Terbit online pada laman web jurnal: **https://uia.e-journal.id/INSIT**

Informatika sains teknologi

FAKULTAS SAIN & TEKNOLOGI
PROGRAM STUDI TEKNIK INFORMATIKA

Vol. 02 No. 01 (2024) 3025-3608 | ISSN : 3025-3608

ANALISIS *SYN FLOOD ATTACK* MENGGUNAKAN METODE *NIST* 800-61 REV 2 PADA *SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)*

Khofifah Indar Parawansa[1], Acmad Nurhadi[2]

[1]Jurusan Teknologi Informasi, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika

[2]Magister Ilmu Komputer, Perguruan Tinggi Manajemen & Informatika Nusa Mandiri Jakarta

[1]17191223@bsi.ac.id, [2]achmad.ahh@bsi.ac.id

ABSTRACT

Increasing cyber threats can result in personal data leakage, identity theft, the spread of viruses or malware, to cyber attacks that can damage critical systems and infrastructure for organizations. One of them is the SYN Flood attack. SYN Flood is a type of Denial of Service attack method that affects hosts running TCP (Transmission Control Protocol) server processes. Due to the danger of various cyber attacks and the increasing need for information security, Security Information and Event Management (SIEM) is needed to monitor these attacks. This study aims to analyze syn flood attacks on (SIEM) . This study used the NIST 800-61 method. It was found that the detected syn flood attack was critical based on the flood event informed by SIEM. Based on this data, the SOC Analyst Team decided to report the attack to the client concerned. Mitigations include using firewalls, setting shorter timeouts to close inactive connections, using the services of Content Delivery Network (CDN) providers or providers that specialize in DoS prevention to filter traffic to specific services

Keyword: *syn flood, SIEM, NIST 800-61, cyber security*

ABSTRAK

Meningkatnya ancaman siber dapat mengakibatkan kebocoran data pribadi, pencurian identitas, penyebaran virus atau malware, hingga serangan siber yang dapat merusak sistem dan infrastruktur yang krusial bagi organisasi. Salah satunya adalah serangan *SYN Flood. SYN Flood* adalah salah satu jenis metode serangan *Denial of Service* yang mempengaruhi *host* yang menjalankan proses *server (Transmission Control Protocol)*. Karena bahayanya berbagai serangan siber dan meningkatnya kebutuhan keamanan informasi, dibutuhkan *Security Information and Event Management (SIEM)* untuk memonitoring serangan-serangan tersebut. Penelitian ini memiliki tujuan untuk menganalisis *syn flood attack* pada (*SIEM)*. Penelitian ini menggunakan metode NIST 800-61. Didapatkan hasil bahwa *syn flood attack* yang terdeteksi adalah *critical* berdasarkan *flood event* yang diinformasikan oleh *Security Information and Event Management(* SIEM). Berdasarkan data tersebut, Tim SOC *Analyst* memutuskan untuk me*report* serangan tersebut kepada klien yang bersangkutan. Mitigasi yang dapat dilakukan dari serangan tersebut adalah menggunakan *firewall*, mengatur *timeout* yang lebih singkat untuk menutup koneksi yang tidak aktif, menggunakan layanan penyedia *Content Delivery Network* atau penyedia yang berspesialisasi dalam pencegahan *DoS* untuk menyaring lalu lintas menuju ke layanan tertentu

Kata Kunci : *syn flood, SIEM, NIST 800-61, cyber security*

Diterima Redaksi : Tahun 2024 | Selesai Revisi : Tahun 2024 | Diterbitkan ISSN : 3025-3608-Tahun 2024

I. PENDAHULUAN

Ancaman siber dapat mengakibatkan kebocoran data pribadi, pencurian identitas, penyebaran virus atau malware, hingga serangan siber yang dapat merusak sistem dan infrastruktur yang krusial bagi organisasi. Salah satunya adalah serangan SYN Flood.

