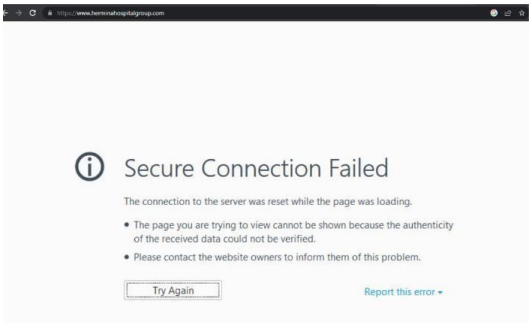
 ISSN 2686-3359 (Online)

https://www.herminahospitalgroup.com sebelum diserang oleh *tools* LOIC.



Gambar 4. Tampilan Website Sebelum Diserang

Berikut adalah tampilan website setelah dilakukan penyerangan.



Gambar 5. Tampilan Website Sesudah Diserang

B. HOIC

Tahapan Serangan

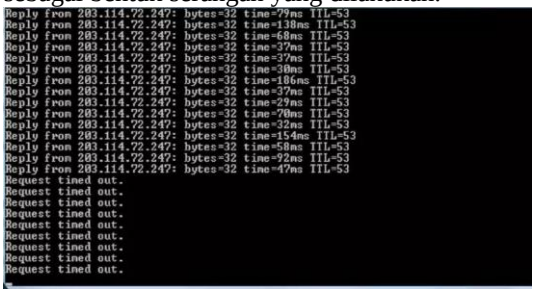
Serangan diawali dengan menginstall HOIC pada kali linux. Lakukan instalasi pada terminal. Setelah instalasi selesai dilakukan, maka akan muncul tampilan awal dari HOIC. Setelah itu masukkan berapa jumlah web yang akan diserang dengan menekan tombol tambah (+), setelah itu masukkan link url dari web yang akan dituju, sesuaikan parameter, lalu simpan dengan klik Add, dan lakukan serangan dengan menekan "*FIRE THE LAZER*!".

Gambar 6. Tampilan Proses Serangan HOIC

Pengujian atau Evaluasi

1. Melakukan Serangan

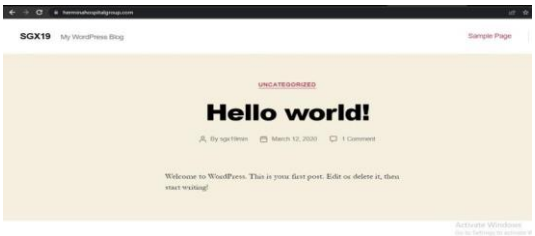
Serangan dilakukan dengan target website https://www.herminahospitalgroup.com/ dengan memasukkan 2 thread, mengatur power serta booster. Dengan status ready pada tampilan HOIC penyerangan sudah siap dilakukan dengan menekan "*Fire The Lazer*!" dan HOIC akan mengirim spam *request* ke system website sebagai bentuk serangan yang dilakukan.



Gambar 7. Tampilan Saat Mengirim *Request*

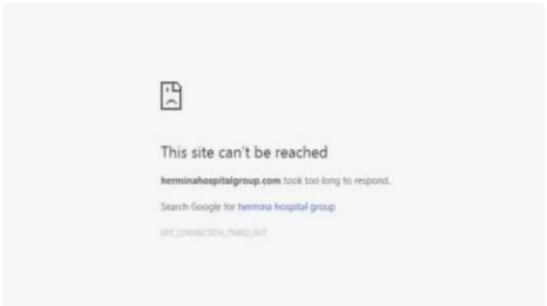
2. Hasil Serangan

Hasil dari serangan yang dilakukan terhadap website yang dituju adalah berhasil membuat website yang dituju tidak lagi dapat diakses oleh pengguna karena banyaknya spam yang diberikan kepada web sehingga web tersebut menjadi down. Berikut adalah tampilan awal *website* https://www.herminahospitalgroup.com/



Gambar 8. Tampilan Website Sebelum Diserang

Berikut adalah tampilan website setelah dilakukan penyerangan.



