Jurnal Teknik Informatika Vol. 20 no. 1 February 2025, pp. 39-50
p-ISSN : 2301-8364, e-ISSN : 2685-6131 , available at : https://ejournal.unsrat.ac.id/index.php/informatika

Vulnerability Analysis of Denial of Service Attacks on Sam Ratulangi University Website

Analisis Kerentanan terhadap Serangan Denial of Service pada Website Universitas Sam Ratulangi

Jovanka Daryl Ruindungan, Sherwin R. U. A. Sompie, Xaverius B. N. Najoan,
Dept. of Electrical Engineering, Sam Ratulangi University Manado, Kampus Bahu St., 95115, Indonesia
e-mails : jruindungan1@gmail.com, xnajoan@unsrat.ac.id, aldo@unsrat.ac.id
Received: 23 July 2024; revised: revised: 17 October 2024; accepted: 20 December 2024

Abstract* — *In the digital era, websites are crucial assets for Sam Ratulangi University (Universitas Sam Ratulangi). Dependence on the website for academic and administrative services makes it vulnerable to cyberattacks, particularly Denial of Service (DoS) attacks. This study analyzes the vulnerability of Universitas Sam Ratulangi's network to DoS attacks using log data from IBM QRadar SIEM CE and the university's internal logs.The findings indicate that Universitas Sam Ratulangi's monitoring system performs well with a very fast Mean Time to Detect (MTTD), namely 2 minutes 16 seconds on the webserver and 8 seconds on the firewall. According to SANS standards, this MTTD is considered good as it is significantly below the detection times of other organizations. The Peak Traffic Volume metric shows a significant traffic spike at 13:09:59, indicating a DoS attack and the need to strengthen the monitoring system. The Attack Distribution metric reveals targeted attacks using the TCP protocol, focusing on 'Entertainment' and 'Network' applications, and weaknesses in network segmentation and protection.Testing with Slowloris and TCP SYN Flood attacks successfully detected suspicious activities using IBM QRadar. Vulnerability analysis shows that the system can detect and withstand DoS attacks well, despite limitations in device specifications. This study provides insights into DoS threats and recommendations to enhance Universitas Sam Ratulangi's website security.

Key words—Sam Ratulangi University; DoS; IBM QRadar, Vulnerability Analysis

Abstrak* — Pada era digital saat ini, *website* merupakan aset penting bagi Universitas Sam Ratulangi (UNSRAT). Ketergantungan pada *website* untuk layanan akademik dan administratif menjadikannya rentan terhadap serangan siber, terutama serangan *Denial of Service* (DoS). Penelitian ini menganalisis kerentanan jaringan Universitas Sam Ratulangi terhadap serangan DoS menggunakan data *log* dari *IBM QRadar SIEM CE* dan *log* internal universitas.Hasil penelitian menunjukkan bahwa sistem pemantauan Universitas Sam Ratulangi memiliki performa baik dengan *Mean Time to Detect* (MTTD) yang sangat cepat, yaitu 2 menit 16 detik pada *webserver* dan 8 detik pada *firewall*. Berdasarkan standar *SANS*, MTTD ini tergolong baik karena jauh di bawah rata-rata waktu deteksi organisasi lain. Metrik *Peak Traffic Volume* menunjukkan lonjakan lalu lintas signifikan pada waktu tertentu, mengindikasikan serangan DoS dan perlunya penguatan sistem pemantauan. Metrik *Distribusi Serangan* menunjukkan serangan terarah dengan protokol TCP yang menargetkan aplikasi kategori 'Entertainment' dan 'Network', serta kelemahan dalam segmentasi dan perlindungan zona jaringan.Pengujian menggunakan serangan *Slowloris* dan *TCP SYN Flood* berhasil mendeteksi aktivitas mencurigakan dengan *IBM QRadar*. Analisis kerentanan menunjukkan bahwa sistem mampu mendeteksi dan menahan serangan DoS dengan baik, meskipun ada limitasi pada spesifikasi perangkat. Penelitian ini memberikan pemahaman tentang ancaman DoS dan rekomendasi untuk meningkatkan keamanan *Website* Universitas Sam Ratulangi.

***Kata kunci* — Analisis Kerentanan, DoS, IBM QRadar, Universitas Sam Ratulangi**

I. PENDAHULUAN

Pada era digital saat ini, *website* telah menjadi salah satu aset terpenting bagi institusi pendidikan seperti Universitas Sam Ratulangi. *Website* Universitas Sam Ratulangi tidak hanya berfungsi sebagai sumber informasi dan sarana komunikasi, tetapi juga mendukung berbagai layanan akademik dan administratif yang penting, seperti pendaftaran mahasiswa baru, pengumuman hasil ujian, dan sistem informasi akademik. Ketergantungan yang tinggi pada *website* ini membuat Universitas Sam Ratulangi rentan terhadap serangan siber yang dapat mengganggu kelancaran layanan dan merugikan reputasi universitas.

Salah satu ancaman siber yang serius adalah serangan *Denial of Service* (DoS), di mana penyerang membanjiri jaringan dengan lalu lintas palsu, sehingga membuat *website* dan layanan daring tidak dapat diakses oleh pengguna yang sah. Serangan DoS dapat melumpuhkan layanan penting, mengganggu kegiatan belajar mengajar, penelitian, dan administrasi, serta menyebabkan kerugian finansial dan merusak citra Universitas Sam Ratulangi sebagai institusi pendidikan yang modern dan dapat dipercaya.

Mengingat potensi dampak yang sangat merugikan dari serangan DoS, analisis kerentanan terhadap serangan ini menjadi sangat penting untuk dilakukan. Analisis kerentanan dapat membantu mengidentifikasi kelemahan dalam sistem keamanan jaringan Universitas Sam Ratulangi dan memberikan rekomendasi tindakan mitigasi yang tepat sebelum serangan terjadi. Dengan demikian, analisis kerentanan merupakan langkah proaktif yang krusial untuk melindungi *website* Universitas Sam Ratulangi dan memastikan kelangsungan layanan yang optimal.

Penelitian ini berfokus pada analisis kerentanan jaringan Universitas Sam Ratulangi terhadap serangan DoS. Dengan

memanfaatkan data *log* dari Pihak Universitas Sam Ratulangi, termasuk data dari *IBM QRadar SIEM CE* dan *log* internal universitas, penelitian ini bertujuan untuk mengidentifikasi pola serangan DoS, menemukan kerentanan yang dapat dieksploitasi oleh penyerang, dan memberikan rekomendasi tindakan yang efektif. Analisis komprehensif ini diharapkan dapat memberikan pemahaman yang lebih mendalam tentang ancaman DoS yang dihadapi Universitas Sam Ratulangi dan membantu dalam meningkatkan keamanan jaringan secara keseluruhan.

A. Penelitian Terkait

Penelitian yang dilakukan oleh Suharmanto et al. (2018) dalam jurnal "Analisis Keamanan Jaringan *Wireless* di Universitas Sam Ratulangi" menjelaskan tentang analisis keamanan jaringan nirkabel di Universitas Sam Ratulangi. Penelitian ini bertujuan untuk menguji dan mengevaluasi tingkat keamanan jaringan *wireless* di universitas tersebut terhadap berbagai jenis serangan siber, terutama serangan *Denial of Service* (DoS) dan *packet sniffing*.

Penelitian yang dilakukan oleh Arief et al. (2017) dalam jurnal "Implementasi Sistem Deteksi Serangan *Slowloris* pada Arsitektur Jaringan *Software-Defined Network* Menggunakan *Random Forest*" menjelaskan tentang implementasi sistem deteksi serangan *Slowloris*, salah satu jenis serangan *Denial of Service* (DoS), pada arsitektur jaringan *Software-Defined Network* (SDN) menggunakan algoritma *Random Forest*.

Penelitian yang dilakukan oleh Christoper & Hermawan (2024) dalam jurnal "Pemantauan dan Pengawasan Serangan Siber *SSH Brute Force* di Indonesia dengan *IBM QRadar Community Edition*" menjelaskan tentang pemantauan dan pengawasan serangan siber *SSH Brute Force* di Indonesia dengan menggunakan *IBM QRadar Community Edition*.

Penelitian yang dilakukan oleh Nida & Adrian (2023) dalam jurnal "Analisis Perbedaan Pengaruh Penggunaan *Iptables Chains* dalam Mencegah *Denial of Service* (DoS) pada Jaringan *IoT*" menjelaskan tentang analisis perbedaan pengaruh penggunaan *iptables chains* dalam mencegah serangan *Denial of Service* (DoS) pada jaringan *Internet of Things* (IoT).

Penelitian yang dilakukan oleh Setiawan & Setiyadi (2018) dalam jurnal "*Web Vulnerability Analysis and Implementation*" menjelaskan tentang analisis kerentanan (*vulnerability*) pada *web* dan implementasi perbaikannya. Jurnal ini membahas berbagai teknik dan cara penyerang melakukan serangan terhadap situs *web* di internet.

