Deteksi Anomali dengan *Security Information and Event Management* (SIEM) Splunk pada Jaringan UII

Muhammad Rijal Kamal
Program Studi Informatika
Universitas Islam Indonesia
Yogyakarta, Indonesia
17523098@students.uii.ac.id

Mukhamad Andri Setiawan
Program Studi Informatika
Universitas Islam Indonesia
Yogyakarta, Indonesia
andri@uii.ac.id

***Abstraks*—Semakin besar penggunaan teknologi semakin banyak pula ancaman serangan siber yang mengintai. Tidak hanya ancaman serangan siber saja yang bertambah tetapi dampak potensial dari serangan ini jua semakin serius. Penggunaan teknologi informasi di Universitas Islam Indonesia sudah semakin besar dan memasuki segala aspek termasuk dalam bidang akademik. Tentu saja banyak ancaman serangan serta anomali yang ada di sistem UII. Belum ada sistem yang digunakan untuk mendeteksi anomali di UII. Oleh karena itu, penelitian ini ditujukan untuk mendeteksi anomali pada sistem UII sebagai langkah antisipasi ancaman dari hal yang tidak diinginkan. Deteksi anomali menggunakan alat SIEM Splunk yang mengolah *log firewall* PaloAlto yang sudah terpasang pada sistem UII serta menampilkan hasil deteksi di dashboard Splunk. Dari penelitian yang telah dilakukan, dapat dideteksi anomaly pada *data log firewall* UII berdasarkan Akan tetapi dataset yang digunakan masih kurang karena hanya mengambil sampel *log traffic firewall* dalam satu hari saja.**

Kata kunci—deteksi anomali, keamanan sistem, firewall, security information and event management, splunk

I. PENDAHULUAN

Saat ini sulit menemukan bisnis dengan ukuran apapun yang tidak menggunakan teknologi setiap hari setidaknya untuk satu aspek utama dalam menjalankan bisnis perusahaan. Keamanan siber telah menjadi masalah besar di dunia bisnis saat ini. Tidak hanya ancaman serangan siber saja yang bertambah setiap tahun, tetapi dampak potensial dari serangan ini juga semakin serius seiring dengan kemajuan teknologi dan persentase yang lebih besar dari transaksi bisnis yang berkembang berada di dunia digital.

Penggunaan teknologi informasi di Universitas Islam Indonesia (UII) memungkinkan terjadinya proses pembuatan, penyimpanan, dan sarana berbagi pengetahuan termasuk dalam bidang akademik. Peran teknologi informasi di UII menjadi sesuatu yang sangat penting. Selepas Badan Sistem Informasi Universitas Islam Indonesia (BSI UII) melakukan transformasi/perubahan infrasturktur teknologi informasi, ada lompatan pengguna internet yang sangat masif, dari yang tadinya hanya berkisar 1000 orang setiap harinya di awal tahun 2016, menjadi 13000 orang di awal 2018. Ini menunjukkan bahwa satu dari dua mahasiswa UII secara aktif berkegiatan di kampus dari pagi hingga sore hari untuk melakukan perkuliahan maupun hal lainnya.

Menurut Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Standar Sistem Manjemen Keamanan Informasi (SMKI), bahwa setiap penyelenggara sistem elektronik harus mematuhi SMKI dengan memegang nilai CIA (*Confidentiality*, *Availability*, dan *Integrity*). Oleh karena itu, sistem dan teknologi informasi yang ada di UII harus mampu untuk menyediakan informasi yang cepat dan akurat. Selain itu, keamanan dari sistem dan teknologi harus dilindungi untuk menjaga aset informasi dari serangan atau penyalahgunaan.