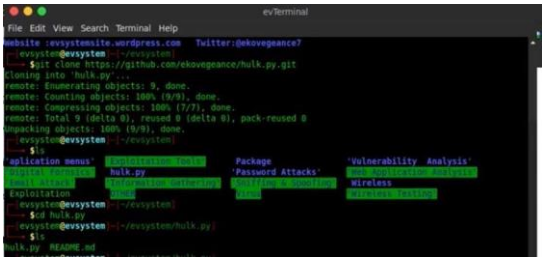
Gambar 9. Tampilan Website Sesudah Diserang

C. HULK

Tahapan Serangan

Serangan diawali dengan penggabungan *tools* HULK dengan mencantumkan script github ke kali linux. Apabila *tools* HULK sudah terhubung ke kali linux maka akan terbaca "hulk.py RAEDME.md".Serangan dilakukan dengan cara pemanggilan script $ sudo python hulk.py www.example.com dengan mengisi link website yang akan digunakan.

 ISSN 2686-3359 (Online)



Gambar 10. Tampilan Terminal Sudah Terhubung Dengan HULK

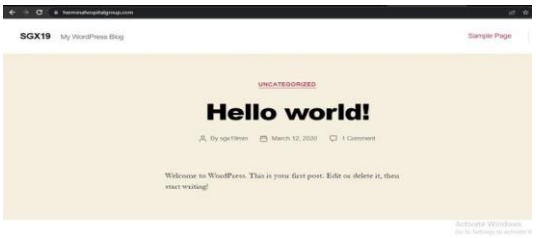
Pengujian atau Evaluasi

1. Melakukan Serangan

Serangan dilakukan dengan target website https://www.herminahospitalg roup.com/ dengan script $ sudo python hulk.py https://www.herminahospitalgroup.com/. Setelah penginputan script kedua beserta link website yang akan diserang, server akan mengirim response sebanyak mungkin dengan bertuliskan "Response Code 500". Pengujian dilakukan dengan RAM 4 GB. Skrip tersebut membuat server website korban berlutut dalam waktu <10 menit. Untuk pengujian ini, penyerang mengirimkan semua permintaan response dari host yang sama.

2. Hasil Serangan

Hasil dari serangan yang dilakukan terhadap website yang dituju adalah berhasil membuat website yang dituju tidak lagi dapat diakses oleh pengguna karena banyaknya *spam* yang diberikan kepada web sehingga web tersebut menjadi down. Berikut adalah tampilan awal *website* https://www.herminahospitalgroup.com/.



Gambar 11. Tampilan Website Sebelum Diserang

Berikut adalah tampilan website setelah dilakukan penyerangan,

Gambar 12. Tampilan *Website* Sesudah Diserang

Pembahasan

Berikut adalah tabel hasil dari perbandingan *tools* LOIC, HOIC ,dan HULK.

Tabel 1. Hasil Pengujian Ketiga *Tools*

Tools	Protokol	Efektivitas
LOIC	TCP	15 detik
HOIC	HTTP GET	60 detik
HULK	HTTP	600 Detik

Berdasarkan hasil yang diperoleh dari pengujian dari ketiga tools tersebut untuk menentukan tools yang paling efektif menggunakan parameter waktu yang paling singkat pada saat melakukan DDoS *Attack* di dapat oleh *tools* LOIC yang menggunakan protokol TCP.

KESIMPULAN DAN SARAN

Kesimpulan

Hasil pengujian menggunakan tiga *tools* serangan DDoS dapat disimpulkan bahwa kegunaan *tools* yang ada dapat disesuaikan dengan keperluan pengguna. Ketiga *tools* yang telah dibandingkan memiliki kelebihan dan kekurangan masing-masing. Dengan pengujian meretas website LOIC memiliki kelebihan yaitu dapat mengambil alih sebuah website dan dapat menjadi host sebuah website dengan waktu yang cukup singkat, sedangkan apabila pengguna ingin meretas banyak website secara sekaligus maka HOIC adalah pilihan yang tepat. Dengan Hulk pengguna dapat langsung menyerang website yang dituju langsung pada terminal tanpa harus masuk ke *tools* tersebut.