Penelitian yang dilakukan oleh Server et al. (2023) dalam jurnal "Analisis Hasil DoS *SYN Flood Attack* Pada *Webserver*" menjelaskan tentang simulasi dan analisis serangan *Denial of Service* (DoS) *SYN Flood* pada *web server*. Serangan DoS *SYN Flood* adalah jenis serangan siber yang bertujuan untuk melumpuhkan *server* dengan membanjiri *server* dengan permintaan koneksi palsu.

Penelitian yang dilakukan oleh Kamilah, Ritzkal, et al. (2019) dalam jurnal "Analisis Keamanan *Vulnerability* pada *Server* Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika" menjelaskan tentang analisis keamanan layanan *e-learning* Universitas Budi Luhur terhadap serangan *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS) serta implementasi mitigasi untuk meningkatkan ketahanannya.

Penelitian yang dilakukan oleh Delsi Samsumar & Gunawan (2017) dalam jurnal "Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (*Wireless LAN*); Studi Kasus Di Kampus STMIK Mataram" menjelaskan tentang analisis dan evaluasi tingkat keamanan jaringan komputer nirkabel (*Wireless LAN*) di kampus STMIK Mataram.

B. Denial Of Service

Denial of Service (DoS) adalah jenis serangan siber yang bertujuan untuk mengganggu atau menghentikan sementara layanan suatu jaringan, *server*, atau *website* dengan membanjiri target dengan lalu lintas atau permintaan yang berlebihan. Hal ini membuat sumber daya target habis atau kewalahan sehingga tidak dapat merespons permintaan yang sah dari pengguna.*Cyber Security*

C. Cybersecurity

Cybersecurity adalah praktik melindungi *sistem*, *jaringan*, dan *program* dari serangan digital. Serangan ini biasanya bertujuan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu operasi bisnis. *Cybersecurity* adalah elemen penting dalam melindungi informasi dan sistem dari berbagai ancaman digital. Dengan pemahaman yang baik tentang risiko dan praktik terbaik dalam keamanan siber, individu dan organisasi dapat mengurangi kerentanan dan meningkatkan kemampuan mereka untuk menghadapi ancaman yang terus berkembang.

D.Slowloris

Slowloris merupakan sebuah serangan *low-rate DoS* yang mengeksploitasi protokol HTTP dengan membangun sejumlah besar permintaan tertunda dengan *web server* yang ditargetkan. *Slowloris* bekerja dengan mengirimkan *HTTP request* yang sah ke *server web* dengan sangat lambat namun cukup cepat untuk membuat *server* tidak memutuskan koneksi. Hal ini memaksa *server* yang ditargetkan untuk menunggu akhir permintaan dalam waktu yang tidak terbatas karena *HTTP request* yang dikirimkan tidak lengkap.

E. TCP SYN Flood

TCP SYN Flood adalah jenis serangan *Denial of Service (DoS)* atau *Distributed Denial of Service (DoS)* yang bertujuan untuk membuat *server* atau layanan tidak tersedia bagi pengguna yang sah dengan cara membanjiri *server* tersebut dengan permintaan koneksi *TCP* yang tidak lengkap. Serangan ini mengeksploitasi proses *"three-way handshake"* yang digunakan untuk membangun koneksi *TCP*.

F. IBM QRadar SIEM CE

IBM QRadar SIEM (*Security Information and Event Management*) *Community Edition* (CE) adalah versi gratis dari platform *IBM QRadar SIEM* yang dirancang untuk digunakan oleh komunitas, termasuk individu, mahasiswa, dan organisasi kecil. *QRadar SIEM* adalah platform yang digunakan untuk mendeteksi ancaman keamanan, mengumpulkan dan

menganalisis *log* serta data peristiwa dari berbagai sumber di jaringan, dan memberikan wawasan yang berguna untuk meningkatkan keamanan.

G. VMWare Workstation Pro

VMware Workstation Pro adalah perangkat lunak virtualisasi yang memungkinkan pengguna untuk menjalankan beberapa sistem operasi secara bersamaan di satu komputer fisik. Dikembangkan oleh *VMware Inc.*, perangkat lunak ini sering digunakan oleh pengembang perangkat lunak, profesional TI, dan perusahaan untuk berbagai keperluan, termasuk pengujian, pengembangan, dan penyebaran aplikasi dalam lingkungan yang terisolasi.*VMware Workstation Pro* adalah alat yang sangat berguna untuk pengembangan perangkat lunak, pengujian, dan pelatihan, memungkinkan pengguna untuk menjalankan dan mengelola beberapa *VM* secara efektif di satu perangkat keras.

H. CentOS

CentOS (*Community Enterprise Operating System*) adalah sebuah sistem operasi *open-source* yang berbasis Linux. Dikembangkan oleh *CentOS Project*, sebuah komunitas pengembang independen, *CentOS* didasarkan pada kode sumber *Red Hat Enterprise Linux* (RHEL), namun tidak memerlukan biaya lisensi seperti RHEL. *CentOS* menawarkan fitur-fitur yang serupa dengan RHEL, termasuk stabilitas, keamanan, dan kompatibilitas dengan berbagai perangkat lunak.*CentOS* banyak digunakan sebagai sistem operasi untuk *server* karena kemampuan dan stabilitasnya dalam menjalankan aplikasi-aplikasi seperti *web server*, *database server*, dan lain-lain. Selain itu, *CentOS* juga populer di kalangan pengembang dan administrator sistem karena kemudahan penggunaan dan kemampuan kustomisasi yang luas.

I. Kali Linux

Kali Linux adalah sebuah sistem operasi (OS) *open-source* yang dirancang khusus untuk keperluan *hacking* dan pengujian penetrasi (*pentesting*) pada jaringan komputer. Dirilis pada tahun 2013 oleh *Offensive Security*, *Kali Linux* adalah turunan dari *Debian Linux* dan menjadi standar industri untuk pengujian penetrasi dan forensik digital. Sistem ini dilengkapi dengan lebih dari 600 alat *hacking* dan *pentesting* seperti *nmap*, *metasploit*, dan *aircrack-ng*, serta memiliki fokus pada keamanan dan privasi. *Kali Linux* dapat digunakan sebagai sistem operasi utama atau sebagai OS *live* pada USB atau CD.

J. Ngrok

Ngrok adalah alat dan layanan *tunneling* yang digunakan untuk membuat koneksi ke sumber daya lokal (seperti *server web* atau aplikasi yang berjalan di komputer Anda) menjadi dapat diakses melalui internet. Ini memberikan kemampuan untuk membuat sumber daya yang sebelumnya hanya dapat diakses secara lokal menjadi dapat diakses dari mana saja di internet, bahkan melalui *firewall* dan jaringan yang diatur secara ketat.

K. Python

Python adalah bahasa pemrograman tujuan umum yang ditafsirkan, tingkat tinggi. Dibuat oleh Guido van Rossum dan pertama kali dirilis pada tahun 1991, filosofi desain *Python* menekankan keterbacaan kode dengan penggunaan spasi putih yang signifikan. Konstruksi bahasanya danpendekatan berorientasi objek bertujuan untuk membantu pemrogram menulis kode yang jelas dan logis untuk proyek skala kecil dan besar. *Python* diketik secara dinamis dan *garbage collection*. Ini mendukung beberapa paradigma pemrograman, termasuk pemrograman terstruktur (terutama, prosedural), berorientasi objek, dan fungsional. *Python* sering dideskripsikan sebagai bahasa "termasuk baterai" karena perpustakaan standarnya yang komprehensif.

L. Website

Website merujuk pada suatu kumpulan halaman web yang saling terhubung dan memiliki keterkaitan antar file-filenya. Konsep website adalah fasilitas internet yang menghubungkan dokumen dalam cakupan lokal maupun jarak jauh. Dokumen di dalam website disebut sebagai web page, dan hyperlink dalam website memungkinkan pengguna untuk berpindah dari satu halaman ke halaman lainnya, baik di antara halaman yang disimpan dalam server yang sama maupun server di seluruh dunia. Halaman-halaman tersebut diakses dan dibaca melalui peramban web seperti Netscape Navigator, Internet Explorer, Mozilla Firefox, Google Chrome, dan aplikasi peramban lainnya.

M. Universitas Sam Ratulangi

Universitas Sam Ratulangi sering disingkat dengan sebutan UNIVERSITAS SAM RATULANGI adalah salah satu Perguruan Tinggi Negeri di Indonesia yang berlokasi di Kota Manado, Provinsi Sulawesi Utara. Universitas Sam Ratulangi dipimpin oleh seorang Rektor Universitas Sam Ratulangi yang sekarang adalah Prof. Dr. Ir. Octovian Berty Alexander Sompie, M.Eng, IPU.

II. METODE

A. Tempat dan Waktu Penelitian

Penelitian ini dilakukan di Jurusan Teknik Program Studi Teknik Informatika,Fakultas Teknik dan UPT TIK Universitas Sam Ratulangi . Penelitian ini dilaksanakan mulai bulan Maret 2024 sampai Juli 2024.

