Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 7 No.6, Desember 2024
P-ISSN 2620-8342
E-ISSN 2621-3052

Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi

Tiara Aula Madina[1*], Mulkan Fadhli[2]
[1,2]Universitas Islam Negeri Ar-Raniry
[1,2]Jl.Syeikh Abdul Rauf Darussalam Kota Banda Aceh 23111
E-mail: 200212012@student.ar-raniry.ac.id[1*]

Submitted Date: 05 November 2024 ***Accepted Date: 11 November 2024***

Abstrak- Aktivitas belajar dan mengajar di Program Studi Pendidikan Teknologi Informasi, seperti pengajuan judul, uji plagiarisme, serta pendaftaran sidang dan seminar proposal, semuanya dilakukan melalui website. Tingginya tingkat akses harian dikhawatirkan dapat menyebabkan website mengalami down, yang tentunya akan menghambat proses belajar mengajar.Metode yang digunakan dalam penelitian ini adalah penetration testing untuk mengetahui celah yang ada pada website, dengan memanfaatkan tools Slowloris dan C2 sebagai alternatif untuk pengujian. Hasil dari pengujian menunjukanserangan DDoS dapat menyebabkan website mengalami *down* akibat kehabisan sumber daya. Dari percobaan yang telah dilakukan, terlihat bahwa website Program Studi Pendidikan Teknologi Informasi masih memiliki banyak celah keamanan. Oleh karena itu, penetrasi testing menjadi solusi yang sangat diperlukan. Disarankan juga agar website server PTI menambah kuota socket, memori, dan secara rutin melakukan uji penetrasi setiap bulan. Tindakan ini diharapkan dapat mencegah berbagai indikasi serangan keamanan jaringan, terutama serangan DDoS.
Kata kunci: Pendidikan Teknologi Informasi,DDoS,C2,Slowloris

Abstract- *Learning and teaching activities in the Information Technology Education Study Program, such as title submission, plagiarism testing, and registration for proposal trials and seminars, are all done through the website. The high level of daily access is feared to cause the website to go down, which of course will hinder the teaching and learning process. The method used in this study is penetration testing to find gaps in the website, by utilizing the Slowloris and C2 tools as alternatives for testing. The results of the test show that DDoS attacks can cause the website to go down due to running out of resources. From the experiments that have been carried out, it can be seen that the Information Technology Education Study Program website still has many security gaps. Therefore, penetration testing is a very necessary solution. It is also recommended that the PTI server website increase the socket quota, memory, and routinely conduct penetration tests every month. This action is expected to prevent various indications of network security attacks, especially DDoS attacks.*
Keywords: Information Technology Education, DDoS, C2, Slowloris

1. Pendahuluan

Dalam proses belajar mengajar di Program Studi Pendidikan Teknologi Informasi (PTI), website merupakan teknologi yang banyak digunakan oleh mahasiswa untuk mengakses informasi, seperti pengajuan judul, pendaftaran seminar, pendaftaran sidang, dan uji plagiarisme. Mengingat tingginya ketergantungan mahasiswa terhadap website tersebut, hal ini dapat memicu lonjakan trafik yang dikhawatirkan akan membuat website mengalami down. Oleh karena itu, perlu dilakukan pengujian untuk mengatasi masalah down pada website.

Penetration testing adalah solusi untuk mengidentifikasi kerentanan pada website, karena metode ini dapat mengevaluasi keamanan sistem. Hasil dari penetration testing sangat bermanfaat bagi pengelolaan sistem. Alat yang digunakan dalam penetration testing ini adalah tools C2 dan Slowloris untuk mengetahui ketahanan website. Selain itu, cara lain yang dapat digunakan untuk mendeteksi lonjakan trafik adalah dengan memonitor server website dan menganalisis log. Analisis terhadap website berguna untuk memahami jumlah lonjakan yang terjadi setiap hari, sehingga dapat dihasilkan kesimpulan mengenai permasalahan yang perlu ditangani [1].