Agar pelayanan berjalan dengan baik maka perlu pengamanan atau perlindungan yang baik pula. UII menggunakan *next-generation firewall* (NGFW) dari *Palo Alto Networks* pada sistemnya sebagai salah satu tindakan antisipasi pengamanan sistem. *Next-generation firewall* ini memiliki kemampuan yang lebih baik dibandingkan *firewall* tradisional. Fitur tambahan yang ada pada NGFW seperti *Intrusion Prevention System* (IPS), *Deep Packet Inspection* (DPI), *Application Control*, *Directory Integration*, serta *Encrypted Traffic Inspection*. *Firewall* adalah sistem yang bertindak sebagai antarmuka antara satu jaringan dengan satu atau lebih jaringan eksternal. *Firewall* membantu menentukan paket yang boleh lewat dan yang diblokir berdasarkan seperangkat aturan yang ditentukan administrator jaringan. Jika terjadi kesalahan dalam mendefinisikan suatu aturan maka dapat membahayakan sistem keamanan dengan membiarkan lalu lintas yang tidak diinginkan dan memblokir lalu lintas yang sah. Aturan ketika didefinisikan secara manual sering menghasilkan set yang berisi aturan yang bertentangan atau berlebihan, yang menciptakan anomali pada kebijakan *firewall*. Dengan demikian perlu dilakukan deteksi anomali pada sistem keamanan *firewall* yang terpasang pada sistem di UII. Deteksi anomali adalah kegiatan menganalisis data penting yang digunakan untuk mendeteksi data yang tidak normal pada lalu lintas jaringan yang kemudian dapat membantu manajemen dan masalah keamanan jaringan.

Karena belum adanya sistem keamanan untuk mendeteksi anomali pada sistem informasi UII, peneliti berupaya untuk melakukan deteksi anomali pada keamanan sistem dan teknologi informasi UII dengan bantuan alat *Security Information and Event Management* (SIEM). SIEM adalah sistem monitoring yang dapat mendeteksi serangan dan respon suatu sistem keamanan melalui analisis *log* dari berbagai *event* yang berasal dari berbagai sumber data secara *realtime*. Teknologi SIEM ini memiliki cakupan pengumpulan data yang besar serta mampu mengkorelasikan dan menganalisis *event* dari berbagai sumber dan menentukan apakah kejadian tersebut merupakan suatu serangan atau tidak.

Pada penelitian ini, deteksi anomali pada sistem keamanan UII dengan bantuan alat SIEM yaitu Splunk. Splunk dipilih karena memungkinkan untuk mengolah data dengan skala besar serta pengembangan yang cepat dan pemeliharaan yang mudah. Selain itu, pada Splunk terdapat fitur masukan, pencarian, penyaringan, pelaporan, penghapusan, dan modifikasi data. Data yang diolah Splunk pada penelitian ini berasal dari *log* yang dihasilkan dari firewall PaloAlto yang sudah terpasang pada sistem informasi UII. Deteksi anomali dilakukan berdasarkan aturan-aturan tertentu. Hasil deteksi dan analisis data ditampilkan pada *dashboard* Splunk.

II. LANDASAN TEORI

A. *Keamanan Sistem Informasi*

Dalam bukunya "*An Analysis of Security Incidents on The Internet*", John D. Howard menyatakan bahwa keamanan komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Keamanan sistem informasi menurut G. J. Simons adalah bagaimana kita dapat mencegah penipuan, atau setidaknya mendeteksi adanya penipuan pada suatu sistem yang berbasis informasi, dimana informasi itu sendiri tidak memiliki arti fisik.

B. *Aspek Keamanan Informasi*

Keamanan informasi harus meliputi beberapa aspek keamanan yaitu: *Confidentiality, Integrity, Availability*.

a. *Confidentiality* atau kerahasiaan yaitu bagaimana data hanya dapat diakses oleh orang yang berwenang. Untuk menjaga kerahasiaan bias dilakukan dengan cara enkripsi maupun membatasi akses pengguna.

b. *Integrity* atau integritas yaitu jaminan bahwa data hanya boleh diakses atau dirubah oleh orang yang berhak. Untuk menjaga integritas bisa dilakukan dengan melakukan autentikasi pengguna.

c. *Availability* atau ketersediaan yaitu bagaimana sistem dapat menjamin ketersediaan data saat pengguna membutuhkannya. Dalam mengatasi masalah pada aspek ini bisa dengan menyediakan redundansi.