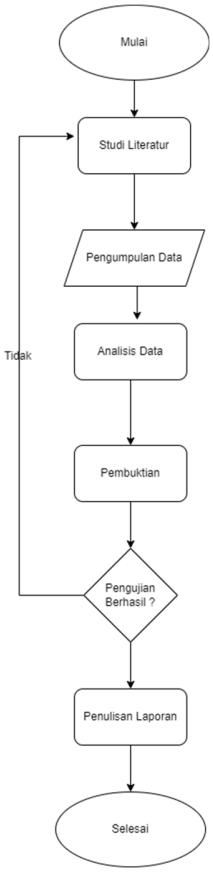
B. Prosedur Pengembangan Penelitian

Penelitian yang dilakukan akan melewati beberapa tahap, menggunakan metode penelitian Kualitatif. Tahap dalam metode Kualitatif adalah Sebagai Berikut :

1) Studi Literatur.
   Pada langkah ini, peneliti melakukan Studi Literatur Dimana pada tahap ini kita melakukan tahap tahap analisis apa yang perlu digunakan dan apa saja yang akan dilakukan nanti.
2) Pengumpulan data.
   Data yang dikumpulkan dalam studi kasus kualitatif biasanya berupa data nonnumerik, seperti teks, gambar, atau video. Data ini dikumpulkan melalui metode seperti

wawancara, observasi, atau analisis dokumen.

3) Analisis data.
   Data yang dikumpulkan kemudian dianalisis untuk memahami fenomena yang diteliti. Analisis data kualitatif dapat dilakukan secara induktif atau deduktif.
4) Pembuktian.
   Hasil analisis data kemudian dibuktikan dengan menggunakan teori atau bukti lain.
5) Penulisan laporan.
   Laporan penelitian kemudian ditulis untuk menyajikan hasil penelitian. Laporan penelitian harus mencakup penjelasan tentang topik, tujuan, metodologi, hasil, dan kesimpulan penelitian.



Gambar 1. Prosedur Penelitian

C. Alur Kerja Penelitian untuk Pengujian di CentOS

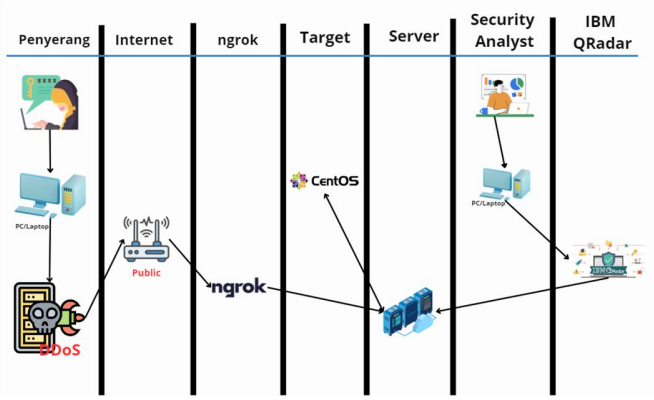
Alur perancangan untuk Pengujian dan Implentasi Sistem *Monitoring* dapat dijelaskan bahwa langkah-langkah yang akan dilakukan dalam penelitian ini adalah sebagai berikut:

1) Penyerang dan Analis melalui *VMWare* sebagai portal penyedia layanan melakukan virtualisasi server. Ini memungkinkan untuk menjalankan beberapa mesin virtual(VM) pada satu fisik *server,* meningkatkan efisiensi penggunaan sumber daya dan fleksibilitas dalam manajemen infrastruktur *IT.*
2) Menjalankan *Virtual Machine (VM)* dengan OS *CentOS* atau VM *CentOS* yang merujuk kepada sebuah mesin virtual yang menjalankan sistem operasi *CentOS.* *CentOS* adalah distribusi Linux yang berbasis pada kode sumber *Red Hat Enterprise Linux* (RHEL) yang umum digunakan dalam lingkungan *server* Analisis Data.
3) Penyerang masuk melalui Portal *SSH.*
4) Penyerang melakukan konfigurasi IP *CentOS* agar menjadi publik menggunakan *NGROK.*
5) Penyerang memulai penyerangan DoS dengan *Python.*
6) Analis membuat *Rules*(Aturan) untuk mendeteksi adanya penyerangan melalui IBM Qradar.
7) Analis melakukan *monitoring* masuknya peringatan melalui log IBM QRadar sesuai dengan *Rules* yang sudah dibuat sebelumnya.

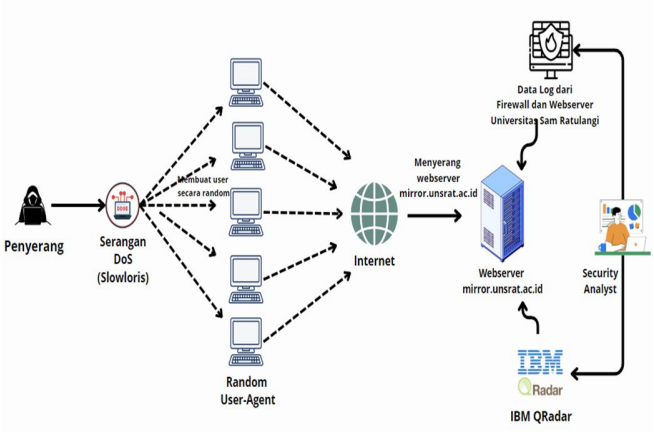
D.Alur Kerja Penelitian untuk Pengujian serta Analisis Kerentanan di Website UNIVERSITAS SAM RATULANGI(mirror.Universitas Sam Ratulangi.ac.id)

Alur Rancangan seperti ditunjukan dapat dijelaskan bahwa langkah-langkah yang akan dilakukan dalam penelitian ini adalah sebagai berikut:

1) Penyerang dan Analis melalui *VMWare* sebagai portal penyedia layanan melakukan virtualisasi *server.* Ini memungkinkan untuk menjalankan beberapa mesin virtual(VM) pada satu fisik *server*, meningkatkan efisiensi penggunaan sumber daya dan fleksibilitas dalam manajemen infrastruktur IT.
2) Menjalankan *Virtual Machine (VM)* dengan Sistem Operasi *Kali Linux* yang merujuk kepada sebuah mesin virtual yang menjalankan Sistem Operasi *Kali Linux.*
3) Penyerang memulai penyerangan DoS dengan diawali dengan membuka *Kali Linux* dan Memulai Serangan DoS menggunakan Jenis Serangan yaitu *Slowloris.*
4) Analis membuat *Rules*(Aturan) untuk mendeteksi adanya penyerangan melalui *IBM Qradar.*
5) Analis melakukan monitoring masuknya peringatan melalui log *IBM QRadar* sesuai dengan *Rules* yang sudah dibuat sebelumnya dengan mengecek *Network Activity, Log Activity* dan *Event* atau *Flow Rules* yang *ter-trigger*
6) Untuk *Log* Serangan yang akan dilakukan Analisis Kerentanan dari Pihak Universitas Sam Ratulangi akan diambil Data *Log* dari *Firewall* dan *Webserver mirror.unsrat.ac.id.*



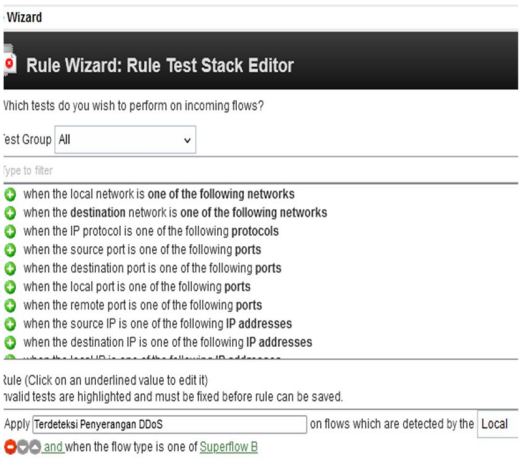
Gambar 2. Alur Kerja Peniltian untuk *Target CentOS*



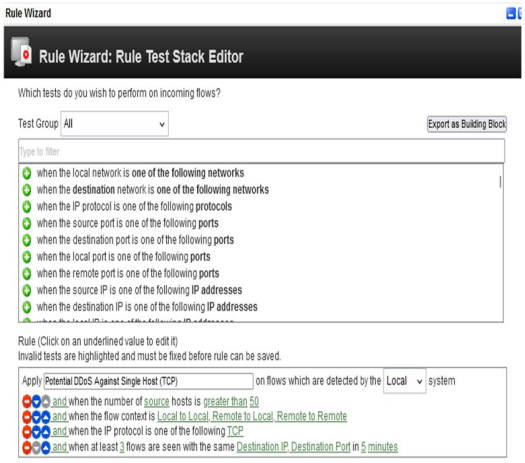
Gambar 3. Alur Kerja Peneltian untuk *Target Website* Universitas Sam Ratulangi(mirror.unsrat.ac.id)