Metode yang dipilih dalam penelitian ini adalah metode penetration testing, karena sangat menguntungkan dalam pengujian server dan nantinya dapat dilakukan pelaporan. Tujuan dari penelitian ini adalah untuk menguji ketahanan server website Program Studi Pendidikan Teknologi Informasi. Harapannya, penelitian ini

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 7 No.6, Desember 2024
P-ISSN 2620-8342
E-ISSN 2621-3052

dapat meningkatkan kinerja server website sehingga tercipta pengalaman pengguna yang baik bagi mahasiswa di program studi PTI.

2. Tinjauan Pustaka

2.1. Distributed Danial Of Service (DDoS)

Menurut Kaspersky DDoS adalah serangan yang dilakukan oleh hacker atau seorang pelaku cyber crime, berfungsi untuk membuat down suatu sistem.Yang mana dengan cara melakukan spam sehingga sever menjadi down total akibat banyaknya permintaan yang masuk [2].DDoS adalah sebuah serangan yang memiliki lebih dari satu alamat paket dan sering juga di samakan dengan serangan zombies,yang mana cara kerjanya dengan melakukan spam permintaan yang mana lebih bertujuan membuat sistem yang di serang sehabisan sumber daya[3].

Menurut *Computer emergency response Team* mengartikan DDoS sebagai sebuah serangan yang terfokus untuk menyerang bandwidth dengan banyaknya permintaan sehingga membuat sistemnya menjadi macet.Adapun menurut perusahahaan *sysmantec* yang bergerak pada cyber security berpendapat bahwa sanya DDoS adalah sebuah serangan yang di compromi oleh beberapa komputer yang digunakan untuk membanjiri sebuah situs agar menjadi down[4]

Dapat di simpulkan dari pengertian di atas bahwa sanya DDoS adalah sebuah virus yang mengangu sebuah website yang di akibatkan oleh traffic yang meningkat pada badwidth yang ada pada bagian download dan updatenya sehingga terjadinya penyerangan pada virtual privatenya sehingga mengakibatkan ketidak wajaran yang terjadi pada website sehingga membuat web itu down akibat banyaknya permintaan.

2.2. Penetrasion testing

Penetrasion testing adalah metode yang digunakan untuk mencari sebuah celah yang ada pada sebuah server yang nantinya dipergunakan sebuagai bahan evaluasi sistem keamanan yang ada pada website server.Pada metode ini nantinya akan menemukan kekurangan serta beberapa hal yang harus segera di pebaiki pada web server yang mana nantinya memungkinkan adanya ekploitasi data yang mana nanti akan digunakan untuk memeras korbannya[5].

Adapun tools yang digunakan dalam Penetrasion testing ini adalah sebagai berikut :1).Slowloris: Dalam penelitian ini kami mengunakan tools slowloris untuk menguji ketahanan website yang kami tujukan untuk menguji kerentanan dalam website dan menurut para ahli tools slowloris ini adalah sejenis tools yang menyerang lapisan aplikasi yang mengunakan reques HTTP yang sangat parsial untuk membuka koneksi antara komputer dan website servernya yang mana tools ini berusaha membuat web tetap terkoneksi sehingga membuat kinerja terbebani[6].2). Tools C&C menurut Github adalah sejenis tools yang menjadi sebuah media alat atau tehnik yang sering sekali digunakan untum menyerang sebuah website yang berfokus untuk melakukan eksploitasi awal.[7]

Dan biasana mekanisme spesifik cara pengunaanya sangat bervariasi antar serangan.Tapi biasanya umumnya terdiri dari satu atau lebih karena antar attacker itu saling berkomunikasi biasa untuk mengunduh muatan tambahan, biasanya juga menyerang pada layer 4 dan layer 7 sehingga tidak jarang rentan membuat website down.