C. *Next-Generation Firewall (NGFW)*

Firewall adalah sistem yang bertindak sebagai antarmuka antara satu jaringan dengan satu atau lebih jaringan eksternal. *Firewall* membantu menentukan paket yang boleh lewat dan yang diblokir berdasarkan seperangkat aturan yang ditentukan administrator jaringan. Jika terjadi kesalahan dalam mendefinisikan suatu aturan maka dapat membahayakan sistem keamanan dengan membiarkan lalu lintas yang tidak diinginkan dan memblokir lalu lintas yang sah. Aturan ketika didefinisikan secara manual sering menghasilkan set yang berisi aturan bertentangan atau berlebihan, yang menciptakan anomali pada kebijakan *firewall*. *Next-generation Firewall* (NGFW) memiliki semua fitur dari *firewall* tradisional dan fitur tambahan yang melengkapi kekurangan dari *firewall* tradisional. Fitur tambahan dari NGFW antara lain :

a. *Intrusion Prevention System* (IPS). Sebuah sistem pencegahan yang secara aktif mendeteksi dan memblokir suatu upaya penyerangan pada jaringan.

b. *Deep Packet Inspection*. Pada *firewall* tradisional sistem hanya memeriksa *headers* dari paket data yang melintas. Sedangkan pada NGFW diperiksa *headers* paket beserta isi dari paketnya. Hal tersebut bertujuan untuk mendeteksi *malware* atau hal berbahaya lainnya.

c. *Application Control*. Selain untuk menganalisis jaringan, NGFW dapat mengatur sumber daya yang dilarang atau dapat diakses oleh suatu aplikasi secara bersamaan.

d. *Directory Integration*. Direktori pengguna memungkinkan organisasi untuk melacak hak istimewa atau izin dari setiap pengguna sehingga data diakses oleh pengguna yang semestinya.

e. *Encrypted Traffic Inspection*. Beberapa NGFW dapat mendekripsi dan menganalisa lalu lintas yang dienkripsi dengan SSL/TLS. *Firewall* dapat melakukan hal ini dengan bertindak sebagai *proxy* untuk proses TLS.

D. *Security Information and Event Management (SIEM)*

SIEM adalah sistem monitoring yang dapat mendeteksi serangan dan respon suatu sistem keamanan melalui analisis *log* dari berbagai *event* yang berasal dari sumber data secara *realtime*. Teknologi SIEM ini memiliki cakupan pengumpulan data yang besar serta mampu mengkorelasikan dan menganalisis *event* dari berbagai sumber dan menentukan apakah kejadian tersebut merupakan suatu serangan atau tidak. Fitur-fitur yang ada pada SIEM, antara lain:

a. *Log/Event Collection*, sistem dapat mengumpulkan *log* dari berbagai macam tipe *log* dan sumber yang berbeda.

b. *Log Analysis*, sistem mengolah dan menganalisis data dari berbagai sumber secara *realtime* dan merepresentasikannya ke dalam suatu grafik atau diagram agar seorang administrator dapat dengan mudah memahami dan mengambil keputusan.

c. *Event Correlation*, fitur ini memungkinkan administrator meningkatan keamanan dengan memproses jutaan log secara bersamaan untuk mendeteksi anomaly pada sistem.

d. *Log Forensics*, SIEM dapat membantu untuk penyelidikan *log forensic* dengan menyediakan atau *event* yang dapat dengan mudah dipahami untuk mencari penyusup atau penyebab masalah pada sistem.

e. *IT Compliance*, SIEM memberikan laporan pelanggaran aturan untuk berbagai standar keamanan.

f. *Application Log Monitoring*, fitur yang membantu administrator memantau *log* dari aplikasi mereka secara *realtime.*

g. *Real Time Alerting*, fitur untuk memberikan peringatan kepada administrator apabila terjadi suatu hal yang mencurigakan pada sistem.

h. *Object Access Auditing*, fitur untuk mengaudit segala aset penting sistem yang ada.

i. *User Activity Monitor*, membantu memantau aktivitas pengguna secara *realtime* dan mendeteksi penyalahgunaan hak.

j. *Dashboard*, fitur untuk menampilkan data dan informasi keamanan yang telah diolah.

k. *Reporting*, SIEM menyediakan laporan sesuai dengan standar keamanan yang ada.
l. *File Integrity Monitoring*, memantau apabila terjadi perubahan data yang tidak wajar, penyalahgunaan haka tau akses dari yang tidak berwenang.
m. *System & Device Log Monitoring*, fitur untuk melakukan otomatisasi pemantauan *log* serta analisis sistem dan *log* secara *realtime.*

E. Splunk

Sebuah *platform* perangkat lunak yang digunakan untuk memantau, mencari, menganalisis dan memvisualisasikan data yang dihasilkan mesin. Splunk melakukan penangkapan, pengindeksan, dan menghubungkan data secara *realtime* ke dalam sebuah wadah yang dapat dengan mudah dicari dan menghasilkan suatu grafik, peringatan, *dashboard* serta visualisasi agar data dapat dengan mudah dibaca dan dianalisis.