E. Pembuatan Rules untuk Mendeteksi Serangan di IBM QRadar

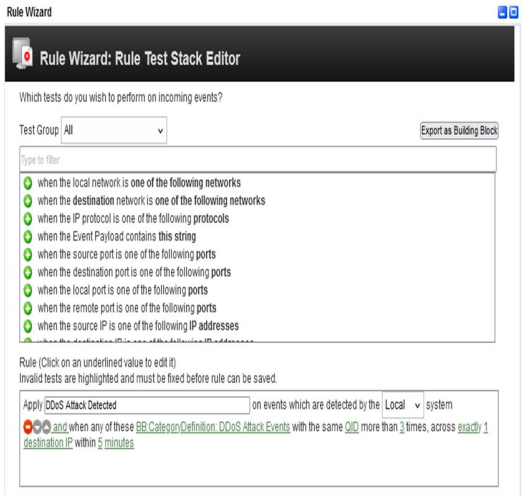
Pembuatan *rules* dalam *IBM QRadar CE* adalah proses mendefinisikan serangkaian kondisi dan tindakan yang akan diambil oleh sistem ketika kondisi tersebut terpenuhi. *Rules* ini digunakan untuk mendeteksi dan merespons berbagai jenis ancaman keamanan, termasuk serangan DoS.



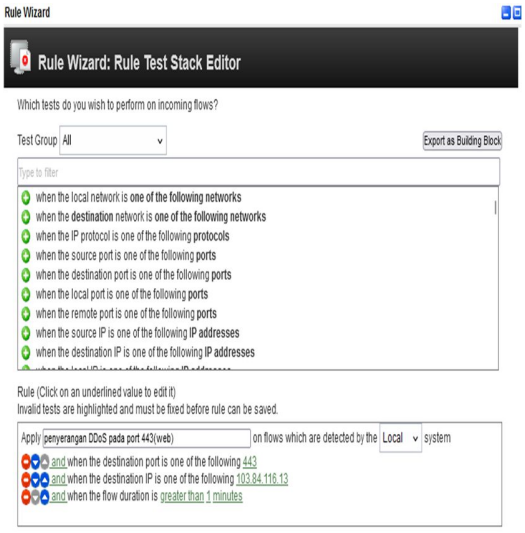
Gambar 4. Pembuatan Rules Terdeteksi Penyerangan DoS



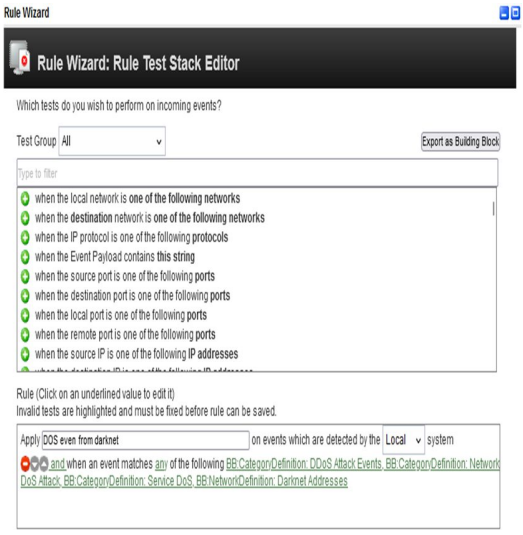
Gambar 5. Pembuatan Rules Potential DoS Againts Single Host(TCP)



Gambar 6. Pembuatan Rules penyerangan DoS Attack Detected



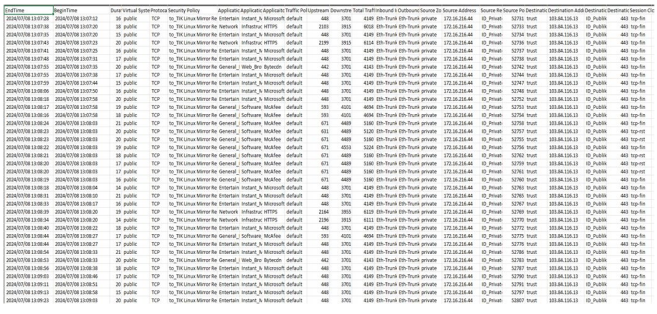
Gambar 7. Pembuatan Rules penyerangan DoS pada port 443(web)



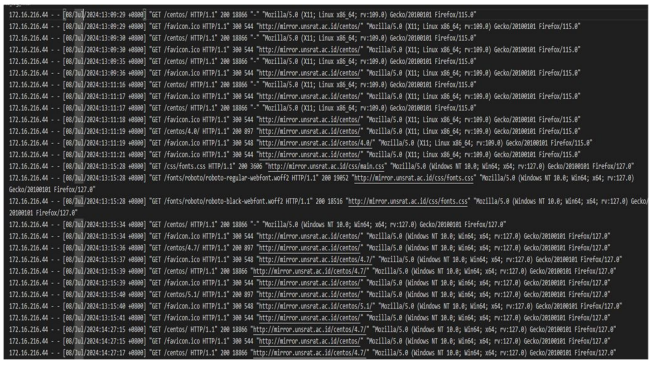
Gambar 8. Pembuatan Rules DoS even from darknet

F. Data Log untuk Analisis Kerentanan dari pihak *Universitas Sam Ratulangi*

Untuk Data yang akan digunakan untuk melakukan Analisis kerentanan dari pihak Universitas Sam Ratulangi yaitu ada *Data Log* dari *Firewall* dan *Webserver* dari *mirror.unsrat.ac.id.*



Gambar 9. *Log* dari *Firewall*

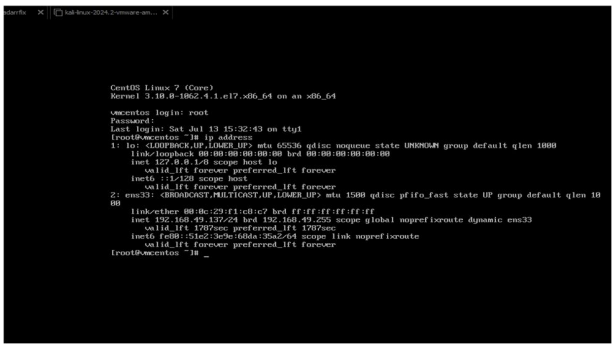


Gambar 10. *Log* dari *Webserver*

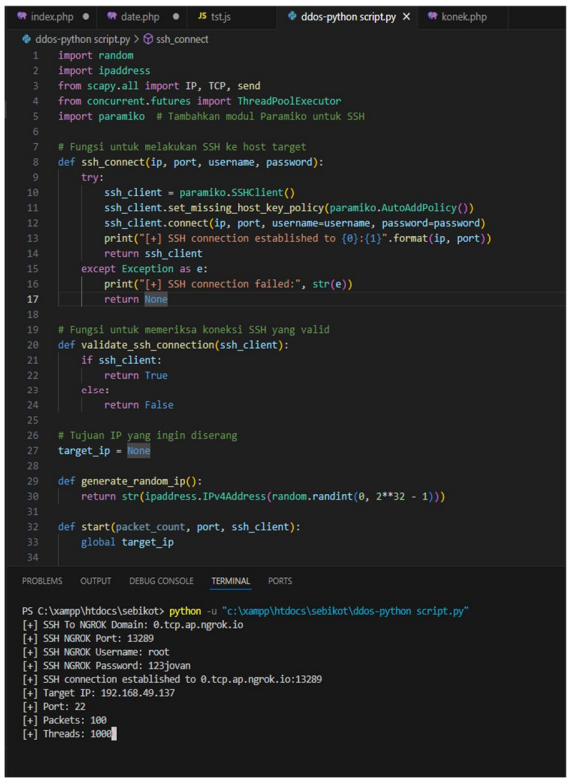
III. HASIL DAN PEMBAHASAN

A. Implementasi pengujian untuk target Sistem Operasi CentOS

Serangan dilakukan dengan menggunakan *TCP SYN Flood* yang digunakan untuk menyerang. *TCP SYN Flood* adalah serangan pertama yang dilakukan untuk melakukan pengujian ke *CentOS* yang dijadikan target penyerangan diawali dengan *SSH* ke bagian penyerang lalu dilanjutkan dengan memasukkan *NGROK port* penyerang, *username* dan *password* penyerang. Setelah *SSH* sudah terkoneksi, dilanjutkan dengan memasukkan target *IP Address* yang akan di serang lalu untuk *port* yang diserang *22* lalu dilanjutkan dengan mengirimkan dengan memasukkan jumlah *Packet* dan *Threads* seperti yang ditentukan.