SYN Flood adalah salah satu jenis metode serangan Denial of Service (DOS) yang mempengaruhi host yang menjalankan proses server TCP (Transmission Control Protocol). (Dehan Pratama et al., n.d.) Serangan SYN Flood bertujuan untuk memblokir atau bahkan mematikan sistem atau layanan yang ditargetkan. Penyerang akan membanjiri server atau sistem dengan permintaan koneksi (SYN) palsu yang menyebabkan server menjadi sibuk dalam melayani permintaan koneksi yang sebenarnya.

Karena bahayanya berbagai serangan siber dan meningkatnya kebutuhan keamanan informasi, dibutuhkan sistem atau tools yang dapat memonitoring serangan-serangan tersebut. Sistem yang bisa digunakan adalah Security Information and Event Management (SIEM). Secara umum, SIEM berguna untuk mengumpulkan, menganalisis, menyimpan dan mengumpulkan event dari berbagai sensor (sistem deteksi intrusi, anti-virus, firewall, dll.), dan menampilkannya di dashboard sebagai peringatan untuk penanganan ancaman dan pelaporan keamanan. (González-Granadillo et al., 2021)

Dalam menganalisis alert yang ditampilkan oleh SIEM, penulis menggunakan metode NIST (National Institute of Standards Technology). NIST adalah metode yang biasa digunakan untuk menganalisis informasi dari bukti digital. (Umar et al., 2018) Pada kesempatan ini, penulis menggunakan metode NIST (National Institute of Standards Technology) 800-61 "Computer Security Incident Handling Guide", yang merupakan publikasi yang membahas respon manajemen keamanan informasi jika terjadi insiden.

Pada penelitian ini akan berfokus ke syn flood, yang mana penelitian ini akan menganalisis syn flood menggunakan SIEM sesuai dengan tahapan metodologi NIST, sehingga penelitian ini berjudul "Analisis SYN Flood Attack menggunakan Metode NIST 800-61 Rev 2 pada Security Information and Event Management (SIEM)".

A. Cyber Attack (Serangan Siber)

Cyber Attack (Serangan Siber) merupakan tindak kejahatan yang dilakukan oleh Attacker (Penyerang) dengan tujuan untuk merusak atau mendapatkan akses ke jaringan atau sistem komputer. (Suharto et al., 2021) Salah satu penyebab terjadinya kasus ancaman siber adalah semakin tingginya penggunaan internet. Banyaknya data pribadi yang masuk dan lemahnya sistem keamanan teknologi internet memudahkan serangan pencurian data. Interpol menyebutkan bahwa serangan siber terjadi karena kesadaran masyarakat masih sangat rendah terutama di negara-negara Asia dan Selatan Pasifik, termasuk Indonesia. (Hendra Wicaksana et al., 2020)

B. Dos Attack

Denial of Service (DoS) Attack merupakan serangan siber yang ditujukan untuk menghabiskan resource suatu sistem dengan cara membanjiri traffic sehingga client tidak bisa mengakses layanan jaringan. (Chandra, 2021)

C. SYN Flood Attack

Saat dua buah komputer melakukan komunikasi, client akan meminta koneksi ke server dengan mengirimkan permintaan SYN (Synchronize), server akan merespon dengan mengirimkan SYN-ACK (Synchronize-Acknowledge) kepada client, kemudian client akan mengirimkan ACK (Acknowledge). Proses komunikasi ini dikenal sebagai Three Way Hand-Shake. Namun, pada kasus SYN Flood Attack, client yang telah dikirimkan SYN-ACK (Synchronize-Acknowledge) oleh server, tidak merespon ACK (Acknowledge) kepada server, akibatnya komputer server akan terus menunggu respon ACK (Acknowledge) dari client, dan jika tidak ada respon yang diterima, koneksi akan tetap terbuka dan computer membuat request baru ke semua port pada

