Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

ANALISIS MANFAAT MACHINE LEARNING PADA NEXT-GENERATION FIREWALL SOPHOS XG 330 DALAM MENGATASI SERANGAN SQL INJECTION

Celvine Adi Putra[1], Rianda Pratama[2], Tata Sutabri[3]

[123,] Program Studi Magister Teknik Informatika, Universitas Bina Darma Palembang

Jl. Jenderal A. Yani No. 3 Palembang, Sumatera Selatan
[1] celvineadiputra@gmail.com, [2] riandapratama08@gmail.com, [3] tata.sutabri@gmail.com

Abstract

With the ongoing development of the digital world, information technology generates a significant amount of valuable data. However, this valuable data also poses risks to the companies that store it, particularly regarding cyber-attacks. One common cyber threat is SQL Injection, which can manipulate access rights and lead to data breaches, data loss, and unauthorized access to databases. Consequently, companies and organizations need to protect their data from potential threats that may arise. To address SQL Injection attacks, the utilization of Next-Generation Firewalls (NGFW), such as Sophos XG 330, has emerged as a superior solution to traditional firewalls. NGFWs can perform more detailed packet inspections and implement machine learning techniques, enabling them to detect more complex security threats or previously unknown attacks. This research analyzes the benefits of implementing machine learning in Next-Generation Firewalls, specifically in identifying and blocking ongoing attacks. The findings of this study provide valuable insights for companies or organizations in selecting the appropriate solutions to protect their data.

Keywords : *Machine Learning, Next-Generation Firewall, SQL Injection, Sophos XG 330*

Abstrak

Dengan perkembangan dunia digital yang terus berkembang, penggunaan teknologi informasi menghasilkan sejumlah besar data yang berharga, dengan adanya data yang berharga ini membuat perusahaan yang menyimpannya memiliki risiko terhadap serangan siber. Salah satu ancaman siber yang umum terjadi adalah SQL Injection yang dapat memanipulasi hak akses dan menyebabkan kebocoran data, kehilangan data, dan kehilangan hak akses ke dalam database. Sehingga membuat perusahaan dan organisasi untuk dapat melindungi data mereka dari segala jenis ancaman yang mungkin akan terjadi. Dalam upaya untuk dapat mengatasi serangan *SQL Injection* penggunaan teknologi Next-Generation Firewall (NGFW) seperti Sophos XG 330 telah muncul sebagai solusi yang lebih unggul dibandingkan dengan firewall tradisional. NGFW mampu melakukan inspeksi paket yang lebih rinci dan menerapkan teknik pembelajaran mesin, memungkinkan mereka untuk mendeteksi ancaman keamanan yang lebih kompleks atau serangan yang sebelumnya tidak diketahui. Dalam penelitian ini kami melakukan analisis terkait dengan manfaat penerapan dari *machine learning* pada *Next-Generation Firewall*, dalam hal untuk dapat mengidentifikasi dan memblokir serangan yang terjadi. Hasil dari penelitian ini memberikan pengetahuan untuk perusahaan atau organisasi dalam memilih solusi yang tepat untuk dapat melindungi data mereka.

Kata kunci : *Machine Learning, Next-Generation Firewall, SQL Injection, Sophos XG 330*

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

1. PENDAHULUAN

Perlindungan terhadap data dan jaringan merupakan aspek yang krusial dalam industri teknologi informasi, karena jaringan merupakan sarana utama dalam melakukan komunikasi dan berbagi data atau informasi[1]. Di era digital saat ini, data telah menjadi salah satu aset yang sangat berharga bagi perusahaan atau organisasi. Data-data ini dapat menjadi sumber informasi yang penting dan digunakan untuk membuat keputusan yang lebih baik dalam bisnis jika dapat diolah dengan benar. Namun, karena data-data tersebut sangat berharga maka akan ada ancaman siber sebagai upaya untuk mendapatkan akses ke dalam data tersebut. Oleh karena itu, perusahaan dan organisasi harus terus dapat berinovasi dalam penggunaan teknologi untuk melindungi data mereka.