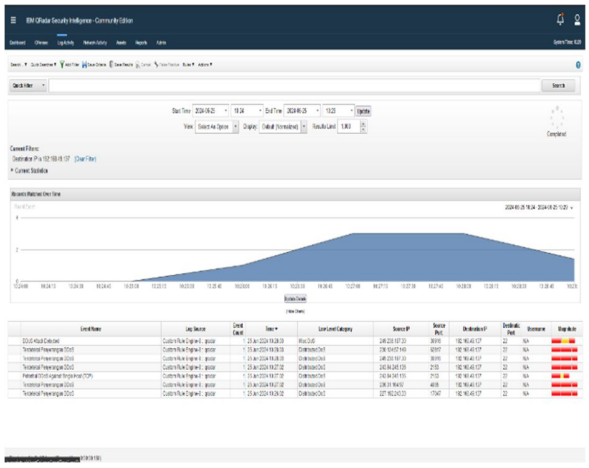


Gambar 11. Tampilan CentOS



Gambar 12. Serangan *DoS* untuk pengujian di CentOS

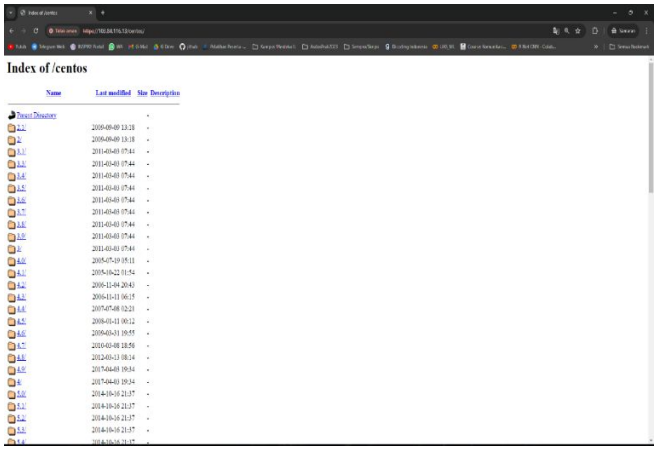
Melakukan *Filter* di *Log Activity* Berdasarkan *Default* kurang dari 15 menit dan seperti yang tertera di Gambar 12 *Log Activity IBM QRadar* ketika mendeteksi serangan *DoS*. terdeteksi 3 *Event Name* yang terdeteksi yaitu *Terdeteksi Penyerangan DoS, DoS Attack Detected dan Potential DoS againts Single Hosts (TCP)*.Lalu disitu juga seperti di gambar ada *Log Source, Event Count, Time, Low Level Category Distributed DoS dan Misc DoS, Source IP, Source Port, Destination IP, Destination Port,Username* dan *Magnitude* berwarna Merah yang menunjukan bahwa *offense* memiliki tingkat keparahan tinggi.



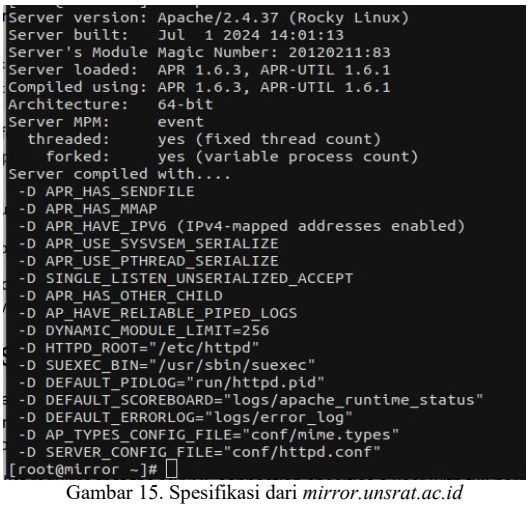
Gambar 13. *Log Activity IBM QRadar* ketika mendeteksi serangan *DoS* di *CentOS*

B. Analisis Kerentanan di Website Universitas Sam Ratulangi(mirror.unsrat.ac.id)

Website mirror.unsrat.ac.id adalah sebuah *website* yang dimiliki Oleh Universitas Sam Ratulangi yang dimana *website* ini adalah Salinan persis dari sebuah *website* yang di simpan di server. *Website* ini bisa juga digunakan untuk pengujian keamanan seperti *DoS* dan pengujian keamanan yang lain.

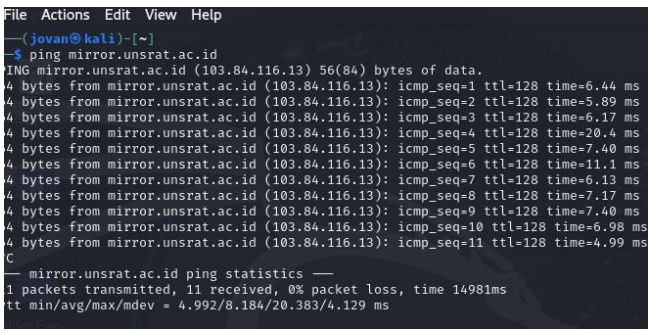


Gambar 14. Tampilan Website *mirror.unsrat.ac.id*



Gambar 15. Spesifikasi dari *mirror.unsrat.ac.id*

Sebelum melakukan penyerangan, akan dilakukan pengecekan terhadap *IP Addres* dari target yang akan dilakukan pengujian yaitu 103.84.116.13.



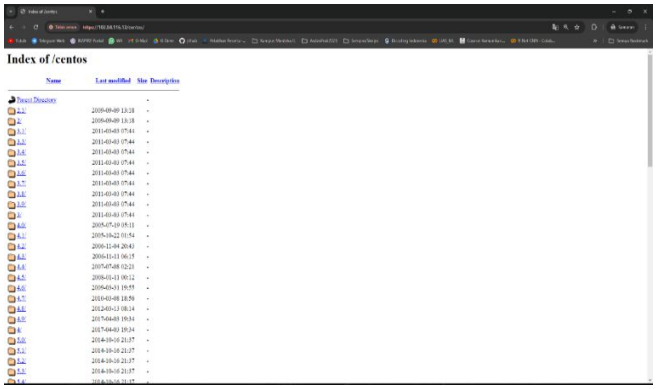
Gambar 16. *IP Adress* dari *mirror.unsrat.ac.id*

Pada *Slowloris*, yang pertama dilakukan ialah membuka *Kali Linux* lalu setelah *Kali Linux* sudah dibuka lanjut akan membuka *terminal* dari *Kali Linux*. Setelah membuka *Terminal* dilanjutkan dengan memulai proses penyerangan dengan mengetikkan *./slowloris.py*(ini adalah skrip *python* untuk melakukan penyerangan) *-p 443*(-p 443 adalah *port* untuk dilakukan penyerangan ke *website* target) *-v*(-v adalah verbose) *-s 1000* untuk pengujian pertama *dan 1020* untuk pengujian kedua(-s adalah socket) *–randuseragents*(untuk membuat user agents acak) *103.84.116.13*(ini adalah IP *Address* dari website mirror.unsrat.ac.id *–sleeptime 2*(untuk waktu tunggu tiap serangan).

Gambar 17. Serangan *DoS pertama*

Gambar 18. Serangan *DoS kedua*

Pada pengujian, *website* target tidak mengalami gangguan yang signifikan ataupun sampai *down* meskipun diserang dengan *Slowloris* dalam intensitas dan durasi yang berbeda. Hal ini mengindikasikan bahwa *firewall* yang digunakan cukup efektif dalam menahan serangan *Slowloris*. Berikut ini adalah penjelasan dari pengujian serangan :

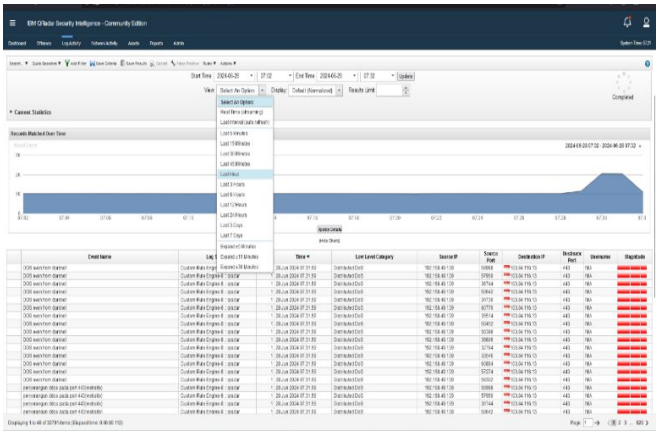


Gambar 19. *Website* yang di serang *DoS* tetap jalan.

TABEL I. PENGUJIAN SERANGAN DOS

Parameter Serangan	Pengujian 1	Pengujian 2
Jumlah Socket	1000	1020(limit socket Ketika menggunakan slowloris
Opsi -v	Menggunakan proxy SOCKS5	Menggunakan proxy SOCKS5
Opsi –randuseragents	Menggunakan user agent acak	Menggunakan user agent acak
Opsi --sleeptime 2	Interval waktu pengiriman 2 detik	Interval waktu pengiriman 2 detik
Durasi Serangan	1 Jam	2 Jam
Kondisi Jaringan	Stabil	Stabil
Target	Website yang dilindungi oleh firewall	Website yang dilindungi oleh firewall

Melakukan *Filter* di *Log Activity* Berdasarkan *Default* kurang lebih hampir 1 jam dan seperti yang tertera di gambar terdeteksi *Rules* yang telah dibuat Lalu disitu juga seperti di gambar ada *Log Source, Event Count, Time, Low Level Category seperti Distributed DoS dan Misc DoS, Source IP, Source Port, Destination IP, Destination Port,Username* dan *Magnitude* berwarna Merah yang menunjukan bahwa *offense* memiliki tingkat keparahan tinggi.