Saran

Saram dari kelompok kami dari hasil pengujian yang dilakukan dalam penggunaan ketiga *tools* ini harus digunakan berdasarkan kemampuan dam waktu yang dimiliki oleh user, dikarenakan jumlah efektivitas waktu yang diperlukan dan protokol yang digunakan oleh ketiga tools berbeda-beda. Seperti nusal jika ingin melakukan uji coba pemrosesan serangan diperlukan waktu yang singkat, bisa menggunakan *tools* LOIC.

DAFTAR PUSTAKA

[1] 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 Non 2, 2022)

[2] Hoda, M. N., Bharati Vidyapeeth's Institute of Computer Applications and Management (New Delhi, I., Institute of Electrical and Electronics Engineers. Delhi Section, & INDIAcom (Conference) (9th : 2015 : New Delhi, I. (n.d.). *2015 International*

 ISSN 2686-3359 (Online)

Conference on Computing for Sustainable Global Development (INDIACom) : 11th to 13th March, 2015, Bharati Vidyapeeth's Institute of Computers, Applications and Management (BVICAM). (diakses Nov 2, 2022)

[3] Lin, H., Cao, S., Wu, J., Cao, Z., & Wang, F. (2019). Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices. IEEE Access, 7, 164480–164491. https://doi.org/10.1109/ACCESS.2019.2950820 (diakses Nov 3, 2022)

[4] Faiz, M. N., Somantri, O., Supriyono, A. R., & Muhammad, A. W. (2022). Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review. JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING, 5(2), 305–314 .https://doi.org/10.31289/jite.v5i2.6112 (diakses Nov 4, 2022

[5] Elektronik, J., & Komputer Udayana, I. (2022). Klasifikasi Serangan Distributed Denial of Service (DDoS) Menggunakan Random Forest dengan CFS. Klasifikasi Serangan Distributed Denial of Service(DDoS) Menggunakan Random ForestdenganCFS, 11, 215–222. www.unb.ca. (diakses Nov 4, 2022)

[6] Pramana, M., Setyati, E., & Ferdinandus, F. X. (2021). Wahana : Tridarma Perguruan Tinggi Identifikasi Serangan Denial Of Service (Dos) Di Jaringan Dengan Algoritma Decision Tree C4.5. Identifikasi Serangan Denial Of Service (Dos) Di Jaringan Dengan Algoritma Decision Tree C4.5, 73(2). http://jurnal.unipasby.ac.id/index.php/whn (diakses Nov 4, 2022)

[7] Dody Firmansyah, M. (2021). Analisa Keamanan Web Server terhadap Serangan Distributed Denial of Service menggunakan Modevasive. TELCOMATICS, 6(1), 2541–5867. https://doi.org/10.37253/telcomatics.v6i1.4990 (diakses Nov 4, 2022)

[8] KRISTANTO. (2018). 05211440000186-Undergraduate_Thesis. ANALISIS FORENSIK JARINGAN TERHADAP SERANGAN DOS PADA SISTEM OPERASI UBUNTU SERVER 16.04 DAN MICROSOFT WINDOWS SERVER 2016. https://repository.its.ac.id/52606/ (diakses Nov 4, 2022)

[9] Adesty, I., Prabowo, W. A., & Sidiq, M. F. (2020). EasyChair Preprint Implementation of Intrusion Prevention System (IPS) as a Security from DDoS (Distributed Denial of Service) Attacks. https://easychair.org/publications/preprint/QLHW (diakses Nov 4, 2022)

[10] Mahjabin, S. (2018). Implementation of DoS and DDoS attacks on cloud servers. *Periodicals of Engineering and Natural Sciences*, *6*(2), 148–158. https://doi.org/10.21533/pen.v6i2.170 (diakses Nov 3, 2022)