F. Kajian Literatur

Pada penelitian yang dilakukan oleh Imam R M, Sukarno P dan Nugroho M A (2019), peneliti melakukan deteksi anomali menggunakan *intrusion detection system* (IDS) dengan algoritma hybrid yaitu *eager learning* dengan algoritma RIPPER dan *lazy learning* yaitu *K-Nearest Neighbour*. Hasilnya diperoleh akurasi 99,89522% dalam mendeteksi anomali. Peneliti menerangkan bahwa terdapat kekurangan dalam metode RIPPER, yaitu kinerjanya akan menurun jika diberi dataset dalam jumlah besar. Sedangkan pada penelitian yang dilakukan oleh Fajrin M I, Sukarno P, dan Satwiko A G P (2018), peneliti mendeteksi anomaly pada serangan *man-in-the-middle* dengan algoritma Markov Chain dan k-NN memperoleh nilai akurasi 95,6% dan 48,6%. Dari penelitian sebelumnya dilakukan untuk menguji nilai akurasi dari algoritma yang digunakan. Dan dataset yang digunakan berasal dari IDS bukan dari firewall.

Pada penelitian Zope A, Vidhate A, dan Harale N (2013) yang berisi kajian literatur mengenai pendekatan *data mining* pada SIEM menunjukkan bahwa SIEM juga dapat menerapkan *data mining* untuk meningkatkan kinerja sistem.

Pada penelitian yang dilakukan Arfanudin C, Sugiantoro B, dan Prayudi Y (2019), peneliti melakukan simulasi serangan terhadap *router* dengan 8 jenis serangan yang kemudian serangan tersebut dianalisis dengan metode OSCAR untuk melihat dampaknya terhadap *router* maupun SIEM. Selain itu juga diukur indeks Keamanan Informasi (KAMI) sebelum dan setelah adanya SIEM. Hasilnya terbukti bahwa penggunaan SIEM berhasil mengenali serangan yang dilakukan walaupun tidak semuanya serta penggunaan SIEM memiliki pengaruh untuk menaikan indeks KAMI dari sisi teknologi.

Pada penelitian Abd Elmajid (2021), peneliti mengintegrasikan Splunk dengan kursus keamanan siber untuk membantu dan mengelola data mesin dari beberapa server. Selain itu, penggunaan Splunk membantu mahasiswa dalam mempelajari cara mendeteksi resiko keamanan dan penyalahgunaan jaringan. peneliti berhasil mengintegrasikan Splunk yang memiliki IP publik dengan *forwarder* yang memiliki IP privat.

Pada penelitian ini dilakukan deteksi anomali pada *traffic log firewall* jaringan UII yang jumlahnya puluhan GigaByte sehingga dibutuhkan pendekatan *data mining*. Oleh karena itu, dibutuhkan SIEM untuk mengolah data tersebut dan SIEM yang digunakan adalah Splunk. Berdasarkan kajian literatur, peneliti belum menemukan penggunaan alat SIEM lain yang digunakan untuk mendeteksi anomaly pada firewall. Dari penelitian sebelumnya, deteksi anomali dilakukan dengan IDS untuk menguji akurasi dari metode deteksi saja.

III. METODOLOGI

Metodologi penelitian ini dimulai dengan studi literatur, perencanaan, pengumpulan data, implementasi, pengujian, dan analisis dengan diagram alir sebagai berikut.

Gambar 1. Metodologi

A. Studi Literatur

Melakukan kajian terhadap artikel, jurnal, website, atau buku terkait topik penelitian.

B. Perencanaan

Merumuskan masalah dan solusi untuk permasalahan yang ada mengenai deteksi anomali pada jaringan UII beserta alat dan teknologi yang digunakan.

C. Pengumpulan Data

Data diperoleh dari *log firewall* PaloAlto yang dipasang pada jaringan UII. Data diambil dalam jangka waktu tertentu. Pada penelitian ini, *log* yang dipakai yaitu *log firewall* tanggal 9 September 2020 dengan tipe *pan:traffic* karena yang akan dideteksi adalah lalu lintas jaringan UII.

D. Implementasi

Proses implementasi terdiri dari berbagai langkah sebagai berikut:

1. Instalasi Splunk
   Penelitian ini menggunakan versi *trial* selama 60 hari dari Splunk Enterprise dengan kebutuhan sistem seperti yang ditunjukkan pada Tabel 1.