3. Metode Penelitian

Metode yang digunakan pada penelitian ini adalah metode kualitatif yang mana berfokus untuk penganalisisan data.Yang mana hasilnya akan digunakan untuk pelaporan dan saran untuk server yang di teliti dan yang kedua metode yang digunakan adalah metode penetrasion testing yang mengunakan tools C2 dan Slowloris untuk menguji ketahanan website terhadap serangan DDoS [8].Adapun gambaran metode penelitiannya dapat di lihat pada gambar 1 berikut ini.

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 7 No.6, Desember 2024
P-ISSN 2620-8342
E-ISSN 2621-3052

Gambar 1. Metode Penelitian

4. Hasil dan Pembahasan

Monotoring Web server (Analisis *Traffic*) proses penelitian ini di mulai dengan mengumpulkan data log,yang ingin di uji untuk mengetahui jumlah *traffic* yang masuk setiap harinya.serta untuk mengetahui jumlah hari atau hari tertentu dengan akses yang lebih banyak.Agar dapat dengan mudah untuk mengolah data log yang di dapatkan perlu membuat semacam aplikasi bantuan untuk menganalisis data mulai dari tanggal 1 -25 Agustus 2024 dan melakukan pengambilan data pada log mulai dari hari senin sampai sabtu mulai dari jam 8.30 sampai dengan jam 16.40 wib.Seperti yang di tujukan pada gambar 2 di bawah ini.

Gambar 2. Log Server Prodi PTI

4.1.Monitoring website

Perancangan tahapan yang digunakan untuk pengaksesan log dengan mengunakan apache2 ,adapun tahapannya adalah sebagai berikut:

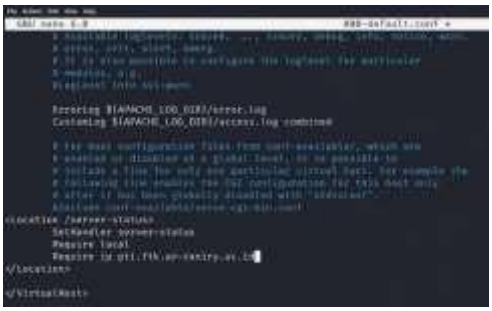
1. Penginstallan apache2

Untuk memudahkan proses pengaksesan log harus mengunakan apache2, sebagai alternatif yang akan digunakan yang mana kemudian membantu dalam membuat program yang bisa dilihat pada gambar di bawah ini.

Gambar 3. Penginstallan Apache2

Accredited SINTA 5
72/E/KPT/2024

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 7 No.6, Desember 2024
P-ISSN 2620-8342
E-ISSN 2621-3052



Gambar 4.Program Akses Log

Adapun setelah melakukan program untuk pengaksesan.dapat dilakukan alternative pengaksesan log dengan mengunakan debian bisa dengan mengunakan ip+ server-status atau bisa langsung dengan mengunakan http+server-status. Setelah itu lakukan pengaksesan pada log server website yang di tuju ,barulah bisa mangambil data untuk kemudian dilakukan penganalisisan data.Mengunakan program pendeteksi *traffic* untuk mengetahui hari dan tanggal dengan lonjakan permintaan pengaksesan tertinggi[9].Dari gambaran di atas bisa disimpulkan bahwa sanya mulai dari tanggal 1 sampai per-tanggal 25 ,tanggal dengan pengaksesan tertinggi adalah pada tanggal 10 Agustus 2024 yaitu dengan 14763 kali permintaan pengaksesan seperti yang di tujukan pada gambar di bawah ini.

