KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 3, No 6, Juni 2023, Hal 1296-1302
DOI 10.30865/klik.v3i6.830
https://djournals.com/klik

Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)

Yunanri W[1,*], Yuliadi[1], Fahri Hamdani[1], Yasinta Bella Fitriana[2], Nabila Oper[3]

[1]Fakultas Rekayasa Sistem, Program Studi Informatika, Universitas Teknologi Sumbawa, Sumbawa, Indonesia
[2]Program Studi Ilmu Komputer, Universitas Muhammadiyah Papua, Jayapura, Indonesia
[3]Prodi. Informatika, Institute Teknologi & Bisnis Stikom Ambon, Ambon, Indonesia
Email: [1,*]yunanri.w@uts.ac.id, [2]yuliadi@uts.ac.id, [3]fahri.hamdani@uts.ac.id, [4]yasintabella13@gmail.com, [5]nabila.093@gmail.com
Email Penulis Korespondensi: yunanri.w@uts.ac.id

Abstrak-Universitas Teknologi Sumbawa adalah salah satu Perguruan Tinggi Swasta yang berada di Kabupaten Sumbawa, dalam pelayanannya Universitas Teknologi Sumbawa menyediakan informasi berupa website baik informasi pengenalan Universitas ataupun yang berkaitan dengan seputar perkuliahan. Penelitian ini bertujuan untuk menganalisa serangan DDoS pada website Universitas Teknologi Sumbawa. Serangan Distributed Denial of Service menjadi salah satu pilihan hacker karena telah terbukti menjadi ancaman didunia internet. Serangan DDoS dapat membuat suatu website menjadi lambat atau bahkan down. Pada penelitian ini melakukan pengujian serangan DDoS menggunkan Low Orbit Ion Cannon (LOIC) pada website kemudian menganalisa serangan DDoS dan memonitoring lalu lintas jaingan menggunakan wireshark. Hasil dari penelitian ini Website UTS meliki keamanan yang baik diketahu dari hasil pengujian serangan DDoS yang walaupun sudah dilakukan penyerangan dari 500, 1000,5000 hingga 10.000 Packet website masih tetap bisa diakses walaupun lambat. Rekomendasi keamanan website dengan menerapkann teknik blacklist IP dan firewall untuk mengantisipasi terjadinya serangan DDoS.

Kata Kunci: Analisis; Security; DDos; Attack; NIST

Abstract−Sumbawa University of Technology is one of the private tertiary institutions located in Sumbawa Regency. In its service, the Sumbawa University of Technology provides information in the form of a website, both university introduction information and related lectures. This study aims to analyze DDoS attacks on the Sumbawa University of Technology website. Distributed Denial of Service attacks are one of the choices of hackers because they have been proven to be a threat in the internet world. DDoS attacks can make a website slow or even down. This study tests DDoS attacks using Low Orbit Ion Cannon (LOIC) on websites then analyzes DDoS attacks and monitors network traffic using Wireshark. The results of this study show that the UTS website has good security, which is known from the results of testing DDoS attacks, even though attacks have been carried out from 500, 1000,5000 to 10,000 packets, the website can still be accessed, even though it is slow. Website security recommendations by implementing IP blacklist and firewall techniques to anticipate DDoS attacks.

Keywords: Analysis; Security; DDOS; Attack; NIST

1. PENDAHULUAN

Kemajuan dan perkembangan teknologi dibidang komputer saat ini begitu cepat, baik perangkat keras (hardware) maupun perangkat lunak (software) hal ini terlihat pada era teknologi informasi yang menjadi salah satu media yang banyak digunakan oleh semua orang, baik instansi atau perusahaan maupun organisasi. Salah satu media informasi yang efisien dan efektif saat ini biasanya berupa situs web (website), dimana semua informasi yang terdapat dalam website disimpan di webserver, sedangkan media yang digunakan untuk mengakses situs web (website) adalah internet[1][2][3]. Penggunaan sistem Informasi menjadi sebuah kewajiban bagi setiap individu maupun oraganisasi/ perusahaan. Namun dibalik kemudahan sistem yang ada, terdapat ancaman yang dapat menggangu keberadaan sistem sehingga dapat menyebabkan hilang data atau informasi, bahkan sampai terganggunya proses bisnis didalam suatu organisasi atau perusahaan. Karena hal tersebut Universitas Teknologi Sumbawa, tempat yang saat ini banyak digunakan di Indonesia dalam hal jasa pengiriman barang, Transfer uang masih banyak fitur yang digunakan secara online[4][5][6].