Gambar 20. *Log Activity IBM QRadar* ketika mendeteksi serangan DoS

TABEL II. SERANGAN SLOWLORIS

Jenis Serangan DoS	*Cara Kerja*	*Status Penyerangan*	*Log/Network Activity*	*Event/Flow Rule*
Slowloris	*Melakukan Flooding pada target yang dituju*	*Berhasil*	*Berhasil/ Muncul*	*Berhasil/ Muncul*

Pada pengujian ini, untuk menganalisis kerentanan terhadap serangan *DoS*. jenis serangan yang digunakan adalah *Slowloris* dan untuk Data dan *Log* mengambil dari pihak Universitas Sam Ratulangi.

Hasil pengujian menunjukkan bahwa serangan *Slowloris* berhasil memasuki sistem dan Terdeteksi di *IBM QRadar SIEM CE* dan dari pihak Universitas Sam Ratulangi berdasarkan data *Log* dari *Firewall* dan *Log Webserver*, belum mampu membuat website target menjadi tidak *responsive* atau *down*. Sistem memiliki menahan serangan ini tanpa mengalami *downtime* yang signifikan.

Serangan *Slowloris* menunjukkan bahwa sistem mampu menahan serangan dan layanan *website* masih tetap tersedia tetapi perlu memperkuat pertahanan untuk mencegah serangan yang lebih intensif juga harus lebih kokoh untuk menangani serangan dalam *volume* yang lebih tinggi. Untuk memahami dan menganalisis kerentanan terhadap serangan *DoS*, diperlukan penggunaan metrik yang relevan dan komprehensif. Metrik-metrik ini membantu dalam mendeteksi, mengukur, dan mengevaluasi potensi ancaman serta dampak dari serangan *DoS* pada sistem jaringan dan aplikasi. Beberapa metrik kunci yang digunakan dalam analisis kerentanan *DoS* seperti :

1. Mean Time to Detection (MTTD)

Mean Time to Detect (MTTD) adalah metrik yang mengukur rata-rata waktu yang dibutuhkan untuk mendeteksi adanya insiden keamanan atau gangguan sistem, sejak insiden tersebut pertama kali terjadi hingga saat teridentifikasi. MTTD merupakan salah satu indikator kunci kinerja (*key performance indicator/KPI*) dalam pengelolaan keamanan dan operasional TI (*Information Technology*). Metrik ini membantu untuk memahami seberapa efektif sistem dan proses dalam mendeteksi ancaman atau masalah dengan cepat. Semakin rendah nilai MTTD, semakin baik kemampuan organisasi dalam mengidentifikasi dan merespons insiden secara proaktif..

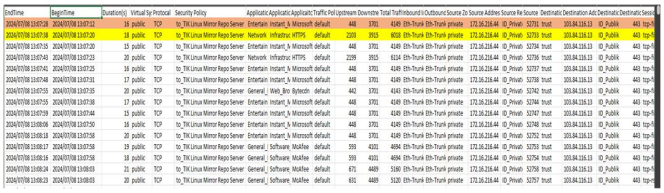
Cara untuk menghitung *Mean Time to Detect* adalah Sebagai berikut :

$$MTTD = Waktu\ Terdeteksi - Waktu\ Terjadi$$

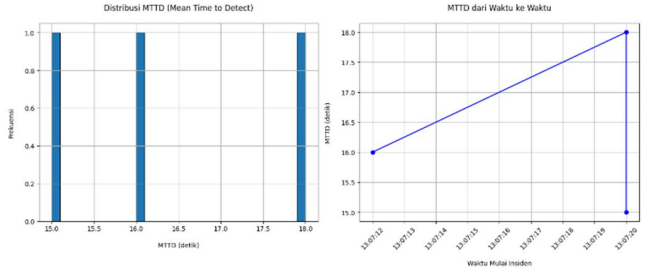
Log Activity dari data yang didapatkan dari *Webserver mirror.unsrat.ac.id* yang dimana serangan dimulai pada jam 13:07:12 dan terdeteksi di *Firewall* pada waktu 13:09:29 jadi untuk perhitungan *Mean Time to Detect* adalah 2 menit 16. detik kategori baik dikarenakan seranganya terdeteksi kurang dari 24 jam.

Log Activity dari data yang didapatkan dari *Firewall* dari pihak Universitas Sam Ratulangi yang dimana serangan dimulai pada jam 13:07:12 dan terdeteksi di *Firewall* pada waktu 13:07:20 jadi untuk perhitungan *Mean Time to Detect* adalah 8 detik. ini termasuk dalam kategori baik dikarenakan seranganya terdeteksi kurang dari 24 jam. Menurut Survei Tanggap Insiden *SANS* 2019, 52,6% organisasi memiliki *MTTD* kurang dari 24 jam, dan 81,4% mendeteksi insiden dalam waktu 30 hari.

Gambar 21. Log dari *Webserver* mirror.unsrat.ac.id



Gambar 22. Log dari Firewall mirror.unsrat.ac.id untuk Metrik *MTTD*



Gambar 23. Visualisasi Data untuk *Mean Time to Detect*

TABEL III. HASIL *MTTD* DARI *LOG FIREWALL* DAN *SERVER WEB*

Sumber Log	Waktu Mulai Serangan	Waktu Deteksi	*MTTD*	*Parameter MTTD*
Firewall	7/8/2024 13:07	7/8/2024 13:07	8 Detik	Baik
Server Web	7/8/2024 13:07	7/8/2024 13:09	2 Menit 16 Detik	Baik

2. Distribusi Serangan

Distribusi serangan dalam keamanan siber adalah analisis penyebaran serangan berdasarkan karakteristik tertentu. Tujuannya adalah memahami tren, pola, dan vektor serangan untuk membantu organisasi dan individu dalam mengidentifikasi ancaman, memprioritaskan tindakan keamanan, dan mengembangkan strategi yang efektif.

Pada Gambar 22. adalah *log* yang digunakan untuk Analisis Kerentanan Distribusi Serangan yang sudah di filter berdasarkan *Protocol, Application Category, Source Zone, Source Address, Destination Zone,* dan *Destination Address.* Itu adalah data-data yang diperlukan untuk melakukan Analisis Kerentanan Distribusi Serangan.

Protocal	Application Category	Source Zone	Source Address	Destination Zone	Destination Address
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	Network	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	Network	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	Entertainment	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13
TCP	General_Internet	private	172.16.216.44	trust	103.84.116.13

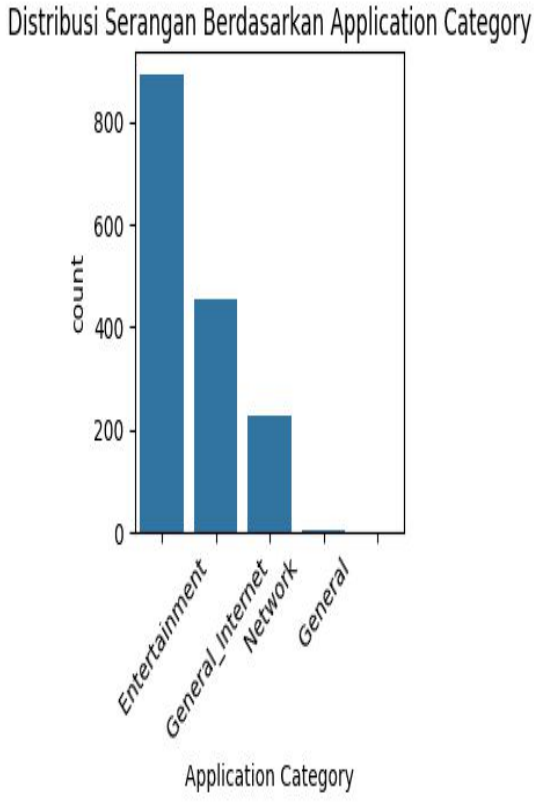
Gambar 24. *Log* di *Firewall* untuk Distribusi Serangan.