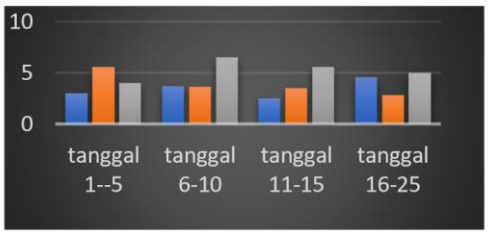
Gambar 5. Pembuatan Program Sites Enable

Gambar 6.Program Analisis *Traffic*

Gambar 7. Tanggal dengan *Traffic* Tertinggi

2. Diagram Barchart

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 7 No.6, Desember 2024
P-ISSN 2620-8342
E-ISSN 2621-3052



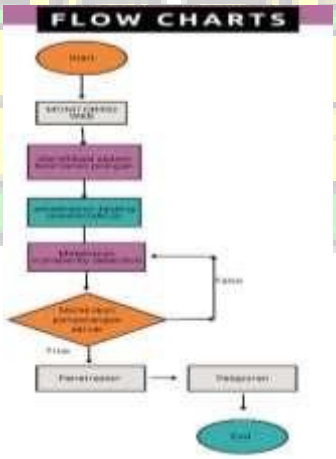
Gambar 8.Diagram Web Server

Gambar 9.Program Pendeteksi DDoS Pada Log

Diagram di atas ini adalah demontrasi data yang mendefinisikan pelonjakan – pelonjakan yang terjadi pe tanggal 1 sampai 25 dan dari log web server yang sudah analisis membuktikan bahwa sanya per-Agustus 2024 web server Prodi Pendidikan Teknologi Informasi sama sekali tidak mengalami serangan DDoS atau down akibat terlalu banyak permintaan akses ,berikut adalah hasil penganalisisan DDoS pada data log yang sudah di kumpulkan yang mana menghasilkan pernyataan bahwa sanya web server PTI aman pada bulan agustus 2024.Dan setelah penganalisis data tersebut dapat di simpulkan per Agustus Web server PTI dalam keadaan yang aman.Dapat dilihat dari pendeteksian DDoS dengan mengunakan program.Adapun demonstrasi programnya dapat di lihat pada gambar 9.

4.2Penetrasion Testing

Penetrasion testing adalah metode yang digunakan untuk mencari sebuah celah yang ada pada sebuah server yang nantinya dipergunakan sebagai bahan evaluasi sistem keamanan yang ada pada website server [10].Dalam pengertian lain penetrasion testing dapat di artikan sebagai proses evaluasi keamanan pada jaringan komputer yang mana aplikasi dengan mensimulasikan serangan yang jahat.[11]Dan di penelitian ini akan melakukan penyerangan mengunakan tools C2 dan juga slowloris , untuk di tahapan pertama akan mencoba dengan tools yang paling sederhana yaitu slowloris.Adapun flawchartnta dapat di lihat di gambar 10.



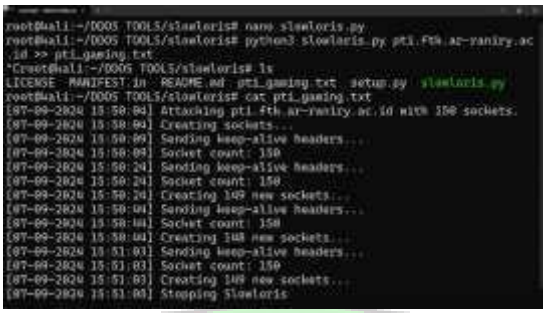
Gambar 10.Flowchart Penyerangan DDoS

1. Penyerangan Slowloris

Accredited SINTA 5
72/E/KPT/2024

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 7 No.6, Desember 2024
P-ISSN 2620-8342
E-ISSN 2621-3052

Pada bagian awal sebelum penyerangan harus memalakukan penginstallan pada tool yang gunakan dan kemudian setelah tools tersebut barulah akan di jalankan.dan gambaran penyerangan dapat di lihat pada gambar di bawah ini.