Hal ini bisa dijadikan niat jahat oleh para hacker atau peretas, yang dengan mudah membajak, merusak, dan mengedit data pada sebuah yayasan perguruan tinggi. Saat mengirim data dari klien keserver (atau sebaliknya), disinilah kemungkinan terjadi tindakan sniffing. Karena itu, ketika Anda mengirim data atau menerima data melalui koneksi Internet, Anda harus selalu waspada,tidak peduli apakah ada proses transmisi, apakah ada sniffer yang mencoba mencuri data. Sulit untuk dapat memeriksa apakah Anda adalah korban sniffer, tidak dapat dideteksi pada awalnya, itu hanya dapat dicegah[7][8]. Sniffing adalah bentuk cybercrime dimana pelaku mencuri username dan password orang lain secara sengaja maupun tidak sengaja. Pelaku kemudian dapat memakai akun korban untuk melakukan penupuan atas nama korban aatau meusak atau menghapus data milik korban[9][10][11]. Sering kali dilakukan dengan program sniffer yang berfungsi sebagai penganalisis jaringan dan berkerja untuk memonitor jaringan computer. Program tersebut mengatur kartu jaringan (LAN Card) untuk memonitor menangkal semua lalu lintas paket data yang melalui jaringan, tanpa mepedulikan kepada siapa paket data yang melalui jaringan, dan tanpa kepada siapa paket data tersebut dikirimkan[12].

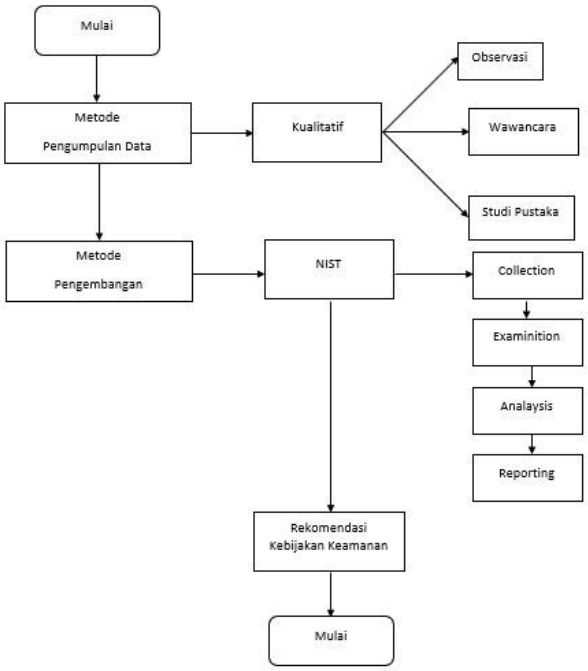
Internet sampai saat ini telah banyak digunakan dan menjadi media informasi yang pertumbuhannya sangat cepat tanpa terkendala ruang dan waktu. Salah satu bagian dari internet yang pertumbuhannya sangat cepat adalah World Wide Web. Berkaitan dengan perkembangan ini maka keamanan dalam sebuah website menjadi sangat penting mengingat website bisa diakes oleh siapapun yang terhubung ke internet. Jika mengabaikan keamanan tersebut maka tidak menutup kemungkinan orang yang tidak bertanggung jawab mengambil data-data penting atau bahkan menyerang sistem yang dapat membuat sistem menjadi down atau dikenal dengan serangan Distributed Denial of Service (DDoS)[13].

Universitas Teknologi Sumbawa merupakan salah satu Perguruan Tinggi Swasta yang berada di Kabupaten Sumbawa, tepatnya di jalan olat maras, Batu Alang, Kecamatan Moyo Hulu Kabupaten Sumbawa, Nusa tenggara Barat. Dalam pelayanannya Universitas Teknologi Sumbawa menyediakan informasi dalam sebuah website, baik informasi untuk pengenalan Universitas ataupun informasi yang berkaitan seputar perkuliahan. Ada beberapa website resmi yang dimiliki diantaranya website yang hanya bisa diakses oleh mahasiswa dan dosen menggunakan akun masing-masing yaitu SIAKAD dengan alamat website https://siakad.uts.ac.id dan ada juga website yang bisa di akses secara umum yaitu www.uts.ac.id. Tersedianya website sebagai media pelayanan untuk memberikan informasi maka akan memudahkan pelayanan kampus. Namun, mengingat website bisa diakses oleh umum atau siapapun yang terhubung ke internet dikhawatirkan pihak yang tidak bertanggung jawab mengambil data atau bahkan membuat website menjadi down dengan melakukan serangan DDoS[14].

Salah satu teknik untuk menguji keamanan suatu website adalah dengan dilakukannya pengujian serangan Distributed Denial Of Service (DDOS).. Berdasarkan penelitian yang dilakukan oleh pengujian serangan Distributed Denial of Service (DDoS) terhadap protocol TCP dan UDP pada sustu webserver diketahui ampuh untuk melumpuhkan suatu website, besarnya bandwidth dari sumber DDoS mempercepat suatu website target menjadi down[15].