Salah satu jenis serangan siber yang umum terjadi dan dapat menyebabkan kerusakan pada data, pencurian data, kehilangan data, dan bahkan penyerang dapat mengambil alih dari kontrol database yaitu *SQL Injection*. *SQL Injection* ini memanfaatkan celah keamanan yang terdapat pada sistem atau aplikasi untuk menyerang database pada website[2], dengan cara menginjeksi atau mengirimkan kode SQL yang berbahaya ke dalam database yang digunakan, sehingga penyerang dapat melakukan manipulasi data dengan mudah dan dapat mengakses data yang seharusnya tidak dapat diakses. *SQL Injection* sendiri dapat terjadi karena kurangnya validasi data input, seperti karakter yang diizinkan, format data, dan jumlah data, sehingga membuat aplikasi langsung mengeksekusi input yang dimasukkan oleh user secara langsung[3]. *SQL Injection* sendiri dapat dideteksi dengan cara tradisional dilakukan dengan menggunakan teknik pengenalan *sign* atau *pattern*.

Selain itu, salah satu cara lain untuk mengatasi *SQL Injection* dapat menggunakan *web application firewall* (WAF)[4]. Namun dengan seiring dengan perkembangan teknologi, serangan *SQL Injection* menjadi semakin kompleks dan sulit untuk dideteksi oleh WAF. Hal ini disebabkan oleh cara kerja WAF yang bekerja dengan menerapkan aturan *(rules)* untuk dapat mendeteksi serangan. Jika serangan tidak sesuai dengan aturan yang telah ditentukan sebelumnya maka WAF tidak dapat mendeteksinya sebagai serangan, sehingga WAF tidak mampu mendeteksi serangan baru atau yang belum diketahui, selain itu masih terdapat kemungkinan WAF salah dalam mendeteksi *requests* sebagai sebuah ancaman ke dalam aplikasi, yang membuat aplikasi tidak dapat diakses oleh pengguna[4].

Sehingga diperlukan solusi yang lebih baik lagi untuk dapat mendeteksi serangan *SQL Injection*, seperti *Next-Generation Firewall (NGFW)*. *Next Generation Firewall* merupakan jenis dari *firewall* yang lebih canggih dan kompleks dibandingkan dengan *firewall* tradisional. NGFW dapat melakukan pemeriksaan paket data secara lebih detail, termasuk pemeriksaan berdasarkan konten dan perilaku, sehingga dapat mendeteksi ancaman keamanan yang lebih kompleks seperti *malware*, *phishing*, *SQL Injection*, dan *DDoS*, selain itu juga NGFW dapat terintegrasi dengan fitur-fitur *tambahan intrusion Prevention System (IPS)*, *Antispam & Mail, Threat Emulation, URL filtering & application control* yang dapat meningkatkan keamanan jaringan[5].

Penggunaan NGFW saja tidak menjamin kalau semua serangan dapat dideteksi, hal ini disebabkan karena serangan siber terus berkembang, dengan pola-pola serangan yang baru, sehingga untuk mengatasi hal ini penggunaan *machine learning* dapat menjadi sebuah solusi untuk dapat meningkatkan efektivitas dan keamanan dari NGFW. Dengan menggunakan *machine learning*, NGFW dapat terus belajar dan dapat memahami pola serangan yang lebih kompleks, sehingga dapat mencegah atau deteksi jika terjadi serangan.

Penerapan machine learning pada NGFW dapat dilakukan dengan menggunakan hardware Sophos XG 330. Layanan ini memiliki kemampuan untuk mendeteksi dan mencegah serangan dengan lebih akurat, menganalisis data jaringan dengan cepat, terintegrasi dengan teknologi keamanan lainnya, serta antarmuka pengguna yang mudah digunakan. Sophos XG 330 dapat memperbarui pola serangan dan membuat keputusan yang lebih akurat dalam menghadapi serangan siber. Dengan adanya teknologi *machine learning* pada Sophos XG 330, perusahaan atau organisasi dapat dengan mudah mengidentifikasi serangan yang sebelumnya belum pernah terjadi dan memberikan respons yang tepat terhadap serangan tersebut. Sehingga dengan adanya penelitian ini diharapkan dapat memberikan gambaran dan informasi kepada pihak kominfo untuk dapat mengambil langkah, dalam mengatasi serangan yang terjadi.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

2. TINJAUAN PUSTAKA

Machine learning (ML) adalah cabang dari kecerdasan buatan yang memungkinkan sistem komputer untuk dapat belajar dan meningkatkan kinerjanya secara otomatis dari pengalaman yang telah diperoleh sebelumnya, tanpa harus diprogram secara eksplisit[6]. Pada machine learning algoritma dan model statistik digunakan untuk dapat menganalisis data, mengidentifikasi pola, dan membuat prediksi atau keputusan dari data tersebut[5].