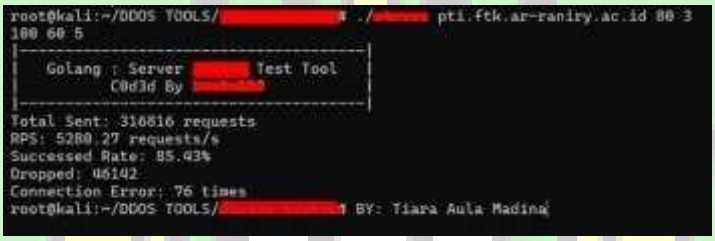


Gambar 11.Penyerangan Slowloris

Pada penyerangan ini web tidak mengalami down dikarekan web server PTI mengunakan fitur firewall[12].

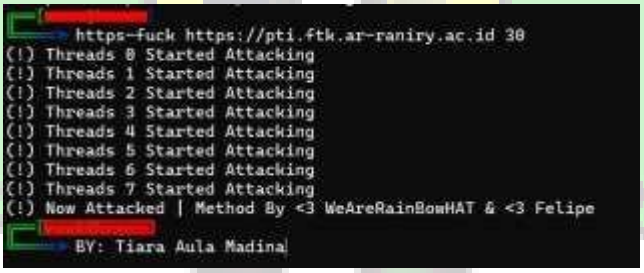
2. Serangan Tools C2

Pada fase penyerangan pertama mungkin web server memiliki ketahanan yang sangat bagus dan kemudian barulah memasuki tahapan kedua yaitu penyerangan mengunakan tools C2, dapat di lihat di gambar 12.



Gambar 12.Serangan Tools C2

Kemudian setelah semua program pada tools sudah siapkan maka barulah masuk ke tahapan *Attacking* (penyerangan) dan mengunakan metode Botnet sebagai alternatif agar ip saat penyerangan tidak terkena blok dan berikut adalah gambaran pengiriman serangan dengan mengunakan tools C2 dapat di lihat pada gambar di bawah ini.



Gambar 13.Pengiriman Serangan

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 7 No.6, Desember 2024
P-ISSN 2620-8342
E-ISSN 2621-3052

Gambar 14.Diagram Penyerangan

3. Cara Penanganan DDoS

Adapun tata cara yang biasanya digunakan untuk penanganan DDoS pada server website menurut BSSN Kepualauan Riau[13].Hal pertama yang harus dilakukan adalah tahap persiapan yang mana akan ada pembentukan Tim untuk mengumpulkan tenaga – tenaga prefisional untuk penanganan serangan DDoS,dan serta *leader* harus bisa memastikan bahwa sanya setiap anggota,dari tim semua sudah mengerti dengan memiliki skill yang mamandai.

Pada tahap kedua yang perlu dilakukan adalah pembangunan kontak ISP, yang mana pada pengunaan ISP ini tim akan berfokus pada pembagian tugas dalam penangulangan serangan.Kemudian yang ketiga pada tahap persiapan ini pemimpin tim harus mempersiapkan dokumen – dokumen izin sebagai sebagai perizinan untuk penangulangan masalah DDoS pada website yang terserang[14].Setelah melewati fase persiapan barulah masuk pada tahap identifikasi analisis yang memiliki tujuan untuk pengidentifikasi dan analisis.Di sini agar penyerang dapat memahami ruang lingkup serangan serta informasi mengenai serangan sehingga dapat mempermudah tim untuk saling berkoordinasi, sehingga akhirnya dapat memeriksa lalu lintas jaringan dan log yang tersedia.Kemudian masuklah ke tahap containment yang mana pada tahap ini bertujuan untuk meminimalisir dampak serangan pada server yang sudah di tergetkan ataupun menjadi korban.

Dan tahapan yang paling penting dalam penangulangan DDoS adalah eradication yang mana penanganan serangan DDoS yaitu mengambil tindakan untuk menghentikan kondisi *denial of service*. Tindakan ini sebagaian besar melibatkan peran ISP. Dengan melakukan pemblokiran jaringan ,filterisasi .Kemudian barulah masuk ke tahap pemulihan server website, tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Memahami karakteristik serangan diperlukan untuk pemulihan yang cepat dan tepat.Setelah memalui beberapa tahapan yang sudah di jelaskan barulah bisa di lakukan tinjak lanjut terhadap website yang terkena serangan biasanya pada tahapan tindak lanjut ini akan berisi berupa dokumentasi kegiatan yang dilakukan,yang mana akan di catat sebagai referensi pada masa mendatang [15].