2. METODOLOGI PENELITIAN

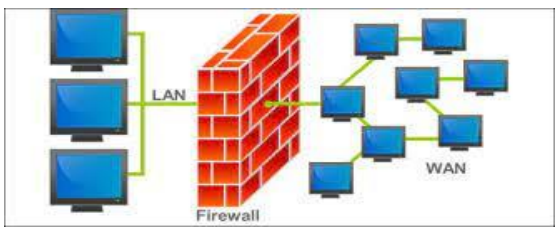
Metode penelitian menggunakan metode kualitatif yang merupakan penelitian yang mendeskripsikan suatu berdasarkan permasalahan yang akan diteliti. Adapun tahapan-tahapan yang akan dilakukan pada penelitian ini adalah sebagai berikut:



Gambar 1. Tahapan alur penelitian NIST.

Gambar 1. Menjelaskan metode yang digunakan baik untuk pengumpulan data dan metode pengembangan nya menggunakan metode National Institute of standards and Technology antara lain[16]:

a. Dimana tahapan terdiri dari Pengumpulan informasi atau data menggunakan metdoe kualitatif:
   1. Observasi
   2. Wawancara
   3. Studi Pustaka
b. Pengujian, pengujian yang dilakukan melakukan demo serangan terhadap website Universitas Teknologi Sumbawa berupa serangan Distributed Denial of Service (DDoS)



Gambar 2. Pengujian Serangan DDOS pada jaringan

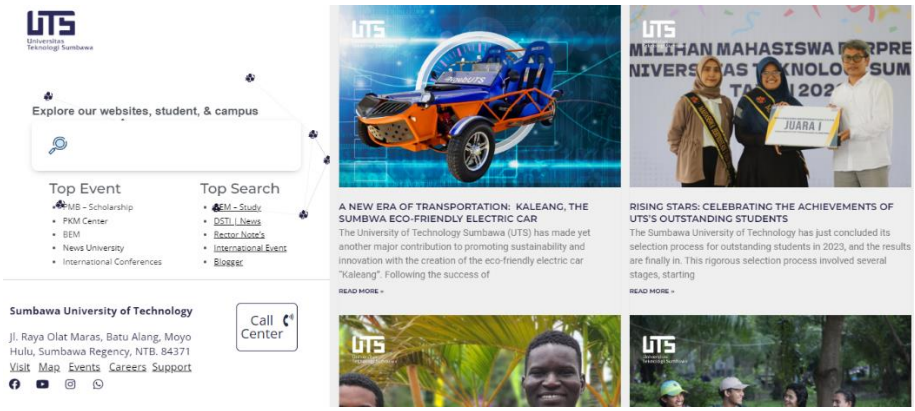
c. Melakukan Analisa dampak dari serangan oleh Distributed Denial of Service (DDoS)
d. Reportingan atau laporan akhir dari penelitian.

3. HASIL DAN PEMBAHASAN

Penelitian ini dilakuakan pada beebrapa framework yang bersifat open-source, baik menggunakan tool mau pun secara soure-code pada jaringam terminal, dimanan tujuan nya untuk menganalisa keamanan pada website Universitas Teknologi Sumabwa (UTS).

3.1 Collection

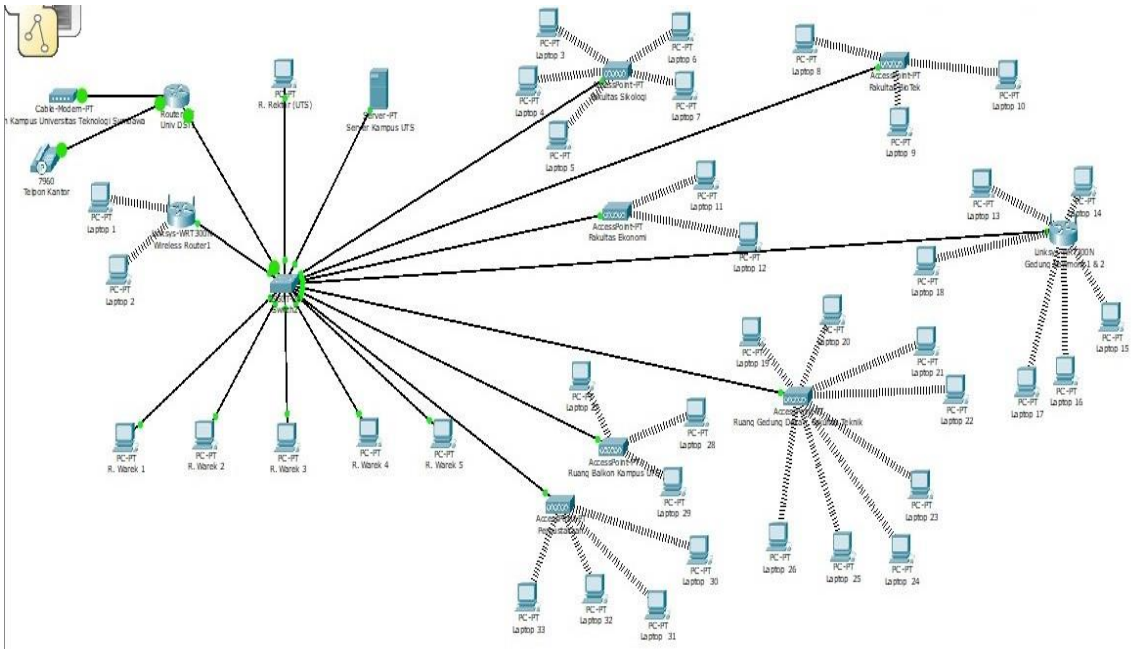
a. Skenario serangan pada Website Universitas Teknologi Sumbawa.