Berdasarkan analisis log firewall, dapat disimpulkan beberapa poin penting terkait potensi kerentanan DoS seperti :

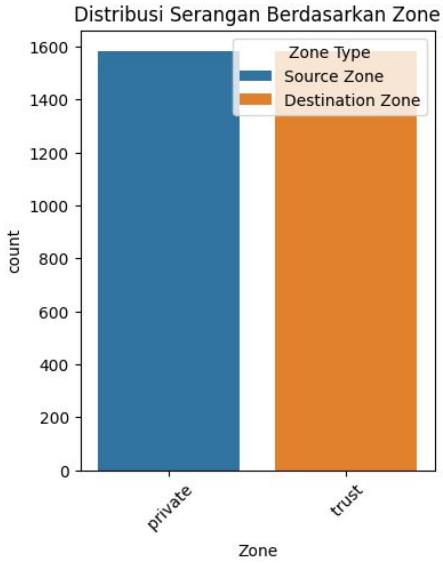
Serangan Terarah yang dimana semua serangan berasal dari satu alamat IP (172.16.216.44) dan menargetkan satu alamat IP tujuan (103.84.116.13), menunjukkan serangan yang terarah dan spesifik, Semua serangan menggunakan protokol *TCP,* yang umum digunakan dalam berbagai jenis serangan *DoS,* Serangan terutama menargetkan kategori aplikasi *'Entertainment'* (56.36%) dan *'Network'* (14.48%), mengindikasikan upaya untuk mengganggu layanan hiburan dan infrastruktur jaringan dan Serangan berasal dari zona *'private'* (kemungkinan besar jaringan internal) dan ditujukan ke zona *'trust'* (zona yang seharusnya lebih terpercaya), menunjukkan potensi kerentanan dalam segmentasi jaringan dan keamanan zona *trust.*

TABEL IV. HASIL DARI DISTRIBUSI SERANGAN

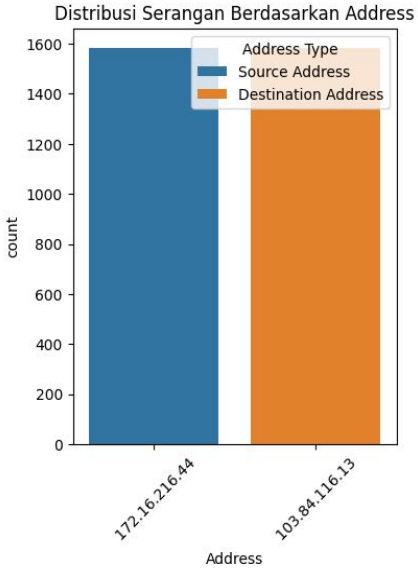
Parameter	Nilai
Sumber Serangan	172.16.216.44
Target Serangan	103.84.116.13
Protokol yang Digunakan	*TCP*
Target Aplikasi	Entertainment (56.36%), Network (14.48%)
Zona Jaringan	*private* (sumber), *trust* (tujuan)



Gambar 25. Visualisasi Data berdasarkan Application Category



Gambar 26. Visualisasi Data berdasarkan Zone



Gambar 27. Visualisasi Data berdasarkan Address Type

3. Peak Traffic Volume

Peak traffic volume adalah jumlah maksimum lalu lintas jaringan yang terjadi pada suatu titik waktu tertentu. Ini mengukur intensitas tertinggi dari data yang ditransfer melalui jaringan, baik dalam bentuk data masuk (downstream) maupun data keluar (upstream). *Peak traffic volume* sering digunakan untuk menilai kapasitas jaringan, mengidentifikasi pola penggunaan, dan mendeteksi potensi serangan seperti Denial of Service (DoS) yang bisa menyebabkan lonjakan lalu lintas secara tiba-tiba.

Ini adalah *Log Activity* yang sudah di *filter* untuk dilakukan analisis kerentanan ada bagian-bagian kolom di *Log Activity seperti EndTime, BeginTime, Upstream Downstream Traffic (bytes) dan Total Traffic (Bytes).*

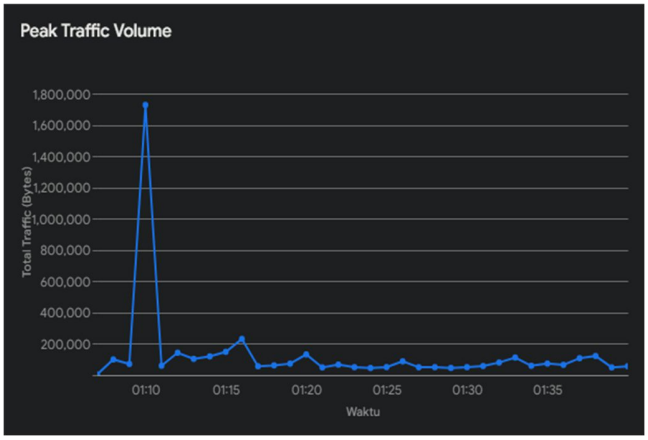
EndTime	BeginTime	Upstream Traffic(Bytes)	Downstream Traffic(Bytes)	Total Traffic(Bytes)
2024/07/08 13:10:07	2024/07/08 13:09:26	2749	61511	64260
2024/07/08 13:09:46	2024/07/08 13:09:27	448	3701	4149
2024/07/08 13:09:52	2024/07/08 13:09:33	448	3701	4149
2024/07/08 13:09:48	2024/07/08 13:09:33	442	3701	4143
2024/07/08 13:09:55	2024/07/08 13:09:39	2155	3919	6074
2024/07/08 13:10:01	2024/07/08 13:09:40	448	3701	4149
2024/07/08 13:10:02	2024/07/08 13:09:41	7082	212108	219190
2024/07/08 13:10:01	2024/07/08 13:09:41	2155	3999	6154
2024/07/08 13:10:01	2024/07/08 13:09:41	2091	3959	6050
2024/07/08 13:10:01	2024/07/08 13:09:41	2123	3959	6082
2024/07/08 13:10:01	2024/07/08 13:09:41	2450	512	2962
2024/07/08 13:10:00	2024/07/08 13:09:41	172	92	264
2024/07/08 13:09:59	2024/07/08 13:09:41	8021	123061	131082
2024/07/08 13:09:59	2024/07/08 13:09:41	2386	512	2898
2024/07/08 13:09:59	2024/07/08 13:09:41	10362	1005572	1015934
2024/07/08 13:09:58	2024/07/08 13:09:41	2524	895	3419
2024/07/08 13:09:58	2024/07/08 13:09:41	2091	3999	6090
2024/07/08 13:09:58	2024/07/08 13:09:41	2187	3999	6186
2024/07/08 13:09:58	2024/07/08 13:09:41	172	92	264
2024/07/08 13:09:56	2024/07/08 13:09:41	3339	17705	21044
2024/07/08 13:10:02	2024/07/08 13:09:44	2386	552	2938
2024/07/08 13:10:12	2024/07/08 13:09:45	16521	52869	69390
2024/07/08 13:10:10	2024/07/08 13:09:45	5935	2540	8475
2024/07/08 13:10:04	2024/07/08 13:09:45	2402	512	2914
2024/07/08 13:10:04	2024/07/08 13:09:45	2187	3919	6106
2024/07/08 13:10:04	2024/07/08 13:09:45	2370	472	2842
2024/07/08 13:10:04	2024/07/08 13:09:45	2450	472	2922
2024/07/08 13:10:03	2024/07/08 13:09:45	2187	3919	6106

Gambar 28. Log dari *Firewall* untuk *Peak Traffic Volume*

Berdasarkan analisis data, dapat disimpulkan bahwa terdapat satu waktu yang memiliki lonjakan lalu lintas signifikan, yaitu pada pukul 13:09:59 dengan total lalu lintas sebesar 1.015.934 *bytes*. Lonjakan ini jauh melebihi rata-rata lalu lintas pada periode waktu tersebut, yang hanya sekitar 13.446,2 bytes.Selain itu, dapat dilihat bahwa sebagian besar lalu lintas berasal dari satu alamat IP yang tidak diketahui, dan lalu lintas tersebut terkonsentrasi pada beberapa detik saja. Hal ini merupakan indikasi kuat adanya serangan *DoS (Denial of Service)*, di mana penyerang mencoba membanjiri *server* dengan lalu lintas yang berlebihan. Berikut adalah beberapa poin penting dari analisis:

TABEL V. HASIL DARI PEAK TRAFFIC VOLUME

Parameter	Nilai
Peak Traffic Volume	1.015.934 bytes pada pukul 13:09:59
Sumber Lalu Lintas Utama	Tidak ada sumber yang dominan
Pola Lalu Lintas	Variasi besar, maksimum 1.015.934 *bytes*
Downstream Traffic (rata-rata)	8225.24 *bytes*
Upstream Traffic (rata-rata)	1054.96 *bytes*



Gambar 29. Visualisasi Data untuk *Peak Traffic Volume*

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari hasil penelitian yang telah dilakukan, maka dapat menarik kesimpulan yaitu:

1. Hasil Deteksi serangan di Universitas Sam Ratulangi memiliki performa yang baik dalam mendeteksi serangan dengan *MTTD* yang sangat cepat, yaitu 2 menit 16 detik pada *webserver* dan 8 detik pada *firewall*. *MTTD* yang cepat ini menunjukkan efektivitas sistem pemantauan dan tanggap insiden yang diterapkan.
2. Berdasarkan standar yang diterapkan oleh *SANS* , hasil ini pengukuran *Mean Time to Detect* masuk dalam kategori baik, karena serangan berhasil dideteksi dalam waktu yang sangat singkat yaitu kurang dari 24 jam, jauh di bawah rata-rata waktu deteksi yang dilaporkan oleh sebagian besar organisasi.
3. Dengan adanya lonjakan lalu lintas yang signifikan untuk Metrik *Peak Traffic Volume* pada pukul 13:09:59 dan indikasi kuat adanya serangan *DoS*, sangat penting bagi Universitas Sam Ratulangi untuk memperkuat sistem pemantauan
4. Untuk Metrik Distribusi Serangan ini menunjukkan bahwa penyerang menggunakan alamat *IP* tertentu untuk melancarkan serangan terarah, menargetkan satu alamat *IP* tujuan dengan memanfaatkan protokol *TCP,* yang andal namun rentan terhadap serangan *DoS.* Fokus serangan pada aplikasi kategori *'Entertainment'* dan *'Network'* bertujuan untuk menyebabkan gangguan signifikan pada layanan vital. Selain itu, serangan yang berasal dari zona '*private*' ke zona *'trust'* mengindikasikan adanya kelemahan dalam segmentasi dan perlindungan zona jaringan yang seharusnya memiliki lapisan keamanan yang lebih ketat untuk mencegah serangan dari jaringan internal maupun eksternal.
5. Hasil dengan menggunakan Jenis Serangan untuk target *website mirror.Universitas Sam Ratulangi.Universitas Sam Ratulangi.ac.id* yaitu *Slowloris* juga untuk pengujian dan analisis kerentanan berhasil terdeteksi aktifitas mencurigakan terdeteksi di *network activity* ataupun *log activity* dan untuk Data Log dari Pihak Universitas Sam Ratulangi Seperti *Log* dari *Firewall* dan *Log Webserver*.
6. Hasil Pengujian dengan menggunakan Serangan *TCP SYN Flood* untuk pengujian serangan *DoS dan*
7. Implementasi Sistem *Monitoring* di Sistem Operasi *CentOS* berhasil terdeteksi aktifitas mencurigakan terdeteksi di *network activity* ataupun *log activity* dalam waktu singkat.
8. Pengujian analisis kerentanan menunjukkan bahwa sistem memiliki kemampuan yang baik dalam
9. mendeteksi dan menahan serangan *DoS*. Layanan tetap tersedia meskipun dibanjiri dengan permintaan dan paket data jadi masih belum terlalu rentan.
10. Dalam pengujian serangan untuk mengirimkan serangan yang lebih besar terkena *Limitasi* dikarenakan Spesifikasi *Device* yang digunakan belum cukup untuk mengirimkan serangan yang lebih besar.

B. Saran

Dalam penelitian ini tentunya masih terdapat kekurangan dan ada beberapa hal yang perlu dikaji kembali agar kedepannya menjadi semakin lebih baik, oleh karena itu ada beberapa saran dapat diberikan untuk pengembangan selanjutnya:

1. Dibutuhkan spesifikasi komputer yang lebih bagus, supaya bisa melakukan serangan yang lebih besar juga Koneksi *Internet* yang lebih Cepat dan Stabil untuk melakukan Serangan *DoS*.
2. Penting untuk mendokumentasikan hasil analisis kerentanan dan tindakan yang diambil untuk mengatasinya.
3. Tingkatkan kapasitas server jika diperlukan.
4. Peningkatan Sistem Pemantauan, Mitigasi Serangan, Penguatan Keamanan Website serta Jaringan dan Strategi Jangka Panjang. Langkah-langkah yang disarankan dapat membantu dalam mendeteksi, mencegah, dan merespons serangan *DoS* secara lebih efektif, sehingga memastikan layanan tetap lancar dan aman.

V. KUTIPAN (TNR 8)

[1] Arief, M., Hari Trisnawan, P., & Data, M. (2017). IMPLEMENTASI SISTEM DETEKSI SERANGAN SLOWLORIS PADA ARSITEKTUR JARINGAN SOFTWARE-DEFINED NETWORK MENGGUNAKAN RANDOM FOREST (Vol. 1, Issue 1). http://j-ptiik.ub.ac.id

[2] Bhor, M. R. V, & Khanuja, K. (2017). Analysis of web application security mechanism and attack detection using vulnerability injection technique. https://ieeexplore.ieee.org/abstract/document/7860004

[3] Bromiley, M. (2019). It's Time for a Change SANS 2019 Incident Response (IR) Survey: It's Time for a Change A SANS Survey. https://sansorg.egnyte.com/dl/BF16d8owD9

[4] Chandra, J. C. (2022). Analisis Keamanan Layanan E-Learning Terhadap Serangan Dos Dan Implementasi Mitigasi Pada Universitas Budi Luhur. *Jurnal TICOM: Technology of Information and Communication*, *10*(3), 2022. https://elearning.budiluhur.ac.id,

[5] Christoper, W., & Hermawan, R. Z. (2024). Pemantauan dan Pengawasan Serangan Siber SSH Brute Force di Indonesia dengan IBM QRadar Community Edition. 120–127. https://doi.org/10.37817/tekinfo.v25i2

[6] Delsi Samsumar, L., & Gunawan, K. (2017). ANALISIS DAN EVALUASI TINGKAT KEAMANAN JARINGAN KOMPUTER NIRKABEL (WIRELESS LAN); STUDI KASUS DI KAMPUS STMIK MATARAM. In *Jurnal Ilmiah Teknologi Informasi Terapan: Vol. IV* (Issue 1). https://journal.widyatama.ac.id/index.php/jitter/article/view/152/142

[7] Deng, S., Gao, X., Lu, Z., Li, Z., & Gao, X. (2019). DoS vulnerabilities and mitigation strategies in software-defined networks. *Journal of Network and Computer Applications*, *125*, 209–219. https://doi.org/10.1016/j.jnca.2018.10.011

[8] Institute of Electrical and Electronics Engineers, IEEE Industry Applications Society, & Shandong da xue. (2020). *Vulnerability Assessment for an Islanded Microgrid with Secondary Control System Suffering from Dynamic DoS Attacks*. doi:10.1109/icpsasia48933.2020.9208407

[9] Kamilah, I., Ritzkal, & Hendri Hendrawan, A. (2019). *Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika* (Vol. 16). https://jurnal.umj.ac.id/index.php/semnastek/article/view/5233/3512

[10] Mohan, A. M., Meskin, N., & Mehrjerdi, H. (2023). LQG-Based Virtual Inertial Control of Islanded Microgrid Load Frequency Control and DoS Attack Vulnerability Analysis. *IEEE Access*, *11*, 42160–42179. https://doi.org/10.1109/ACCESS.2023.3271012

[11] Nida, H., & Adrian, R. (2023). Analisis Perbedaan Pengaruh Penggunaan Iptables Chains dalam Mencegah Denial of Service (DoS) pada Jaringan IoT. *Journal of Internet and Software Engineering*, *4*(1).

[12] Riadi, I., & Yudhana, A. (2016). *Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST)* (Vol. 2, Issue 1). http://ars.ilkom.unsri.ac.id300

[13] Server, W., Indrajid, F., Andika, K. F., Surya, G. K., Putra, A., Karisma Bramanda, K., Arna, G., Saskara, J., Made, I., & Listartha, E. (2023). Analisis Hasil DoS SYN Flood Attack Pada. In *Jurnal Format* (Vol. 12).

[14] Setiawan, E. B., & Setiyadi, A. (2018). Web vulnerability analysis and implementation. *IOP Conference Series: Materials Science and Engineering*, *407*(1). https://doi.org/10.1088/1757-899X/407/1/012081

[15] Suharmanto, A. Y., Lumenta, A. S. M., & Najoan, X. B. N. (2018). Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi. *Jurnal Teknik Informatika* , *13*, 1–10. https://ejournal.Universitas Sam Ratulangi.ac.id/v3/index.php/informatika/article/view/28074/27546

Jovanka Daryl Ruindungan lahir pada tahun 2002.Penulis Mulai menempuh Pendidikan Sekolah dasar pada tahun 2008 sampai tahun 2014.setelah menamatkan Sekolah Dasar kemudian melanjutkan Sekolah Menengah Pertama pada tahun 2014 sampai tahun 2017.Setelah menamatkan Pendidikan menengah pertama, penulis melanjutkan Sekolah Menengah Atas dari tahun 2017 sampai tahun 2020.

Setelah lulus pada tahun 2020 melanjutkan Pendidikan S1(Strata 1) di Universitas Sam Ratulangi dan penulis terdaftar sebagai mahasiswa S1 pada Program Studi Teknik Informatika, Jurusan Teknik Elektro, Fakultas Teknik Universitas Sam Ratulangi mulai September 2020.Selama masa kuliah, penulis aktif dalam kegiatan kemahasiswaan seperti Himpunan Mahasiswa Elektro (HME).