Terdapat beberapa teknik yang digunakan dalam *machine learning* untuk menghasilkan model yang dapat digunakan untuk memprediksi atau mengklasifikasikan data. Namun, pada dasarnya terdapat dua teknik utama yang sering digunakan, yaitu pembelajaran *supervised learning* dan *unsupervised learning*[7].

Supervised learning adalah teknik yang menggunakan data yang telah diberi label atau di kategori oleh manusia. Dengan teknik ini, mesin mempelajari pola dan hubungan antara data masukan dan keluaran yang telah ditentukan sebelumnya[8].

Sedangkan, *Unsupervised learning* adalah teknik yang tidak menggunakan data yang telah diberi label atau kategori oleh manusia. Dalam teknik ini, mesin dapat mencari pola dan hubungan dalam data tanpa adanya panduan atau kategori tertentu[9].

Next-Generation firewall (NGFW) lebih baik dibandingkan dengan *firewall* tradisional, karena NGFW memiliki kemampuan *firewall* tradisional dan juga memiliki beberapa fitur tambahan untuk dapat mengatasi lebih banyak jenis ancaman, dan NGFW dapat melakukan inspeksi paket lebih dalam lagi hingga level aplikasi[10].

SQL Injection adalah serangan pada aplikasi web yang memungkinkan penyerang untuk dapat memanipulasi perintah SQL yang akan dieksekusi oleh aplikasi[11]. Serang ini dilakukan dengan menyisipkan kode SQL kedalam input yang diterima oleh aplikasi, sehingga dapat mengakses atau merubah data dalam *database*. Terdapat beberapa jenis *SQL Injection*, pertama, *In-band SQLi*, di mana serangan dilakukan melalui satu saluran komunikasi dan data diambil langsung dari database. Kedua, *Inferential SQLi*, di mana teknik *blind injection* digunakan dan penyerang tidak dapat melihat hasil langsung dari serangan. Ketiga, *Out-of-band SQLi*, di mana saluran komunikasi lain selain HTTP digunakan untuk mengambil data dari *database*. Keempat, *Error-based SQLi*, di mana pesan error yang dihasilkan oleh server *database* dimanfaatkan untuk mendapatkan informasi sensitif. Kelima, *Union-based SQLi*, di mana operator UNION pada perintah SQL digunakan untuk menggabungkan hasil query dari dua atau lebih tabel. Keenam, *Boolean-based SQLi*, di mana pernyataan boolean pada perintah SQL digunakan untuk mengekstrak informasi sensitif dari *database*. Ketujuh, *Time-based SQLi*, di mana eksekusi query pada server database diperlambat untuk mendapatkan informasi sensitif secara bertahap[12]. Terakhir *Piggy-backed Query* pada jenis ini penyerang akan mencoba untuk memasukkan query tambahan untuk dapat mengekstrak data, memanipulasi, atau menambah data[13]. Semua jenis SQL Injection ini perlu diwaspadai dan dihindari untuk menjaga keamanan database.

Untuk mencegah *SQL injection*, ada beberapa cara yang dapat dilakukan. Pertama, pastikan *input* yang diterima oleh aplikasi web valid dan sesuai dengan tipe data yang diharapkan. Kedua, gunakan *parameterized statements* pada perintah SQL untuk memastikan bahwa input dari pengguna tidak dieksekusi sebagai bagian dari perintah SQL. Ketiga, gunakan *escape characters* pada *input* yang diterima oleh aplikasi web untuk menghindari karakter-karakter khusus yang dapat dimanipulasi oleh penyerang[14]. Keempat, berikan hak akses terendah yang memungkinkan pada user atau role database, sehingga jika terjadi serangan *SQL injection*, kerusakan yang ditimbulkan dapat diminimalkan. Terakhir, pastikan bahwa *software* dan sistem operasi yang digunakan selalu diperbarui dengan patch terbaru untuk mengatasi kerentanan keamanan.

Firewall merupakan sebuah sistem atau pun perangkat yang mengatur izin dalam lalu lintas jaringan, yang berfungsi untuk melakukan filter terhadap *request* yang aman dan tidak aman[15].

Sophos XG 330 adalah jenis *Next-Generation Firewall (NGFW)* yang dirancang untuk memberikan perlindungan yang lebih canggih dan efektif dalam menghadapi serangan *cyber*. Dengan fitur-fiturnya, Sophos XG 330 bisa memblokir serangan seperti *malware, ransomware*, dan serangan DDoS. Selain itu, Sophos XG 330 juga dilengkapi dengan teknologi *machine learning* yang bisa mempelajari pola serangan dan memberikan perlindungan yang lebih adaptif. Anda juga bisa mengintegrasikan Sophos XG 330 dengan berbagai sistem keamanan lainnya, seperti antivirus, IPS, dan web filtering, sehingga

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

bisa memberikan perlindungan yang lebih komprehensif.

Penelitian terdahulu yang membahas tentang masalah yang sama, memiliki judul "*Detection of SQL Injection Attacks: A Machine Learning Approach*", pada penelitian menggunakan 23 metode dari machine learning dengan menggunakan MATLAB, dengan total 616 SQL *statements*, dari 23 metode yang digunakan mereka mendapatkan 5 model yang terbaik, dengan menggunakan ensemble boosted, bagged trees, linear discriminant, cubic SVM, dan fine Gaussian SVM[16].

Penelitian selanjutnya dengan judul "*A CNN-BiLSTM based Approach for Detection of SQL Injection Attacks*", pada penelitian ini menggunakan *hybrid CNN-BiLSTM-based* yang digunakan untuk mendeteksi serangan, pada penelitian ini mendapatkan akurasi sebesar 98%.

Penelitian selanjutnya memiliki judul "*Hybrid Approach to Detect SQLi Attacks and evansion techniques*", pada penelitian ini menggunakan dua pendekatan yang pertama dengan menggunakan metode pencocokan pola, yang sama dengan metode signature-based, dan pendekatan kedua dengan menggunakan machine learning, dengan cara mengekstraksi fitur data-data yang berbahaya, dengan menggunakan SVM, naive Bayes, dan K-NN[17].

Penelitian dengan judul "*Next Generation Firewall for Improving Security in Company and IoT Network*", tujuan dari penelitian ini adalah menganalisis efektivitas NGFW dalam meningkatkan keamanan pada jaringan IoT pada rumah dan perusahaan. Hasil dari penelitian ini menunjukkan bahwa *Next-Generation Firewall* secara signifikan meningkatkan keamanan jaringan komunikasi data terhadap ancaman seperti DDoS, *phishing*, dan *SQL Injection*. Penelitian ini menggunakan metode perbandingan dengan pengujian serangan DDoS, *phishing*, dan *SQL Injection* pada kedua jaringan, yaitu jaringan rumah pintar dan jaringan perusahaan[18].

Penelitian Selanjutnya dengan judul "*Detecting SQL Injection Attacks Using Grammar Recognition and Access Behavior Mining",* pada penelitian ini peneliti mengusulkan model yang disebut sebagai ATTAR, yang berfungsi untuk mendeteksi serangan *SQL Injection* dengan cara menganalisis *log* akses *web* untuk mengekstrak fitur dari serangan *SQL Injection.* Mereka menggunakan lima algoritma *machine learning*, *naïve Bayesian, random forest, SVM, ID3, dan K-means.* Mendapatkan hasil bahwa dengan menggunakan *random forest* dan *ID3,* mendapatkan hasil yang terbaik, dalam mendeteksi serangan *SQL Injection*[19].

Penelitian Selanjutnya dengan judul *"DeepSQLi: Deep Semantic Learning for Testing SQL Injection",* mengusulkan *deep learning* yang disebut dengan DeepSQLi. Pada penelitian ini mereka membandingkan DeepSQLi dengan SQLmap, yang menghasilkan bahwa DeepSQLi dapat mengidentifikasi kerentanan pada sistem lebih banyak dibandingkan dengan SQLmap[20].

Penelitian Selanjutnya dengan judul "*SQL Injection Attack Detection Using Machine Learning Algorithm*", mendapatkan hasil bahwa algoritma dari *machine learning* dapat dengan efektif dalam mendeteksi serangan *SQL Injection.* Pada penelitian ini menggunakan algoritma *Logistic Regression (LRN), Stochastic Gradient Descent (SDG), Sequential Minimal Optimization (SMO), Bayes Network (BNK), Instance-Based Learner (IBK), Multilayer Perceptron (MLP), Naive Bayes (NBS),* dan *J48.* Kinerja algoritma ini di evaluasi dengan menggunakan metode *Hold-Out* dan *10-fold cross validation.* Berdasarkan hasil penelitian mendapatkan algoritma SMO, IBK, dan J48 mendapatkan akurasi yang tertinggi[21].

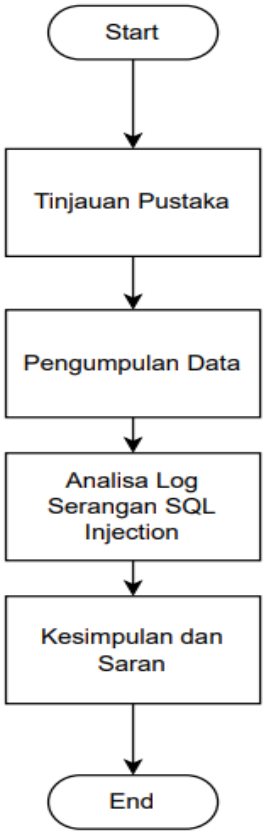
Dalam penelitian, kami melakukan analisis data lalu lintas jaringan yang terjadi, untuk mengevaluasi kemampuan dari penerapan *machine learning* pada *next-generation firewall,* dalam mengidentifikasi *SQL Injection.*

3. METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Penelitian ini terdapat empat tahapan utama yang dilakukan secara sistematis untuk dapat mencapai tujuan dari penelitian yang telah direncanakan sebelumnya. Tahapan penelitian tersebut yaitu tinjauan pustaka, pengumpulan data, analisis log serangan, dan pembuatan kesimpulan serta saran.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi



Gambar 1. Tahapan Penelitian

Tahap pertama adalah tinjau pustaka, pada tahap ini melakukan studi terhadap penelitian dan sumber-sumber yang relevan mengenai topik penelitian, yang bertujuan untuk memperoleh pemahaman yang lebih mendalam tentang topik yang akan diteliti.

Tahap kedua dilanjutkan dengan pengumpulan data, pada tahap ini proses pengumpulan data dilakukan dengan cara wawancara dan diskusi bersama dengan pihak yang terkait, yang dilanjutkan dengan pengambilan data berupa log serangan yang telah terjadi.

Setelah semua yang diperlukan terkumpul dilanjutkan dengan melakukan analisis terhadap data yang telah diperoleh.

Tahap terakhir membuat kesimpulan serta saran, yang diperoleh berdasarkan hasil analisis pada tahap sebelumnya.

3.2. Tinjau Pustaka

Metode penelitian yang digunakan dalam penelitian ini adalah tinjauan pustaka. Tinjauan pustaka adalah pendekatan yang sering digunakan untuk mengumpulkan, mengevaluasi, dan merangkum penelitian yang telah ada tentang topik tertentu.

3.3. Pengumpulan Data

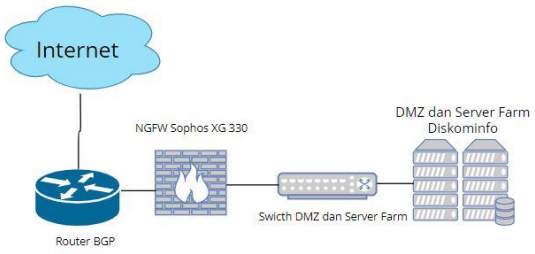
Pengumpulan data diperoleh dengan melakukan wawancara dan diskusi dengan pihak seksi keamanan informasi dan persandian dinas komunikasi dan informatika kota Palembang. Kemudian dilanjutkan dengan proses pengambilan data berupa log serangan yang terjadi, dimulai dari tanggal 1 januari 2023 sampai dengan 23 mei 2023, yang akan digunakan untuk melakukan analisis serangan yang telah terjadi.

3.4. Analisa Log Serangan

Pada tahapan ini dilakukan proses analisis log serangan pada perangkat NGFW Sophos XG330 dan memilah data yang berkaitan dengan serangan SQL injection yaitu data jenis serangan sql injection, port yang di eksploitasi, ip penyerang dan asal negara ip penyerang.

4. HASIL DAN PEMBAHASAN

Implementasi NGFW pada Sophos XG330 terletak sebagai pintu masuk yang menuju *demilitarized zone* (DMZ) dan *server farm*, sehingga seluruh *traffic* yang masuk ke *demilitarized zone* (DMZ) dan *server farm* akan di *scanning* oleh NGFW Sophos XG330. *Machine learning* yang terdapat pada sistem NGFW Sophos XG330 ini memungkinkan dinas komunikasi dan informatika dapat menyaring berbagai jenis serangan dan dapat melakukan klasifikasi terhadap serangan *SQL Injection.*



Gambar 2. Topologi Implementasi NGFW Sophos XG330

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

Berdasarkan data hasil *scanning* Sophos XG330, dilakukan analisis dari serangan yang telah terjadi berdasarkan *log* yang diperoleh sebelumnya, dilanjutkan dengan memilih *feature* yang akan menjadi fokus pada penelitian ini, maka dipilihlah kategori *SQL Injection*. Sehingga diperoleh data *log SQL Injection*, yang terjadi sebanyak 11002 serangan, dengan detail sebagai berikut ini.

Tabel 1. Serangan SQL Injection 1 Januari – 23 Mei 2023

No	SQL Attack	Hits
1	SQL use of sleep function with select - likely SQL injection	3888
2	SQL union select - possible sql injection attempt - GET parameter	1964
3	SQL 1 = 1 - possible sql injection attempt	1497
4	SQL use of sleep function with and - likely SQL injection	1131
5	SQL use of concat function with select - likely SQL injection	792
6	SQL 1 = 0 - possible sql injection attempt	699
7	SQL url ending in comment characters - possible sql injection attempt	587
8	SQL union select - possible sql injection attempt - POST parameter	444

Dari table 1, dapat dilihat bahwa terdapat 8 jenis variasi serangan yang telah terjadi. Serangan tersebut dapat dikategorikan berdasarkan tingkat *severity,* yaitu *severity critical* dan *severity* major. Tingkat *serverity critical* terjadi sebanyak 10415 kali, dan sedangkan untuk *severity major* sebanyak 587 kali.

Berdasarkan table 1, serangan yang termasuk dalam kategori *severity major* adalah *SQL url ending in comment character - possible sql injection attempt.* Selain dari itu termasuk dalam kategori *critical*.

Selain itu, terdapat data yang menunjukkan bahwa terdapat 16 port yang dieksploitasi oleh penyerang untuk melakukan SQL Injection, dapat dilihat pada tabel 2.

Tabel 2. Daftar Port Yang Dieksploitasi

No	App / Porto : Port	Hits
1	HTTP	3660
2	TCP:3005	2020
3	TCP:3003	804
4	TCP:5003	788
5	TCP:3001	493
6	TCP:3013	424
7	TCP:3007	402
8	TCP:3012	352
9	TCP:3311	330
10	TCP:3008	279
11	TCP:3004	270
12	TCP:5005	266
13	TCP:3014	250
14	TCP:5013	108
15	TCP:5004	100
16	TCP:5001	97
17	TCP:5012	66
18	TCP:5007	63
19	TCP:5008	55
20	TCP:5014	45
21	TCP:3312	33
22	TCP:30021	29
23	TCP:5000	24
24	TCP:5511	21
25	TCP:5002	19

Selanjutnya, proses analisis data dapat dilanjutkan dengan mencari alamat IP yang digunakan oleh penyerang beserta dengan jumlah serangan yang dilakukan. Data tersebut dapat dilihat pada tabel 3.

Tabel 3. Alamat IP Penyerang

No	App / Porto : Port	Hits
1	103.138.143.34	7868
2	101.128.98.105	775
3	139.162.45.240	573
4	190.2.132.213	379
5	91.205.172.31	346
6	103.132.52.199	277
7	143.92.35.90	198
8	103.104.12.80	185
9	103.132.55.26	92
10	20.198.216.96	85
11	182.253.36.38	73
12	37.187.158.97	60
13	178.18.242.213	32
14	62.233.50.73	16
15	202.43.249.91	14
16	96.9.70.188	8

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

17	103.144.175.157	8
18	206.189.136.21	2
19	202.112.238.179	2
20	185.191.171.45	2
21	173.245.203.129	2
22	185.191.171.22	2
23	185.191.171.11	2
24	45.14.165.117	1

Berdasarkan Tabel 3, dilakukan proses klasifikasi alamat IP berdasarkan asal negara dan jumlah serangan. Berdasarkan Tabel 4, ditemukan bahwa alamat IP yang berasal dari Indonesia merupakan yang paling banyak melakukan serangan. Alamat IP 103.138.143.34 merupakan alamat IP internal diskominfo yang digunakan untuk melakukan uji coba penggunaan machine learning pada NGFW, dengan jumlah uji coba sebanyak 7868 kali. Total alamat IP yang berasal dari Indonesia sebanyak 9292, sehingga sebanyak 1424 lainnya merupakan serangan yang masuk ke dalam sistem Kominfo.

Tabel 4. Jumlah Serangan Berdasarkan Negara

No	SQL Attack	Hits
1	Indonesia	9292
2	Singapore	658
3	Netherlands	379
4	Germany	378
5	Hong Kong SAR China	198
6	France	60
7	Rusia	16
8	Cambodia	8
10	United Kingdom	6
11	United States	3
12	China	2

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis log yang ada pada Next-Generation Firewall dengan Sophos XG330 dengan penerapan Machine Learning Intercept X, didapat bahwa serangan SQL Injection sering terjadi pada port TCP:80 (HTTP) dengan jumlah serangan sebanyak 3060 kali, dan port TCP:3005 dengan jumlah serangan sebanyak 2020 kali. Variasi serangan yang paling dominan adalah SQL use of sleep function with select - likely SQL Injection, dengan jumlah percobaan serangan sebanyak 3888 kali. Data-data tersebut dapat membantu pihak pengelola untuk melakukan analisis dan memperkuat konfigurasi baik dari sisi jaringan maupun dari sisi aplikasi sehingga meningkatkan keamanan jaringan diskominfo kota Palembang.

6. UCAPAN TERIMA KASIH

Terima kasih kepada Kementerian Komunikasi dan Informatika kota Palembang yang telah memberikan izin untuk pengambilan data yang diperlukan dalam penelitian ini. Terima kasih juga kepada Universitas Bina Darma yang telah mendukung penelitian ini secara akademik. Kami mengapresiasi semua pihak yang terlibat dalam terbitnya penelitian ini, baik secara langsung maupun tidak langsung. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan dan teknologi di bidang komunikasi dan informatika.

DAFTAR PUSTAKA:

[1] T. Sutabri, *Sistem Informasi Manajemen*, 2nd ed. Yogyakarta: Andi, 2016.

[2] R. Dinata, "Implementasi Sistem Pendeteksi Serangan SQL Injection dengan Menggunakan Algoritme K-Nearest Neighbor," 2019. [Online]. Available: http://j-ptiik.ub.ac.id

[3] J. Friadi and S. Septian, "ZONA TEKNIK: JURNAL ILMIAH Aplikasi Machine Learning Untuk Deteksi Serangan Code Injection," pp. 443–451, 2021, doi: 10.37776/zt.vxix.xxx.

[4] R. Dinata, "Implementasi Sistem Pendeteksi Serangan SQL Injection dengan Menggunakan Algoritme K-Nearest Neighbor," 2019. [Online]. Available: http://j-ptiik.ub.ac.id

[5] B. Soewito and C. E. Andhika, "Next Generation Firewall for Improving Security in Company and IoT Network," 2019.

[6] P. Ramayanti and T. Sutabri, "PERBANDINGAN ALGORITMA NAÏVE BAYES DAN SVMUNTUK ANALISIS PENYALAHGUNAAN KEJAHATAN CARDING," pp. 18–24, 2023.