Gambar 3. Website Universitas Teknologi Sumbawa

Website Universitas Teknologi Sumbawa, merupakan wajah utama sebagai asset utama bagi kampus yang berfungsi sebagai pemberi informasi bagi masyarakat luas, berisi banyak informasi yang harus diuji tingkat keamanan apakah masuk dalam kategori bagus atau tidak bagus nya sebuah informasi ini. Pada website tersebut menyajikan berbagi informasi terkait Universitas Teknologi Sumbawa diantaranya akademik, riset, inovasi, penerimaan beasiswa, tentang kampus, berita serta tentang alumni.

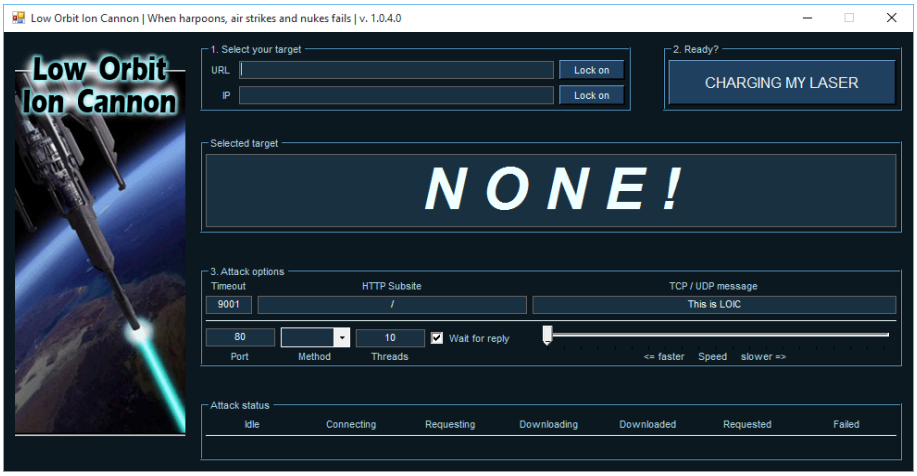
b. Infrastrukur Jaringan Berdasarkan Simulasi Sirangan:



Gambar 4. Jaringan Infrstuktur Univ silmulasi Serangan DDOS.

Gambar 4. Menejelaskan infrastruktut menjadi target serangan DDOS. Terdiri dari bebebrapa perangkat terkena dampak serangan low orbit ion cannon. Terdiri dari modem, switch atau hub terminal, mikrotik, server, router, perangkat admin, pc user 8 unit[17][18].

c. Tool pengujian menggunakan Low Orbit Ion Cannon



Gambar 5. Tool Low Orbit Ion Cannon

Loic Adalah Low Orbit Ion Cannon atau bisa disebut LOIC berfungsi untuk melumpuhkan server sebuah situs website. Terbukti komunitas hacker sekelas 'Anonymous' menggunakan tool loic ini untuk melancarkan aksinya. software Loic ini juga pernah melumpuhkan server facebook yang memiliki 60 server yang tersebar luas di seluruh dunia walau hanya beberapa menit[19][20].

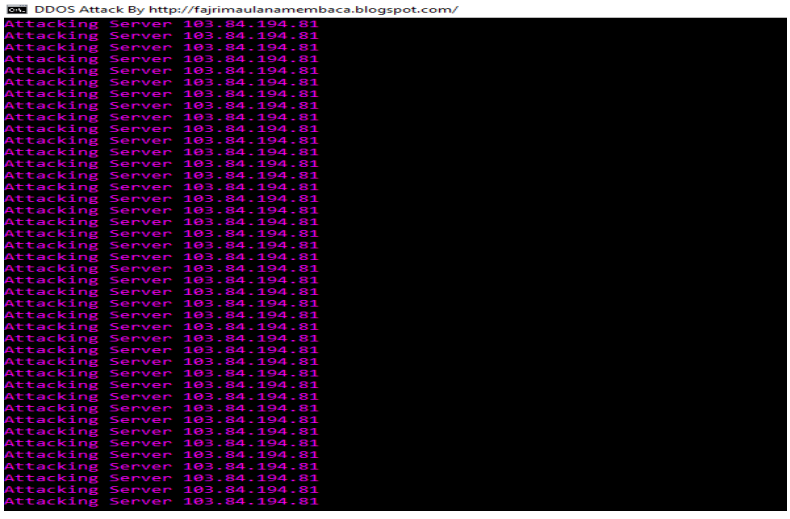
d. Pengujian ke 2 menggunakan sourcode pada terminal CMD pada windows 10.

Gambar 6. Serangan DDos menggunakan terminal Get pada CMD Windows 10.

DDos (Denial of Service Attack) adalah sebuah serangan yang melibatkan satu komputer atau satu jaringan. DDos berfungsi untuk membanjiri salah satu server atau website dengan paket ICMPT, TCP, UDP. Serangan ini bertujuan untuk membuat bandwith server atau web menjadi overload sehingga server atau web tidak bisa lagi menangulangi trafik yang masuk sampai akhirnya server atau web tersebut Down.

3.2 Examinition

Yaitu melakukan pemerosesan data secara digital forensic, menggunakan tool low orbit ion cannon (LOIC) untuk mengkobinasikan dari berbagai skenario dan menampilkan traffic jaringan.

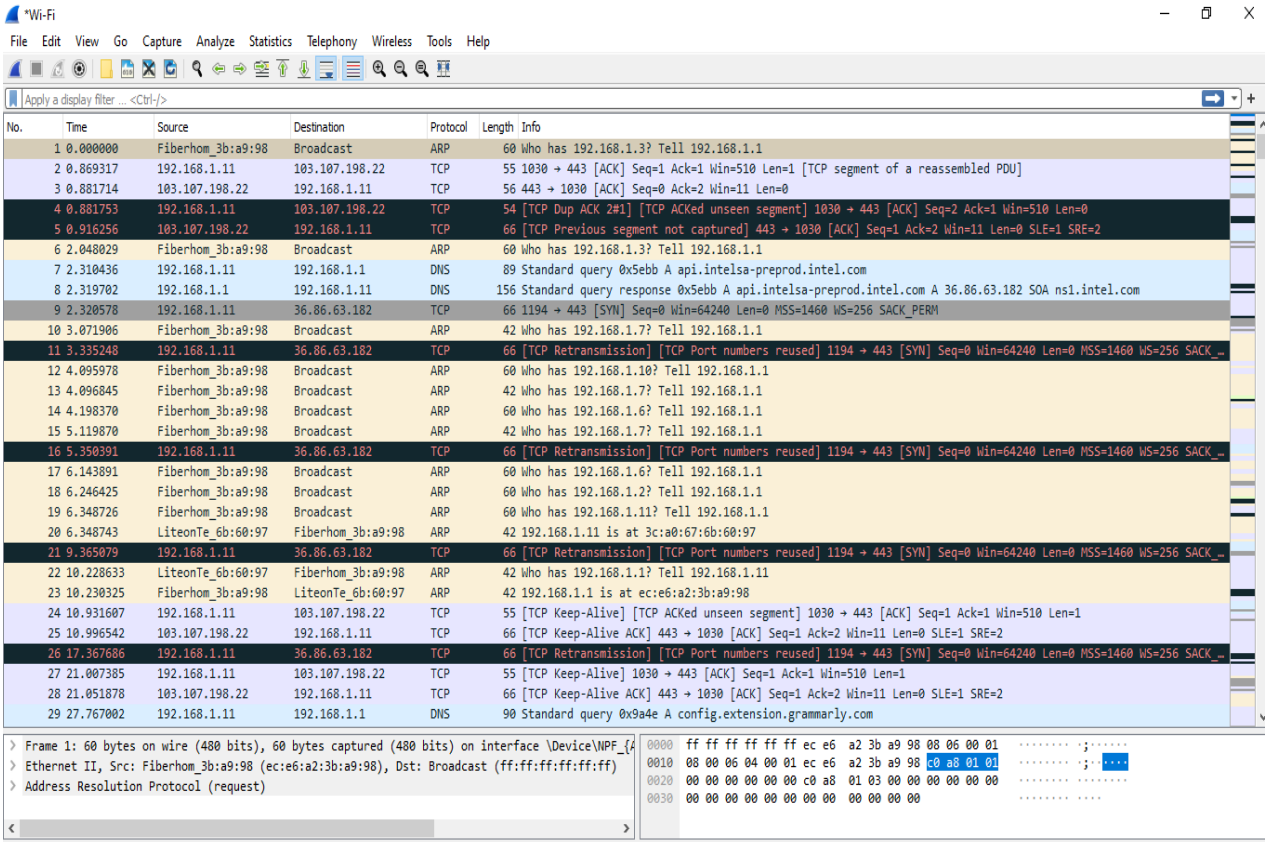


Gambar 7. Serangan DDos menggunakan terminal Get pada CMD Windows 10

3.3 Analysis

Berdasarkan hasil pengujian analisis keamanan website Universitas Teknologi Sumbawa dari serangan DDoS dengan mengirimkan 1000 packet, 5000 packet dan 10.000 packet kemudian dilakukan monitoring kondisi trafik website pada Low orbit Ion Cannon dan Terminal Get CMD pada Windows 10 (OS) didapatkan hasil sebelum dan sesudah serangan DDoS antara lain :