5. Kesimpulan

Penelitian ini menunjukkan bahwa serangan DDoS dapat menyebabkan website mengalami downtime akibat kehabisan sumber daya. Dari percobaan yang telah dilakukan, terlihat bahwa website Program Studi Pendidikan Teknologi Informasi masih memiliki banyak celah keamanan. Oleh karena itu, penetrasi testing menjadi solusi yang sangat diperlukan. Disarankan juga agar website server PTI menambah kuota socket, memori, dan secara rutin melakukan uji penetrasi setiap bulan. Tindakan ini diharapkan dapat mencegah berbagai indikasi serangan keamanan jaringan, terutama serangan DDoS.

Daftar Pustaka

[1] Irfan Murti Raazi and others, ‘Analysis Server Security Assessment of Staffing Management Information System Using the NIST SP 800-115 Method at UIN Ar-Raniry Banda Aceh’, Circuit: Jurnal Ilmiah Pendidikan Teknik Elektro, 8.1 (2024), p. 46, doi:10.22373/crc.v8i1.20808

[2] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes,” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 6, no. 1, pp. 172–180, 2022, [Online]. Available: http://j-ptiik.ub.ac.id

[3] M. K. Harto and A. Basuki, “Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest,” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 5, no. 4, pp. 1329–1333, 2021, [Online]. Available: http://j-ptiik.ub.ac.id

[4] Future Plan and Contact Information, ‘ID-CERT Activity Annual Report 2011’, 3, 2011, pp. 1–12.

[5] Petkovic, M., Basicevic, I., Kukolj, D., & Popovic, M. (2015). Evaluation of Takagi-Sugeno-Kang Fuzzy Method in Entropy-based Detection of DDoS Attacks. Computer Science and Information Systems, 139162.

[6] F. Fachri, A. Fadlil, and I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” J. Inform., vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[7] Mulkan Fadhli, ‘Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends, Challenges, and Opportunities’, 4.June (2024), pp. 15–22.

[8] Yuliadi, Yuliadi, et al. "Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)." *KLIK: Kajian Ilmiah Informatika dan Komputer* 3.6 (2023): 1296-1302.
[9] Silalahi, Ulber, and Nurul Falah Atif. "Metode penelitian sosial kuantitatif." (2015).
[10] Zaen, Mohammad Taufan Asri, and Ahmad Tantoni. "Analisis dan Implementasi Pengalihan Trafik Data (Failover) Akses Internet Pada Dua ISP." *KLIK: Kajian Ilmiah Informatika dan Komputer* 4.3 (2023): 1726-1736.
[11] Pohan, Yosua Ade, Y. Yuhandri, and Sumijan Sumijan. "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar." *Jurnal Sistim Informasi dan Teknologi* (2021): 1-6.
[12] Pratiwi, Dheni Yulia Dinda, and Ronald Adrian. "Deteksi Dan Mitigasi Serangan Distributed Denial of Service Pada Software Defined Network." *Jurnal Teknik Informatika Dan Sistem Informasi* 10.1 (2024): 63-75.
[13] https://www.bssn.go.id/security-advisory/
[14] Razali, Mohd Onn Fikrie Mohd. "Perkhidmatan profiling pintar ISP (intelligent service profiling) pembangunan sistem berdasarkan web bagi menjana konfigurasi rangkaian." (2021).
[15] Setyaningrum, Ismayani. *Pengembangan Aplikasi Monitoring Keamanan Untuk Pengujian Celah Keamanan Aplikasi Laporan Pelaksanaan Anggaran Berbasis Website Dengan Standarisasi Owasp*. Diss. Universitas Komputer Indonesia, 2023.