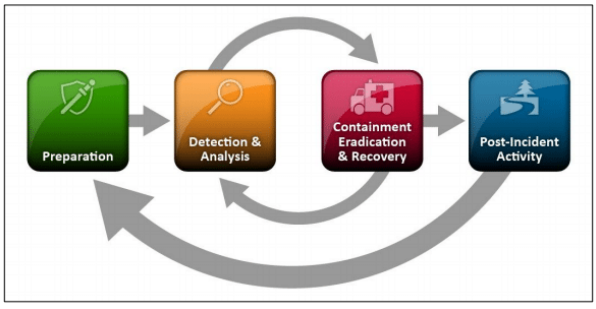
server yang akan membebankan sistem. (Sahren, 2021)

D. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) adalah sistem pemantauan yang dapat mendeteksi serangan dan respons sistem keamanan terhadap serangan melalui analisis log dari berbagai log peristiwa dari data real-time. Log adalah informasi tentang perangkat yang menyertakan fungsi logging yang dimulai dengan lalu lintas jaringan, status perangkat, dan lainnya. (Khotimah et al., n.d. 2022).

E. NIST (National Institute of Standards Technology) 800-61

NIST 800-61 adalah salah satu metode yang dikeluarkan oleh National Institute of Standard and Technology. NIST 800-61 membahas tentang penanganan insiden (Incident Handling). NIST adalah lembaga yang bertanggung jawab untuk mengembangkan standar, pedoman, dan persyaratan minimum untuk memastikan keamanan yang memadai untuk semua aset dan pihak yang memenuhi syarat dalam forensik digital. Metode ini digunakan oleh lembaga pemerintah AS pusat, tetapi bisa juga digunakan oleh organisasi seperti akademisi, lembaga penelitian swasta dan lain-lain. (Riadi, n.d.)



Gambar 1. Tahapan *NIST* 800-61

Tujuan Penelitian

Tujuan penelitian yang ingin dicapai adalah:

1. Menganalisis serangan SYN Flood menggunakan Security Information and Event Management (SIEM) Stellar Cyber.
2. Memberikan mitigasi terhadap serangan SYN Flood yang terjadi.
3. Menginfokan atau mereport serangan kepada Klien agar Klien mengambil keputusan yang sesuai dengan mitigasi yang Penulis berikan.

II. METODOLOGI PENELITIAN

Teknik Pengumpulan Data

1. Observasi

Penulis melakukan pemantauan dan analisis terhadap alert dan lalu lintas jaringan menggunakan SIEM Stellar Cyber. Penulis juga menarik data sekunder yang berasal dari SIEM Stellar Cyber. Selain itu, penulis juga melakukan observasi terhadap parameter-parameter yang terkait dengan serangan syn flood, seperti jumlah paket yang diterima atau dikirim, jumlah flood

.

2. Wawancara

Penulis mewawancarai Bapak Zumardi Irfan sebagai L2 Team, untuk menanyakan tentang bagaimana cara kerja SIEM Stellar Cyber, penjelasan syn flood attack, dan mitigasi syn flood attack.

3. Studi Literatur

Teknik pengumpulan data lain yang dapat digunakan adalah dengan mempelajari literatur dan dokumentasi terkait serangan syn flood. Dalam mempelajari literatur dan dokumentasi terkait serangan syn flood, penulis dapat memperoleh informasi tentang karakteristik serangan, cara kerja serangan, dan teknik mitigasi yang dapat diterapkan untuk mengatasi serangan tersebut.

III. HASIL DAN PEMBAHASAN

A. Pengumpulan Data

Data diambil dari SIEM, Penulis mengambil alert syn flood attacker dalam interval waktu 1 bulan, terhitung sejak tanggal 07 April 2023 – 07 Mei 20

B. Membuat Skenario

Skenario dibuat dengan tujuan untuk mengetahui apakah SYN flood attack yang ditangkap oleh SIEM Stellar Cyber benar-benar serangan yang critical atau hanya traffic, dan apakah serangan tersebut perlu direport kepada klien. Langkah-langkah nya sebagai berikut:

1. Mengumpulkan data-data serangan syn flood attack.
2. Mengambil 2 sample serangan.
3. Menganalisis syn flood attack.
4. Membuat kesimpulan.