TABEL I. KEBUTUHAN SISTEM SPLUNK

Operating System	Windows / Mac OS / Linux
Processor	Minimal 2-core 64-bit CPU 2GHz
Memory	Minimal 4GB
Web Browser	Versi terbaru dari Chrome / Firefox / Safari
Port Splunk Web	8000

2. Instalasi Add-On Palo Alto Networks
   Digunakan untuk membaca *fields* dari data *log firewall* karena data yang diolah berasal dari *log firewall* Palo Alto Networks.
3. Mengunggah data
   Data yang diambil dari *log firewall* pada tanggal 9 September 2020 sebesar 30.035.573 KB. Karena pada versi *trial* ini hanya dibatasi 500 MB dalam

sekali unggah data maka data tersebut dibagi menjadi beberapa bagian dengan ukuran kurang dari 500 MB. Pembagian data ini menggunakan alat dari Linux yaitu “Split”.

4. Pencarian

Setelah data sudah siap, langkah selanjutnya yaitu mengolah data tersebut dengan membuat aturan-aturan yang digunakan untuk mencari dan menampilkan data. Pencarian dilakukan pada menu “*Search & Reporting*” pada Splunk. Berikut merupakan aturan-aturan yang digunakan:

- Mendeteksi dan menampilkan aksi yang telah dilakukan firewall pada lalu lintas berdasarkan teknologi yang digunakan

```
index=* sourcetype="pan:traffic"
| chart count over app:technology
by action
```

Gambar 2. Traffic Action

- Mendeteksi dan menampilkan jumlah user

```
index=* sourcetype="pan:traffic"
| stats  dc(user) as total_pengguna
```

Gambar 3. Traffic User

- Menampilkan jumlah *event* pada *log*

```
index=* sourcetype="pan:traffic"
|stats count
```

Gambar 4. Jumlah Events

- Mendeteksi anomali dan menampilkan jumlah anomali pada jaringan

```
index=* sourcetype="pan:traffic"
| anomalydetection
“app:able_to_transfer_file”
“app:excessive_bandwith”
“app:evasive”
“app:has_known_vulerability”
“app:used_by_malware”
“app:pervasive_use”
“app:prone_to_misuse”
“app:tunnels_other_application”
“action” “app:risk”
“app:technology” “user” “app”
“src” “dest” “date_minute”
“date_hour” “date_year”
“date_wday” “date_zone”
“date_month” “date_second”
“date_mday”
|stats count as outlierCount
```

Gambar 5. Jumlah Anomali

- Mendeteksi anomali dan menampilkan hasil sebagai tabel anomali pada lalu lintas jaringan

```
index=* sourcetype=”pan:traffic”
|anomalydetection
“app:able_to_transfer_file”
“app:excessive_bandwith”
“app:evasive”
“app:has_known_vulerability”
“app:used_by_malware”
“app:pervasive_use”
“app:prone_to_misuse”
“app:tunnels_other_application”
“action” “app:risk”
“app:technology” “user” “app”
“src” “dest” “date_minute”
“date_hour” “date_year”
“date_wday” “date_zone”
“date_month” “date_second”
“date_mday” action=annotate

|eval isOutlier =
if(probable_cause != “”,”1”,”0”)

|table “app:able_to_transfer_file”
“app:excessive_bandwith”
“app:evasive”
“app:has_known_vulerability”
“app:used_by_malware”
“app:pervasive_use”
“app:prone_to_misuse”
“app:tunnels_other_application”
“action” “app:risk”
“app:technology” “user” “app”
“src” “dest” “date_minute”
“date_hour” “date_year”
“date_wday” “date_zone”
“date_month” “date_second”
“date_mday”, probable_cause,
isOutlier

|sort 100000 probable_cause
```

Gambar 6. Hasil Deteksi Anomali

5. Visualisasi Dashboard

Setelah proses pencarian dan pengolahan data selesai, selanjutnya hasil dari pengolahan tadi disimpan sebagai “*Dashboard Panel*” untuk ditampilkan ke dashboard Splunk.

E. Analisis

Analisis dilakukan untuk melihat apakah penelitian yang dilakukan sudah sesuai dengan tujuan serta sebagai acuan untuk menulis kesimpulan.