[7] R. Handoko and T. Sutabri, "ANALISA MACHINE LEARNING DENGAN ALGORITMA MULTI-LAYER PERCEPTRON UNTUK PENANGANAN KEJAHATAN PHISHING," 2023.

[8] Q. Liu and Y. Wu, "Supervised Learning," in *Encyclopedia of the Sciences of Learning*,

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 2, Juni 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

Springer US, 2012, pp. 3243–3245. doi: 10.1007/978-1-4419-1428-6_451.

[9] G. Wang, S. Ren, and H. Wang, "NccFlow: Unsupervised Learning of Optical Flow With Non-occlusion from Geometry," Jul. 2021, [Online]. Available: http://arxiv.org/abs/2107.03610

[10] E. Dwi Setiawan and M. Raharjo, "PERANCANGAN KEAMANAN JARINGAN NEXT-GENERATION FIREWALLMENGGUNAKAN ROUTER FORTINETPADA PT. ALODOKTER TEKNOLOGI SOLUSI," *Jurnal Informatika Terpadu*, vol. 9, no. 1, pp. 34–39, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[11] A. Mutedi and B. Tjahjono, "Systematic Literature Review: Preventing SQL Injection Attacks Using Tools OWASP CSR Web Application Firewall," *Maret*, vol. 7, no. 1, pp. 151–156, doi: 10.32493/informatika.v7i1.17590.

[12] W. G. J. Halfond, J. Viegas, and A. Orso, "A Classification of SQL Injection Attacks and Countermeasures," 2006.

[13] I. Jemal, O. Cheikhrouhou, H. Hamam, and A. Mahfoudhi, "SQL Injection Attack Detection and Prevention Techniques Using Machine Learning," 2020. [Online]. Available: http://www.ripublication.com

[14] F. South, T. Usf, D. Graduate, G. Usf, D. Theses, and C. Cetin, "Authentication and SQL-Injection Prevention Techniques in Web Authentication and SQL-Injection Prevention Techniques in Web Applications Applications," 2019. [Online]. Available: https://digitalcommons.usf.edu/etd

[15] D. R. Akhiruddin and T. Sutabri, "ANALISIS PENINGKATAN KEAMANAN PADA SIMPLE NETWORK TIME PROTOCOL (SNTP) UNTUK MENDETEKSI CYBERCRIME DALAM AKTIFITAS JARINGAN MENGGUNAKAN METODE FIREWALL," *Blantika : Multidisciplinary Jornal*, vol. 2, no. 1, p. 2023, [Online]. Available: https://blantika.publikasiku.id/

[16] M. Hasan, Z. Balbahaith, and M. Tarique, *Detection of SQL Injection Attacks: A Machine Learning Approach*. 2019.

[17] A. Makiou, Y. Begriche, and A. Serhrouchni, "Hybrid approach to detect SQLi attacks and evasion techniques," in *CollaborateCom 2014 - Proceedings of the 10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Institute of Electrical and Electronics Engineers Inc., Jan. 2015, pp. 452–456. doi: 10.4108/icst.collaboratecom.2014.257568.

[18] N. Gandhi, J. Patel, R. Sisodiya, N. Doshi, and S. Mishra, "A CNN-BiLSTM based Approach for Detection of SQL Injection Attacks," in *Proceedings of 2nd IEEE International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 378–383. doi: 10.1109/ICCIKE51210.2021.9410675.

[19] H. Gao, J. Zhu, L. Liu, J. Xu, Y. Wu, and A. Liu, "Detecting SQL injection attacks using grammar pattern recognition and access behavior mining," in *Proceedings - IEEE International Conference on Energy Internet, ICEI 2019*, Institute of Electrical and Electronics Engineers Inc., May 2019, pp. 493–498. doi: 10.1109/ICEI.2019.00093.

[20] M. Liu, K. Li, and T. Chen, "DeepSQLi: Deep Semantic Learning for Testing SQL Injection," May 2020, [Online]. Available: http://arxiv.org/abs/2005.11728

[21] T. Muhammad and H. Ghafory, "SQL Injection Attack Detection Using Machine Learning Algorithm," *Mesopotamian Journal of Cyber Security*, pp. 5–17, Feb. 2022, doi: 10.58496/mjcs/2022/002.