C. Implementasi Metode NIST

1. *Preparation*

Pada tahap ini, terdapat beberapa tools dan sumber daya yang harus disediakan oleh Tim SOC Analyst sebagai berikut:

Tabel 1
Tabel Preparation

Persiapan	**Deskripsi**
Informasi Kontak	Informasi kontak untuk keperluan komunikasi antar tim
Mekanisme *Report* Insiden	*Report alert* menggunakan WhatsApp Grup dan *ticketing* menggunakan form online
Smartphone	Samsung *Galaxy* M20 3/32 GB Octa-Core
Ruang Kerja	PT Sembilan Pilar Semesta
Ruang meeting	PT Sembilan Pilar Semesta
SIEM	*Stellar Cyber*
Laptop	Dell 8 GB 11th Gen Intel® Core™ i5-1135G7

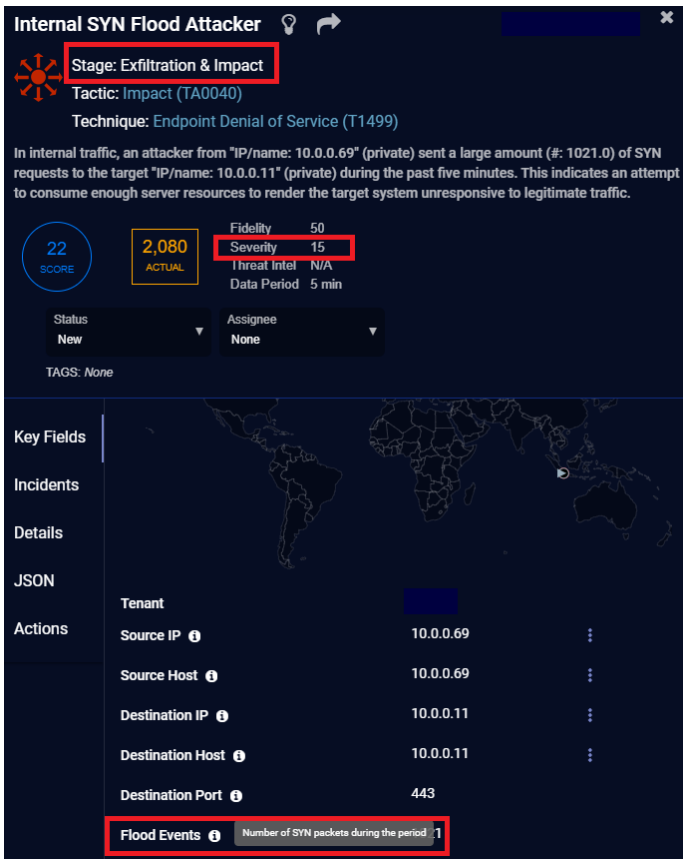
Tabel 1
Alert syn flood attacker

Source IP	*Source Country*	*Destination IP*	*Destination Country*	*Destination Port*	*Flood Event*
10.0.0.69	Indonesia	10.0.0.11	Indonesia	443	1,021
10.0.0.33	Indonesia	10.0.0.11	Indonesia	-	515
3.64.163.50	Germany	10.0.0.11	Indonesia	80	4,235
172.217.194.113	United States	10.0.0.11	Indonesia	443	11,058
157.185.188.1	China	10.0.0.11	Indonesia	443	11,562
190.92.210.97	Singapore	10.0.0.11	Indonesia	443	257
31.13.95.61	Indonesia	10.0.0.11	Indonesia	5,222	2
149.154.175.52	Antigua and Barbuda	10.0.0.11	Indonesia	443	955
35.213.190.132	Singapore	10.0.0.11	Indonesia	443	9,387
142.251.12.188	United States	10.0.0.11	Indonesia	5,228	1,917
74.125.24.94	United States	10.0.0.11	Indonesia	80	907
23.56.239.131	Indonesia	10.0.0.11	Indonesia	443	717
31.13.95.60	Indonesia	10.0.0.11	Indonesia	443	7,207
31.13.95.61	Indonesia	10.0.0.11	Indonesia	443	2,943
31.13.95.1	Indonesia	10.0.0.11	Indonesia	443	3,377
23.44.10.123	India	10.0.0.11	Indonesia	443	4,912
23.50.117.176	Indonesia	10.0.0.11	Indonesia	443	3,062
172.217.194.99	United States	10.0.0.11	Indonesia	443	2,656
172.217.194.147	United States	10.0.0.11	Indonesia	443	1,213
172.217.194.99	United States	10.0.0.11	Indonesia	443	3,088

2. Detection & Analysis

Pada tahap ini, Penulis mengambil satu sampel IP penyerang yang terdeteksi oleh SIEM sebagai syn flood attack.

Gambar 2. Sample serangan syn flood



Gambar 3. Tampilan more info dari alert sample syn flood

Tabel 2
Sample syn flood

Source IP	***Source Country***	***Destination IP***	***Dst Country***	***Dst Port***	***Flood Event***
10.0.0.69	Indonesia	10.0.0.11	Indonesia	443	1,021

Berdasarkan table 3, dapat kita ketahui, bahwa pada *traffic* internal, *attacker* dari "IP: 10.0.0.69" (IP *private*) mengirimkan sebesar 1,021 bytes permintaan SYN ke target "IP: 10.0.0.11" (IP *Private*) dalam waktu 5 menit. Hal ini mengindikasikan percobaan untuk menggunakan sumber daya *server* yang tinggi untuk membuat sistem target tidak merespon terhadap *traffic* yang sah.

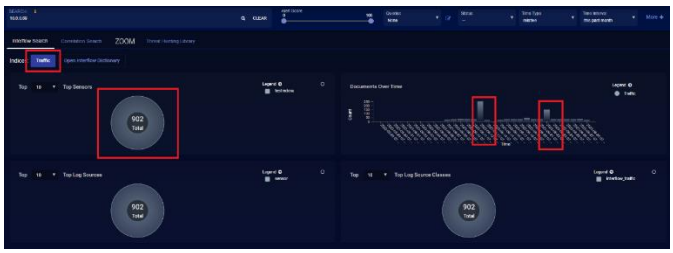
Jumlah normal *syn flood* biasanya bergantung pada lalu lintas jaringan yang sah dan jumlah permintaan koneksi yang diterima *server* dalam kondisi normal. Biasanya jumlah tersebut berkisar antara 60 – 80 bytes. Sedangkan pada serangan ini, yaitu *attacker* mengirimkan syn flood dengan jumlah tinggi yaitu 1,201 bytes.

a. Analisis SIEM

Source IP, alamat IP penyerang yaitu 10.0.0.69 (IP private).
Source Country, negara asal IP penyerang yaitu Indonesia.
Destination IP, alamat IP tujuan, yaitu 10.0.0.11 (IP Private).
Destination Country, asal negara IP tujuan, yaitu Indonesia.
Destination Port, Port tujuan atau port yang diserang, yaitu port 443. Port 443 adalah port default yang digunakan oleh server web yang mendukung HTTPS.
Flood Event, Paket syn flood yang dikirimkan, sebanyak 1,021 byte.

b. Threat Hunting

Selanjutnya, Penulis melakukan pengecekan pada threat hunting untuk melihat lalu lintas IP penyerang dalam 1 minggu ke belakang.



Gambar 4. Threat Hunting IP 10.0.0.69

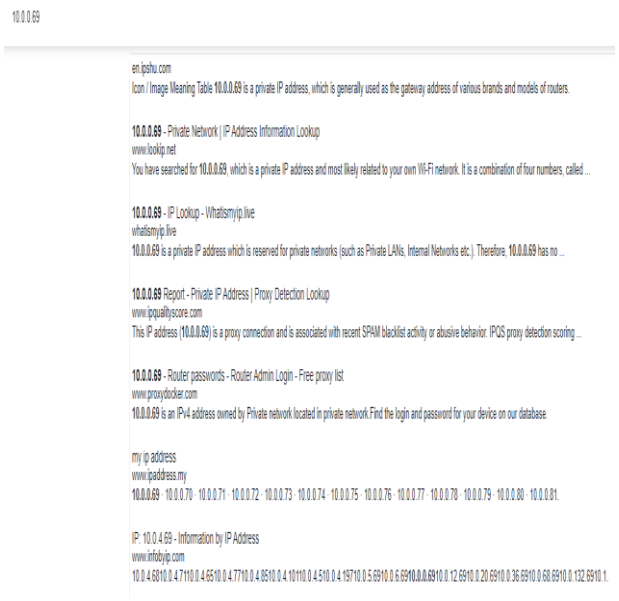
Time	Source Host	Source Country	Destination Host	Destination Count...	App	Total Bytes	Flood Events	
2023-06-20 16:00:21	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,040	-	More Info
2023-06-20 15:00:25	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,040	-	More Info
2023-06-20 14:19:04	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	587	-	More Info
2023-06-20 14:00:28	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,040	-	More Info
2023-06-20 13:00:24	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,039	-	More Info
2023-06-20 12:00:22	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,039	-	More Info
2023-06-20 11:00:20	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,040	-	More Info
2023-06-20 10:00:18	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,039	-	More Info
2023-06-20 09:00:17	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,040	-	More Info
2023-06-20 08:00:12	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,039	-	More Info
2023-06-20 07:00:10	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,039	-	More Info
2023-06-20 06:00:07	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,040	-	More Info
2023-06-20 05:00:08	10.0.0.69	Indonesia	10.0.0.11	Indonesia	syslog	1,040	-	More Info

Gambar 5. Threat Hunting IP 10.0.0.69

Pada gambar 3 dan 4, dapat diketahui bahwa traffic/lalu lintas dalam waktu 1 minggu dari IP 10.0.0.69 sebanyak 152 kali, dengan total lebih dari 3000 bytes permintaan syn dalam waktu 5 menit, serta ada kegiatan anomaly pada tanggal 19 Juni 2023 yang mana traffic nya sangat tinggi dan ini mengindikasikan sebagai syn flood attack.

c. Analisis Threat Intelligence

VirusTotal

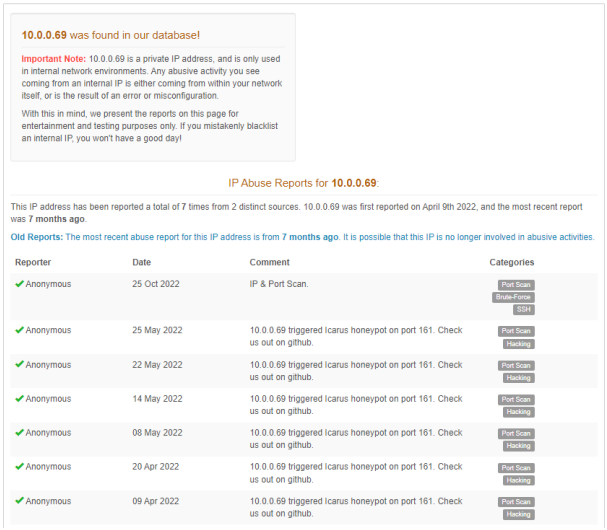


Gambar 6. Pengecekan VirusTotal

Berdasarkan pengecekan pada VirusTotal, IP 10.0.0.69 terindikasi menggunakan koneksi proxy dan memiliki reputasi sebagai SPAM blacklist dan memiliki aktivitas abusive.

AbuseIPDB

Gambar IV. 6



Gambar 1 7. Pengecekan pada AbuseIPDB

Berdasarkan pengecekan pada AbuseIPDB, IP 10.0.0.69 terindikasi sebagai IP / Port Scan, Brute-Force, dan Hacking.

3. Containment, Eradication & Recovery

Tahap Containment, Eradication, & Recovery dilakukan untuk meminimalkan dampak peristiwa pada sistem yang diserang. Pada tahap ini, Tim SOC Analyst memberikan mitigasi atas serangan syn flood yang terjadi berdasarkan MITREATT&CK.

Gambar 8. Mitigasi Based on MITREATT&CK

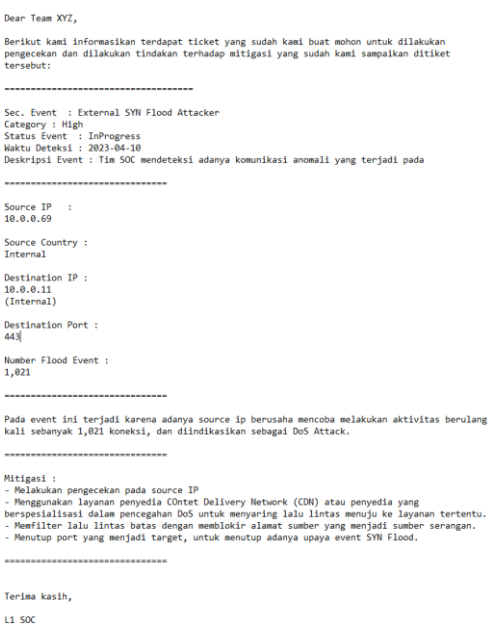
Berdasarkan mitigasi dari MITREATT&CK, dapat kita ketahui sebagai berikut:

a. Gunakan firewall atau perangkat jaringan yang dapat menggunakan pemfilteran paket untuk memblokir lalu lintas yang mencurigakan atau berlebihan. Ini memerlukan penyiapan aturan firewall yang membatasi jumlah permintaan koneksi TCP yang diizinkan pada saat yang bersamaan.

b. Mengubah beberapa parameter konfigurasi TCP/IP server untuk meningkatkan ketahanannya terhadap serangan syn flooding. Misalnya, mengatur timeout (Batasan waktu) yang lebih singkat untuk menutup koneksi yang tidak aktif, mengurangi waktu tunggu sinkronisasi (SYN) untuk mengurangi jumlah permintaan SYN yang belum selesai, atau mengaktifkan cookie TCP SYN untuk mengidentifikasi dan memproses permintaan SYN yang mencurigakan.
c. Menggunakan layanan penyedia Content Delivery Network (CDN) atau penyedia yang berspesialisasi dalam pencegahan DoS untuk menyaring lalu lintas menuju ke layanan tertentu.
d. Memfilter lalu lintas batas dengan memblokir alamat sumber yang menjadi sumber serangan.

4. Post-Incident Activity

Pada tahap ini, Tim SOC Analyst membuat melakukan reporting kepada klien yang mendapatkan serangan syn flood.



```
Dear Team XYZ,

Berikut kami informasikan terdapat ticket yang sudah kami buat mohon untuk dilakukan
pengecekan dan dilakukan tindakan terhadap mitigasi yang sudah kami sampaikan ditiket
tersebut:

--------------------------------------

Sec. Event  : External SYN Flood Attacker
Category : High
Status Event  : InProgress
Waktu Deteksi : 2023-04-10
Deskripsi Event : Tim SOC mendeteksi adanya komunikasi anomali yang terjadi pada

--------------------------------

Source IP   :
10.0.0.69

Source Country :
Internal

Destination IP :
10.0.0.11
(Internal)

Destination Port :
443

Number Flood Event :
1,021

--------------------------------

Pada event ini terjadi karena adanya source ip berusaha mencoba melakukan aktivitas berulang
kali sebanyak 1,021 koneksi, dan diindikasikan sebagai DoS Attack.

--------------------------------

Mitigasi :
- Melakukan pengecekan pada source IP
- Menggunakan layanan penyedia COntet Delivery Network (CDN) atau penyedia yang
berspesialisasi dalam pencegahan DoS untuk menyaring lalu lintas menuju ke layanan tertentu.
- Memfilter lalu lintas batas dengan memblokir alamat sumber yang menjadi sumber serangan.
- Menutup port yang menjadi target, untuk menutup adanya upaya event SYN Flood.

--------------------------------


Terima kasih,

L1 SOC
```

Gambar 9. Hasil report syn flood attack

4.4. Hasil Penelitian

Dari data penelitian dan analisis di atas, didapatkan syn flood attack dari IP 10.0.0.69 adalah critical berdasarkan flood event yang diinformasikan oleh SIEM, traffic dalam time interval past week sebanyak 152 kali, dengan total lebih dari 3000 bytes permintaan syn dalam waktu 5 menit, serta ada kegiatan anomaly pada tanggal 19 Juni 2023 yang mana traffic nya sangat tinggi. Berdasarkan data tersebut, Tim SOC Analyst memutuskan untuk mereport serangan tersebut kepada klien yang bersangkutan.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terhadap analisis syn flood attack menggunakan metode NIST 800-61 Rev 2 pada Security information and event management (SIEM), dapat ditarik kesimpulan sebagai berikut:

1. Security information and event management (SIEM) terbukti efektif dapat mendeteksi serangan SYN Flood.
2. Metodologi NIST 800-61 Rev 2 menyediakan kerangka kerja komprehensif untuk mendeteksi, menganalisis, dan merespons serangan SYN Flood.
3. Dalam kurun waktu 1 bulan, banyak serangan syn flood yang terdeteksi oleh Security information and event management (SIEM).
4. Adanya serangan-serangan lain selain yang diinformasikan oleh Security information and event management (SIEM), seperti External Trojan, External Spyware, External Ransomware, dan lain-lain.

B. Saran

1. Integrasikan SIEM dengan sistem keamanan lain seperti Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) untuk

meningkatkan deteksi dan respons terhadap SYN Flood Attack.
2. Untuk penelitian selanjutnya, dapat menggunakan metode lain seperti ISO, dan juga menggunakan Security information and event management (SIEM) lain, seperti Splunk, Wazuh, ataupun Elastic.
3. Untuk mencegah terjadinya serangan syn flood yang critical, disarankan untuk melakukan pemeriksaan secara berkala pada perangkat-perangkat yang digunakan.
4. Melakukan pemeriksaan secara berkala untuk mencegah terjadinya serangan-serangan siber yang lainnya.

DAFTAR PUSTAKA

Chandra, J. C. (2021). *MODEL FRAMEWORK UNTUK ANALISIS KEAMANAN DARI SERANGAN DENIAL OF SERVICE PADA SISTEM E-LEARNING UNIVERSITAS BUDI LUHUR*.

Dehan Pratama, M., Nova, F., & Prayama, D. (n.d.). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. In *Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos JITSI : Jurnal Ilmiah Teknologi Sistem Informasi* (Vol. 3, Issue 1). http://jurnal-itsi.org

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14). https://doi.org/10.3390/s21144759

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (n.d.). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158. https://doi.org/10.33164/iptekkom.22.2.2020.143-158

Khotimah, H., Bimantoro, F., Silas Kabanga, R., Bagus, I., & Widiartha, K. (n.d.). *IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PADA APLIKASI SMS CENTER PEMERINTAH DAERAH PROVINSI NUSA TENGGARA BARAT (Implementation of Security Information And Event Management (SIEM) in The SMS Center Application for The West Nusa Tenggara Provincial Government)*. http://begawe.unram.ac.id/index.php/JBTI/

Riadi, I. (n.d.). *Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express*. http://openjournal.unpam.ac.id/index.php/informatika89

Sahren, S. (2021). IMPLEMENTASI TEKNOLOGI FIREWALL SEBAGAI KEAMANAN SERVER DARI SYN FLOOD ATTACK. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *7*(2), 159–164. https://doi.org/10.33330/jurteksi.v7i2.933

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. In *Risalah Hukum* (Vol. 17, Issue 2).

Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(3), 949–955. https://doi.org/10.18517/ijaseit.8.3.3591