IV. HASIL DAN PEMBAHASAN

Setelah proses pencarian dengan aturan yang telah dibuat pada “Search & Reporting” maka diperoleh hasil visualisasi sebagai berikut:

Dari aturan pada Gambar 2. memperoleh hasil seperti pada Gambar 7.

Gambar7. Visual Traffic Action

Visualisasi yang dipilih yaitu menggunakan “*Column Chart*”. Dari panel tersebut dapat dilihat tindakan yang

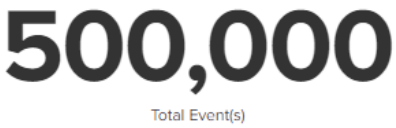
diambil *firewall* pada setiap lalu lintas berdasarkan teknologi yang digunakan yaitu *browser-based*, *client-server*, *network-protocol*, dan *peer-to-peer*.

Dari aturan pada Gambar 3. memperoleh hasil seperti pada Gambar 8.

Gambar 8. Visual Traffic User

Visualisasi yang dipilih yaitu menggunakan "Single Value" untuk menunjukkan jumlah pengguna.

Dari aturan pada Gambar 4. memperoleh hasil seperti pada Gambar 9.



Gambar 9. Visual Jumlah Events

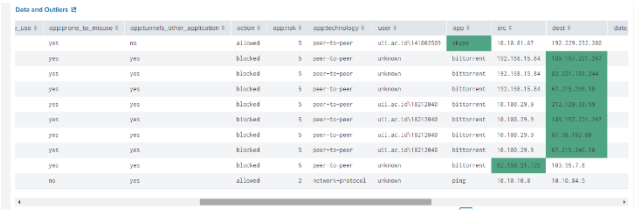
Visualisasi yang dipilih yaitu menggunakan "Single Value" untuk menunjukkan jumlah *events*. Jumlah *events* sebenarnya dalam data *log* yang dipakai adalah 74.598.836 *events*. Hasil visualisasi tersebut hanya diambil dari sebagian *log* saja yang dimasukkan.

Dari aturan pada Gambar 5. memperoleh hasil seperti pada Gambar 10.

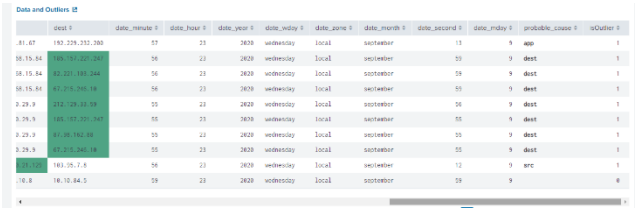
Gambar 10. Visual jumlah anomali

Visualisasi yang dipilih yaitu menggunakan "Single Value" untuk menunjukkan jumlah anomali. Jumlah anomali tersebut hanya dihitung dari sebagian data *log* karena pada saat penelitian dilakukan pada data *log* utuh sering mengalami kegagalan. Hal itu disebabkan karena perangkat yang dipakai penulis kurang mumpuni untuk mengolah data sebanyak itu.

Dari aturan pada Gambar 6. memperoleh hasil seperti pada Gambar 11 dan Gambar 12.



Gambar 11. Visual deteksi anomali (1)



Gambar 12. Visual deteksi anomali (2)

Visualisasi yang dipilih yaitu menggunakan table statistik untuk menunjukkan jumlah anomali. Jumlah anomaly ditunjukkan dengan adanya kolom table berwarna hijau. Jumlah tersebut hanya dihitung dari sebagian data *log* karena pada saat penelitian dilakukan pada data *log* utuh sering mengalami kegagalan.

Aturan-aturan yang dipakai untuk mendeteksi anomali ini mempertimbangkan beberapa karakteristik paket data pada *log firewall*. Karakteristiknya antara lain:

1. *Capable of file transfer*. Paket data ini mampu untuk mentransfer file dari satu sistem ke sistem yang lain pada jaringan.
2. *Excessive bandwith*. Menggunakan setidaknya 1Mbps secara teratur melalui penggunaan normal.
3. *Evasive*. menggunakan port atau protokol untuk sesuatu selain tujuan aslinya dengan harapan akan melintasi firewall.
4. *Has known vulnerability*. Telah dilaporkan secara public sebagai kerentanan.
5. *Used by malware*. Telah digunakan untuk mennyebarkan malware, memulai serangan, atau mencuri data.
6. *Persasive use*. Kemungkinan untuk memiliki lebih dari 1.000.000 pengguna.
7. *Prone to misuse*. Sering ditujukan untuk hal yang tidak semestinya.
8. *Tunnels other application*. Mampu membawa aplikasi lain di dalam protokolnya.