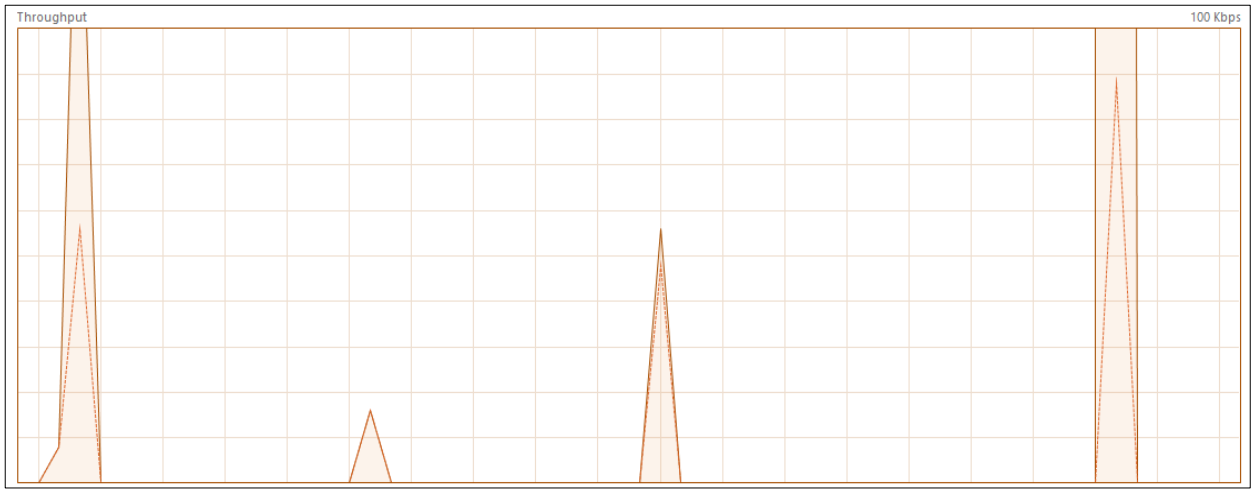
a. Wireshark



Gambar 8. Analisis pada Trafik network menggunakan Wireshark

Wireshark mendeteksi ada nya serangan DDos pada jaringan, memeberikan bebankerja lebih pada webserver sehingga dapat mengancap kelancaran Sebuah proses Browsing dan lain-lain nya.

b. Grafik monitoring.



Gambar 9. Analisis pada Trafik network menggunakan Wireshark

Dari gambar diatas dapat diketahui bahwa semakin besar jumlah packet yang dikirim, maka akan semakin lama proses request dari website tersebut. Selanjutnya dapat dilihat kondisi dari website facebook.com setelah dilakukan serangan DDoS berdasarkan quantity antara lain:

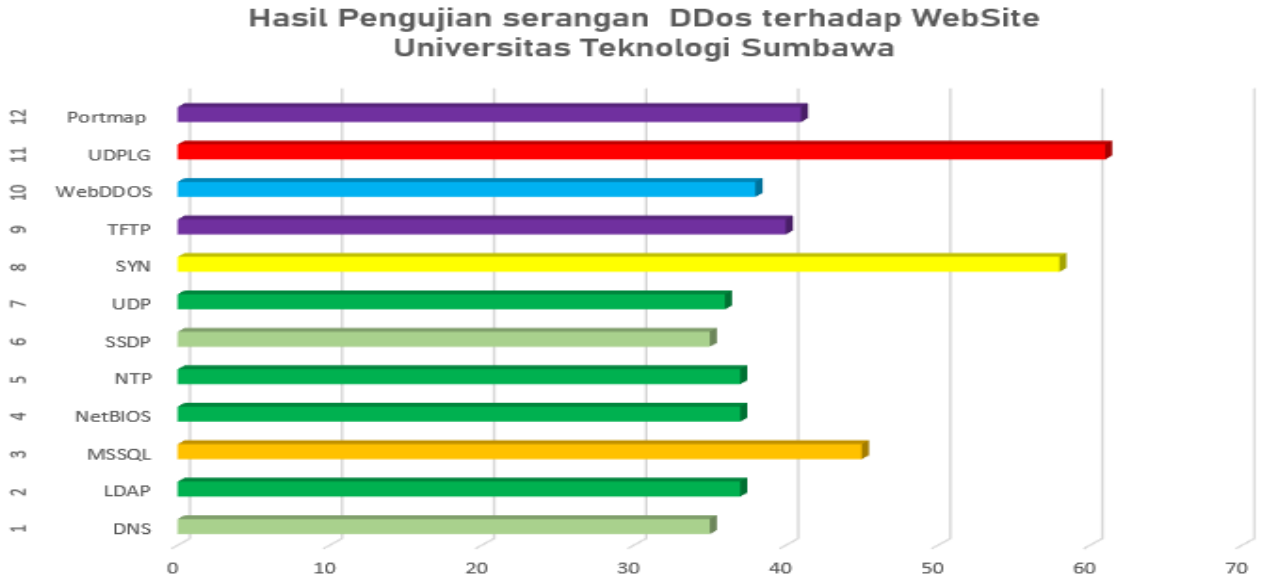
3.4 Reporting

Pengujian serangan DDoS yang dilakukan tidak sampai membuat website UTS down namun dari pengirimian packet 1000,5000 dan 10.000 packet membuat website menjadi lambat. Dikarenakan speed rata – rata sebelum serangan adalah 3 second dan setelah serangan adalah 40 second. Maka dapat disimpulkan bahwa keamanan website UTS sudah baik.

Tabel 1. Pengujian serangan DDOS terhadap Website Kampus UTS

No	Jumlah paket	Quantity Serangan	Reporting	
			Sebelum	Sesudah
1	500	10	3 sec	12 sec
2	1000	30	3 sec	30 sec
3	5000	70	3 sec	80 sec
4	10.000	90	3 sec	90 sec
	Rata-rata	55 Menit		50 Sec

Serangan pada seluruh infrastuktur jaringan memiliki rentang waktu 55 menit untuk demo serangan terdiri dari 4 jenis serangan yaitu : serangan 1. 500 paket requesting Flood, 2. 1000 paket request Flood, 3. paket request Flood 5000, 4. paket request Flood 10.000.



Gambar 10. Grafik Pengujian serangan DDOS pada kamus denga Low Orbit Ion Cannon

Serangan DDOS memeberikan Dampak Signifikan pada insfrastruktur serangan, serangan yang di lakukan oleh Tool Low Orbit Inon Cannon antara lain: Portmap, UDPLG, WebDDOS, TFTP, SYN, UDP, SSDP, NTP, NetBIOS, MSSQL, LDAP, DNS.

Gambar grafik 10 Menunjukan nilai parameter rate terhadap hasil akurasi dengan nilai paliang rendah 35 detik pada DNS, 35 detik SSDP, 36 detik UDP, 37 detik LDAP, NetBios, NTP, 40 detik TFTP, 41 detik Portmap, 58 detik SYN, 61 detik UDPLG. Di karenakan kelas serangan WebDDOS Unbalancing dataset. Pengujian disimpulkan jika learning rate set terlalu rendah maka akan melambat pada trafik jaringan dan jika serangan makin besar 10.000 paket request Flood makan server akan menanggung beban poros kerja harddrive loss system terganngu.

4. KESIMPULAN

Berdasarkan pengujian serangan DDoS dan analisis keamanan website dilakaukan, dapat disimpulkan bahwa, Pengujian menggunakan Low Orbit Ion Cannon (LOIC) untuk mengirim serangan packet dengan jumlah yang besar mampu membuat suatu website lambat. Semakin besar jumlah serangan yang dikirim oleh IP penyerang maka IP target akan semakin lambat. Dengan menggunakan pagespeedinsight dapat mengetahui speed dari website UTS sebelum dan sesusah dilakukakanya pengujian serangan DDoS. Website UTS meliki keamanan yang baik diketahu dari hasil pengujian serangan DDoS yang walaupun sudah dilakukan penyerangan dari 500, 1000,5000 hingga 10.000 Packet website masih tetap bisa diakses walaupun lambat. Rekomendasi keamanan website dengan menerapkann teknik blacklist IP dan firewall untuk mengantisipasi terjadinya serangan DDoS.

REFERENCES

[1] A. F. Khumara, A. Sediyono, and G. B. Santoso, “Analysis of DDoS Attack Detection Using Neural Network Backpropagation

Approach," CESS (Journal Comput. Eng. Syst. Sci., vol. 7, no. 1, p. 129, 2022, doi: 10.24114/cess.v7i1.27090.
[2] D. Kurnia, "Analisis Forensik Serangan SQL Injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal," InfoTekJar J. Nas. Inform. dan Teknol. Jar., vol. 4, no. 2, pp. 208–212, 2020, [Online]. Available: https://jurnal.uisu.ac.id/index.php/infotekjar/article/view/2420.
[3] J. Thome, L. K. Shar, D. Bianculli, and L. Briand, "An Integrated Approach for Effective Injection Vulnerability Analysis of Web Applications through Security Slicing and Hybrid Constraint Solving," IEEE Trans. Softw. Eng., vol. 46, no. 2, pp. 163–195, 2020, doi: 10.1109/TSE.2018.2844343.
[4] R. Umar and A. P. Marsaid, "Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing," vol. 10, no. 1, pp. 317–329, 2023, doi: 10.30865/jurikom.v10i1.5835.
[5] C. D. Berliana, T. A. Saputra, and I. Gunawan, "Analisis Serangan dan Keamanan pada Denial of Service (DOS): Sebuah Review Sistematik," JIIFKOM (Jurnal Ilm. Inform. Komputer) STTR Cepu, vol. 1, no. 2, pp. 33–38, 2022, [Online]. Available: https://www.sttrcepu.ac.id/jurnal/index.php/jiifkom/article/view/229/140.
[6] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," J. Sisfokom (Sistem Inf. dan Komputer), vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.
[7] S. K. Ajagekar and V. Jadhav, "Automated Approach for DDOS Attacks Detection Based on Naive Bayes Multinomial Classifier," Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018, pp. 1–5, 2018, doi: 10.1109/ICOEI.2018.8553848.
[8] M. Cirillo, M. Di Mauro, V. Matta, and M. Tambasco, "Application-layer DDoS attacks with multiple emulation dictionaries," ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc., vol. 2021-June, pp. 2610–2614, 2021, doi: 10.1109/ICASSP39728.2021.9413570.
[9] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput., vol. 21, no. 1, pp. 43–52, 2021, doi: 10.30812/matrik.v21i1.1078.
[10] R. Purba, W. S. Lestari, and M. Ulina, "Deteksi Serangan DDoS Mengunakan Deep Q-Network," J. Tek. Inform. dan Sist. Inf., vol. 9, no. 1, pp. 648–658, 2022, [Online]. Available: http://jurnal.mdp.ac.id.
[11] M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating Performance of Web Application Security through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective," IEEE Access, vol. 8, pp. 25543–25556, 2020, doi: 10.1109/ACCESS.2020.2970784.
[12] H. Lin, S. Cao, J. Wu, Z. Cao, and F. Wang, "Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices," IEEE Access, vol. 7, pp. 164480–164491, 2019, doi: 10.1109/ACCESS.2019.2950820.
[13] W. Meng, J. Lopez, S. Xu, C. Su, and R. Lu, "IEEE Access Special Section Editorial: Internet-of-Things Attacks and Defenses: Recent Advances and Challenges," IEEE Access, vol. 9, pp. 108846–108850, 2021, doi: 10.1109/ACCESS.2021.3101889.
[14] M. Zidane, "Klasifikasi Serangan Distributed Denial-Of-Service (DDOS) Menggunakan Metode Data Mining Naïve Bayes memperoleh gelar Sarjana Komputer Disusun oleh :," Univ. Brawijaya, vol. 6, no. 1, p. 63, 2021.
[15] T. Mahjabin, Y. Xiao, T. Li, and C. L. P. Chen, "Load Distributed and Benign-Bot Mitigation Methods for IoT DNS Flood Attacks," IEEE Internet Things J., vol. 7, no. 2, pp. 986–1000, 2020, doi: 10.1109/JIOT.2019.2947659.
[16] T. H. Damayanti and I. R. Hikmah, "Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF)," Edumatic J. Pendidik. Inform., vol. 6, no. 2, pp. 334–343, 2022, doi: 10.29408/edumatic.v6i2.6466.
[17] S. Dwiyatno, A. P. Sari, A. Irawan, and S. Safig, "PENDETEKSI SERANGAN DDoS (DISTRIBUTED DENIAL OF SERVICE) MENGGUNAKAN HONEYPOT DI PT. TORINI JAYA ABADI," J. Sist. Inf. dan Inform., vol. 2, no. 2, pp. 64–80, 2019, doi: 10.47080/simika.v2i2.606.
[18] M. H. Hawarizmi, M. T. Kurniawan, and M. Fathinuddin, "Sistem Deteksi Serangan Ddos pada Software Defined Network Menggunakan Metode Entropy," pp. 615–628.
[19] H. Shimamoto, N. Yanai, S. Okamura, J. P. Cruz, S. Ou, and T. Okubo, "Towards Further Formal Foundation of Web Security: Expression of Temporal Logic in Alloy and Its Application to a Security Model with Cache," IEEE Access, vol. 7, pp. 74941–74960, 2019, doi: 10.1109/ACCESS.2019.2920675.
[20] R. Sardar and T. Anees, "Web of Things: Security Challenges and Mechanisms," IEEE Access, vol. 9, pp. 31695–31711, 2021, doi: 10.1109/ACCESS.2021.3057655.