Dari hasil deteksi anomali yang dilakukan terlihat bahwa ada *events* yang terdeteksi sebagai anomaly tapi masih "diijinkan" untuk melewati *firewall*. Selain itu, penyebab dari kenapa *events* tersebut dianggap sebagai suatu anomali juga dapat dilihat pada kolom "*probable_cause*".

KESIMPULAN

Dari penelitian yang telah dilakukan, penulis dapat menyimpulkan bahwa deteksi anomali pada log firewall jaringan UII berhasil dilakukan dengan aturan yang sudah dibuat berdasarkan nilai resiko atau karakteristik paket data dari *log firewall*. Akan tetapi, pengujian masih sebatas sebagian log firewall dan belum utuh dalam satu hari penuh atau membandingkan dengan hari lainnya. Penelitian ini diharapkan dapat membantu administrator sistem UII untuk melihat anomali yang ada pada sistem, sehingga kemudian anomali atau ancaman tersebut dapat segera diatasi dengan meninjau kembali sistem keamanan yang ada. Selain itu masih banyak *fields* yang masih belum dieksplorasi untuk deteksi anomali ini. Saran untuk penelitian selanjutnya yaitu dengan

memasukkan dan mengujikan data lebih banyak lagi serta mencoba mengeksplorasi *fields* dari *log firewall* yang mungkin rentan terhadap serangan.

REFERENSI

UII, B. S. I. (n.d.). *Rencana Strategis BSI 2018 - 2022 cq Blue Print Teknologi Informasi.pdf*.

Ryan, T. (2016). *Demystifying Machine Learning And Anomaly Detection : Bio*.

Cloudflare. (n.d.). *What is a next-generation firewall (NGFW)? | NGFW vs. FWaaS*. Retrieved June 9, 2021, from https://www.cloudflare.com/learning/cloud/what-is-a-next-generation-firewall/

Umum, G., Komunikasi, D., Kota, I., Berdasarkan, T., Tegal, W., Komunikasi, D., Tegal, I. K., Tegal, K., Komunikasi, D., Tegal, K., Komunikasi, D., Organisasi, S., Komunikasi, D., Kota, I., Tugas, T., Pengembangan, F. K., Tik, P., Komunikasi, D., & Komunikasi, D. (2016). *BAB 2 Tinjauan Pustaka*. 8–32.

Azhar, C. (1884). STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005. *Notes and Queries*, *s6-IX*(213), 77. https://doi.org/10.1093/nq/s6-IX.213.77-d

Rahardjo, B. (2017). *Keamanan Informasi & Jaringan*. 47. http://budi.rahardjo.id/files/keamanan.pdf

Imam, R. M., Sukarno, P., & Nugroho, M. A. (2019). Deteksi Anomali Jaringan Menggunakan Hybrid Algorithm. *eProceedings of Engineering*, *6*(2).

Fajrin, M. I., Sukarno, P., & Satwiko, A. G. P. (2018). Perbandingan Metode K-NN dan Markov Chain Untuk Deteksi Anomali Serangan Man-in-the-Middle Pada Smart Lock Berbasis Wifi. *eProceedings of Engineering*, *5*(3).

Zope, A., Vidhate, A., & Harale, N. (2013). Data Mining Approach in Security Information and Event Management. *International Journal of Future Computer and Communication*, 80-84.

ARFANUDIN, C., Sugiantoro, B., & Prayudi, Y. (2019). ANALYSIS OF ROUTER ATTACK WITH SECURITY INFORMATION AND EVENT MANAGEMENT AND IMPLICATIONS IN INFORMATION SECURITY INDEX. *Cyber Security Dan Forensik Digital*, *2*(1), 1–7. https://doi.org/10.14421/csecurity.2019.2.1.1388

Abd Elmajid, F. (2021). Integrating Splunk Into Some of Cybersecurity Courses.

Palo Alto Networks. (n.d.). *HOW TO DETERMINE RISK LEVEL OF APPLICATION, SPYWARE, AND ANTI-VIRUS*. Retrieved June 9, 2020, from https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClmQCAS