

**ANALISA SECURITY INFORMATION AND EVENT
MANAGEMENT (SIEM) MENGGUNAKAN
ELASTIC STACK SIEM DAN SPLUNK**

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Memperoleh
Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau



MUHAMMAD ALFANDI
183510165

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU**

2022

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI II

Nama : Muhammad Alfandi
NPM : 183510165
Fakultas : Teknik
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata Satu (S1)
Judul Skripsi : Analisa *Security Information and Event Management* (SIEM)
Menggunakan Elastic Stack SIEM Dan Splunk

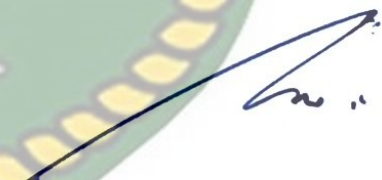
Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria - kriteria dalam metode penulisan ilmiah. Oleh karena itu, skripsi ini dinilai layak dapat disetujui untuk disidangkan dalam ujian komprehensif.

Pekanbaru, 15 Maret 2022

Disetujui Oleh :
Ketua Prodi Teknik Informatika

Disahkan Oleh :
Dosen Pembimbing


Dr. Apri Siswanto., S.Kom., M.Kom


Dr. Apri Siswanto., S.Kom., M.Kom

LEMBAR PENGESAHAN TIM PENGUJI UJIAN SKRIPSI

Nama : Muhammad Alfandi
NPM : 183510165
Fakultas : Teknik
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata Satu (S1)
Judul Skripsi : *Analisa Security Information And Event Management*
(SIEM) Menggunakan Elastic Stack SIEM Dan Splunk

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah serta telah diuji dan dapat dipertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 25 Maret 2022** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu **Teknik Informatika**.

25 Maret 2022

Tim Penguji

1. **Yudhi Arta, S.T., M.Kom.** Sebagai Tim Penguji I (.....)
2. **Rizdqi Akbar Ramadhan, S.Kom., M.Kom.** Sebagai Tim Penguji II (.....)

Disahkan Oleh

Ketua Prodi Teknik Informatika

Dosen Pembimbing

Dr. Apri Siswanto, S.Kom., M.Kom

Dr. Apri Siswanto, S.Kom., M.Kom

KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Penayang. Penulis mengucapkan puji syukur atas kehadiran-Nya, yang telah melimpahkan rahmat dan hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisa *Security Information And Event Management* (SIEM) Menggunakan Elastic Stack SIEM Dan Splunk”.

Penulisan skripsi ini diajukan sebagai persyaratan dalam menempuh ujian program Strata-1 pada Fakultas Teknik dengan Program Studi Teknik Informatika Universitas Islam Riau. Penulis sangat menyadari bahwa di dalam penulisan skripsi ini masih terdapat kesalahan dan kekurangan yang disebabkan oleh keterbatasan dan kemampuan penulis.

Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada pihak yang telah memberikan bantuan dan dukungan yang secara langsung maupun tidak langsung. Ucapan terima kasih tersebut penulis tujukan kepada:

1. Allah SWT, karena dengan rahmat dan karunia-nya, penulis dapat menyelesaikan tugas akhir ini dengan tepat waktu.
2. Kedua orang tua penulis yaitu Bapak Tasbeh dan Ibu Rosmaili atas kasih sayang yang tak terhingga dan selalu mendo'akan penulis selama perkuliahan berlangsung.
3. Kepada Bapak Dr. Apri Siswanto, S.Kom,. M.Kom sebagai kepala prodi teknik informatika UIR dan sekaligus dosen pembimbing saya yang telah

memberikan arahan selama proses pembuatan laporan skripsi sehingga penulis dapat belajar lebih baik lagi.

4. Kepada dosen penguji yang saya banggakan yaitu Bapak Rizdqi Akbar Ramadhan, S.Kom., M.Kom., CHFI dan Bapak Yudhi Arta, S.T., M.Kom yang telah memberikan saran dan masukan selama penulis melakukan penelitian dan membuat laporan.
5. Kepada seluruh Bapak dan Ibu dosen program studi Teknik Informatika UIR yang telah memberikan ilmunya selama penulis belajar di bangku perkuliahan.
6. Kepada laboran teknik informatika UIR yang telah berkenan untuk meminjamkan laboratorium jaringan komputer kepada penulis dalam penelitian berlangsung.
7. Kepada Bang Algi Fahri yang telah memberikan dukungan dan memberikan ilmu baru yang penulis dapatkan diluar mata kuliah.
8. Dwi Shahna Amrisa yang telah mendukung dan memberi semangat kepada penulis dalam mengerjakan laporan skripsi.
9. Kepada semua teman dan sahabat penulis khusus nya kelas B angkatan 2018 teknik informatika UIR yang telah memberi dukungan dan semangat kepada penulis.
10. Kepada seluruh staff TU teknik yang telah membantu penulis dalam proses administrasi selama KP (Kerja Praktik) dan juga Skripsi penulis.

Akhir kata penulis berharap semoga skripsi ini dapat memberikan manfaat dan inspirasi kepada pembacanya.

Pekanbaru, 20 Januari 2022

Muhammad Alfandi



Dokumen ini adalah Arsip Miik :
Perpustakaan Universitas Islam Riau

ANALISA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MENGGUNAKAN ELASTIC STACK SIEM DAN SPLUNK

Muhammad Alfandi¹

^{1,2}Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau
e-mail: 1muhammadalfandi@student.uir.ac.id

ABSTRAK

Perkembangan teknologi informasi pada saat ini begitu pesat, dibalik kemajuan teknologi pada saat ini, juga terdapat ancaman dan serangan yang bisa terjadi kapan saja. Serangan dan ancaman ini dapat merusak sistem dan membocorkan data penting dari suatu instansi atau perusahaan. Dengan adanya ancaman dan serangan ini maka keamanan informasi (*information security*) berperan penting untuk dapat melakukan keamanan dari serangan dan ancaman yang terjadi. SIEM (*Security Information and Event Management*) merupakan salah satu metode dalam keamanan informasi untuk menganalisa *log* yang terjadi di dalam suatu sistem. Pada penelitian ini SIEM yang digunakan adalah Elastic Stack SIEM dan Splunk untuk melakukan monitoring dan analisa *log* serangan yang masuk kedalam sistem. Serangan yang dilakukan dalam penelitian ini yaitu *Fingerprinting*, *SQL Injection*, *DoS*, dan *Port Scanning*, dan hasil pengujian tersebut Elastic Stack SIEM dan Splunk mampu mendeteksi semua serangan yang masuk ke *web server* secara *realtime*. Setelah serangan berhasil terdeteksi, selanjutnya Splunk dan Elastic Stack SIEM mengirimkan *e-mail* notifikasi kepada administrator mengenai serangan yang terjadi.

Kata Kunci: *Monitoring*, SIEM, Elastic Stack SIEM, Splunk

ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) USING ELASTIC STACK SIEM AND SPLUNK

Muhammad Alfandi¹

^{1,2}*Informatics Engineering Study Program, Faculty of Engineering, Islamic
University of Riau*

e-mail: 1muhammadalfandi@student.uir.ac.id

ABSTRACT

The development of information technology at this time is so rapid, behind the current technological advances, there are also threats and attacks that can occur at any time. These attacks and threats can damage systems and leak important data from an agency or company. With these threats and attacks, information security plays an important role in being able to carry out security from attacks and threats that occur. SIEM (Security Information and Event Management) is one of the methods in information security to analyze logs that occur in a system. In this research, the SIEM used is Elastic Stack SIEM and Splunk to monitor and analyze the attack logs that enter the system. The attacks carried out in this research are Fingerprinting, SQL Injection, DoS, and Port Scanning, and the test results are Elastic Stack SIEM and Splunk are able to detect all attacks that enter the web server in real time. After the attack has been detected, Splunk and Elastic Stack SIEM will then send an e-mail notification to the administrator about the attack.

Keywords: *Monitoring, SIEM, Elastic Stack SIEM, Splunk*

DAFTAR ISI

KATA PENGANTAR	i
ABSTRAK	iv
ABSTRACT	v
DAFTAR ISI	vi
DAFTAR GAMBAR	xi
DAFTAR TABEL	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	2
1.3 Batasan Masalah	3
1.4 Rumusan Masalah	4
1.5 Tujuan Penelitian	4
1.6 Manfaat	4
1.7 Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1 Tinjauan Pustaka	7
2.2 Dasar Teori	22
2.2.1 <i>Security Information and Event Management (SIEM)</i>	22

2.2.2	<i>Elasticsearch</i>	23
2.2.3	<i>Splunk</i>	23
2.2.4	<i>VirtualBox</i>	24
2.2.5	<i>Linux</i>	24
2.2.6	<i>Ubuntu</i>	24
2.2.7	<i>Kali Linux</i>	25
2.2.8	<i>IP Address</i>	25
2.2.9	<i>Client dan Server</i>	25
2.2.10	<i>Web Server</i>	26
2.2.11	<i>Apache Web Server</i>	26
2.2.12	<i>Damn Vulnerable Web App (DVWA)</i>	27
2.2.13	<i>Fingerprinting</i>	27
2.2.14	<i>SQL Injection</i>	27
2.2.15	<i>Denial of Service (DoS)</i>	28
2.2.16	<i>Port Scanning</i>	28
2.2.17	<i>Switch</i>	28
2.2.18	<i>Secure Shell (SSH)</i>	29
2.2.19	<i>Putty</i>	29

BAB III METODOLOGI PENELITIAN..... 30

3.1	<i>Alat Dan Bahan Penelitian</i>	30
-----	--	----

3.1.1	Spesifikasi Perangkat Keras (<i>Hardware</i>).....	30
3.1.2	Spesifikasi Perangkat Lunak (<i>Software</i>).....	31
3.2	Prosedur Penelitian.....	34
3.2.1	Teknik Pengumpulan Data.....	34
3.2.2	Jenis Data	35
3.3	Perancangan Dan Pengembangan Topologi Jaringan	36
3.3.1	Desain Topologi Jaringan	36
3.3.2	Topologi Fisik.....	37
3.3.3	Topologi <i>Logic</i>	38
3.4	Metode Pengujian.....	40
3.4.1	<i>Fingerprinting</i>	40
3.4.2	<i>SQL Injection</i>	40
3.4.3	<i>Denial of Service (DoS)</i>	40
3.4.4	<i>Port Scanning</i>	41
3.5	Skenario Pengujian.....	41
BAB IV HASIL DAN PEMBAHASAN		43
4.1	Implementasi	43
4.1.1	Instalasi Perangkat Keras Jaringan.....	43
4.1.2	Instalasi dan Konfigurasi Elastic Stack SIEM	44
4.1.3	Instalasi dan Konfigurasi Splunk	50

4.1.4	Menghubungkan SIEM dengan <i>Web Server</i>	52
4.2	Pengujian	55
4.2.1	Pengujian <i>Client</i> atau <i>Attacker</i> Mengakses <i>Web Server</i> Hari Ke 1	57
4.2.2	Pengujian <i>Fingerprinting</i> Hari Ke 1	59
4.2.3	Pengujian <i>SQL Injection</i> Hari Ke 1	61
4.2.4	Pengujian <i>Denial of Service (DoS)</i> Hari Ke 1	64
4.2.5	Pengujian <i>Port Scanning</i> Hari Ke 1	66
4.2.6	Pengujian <i>Client</i> atau <i>Attacker</i> Mengakses <i>Web Server</i> Hari Ke 2	68
4.2.7	Pengujian <i>Fingerprinting</i> Hari Ke 2	70
4.2.8	Pengujian <i>SQL Injection</i> Hari Ke 2	73
4.2.9	Pengujian <i>Denial of Service (DoS)</i> Hari Ke 2	76
4.2.10	Pengujian <i>Port Scanning</i> Hari Ke 2	78
4.2.11	Pengujian <i>Client</i> atau <i>Attacker</i> Mengakses <i>Web Server</i> Hari Ke 3	80
4.2.12	Pengujian <i>Fingerprinting</i> Hari Ke 3	82
4.2.13	Pengujian <i>SQL Injection</i> Hari Ke 3	84
4.2.14	Pengujian <i>Denial of Service (DoS)</i> Hari Ke 3	87
4.2.15	Pengujian <i>Port Scanning</i> Hari Ke 3	89
4.3	Analisa	91
4.3.1	Analisa <i>Client</i> atau <i>Attacker</i> Mengakses <i>Web Server</i>	91
4.3.2	Analisa Pengujian <i>Fingerprinting</i> Menggunakan Nikto	92

4.3.3	Analisa Pengujian <i>SQL Injection</i> Menggunakan Sqlmap.....	92
4.3.4	Analisa Pengujian <i>Denial of Service</i> (DoS) Menggunakan Slowhttptest.....	93
4.3.5	Analisa Pengujian <i>Port Scanning</i> Menggunakan Nmap.....	93
4.3.6	Penjelasan <i>Output Monitoring</i>	94
4.3.7	Visualisasi Hasil Serangan.....	105
BAB V PENUTUP.....		110
5.1	Kesimpulan.....	110
5.2	Saran.....	111
DAFTAR PUSTAKA		112

DAFTAR GAMBAR

Gambar 3. 1 Desain Topologi Jaringan	37
Gambar 3. 2 Topologi Fisik.....	38
Gambar 3. 3 Topologi Logic	39
Gambar 3. 4 Skenario Pengujian	42
Gambar 4. 1 Instalasi Perangkat Keras Jaringan.....	44
Gambar 4. 2 Penambahan Sumber Elastic Stack.....	45
Gambar 4. 3 Penambahan Package Elastic Stack.....	45
Gambar 4. 4 Instalasi Elastic Stack SIEM.....	45
Gambar 4. 5 File Konfigurasi Elasticsearch.....	46
Gambar 4. 6 Konfigurasi Elasticsearch.....	46
Gambar 4. 7 Elastitcsearch Running	47
Gambar 4. 8 Tampilan Elasticsearch di Web Browser.....	47
Gambar 4. 9 File Konfigurasi Kibana	48
Gambar 4. 10 Konfigurasi Kibana.....	49
Gambar 4. 11 Kibana Running	49
Gambar 4. 12 Tampilan Kibana di Web Browser	50
Gambar 4. 13 Download Package Splunk	50
Gambar 4. 14 Instalasi Package Splunk	51
Gambar 4. 15 Konfigurasi Splunk.....	51
Gambar 4. 16 Tampilan Splunk di Web Browser	52
Gambar 4. 17 Instalasi Filebeat di Web Server	52
Gambar 4. 18 File Konfigurasi Filebeat	53

Gambar 4. 19 Konfigurasi Kibana didalam Filebeat.....	53
Gambar 4. 20 Konfigurasi Elasticsearch di dalam Filebeat	53
Gambar 4. 21 Filebeat Running.....	54
Gambar 4. 22 Folder Splunk Forwarder	54
Gambar 4. 23 Splunk Forwarder Running.....	55
Gambar 4. 24 Elastic Stack SIEM Diatur Secara Realtime.....	56
Gambar 4. 25 Splunk Yang Diatur Secara Realtime	56
Gambar 4. 26 Client atau Attacker Mengakses Web Server Hari Ke 1	57
Gambar 4. 27 Hasil Monitoring Log Akses Elastic Stack SIEM Hari Ke 1	57
Gambar 4. 28 Hasil Monitoring Log Akses Splunk Hari Ke 1	58
Gambar 4. 29 Notifikasi Log Masuk di Splunk Melalui E-mail Hari Ke 1	58
Gambar 4. 30 Pengujian Fingerprinting Menggunakan Nikto Hari Ke 1	59
Gambar 4. 31 Hasil Monitoring Serangan Fingerprinting Elastic Stack SIEM Hari Ke 1	60
Gambar 4. 32 Hasil Monitoring Serangan Fingerprinting Splunk Hari Ke 1.....	60
Gambar 4. 33 Notifikasi Serangan Fingerprinting di Splunk Melalui E-mail Hari Ke 1	61
Gambar 4. 34 Pengujian SQL Injection Menggunakan Sqlmap Hari Ke 1.....	61
Gambar 4. 35 Informasi Database Yang Didapatkan Oleh Attacker Menggunakan Sqlmap Hari Ke 1.....	62
Gambar 4. 36 Data User DVWA Yang Didapatkan Oleh Attacker Hari Ke 1 ...	62
Gambar 4. 37 Hasil Monitoring SQL Injection Elastic Stack SIEM Hari Ke 1..	63
Gambar 4. 38 Hasil Monitoring SQL Injection Splunk Hari Ke 1.....	63

Gambar 4. 39 Hasil Notifikasi SQL Injection di Splunk Melalui E-mail Hari Ke 1	64
Gambar 4. 40 Pengujian Denial of Service (DoS) Menggunakan Slowhttptest Hari Ke 1	64
Gambar 4. 41 Hasil Monitoring Serangan DoS Elastic Stack SIEM Hari Ke 1..	65
Gambar 4. 42 Hasil Monitoring Serangan DoS Splunk Hari Ke 1.....	65
Gambar 4. 43 Notifikasi Serangan DoS di Splunk Melalui E-mail Hari Ke 1....	66
Gambar 4. 44 Pengujian Port Scanning Menggunakan Nmap Hari Ke 1	66
Gambar 4. 45 Hasil Monitoring Serangan Port Scanning Elastic Stack SIEM Hari Ke 1	67
Gambar 4. 46 Hasil Monitoring Serangan Port Scanning Splunk Hari Ke 1	67
Gambar 4. 47 Notifikasi Serangan Port Scanning di Splunk Melalui E-mail Hari Ke 1	68
Gambar 4. 48 Client Atau Attacker Mengakses Website Hari Ke 2	69
Gambar 4. 49 Hasil Monitoring Log Akses Elastic Stack SIEM Hari Ke 2	69
Gambar 4. 50 Hasil Monitoring Log Akses Splunk Hari Ke 2	69
Gambar 4. 51 Notifikasi Log Masuk di Splunk Melalui E-mail Hari Ke 2	70
Gambar 4. 52 Pengujian Fingerprinting Menggunakan Nikto Hari Ke 2	71
Gambar 4. 53 Hasil Monitoring Serangan Fingerprinting Elastic Stack SIEM Hari Ke 2	71
Gambar 4. 54 Hasil Monitoring Serangan Fingerprinting Splunk Hari Ke 2.....	72
Gambar 4. 55 Notifikasi Serangan Fingerprinting di Splunk Melalui E-mail Hari ke 2.....	72

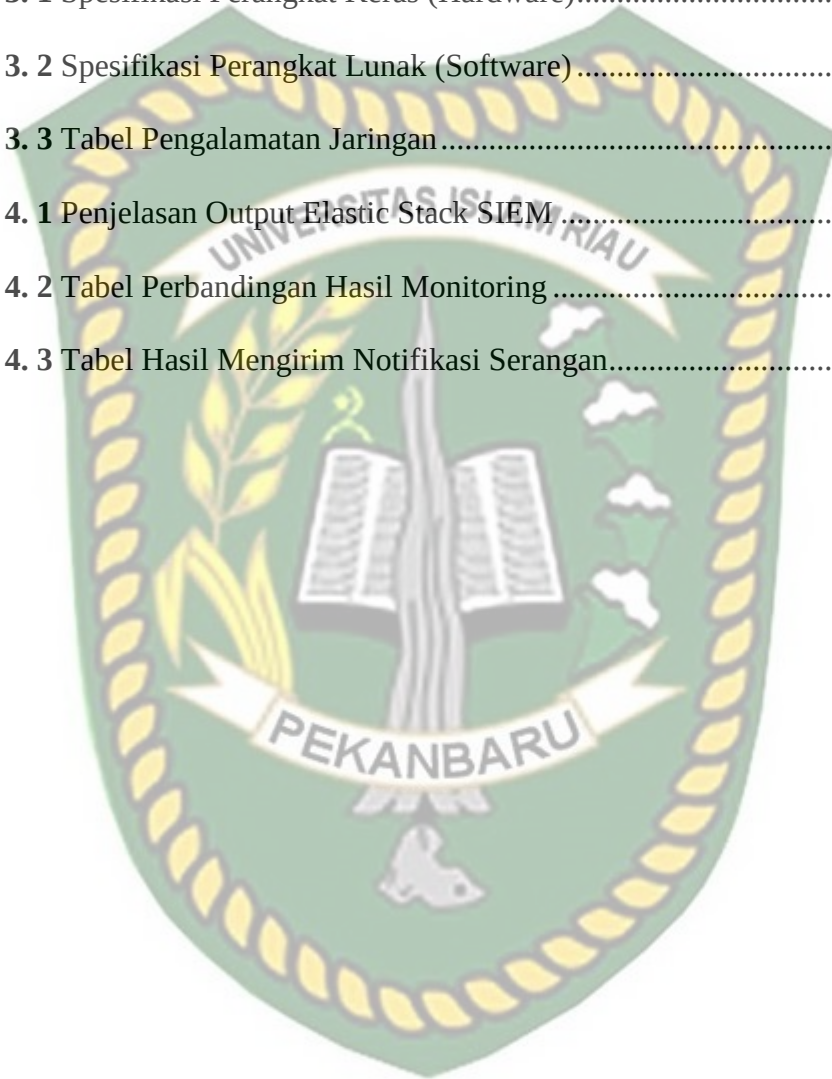
Gambar 4. 56 Pengujian SQL Injection Menggunakan Sqlmap Hari Ke 2.....	73
Gambar 4. 57 Informasi Database Yang Didapatkan Oleh Attacker Menggunakan Sqlmap Hari Ke 2.....	74
Gambar 4. 58 Informasi Data User DVWA Yang Didapatkan Oleh Attacker Hari Ke 2	74
Gambar 4. 59 Hasil Monitoring SQL Injection Elastic Stack SIEM Hari Ke 2..	75
Gambar 4. 60 Hasil Monitoring SQL Injection Splunk Hari Ke 2.....	75
Gambar 4. 61 Hasil Notifikasi SQL Injection di Splunk Melalui E-mail Hari Ke 2	76
Gambar 4. 62 Pengujian Denial of Service (DoS) Menggunakan Slowhttptest Hari Ke 2	76
Gambar 4. 63 Hasil Monitoring Serangan DoS Elastic Stack SIEM Hari Ke 2..	77
Gambar 4. 64 Hasil Monitoring Serangan DoS Splunk Hari Ke 2.....	77
Gambar 4. 65 Notifikasi Serangan DoS di Splunk Melalui E-mail Hari Ke 2....	78
Gambar 4. 66 Pengujian Port Scanning Menggunakan Nmap Hari Ke 2	78
Gambar 4. 67 Hasil Monitoring Serangan Port Scanning Elastic Stack SIEM Hari Ke 2	79
Gambar 4. 68 Hasil Monitoring Serangan Port Scanning Splunk Hari Ke 2	79
Gambar 4. 69 Notifikasi Serangan Port Scanning di Splunk Melalui E-mail Hari Ke 2	80
Gambar 4. 70 Client atau Attacker Mengakse Web Server Hari Ke 3	80
Gambar 4. 71 Hasil Monitoring Log Akses Elastc Stack SIEM Hari Ke 3	81
Gambar 4. 72 Hasil Monitoring Log Akses Splunk Hari Ke 3	81

Gambar 4. 73 Notifikasi Log Masuk di Splunk Melalui E-mail Hari Ke 3	82
Gambar 4. 74 Pengujian Fingerprinting Menggunakan Nikto Hari Ke 3	82
Gambar 4. 75 Hasil Monitoring Serangan Fingerprinting Elastic Stack SIEM Hari Ke 3	83
Gambar 4. 76 Hasil Monitoring Serangan Fingerprinting Splunk Hari Ke 3.....	83
Gambar 4. 77 Notifikasi Serangan Fingerprinting di Splunk Melalui E-mail Hari Ke 3	84
Gambar 4. 78 Pengujian SQL Injection Menggunakan Sqlmap Hari Ke 3.....	84
Gambar 4. 79 Informasi Database Yang Didapatkan Oleh Attacker Menggunakan Sqlmap Hari Ke 3.....	85
Gambar 4. 80 Data User DVWA Yang Didapatkan Oleh Attacker Hari Ke 3 ...	85
Gambar 4. 81 Hasil Monitoring Serangan SQL Injection Elastic Stack SIEM Hari Ke 3	86
Gambar 4. 82 Hasil Monitoring Serangan SQL Injection Splunk Hari Ke 3.....	86
Gambar 4. 83 Hasil Notifikasi SQL Injection di Splunk Melalui E-mail Hari Ke 3	87
Gambar 4. 84 Pengujian Denial of Service (DoS) Menggunakan Slowhttptest Hari Ke 3	87
Gambar 4. 85 Hasil Monitoring Serangan DoS Elastic Stack SIEM Hari Ke 3..	88
Gambar 4. 86 Hasil Monitoring Serangan DoS Splunk Hari Ke 3.....	88
Gambar 4. 87 Notifikasi Serangan DoS di Splunk Melalui E-mail Hari Ke 3....	89
Gambar 4. 88 Pengujian Port Scanning Menggunakan Nmap Hari Ke 3	89

Gambar 4. 89 Hasil Monitoring Serangan Port Scanning Elastic Stack SIEM Hari Ke 3	90
Gambar 4. 90 Hasil Monitoring Serangan Port Scanning Splunk Hari Ke 3	90
Gambar 4. 91 Notifikasi Serangan Port Scanning di Splunk Melalui E-mail Hari Ke 3	91
Gambar 4. 92 Diagram Batang Hasil Monitoring Elastic Stack SIEM Hari Ke 1	106
Gambar 4. 93 Diagram Batang Hasil Monitoring Elastic Stack SIEM Hari Ke 2	106
Gambar 4. 94 Diagram Batang Hasil Monitoring Elastic Stack SIEM Hari Ke 3	107
Gambar 4. 95 Diagram Batang Hasil Monitoring Splunk Hari Ke 1	108
Gambar 4. 96 Diagram Batang Hasil Monitoring Splunk Hari Ke 2	108
Gambar 4. 97 Diagram Batang Hasil Monitoring Splunk Hari Ke 3	109

DAFTAR TABEL

Tabel 2. 1 Tabel Perbandingan Penelitian Terdahulu	11
Tabel 3. 1 Spesifikasi Perangkat Keras (Hardware).....	30
Tabel 3. 2 Spesifikasi Perangkat Lunak (Software)	32
Tabel 3. 3 Tabel Pengalamatan Jaringan	39
Tabel 4. 1 Penjelasan Output Elastic Stack SIEM	94
Tabel 4. 2 Tabel Perbandingan Hasil Monitoring	99
Tabel 4. 3 Tabel Hasil Mengirim Notifikasi Serangan.....	105



BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini sangat pesat sehingga memudahkan manusia dalam melakukan aktivitas dalam berbagai bidang, khususnya dibidang teknologi informasi. Semua informasi yang didapatkan sangatlah mudah, cepat, dan praktis. Dibalik kemajuan teknologi tersebut, juga terdapat ancaman dan serangan yang bisa saja terjadi disetiap saat. Ancaman dan serangan tersebut bisa terjadi pada *server* dikendalikan baik secara individu ataupun organisasi, misalnya pada *server* dibidang pemerintahan, pendidikan, serta perusahaan.

Keamanan informasi (*information security*) berperan penting dalam upaya melindungi informasi yang bersifat penting dan rahasia. Keamanan dilakukan untuk melindungi informasi penting dari ancaman dan serangan yang bisa datang kapan saja. Karena dengan semakin berkembangnya teknologi informasi, ancaman dan serangan juga ikut meluas. Teknologi dalam keamanan informasi dapat membantu seorang administrator dalam melakukan *monitoring* dan analisa jaringan pada suatu perusahaan terhadap ancaman dan serangan yang terjadi.

Ancaman dan serangan yang dilakukan oleh pihak yang tidak bertanggung jawab tidak dapat dideteksi secara keseluruhan. Ancaman dan serangan ini memberikan dampak negatif seperti kebocoran dan kehilangan data penting, kerusakan pada *server* seperti kerusakan *logic* dan sistem komputer yang tentunya

dapat merugikan instansi terkait. Oleh karena itu dibutuhkan suatu teknologi keamanan yang dapat membantu dalam membaca dan menganalisa serangan yang masuk ke dalam sebuah *server*.

Security Information And Event Management (SIEM) termasuk salah satu teknologi keamanan informasi yang mengadopsi metodologi untuk membaca dan menganalisa sebuah data atau informasi yang masuk ke dalam *server* yang diakses dengan izin maupun tanpa izin. Data yang terkumpul dan dianalisa secara *realtime* yaitu berupa *log* dari berbagai *event log* yang berasal dari berbagai aplikasi dan perangkat keamanan seperti *server*, *network*, *firewall*, dan lain sebagainya.

Penerapan SIEM sangat membantu dalam melakukan analisa *log* dari suatu *server* yang sedang berjalan. SIEM memiliki beberapa *tools* yang dapat membantu dalam menganalisa *log* dengan mengumpulkan semua informasi yang mengakses *server* yang sedang berjalan. Pada tugas akhir ini telah dilakukan pengujian *tools* SIEM yaitu Elastic Stack SIEM dan Splunk untuk merekam data *log* dari *server* yang dimonitoring kemudian dilakukan analisa terkait data *log* yang direkam. Tujuan dari perekaman dan analisa *log* menggunakan *tools* tersebut adalah untuk membandingkan performansi antara Elastic Stack SIEM dan Splunk dalam kecepatan membaca data dan informasi yang masuk ke dalam *server* yang dapat memudahkan dalam menemukan permasalahan yang terjadi dalam *server*.

1.2 Identifikasi Masalah

Berdasarkan uraian latar belakang di atas, maka dapat dibuat suatu identifikasi masalah yaitu :

1. Serangan dari luar sistem atau *server* dapat membocorkan data, kehilangan data penting, serta mengakibatkan berupa kerusakan *logic* pada *server*.
2. Pengumpulan informasi dari serangan yang masuk ke dalam sistem atau *server* belum bisa terdeteksi secara keseluruhan.
3. Kurangnya informasi mengenai *tools* untuk membaca *log* yang masuk ke dalam *server*.

1.3 Batasan Masalah

Agar penelitian tidak menyimpang dari maksud dan tujuan, maka penulis membuat batasan masalah yaitu :

1. *Tools* SIEM yang digunakan adalah Elastic Stack SIEM dan Splunk.
2. Menjalankan Elastic Stack SIEM dan Splunk menggunakan Ubuntu Server secara bersamaan.
3. Pengujian dilakukan dalam satu jaringan yang sama dengan menggunakan *Switch*.
4. Target yang menjadi serangan adalah sebuah aplikasi *web vulner* yaitu DVWA *web*.
5. Parameter pengujian adalah kecepatan dalam membaca dan menganalisa *log* yang masuk ke dalam *server*.
6. Hanya administrator yang paham dasar jaringan dan *information security* yang dapat menginterpretasikan *output log* dan simulasi pada penelitian ini.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas terdapat beberapa rumusan masalah yaitu :

1. Bagaimana implementasi Elastic Stack SIEM dan Splunk dalam merekam dan mengumpulkan *log* dari serangan yang terjadi?
2. Apakah semua *log* yang terjadi dapat direkam pada saat terjadi serangan?
3. Apa saja komponen yang digunakan dalam menganalisa *log* menggunakan Elastic Stack SIEM dan Splunk?

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian tugas akhir ini adalah :

1. Melakukan implementasi Elastic Stack SIEM dan Splunk pada *Ubuntu Server* guna mengumpulkan *log* yang masuk.
2. Menghasilkan laporan dan hasil analisa data (*log*) dari perekaman semua peristiwa yang masuk ke dalam *server*.

1.6 Manfaat

Adapun manfaat dari penelitian ini adalah :

1. Mengetahui perbandingan dari kemampuan deteksi serangan antara Elastic Stack SIEM dan Splunk.
2. Membantu dalam mengumpulkan informasi berupa *log* dari semua kejadian yang masuk ke dalam *server*.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini secara keseluruhan terdiri dari lima bab dan masing-masing bab terbagi dalam beberapa sub bab. Berikut adalah sistematika penulisan yang dilakukan oleh penulis :

BAB I PENDAHULUAN

Pada bab ini penulis menguraikan tentang latar belakang, identifikasi masalah, batasan masalah, rumusan masalah, tujuan penelitian, manfaat, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini penulis menguraikan tentang tinjauan pustaka dan dasar teori dari hasil penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Pada bab ini penulis menguraikan rancangan proyek akhir yang akan dirancang. Perancangan yang dilakukan meliputi perancangan topologi jaringan, metode pengujian, dan scenario pengujian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini penulis menguraikan tentang hasil dari penelitian yang sudah dilakukan dan dijelaskan sesuai dengan pengujian yang telah dilakukan.

BAB V PENUTUP

Pada bab ini penulis menguraikan tentang kesimpulan dari hasil analisis dan pengujian yang telah dilakukan dan saran hasil penelitian.



BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Walidatush Sholihah, dkk (2020) melakukan penelitian dengan judul “*Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack)*”. Penelitian ini bertujuan untuk membuat *Log Event Management Server* menggunakan ELK Stack yang dapat memudahkan dalam membaca dan menganalisis *log service* pada server.

Muhammad Rijal Kamal dan Mukhamad Andri Setiawan (2021) melakukan penelitian dengan judul “*Deteksi Anomali Security Information and Event Management (SIEM) Splunk pada Jaringan UII*”. Penelitian ini ditujukan untuk mendeteksi anomaly pada sistem UII sebagai langkah antisipasi ancaman menggunakan alat SIEM Splunk yang mengolah *log firewall* PaloAlto yang sudah terpasang pada sistem UII dan menampilkan hasil deteksi di *dashboard* Splunk.

Mustafa Dzul Akmal, dkk (2018) melakukan penelitian dengan judul “*Implementasi Security Information And Event Management (SIEM) Menggunakan Ossim*”. Pada penelitian ini diimplementasikan SIEM dengan menggunakan tools SIEM OSSIM (*Open Source Security Information Management*) untuk melakukan *monitoring* aktivitas pada sebuah jaringan. OSSIM dapat melakukan analisa data yang dihasilkan dari setiap serangan yang masuk dan ditampilkan dalam bentuk diagram pada *dashboard* OSSIM.

Adrian Admi dan Abdul Hakim Nur Maulana (2020) melakukan penelitian dengan judul “Penerapan Elastic Stack Sebagai *Tools* Alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia”. Elastic Stack dipilih karena mudah untuk dikembangkan sesuai kebutuhan dan kemampuan anggaran instansi pemerintah yang berbeda-beda, bersifat *open source* yang didukung oleh komunitas sehingga dapat terus dikembangkan.

Claudia Tarigan, dkk (2018) melakukan penelitian dengan judul “Sistem Pengawasan Kinerja Jaringan Server Web Apache dengan *Log Management System* ELK (Elasticsearch, Logstash, Kibana)”. Pada penelitian ini menggunakan ELK sebagai *tools* yang dikombinasikan di dalam *web server* Apache untuk mengelola, menampilkan, dan mengawasi data-data *log* yang ada sehingga administrator dapat mengetahui kinerja yang terdapat pada *web server*.

Daniel Stevan Sampurno, dkk (2019) melakukan penelitian dengan judul “Implementasi Pembuatan Distro Linux Untuk Keperluan Laboratorium Informatika”. Penelitian ini bertujuan untuk membantu dalam membuat *environment* yang spesifik karena seluruh *software* yang diperlukan sudah berada didalam satu tempat dan penggunaan Linux sangat membantu dalam menekan biaya operasi dari sebuah perusahaan atau lembaga karena bersifat *open source*.

I Kadek Susila Satwika dan Ketut Ngurah Semadi (2020) melakukan penelitian dengan judul “Perbandingan Performansi *Web Server* Apache dan Nginx Dengan Menggunakan Ipv6”. Pada penelitian ini membangun dua buah *web server* yang

diinstall dengan APACHE dan NGINX. Server yang digunakan adalah virtual server dengan menggunakan aplikasi *virtual box*. Kemudian masing-masing server dikonfigurasi menggunakan IPv6 sebagai alamat identik dan *server virtual*. Pengukuran performansi server dengan parameter *load average*, *response time*, dan *request loss*.

Nana Suryana dan Dedi Dwi Saputra (2018) melakukan penelitian dengan judul “Perancangan Penggunaan *Firewall* Dan *Proxy Server* Untuk Membatasi Hak Akses Internet”. Pada penelitian ini *firewall* menggunakan *iptables* pada *proxy server* dan menggunakan *proxy squid* dengan server Linux Ubuntu yang telah di implementasikan di laboratorium. Sehingga dalam mengakses *internet*, *firewall* akan mem-*block* situs-situs yang tidak bermanfaat bagi mahasiswa dan dosen sehingga keamanan dari jaringan lebih aman.

Afit Muhammad Lukman dan Yusuf Bachtiar (2018) melakukan penelitian dengan judul “Analisis Sistem Pengelolaan, Pemeliharaan Dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto”. Penelitian ini dilakukan di IT Purwokerto dengan menggunakan topologi star dengan tipe jaringan *client-server*. Server yang digunakan adalah *linux debian*. Sistem keamanan jaringan dari IT Telkom Puwokerto dianalisis menggunakan sistem *server* autentifikasi dan menggunakan *Virtual Private Network* (VPN). Dalam sistem keamanan jaringan yang digunakan juga ditambahkan suatu *firewall* yaitu *demilitarized zone* (DMZ) agar ada tembok pemisah antara jaringan publik dan jaringan lokal sehingga sistem keamanan lebih efektif.

Ibnu Muakhori, dkk (2018) melakukan penelitian dengan judul “Membangun *Web Server* Menggunakan *Dynamic Domain Name System* (DNS) Berbasis *Berkeley Internet Name Domain* (BIND9) Pada IP Dinamis”. Pada penelitian ini menggunakan IP Dinamis untuk membangun *web server* sendiri dengan biaya yang terjangkau. *Dynamic Domain System* merupakan solusi bagi yang menginginkan *web server* sendiri dengan biaya yang lebih terjangkau.

Yacob Hae dan Wiwin Sulisty (2021) melakukan penelitian dengan judul “Analisis Keamanan Jaringan Pada *Web* Dari Serangan *Sniffing* Dengan Metode Eksperimen”. Pada penelitian ini menunjukkan bahwa meskipun *web* telah memakai protokol HTTPS yang merupakan bagian teraman dari HTTP namun *hacker* tetap bisa mencuri data dengan cara menurunkan protokol *web* yang harusnya HTTPS menjadi HTTP dengan teknik *sniffing* yang dibantu dengan *tools* Bettercap.

Tito Brades dan Irwansyah (2022) melakukan penelitian dengan judul “Pemanfaatan Metode *Port Knocking* Dan *Blocking* Untuk Keamanan Jaringan BPKAD Provinsi Sumsel”. Pada penelitian ini dilakukan pencegahan untuk mengamankan *service port* yaitu dengan melakukan *blocking port* menggunakan *firewall*. *Port knocking* merupakan metode untuk mengakses *port* yang telah diblok dengan mengirimkan *packet* atau koneksi sesuai dengan aturan *knocking* yang telah dibuat.

Ahmad Zafrullah Mardiansyah, dkk (2021) melakukan penelitian dengan judul “Optimasi *Port Knocking* Dan *Honeypot* Menggunakan *IPtables* Sebagai

Keamanan Jaringan Pada Server”. Penelitian ini dilakukan untuk membuktikan performance keamanan jaringan menggunakan metode *port knocking* dan *honeypot* dimana metode ini akan dikombinasikan dengan metode *Iptables*.

Audy Gerald Palilingan, dkk (2020) melakukan penelitian dengan judul “Sistem Komunikasi Darurat Bencana Dengan Teknologi Mobile *Ad-Hock Network* (MANET)”. Penelitian ini dilakukan untuk memperoleh hasil bahwa teknologi manet cocok digunakan untuk sistem komunikasi pada daerah bencana, karena telah dilakukan uji konektifitasnya yang dapat melakukan *self configure* dan *self healing* pada sistem *wifi* yang telah terpasang di tiap *node* manet.

Tabel 2. 1 Tabel Perbandingan Penelitian Terdahulu

Peneliti	Tahun	Judul	Tools	Tinjauan
Walidatush Sholihah, dkk	2020	Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack)	Elastic Search Logstash Kibana (ELK Stack)	Penelitian ini bertujuan untuk membuat Log Event Management Server menggunakan ELK Stack yang dapat memudahkan dalam membaca dan menganalisis log service pada server.

Muhammad Rijal Kamal dan Mukhamad Andri Setiawan	2021	Deteksi Anomali dengan <i>Security Information and Event Management (SIEM) Splunk pada Jaringan UII</i>	Splunk	Penelitian ini ditujukan untuk mendeteksi anomaly pada sistem UII sebagai langkah antisipasi ancaman menggunakan alat SIEM Splunk yang mengolah <i>log firewall</i> PaloAlto yang sudah terpasang pada sistem UII dan menampilkan hasil deteksi di <i>dashboard</i> Splunk.
Mustafa Dzul Akmal, dkk	2018	Implementasi <i>Security Information And Event Management (SIEM)</i>	Ossim	Penelitian ini diimplementasikan SIEM dengan menggunakan <i>tools</i> SIEM OSSIM (<i>Open Source Security</i>)

		Menggunakan Ossim		<i>Information Management</i>) untuk melakukan monitoring aktivitas pada sebuah jaringan. OSSIM dapat melakukan analisa data yang dihasilkan dari setiap serangan yang masuk dan ditampilkan dalam bentuk diagram pada <i>dashboard</i> OSSIM.
Adrian Admi dan Abdul Hakim Nur Maulana	2020	Penerapan Elastic Stack Sebagai Tools Alternatif Pemantauan Traffic Jaringan dan Host pada	Elastic Stack	Penelitian ini menggunakan <i>tools</i> SIEM yaitu Elastic Stack karena mudah untuk dikembangkan sesuai kebutuhan dan kemampuan anggaran instansi

		Instansi Pemerintah untuk Memperkuat Keamanan dan Keamanan Siber Indonesia		pemerintah yang berbeda-beda, bersifat <i>open source</i> yang didukung oleh komunitas sehingga dapat terus dikembangkan.
Claudia Tarigan, dkk	2018	Sistem Pengawasan Kinerja Jaringan Server Web Apache dengan Log Management System ELK (Elasticsearch, Logstash, Kibana)	ELK Stack, Web Server Apache	Penelitian ini menggunakan ELK sebagai <i>tools</i> yang dikombinasikan di dalam <i>web server</i> Apache untuk mengelola, menampilkan, dan mengawasi data-data <i>log</i> yang ada sehingga administrator dapat mengetahui kinerja

				yang terdapat pada <i>web server</i> .
Daniel Stevan Sampurno, dkk	2019	Implementasi Pembuatan Distro Linux Untuk Keperluan Laboratorim Informatika	Linux Ubuntu Versi 18.04	Penelitian ini bertujuan untuk membantu dalam membuat <i>environment</i> yang spesifik karena seluruh <i>software</i> yang diperlukan sudah berada didalam satu tempat dan penggunaan Linux sangat membantu dalam menekan biaya operasi dari sebuah perusahaan atau lembaga karena bersifat <i>open source</i> .
I Kadek Susila	2020	Perbandingan Performansi	Web Server Apache dan	Penelitian ini membangun dua

Satwika dan Ketut Ngurah Semadi		Web Server Apache Dan Nginx Dengan Menggunakan IPv6	<i>web server</i> Nginx	buah <i>web server</i> yang diinstall dengan APACHE dan NGINX. <i>Server</i> yang digunakan adalah <i>virtual server</i> dengan menggunakan aplikasi <i>virtual box</i> . Kemudian masing- masing <i>server</i> dikonfigurasi menggunakan IPv6 sebagai alamat identik dan <i>server</i> <i>virtual</i> . Pengukuran performansi <i>server</i> dengan parameter <i>load average</i> , <i>response time</i> , dan <i>request loss</i> .
---------------------------------------	--	---	--------------------------------	---

Nana Suryana dan Dedi Dwi Saputra	2018	Perancangan Penggunaan <i>Firewall</i> Dan <i>Proxy Server</i> Untuk Membatasi Hak Akses Internet	<i>Firewall</i> , <i>Proxy Server</i>	Penelitian ini <i>firewall</i> menggunakan <i>iptables</i> pada <i>proxy server</i> dan menggunakan <i>proxy squid</i> dengan <i>server Linux Ubuntu</i> yang telah di implementasikan di laboratorium. Sehingga dalam mengakses <i>internet</i>, <i>firewall</i> akan mem-<i>block</i> situs-situs yang tidak bermanfaat bagi mahasiswa dan dosen sehingga keamanan dari jaringan lebih aman.
--	------	--	--	--

Afit Muhammad Lukman dan Yusuf Bachtiar	2018	Analisis Sistem Pengelolaan, Pemeliharaan Dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto	VPN, <i>firewall</i>	Penelitian ini dilakukan di IT Purwokerto <i>Server</i> yang digunakan adalah <i>linux debian</i>. Sistem keamanan jaringan dari IT Telkom Purwokerto dianalisis menggunakan sistem <i>server</i> autentifikasi dan menggunakan <i>Virtual Private Network (VPN)</i>. Dalam sistem keamanan jaringan ditambahkan suatu <i>firewall</i> yaitu <i>demilitarized zone (DMZ)</i> agar ada tembok pemisah antara jaringan publik dan jaringan
---	------	---	-------------------------	---

				lokal sehingga sistem keamanan lebih efektif.
Ibnu Muakhori, dkk	2018	Membangun <i>Web Server</i> Menggunakan <i>Dynamic Domain Name System (DNS)</i> Berbasis Berkeley <i>Internet Name Domain (BIND9)</i> Pada IP Dinamis	BIND9	Penelitian ini menggunakan IP Dinamis untuk membangun <i>web server</i> sendiri dengan biaya yang terjangkau. <i>Dynamic Domain System</i> merupakan solusi bagi yang menginginkan <i>web server</i> sendiri dengan biaya yang lebih terjangkau.
Yacob Hae dan Wiwin Sulistyo	2021	Analisis Keamanan Jaringan Pada <i>Web</i> Dari Serangan	Bettercap	Penelitian ini menunjukkan bahwa meskipun <i>web</i> telah memakai protokol HTTPS yang

		<i>Sniffing</i> Dengan Metode Eksperimen		merupakan bagian teraman dari HTTP namun <i>hacker</i> tetap bisa mencuri data dengan cara menurunkan protokol <i>web</i> yang harusnya HTTPS menjadi HTTP dengan teknik <i>sniffing</i> yang dibantu dengan <i>tools</i> Bettercap.
Tito Brades dan Irwansyah	2022	Pemanfaatan Metode <i>Port</i> <i>Knocking</i> Dan <i>Blocking</i> Untuk Keamanan Jaringan BPKAD	<i>Firewall</i> , <i>PuTTY</i> , <i>Mikrotik</i>	Penelitian ini dilakukan pencegahan untuk mengamankan <i>service port</i> yaitu dengan melakukan <i>blocking port</i> menggunakan <i>firewall. Port</i>

		Provinsi Sumsel		<i>knocking</i> merupakan metode untuk mengakses <i>port</i> yang telah diblok dengan mengirimkan <i>packet</i> atau koneksi sesuai dengan aturan <i>knocking</i> yang telah dibuat.
Ahmad Zafrullah Mardiansyah, dkk	2021	Optimasi Port <i>Knocking</i> Dan <i>Honeypot</i> Menggunakan <i>Iptables</i> Sebagai Keamanan Jaringan Pada <i>Server</i>	<i>Firewall</i> , VirtualBox, <i>Honeypot</i>	Penelitian ini dilakukan untuk membuktikan <i>performance</i> keamanan jaringan menggunakan metode <i>port knocking</i> dan <i>honeypot</i> dimana metode ini akan dikombinasikan dengan metode <i>Iptables</i> .

Audy Gerald Palilingan, dkk	2020	Sistem Komunikasi Darurat Bencana Dengan Teknologi Mobile Ad- Hock Network (MANET)	<i>SSH, FTP,</i> <i>Raspberry Pi,</i> <i>Iperf</i>	Penelitian ini dilakukan untuk memperoleh hasil bahwa teknologi manet cocok digunakan untuk sistem komunikasi pada daerah bencana, karena telah dilakukan uji konektifitasnya yang dapat melakukan <i>self</i> <i>configure</i> dan <i>self</i> <i>healing</i> pada sistem <i>wifi</i> yang telah terpasang di tiap <i>node</i> manet.
-----------------------------------	------	--	--	--

2.2 Dasar Teori

2.2.1 Security Information and Event Management (SIEM)

Menurut Akmal, dkk (2018) SIEM adalah sebuah aplikasi *software* yang berfungsi mengumpulkan informasi dan *event* terkait dengan keamanan sebuah *network* (WAN maupun LAN). SIEM merupakan gabungan dari sebuah produk

yang sebelumnya terpisah, yaitu *Security Information Management* (SIM) dan *Security Event Management* (SIEM). Produk dari (SIEM), bisa berupa peralatan, *software* ataupun *service* dan dapat digunakan untuk membuat *log* data keamanan dan men-*generate report* sesuai dengan keadaan yang terjadi.

Menurut Kamal dan Setiawan (2021) 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.

2.2.2 *Elasticsearch*

Menurut Sholihah, dkk (2020) *Elasticsearch* merupakan mesin pencari dan analitik yang membuat data mudah untuk dijelajahi. *Elasticsearch Platform* *open source* yang terdistribusi.

2.2.3 *Splunk*

Menurut Kamal dan Setiawan (2021) *Splunk* merupakan 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.

2.2.4 VirtualBox

VirtualBox adalah *hypervisor* yang dapat menjalankan banyak sistem operasi tamu didalamnya sehingga dapat melakukan percobaan dengan *tools hacking*. Saat menggunakan VirtualBox, sistem operasi utama tidak akan berpengaruh. OS *Host* dan sistem operasi tamu masih dapat berkomunikasi satu sama lain. VirtualBox berisi *recompiler* dinamis berdasarkan teknologi QEMU, yang dapat membantu dalam pencapaian penggunaanya (Sinha, 2018).

2.2.5 Linux

Menurut Sampurno, dkk (2019) Linux adalah sistem operasi yang bersifat *open source* dan bebas (*free*) di bawah lisensi *GNU (GNU is not Unix) GPL (General Public License)*. Arti kata *open source* adalah pada Linux kode sumber yang menjadi inti diikutsertakan dalam *program* sehingga dapat dilihat oleh siapa saja tanpa harus menandatangani suatu perjanjian khusus. Arti kata bebas atau *free* mengacu pada kebebasan bukan berarti bebas biaya. Linux bebas untuk dipublikasikan, dimodifikasi, dan disebarluaskan.

2.2.6 Ubuntu

Ubuntu adalah distro Linux yang berbasis Debian Linux. Distribusi Linux yang berbeda menagertkan fungsional yang berbeda. Tujuan Ubuntu adalah membawa Linux ke ruang lingkup *desktop*. Untuk melakukan ini, perlu menyediakan antarmuka pengguna yang stabil, banyak alat kantor, dan *driver* untuk berbagai *peripheral* yang mudah digunakan. Meskipun dari kelompok distro yang berbeda namun Canocial Ltd, menyediakan sebuah titik sentral untuk dukungan dan pengembangan (Krawetz, 2010).

2.2.7 Kali Linux

Menurut Hae dan Sulisty (2021) Kali Linux adalah sistem operasi yang berbasis debian dikembangkan oleh Offensive Security. Kali Linux lebih sering digunakan untuk melakukan penetrasi sistem, keamanan pada *web* dan juga pada jaringan.

2.2.8 IP Address

Menurut Lukman dan Bachtiar (2018) IP Address adalah sebuah sistem pengalamatan unik setiap *host* yang terkoneksi ke jaringan berbasis TCP/IP. IP address bisa dianalogikan seperti alamat rumah. Ketika sebuah datagram dikirim, informasi alamat inilah yang menjadi acuan *datagram* agar bisa sampai ke *device* yang dituju. IP address terbagi dalam 2 versi, IPv4 dan IPv6.

2.2.9 Client dan Server

Menurut Lukman dan Bachtiar (2018) Jaringan *client-server* didefinisikan sebagai suatu arsitektur jaringan komputer dimana perangkat *client* melakukan proses meminta data dan *server* yang memiliki tugas untuk memberikan respon berupa data terhadap *request* tersebut. Perangkat *client* biasanya berupa perangkat komputer dengan aplikasi *software* jaringan yang telah teinstal guna untuk meminta dan menerima data melalui jaringan. Salah satu contoh aplikasi *software* yang paling sering digunakan untuk meminta dan menerima data pada jaringan ialah *web browser*, dimana *user* dapat melakukan *request* untuk sebuah halaman *web*. *Server* menyimpan informasi dan data yang kompleks yang mungkin dibutuhkan *client*, oleh karena itu biasanya *server* terdiri dari komputer dengan performansi yang

tinggi baik dari segi pemrosesan maupun dari segi memori, hal tersebut agar *server* mampu melayani *request* dari banyak *client* secara bersamaan.

2.2.10 Web Server

Menurut Muakhori, dkk (2018) *Web Server* merupakan salah satu mesin dimana tempat aplikasi atau perangkat lunak beroperasi dalam mendistribusikan halaman *web* kepada pengguna melalui protokol komunikasi tertentu (*IP Address*). Oleh karena dalam satu halaman *web* biasanya terdiri dari berbagai macam jenis berkas seperti gambar, *video*, teks, *audio*, *file*, dan lain sebagainya, maka pemanfaatan *web server* berfungsi juga untuk mentransfer keseluruhan aspek pemberkasan dalam halaman tersebut, termasuk teks, gambar, *video*, *audio*, *file*, dan sebagainya. *Web server* akan mencari data yang diminta *browser*, lalu mengirimkan data tersebut ke *browser* atau menolaknya jika ternyata data yang diminta tidak ditemukan.

2.2.11 Apache Web Server

Menurut Satwika dan Semadi (2020) *Apache Web Server* merupakan *unix-based web server*. *Apache* merupakan *web server* yang paling populer dan banyak digunakan lebih dari 42% dari berbagai domain *website* yang ada di *internet*. *Apache* pertama kali dikembangkan berbasis kode pada NCSA HTTPD 1.3 yang diprogram ulang menjadi sebuah *web server*. *Apache* memiliki fitur yang sangat lengkap mulai dari performa yang tinggi, fungsionalitas, efisiensi, serta kecepatan. *Apache* juga merupakan *web server* berbasis *open source*.

Menurut Tarigan, dkk (2018) Apache *web server* menyimpan file *log* yang mana terdapat dua jenis *log* yaitu, *error.log* dan *access.log*. *Error.log* menyimpan pesan kesalahan pada *web server*, sedangkan *access.log* menyimpan data-data yang berupa IP akses *web*, *timestamp*, *status code*, besar *bandwith* yang diakses, keterangan lokasi yang diakses, dan *engine* yang digunakan.

2.2.12 *Damn Vulnerable Web App (DVWA)*

Damn Vulnerable Web App (DVWA) adalah sebuah aplikasi *web* PHP/MySQL yang sangat rentan. Tujuan utamanya adalah untuk menjadi bantuan bagi profesional keamanan untuk melatih kemampuan mereka dan penggunaan *tools* yang legal, membantu *web developer* supaya mengerti tentang proses keamanan aplikasi *web* dan melatih guru atau murid untuk belajar tentang keamanan aplikasi di ruangan kelas (DVWA, 20 September 2021.).

2.2.13 *Fingerprinting*

Fingerprinting adalah teknik untuk mendapatkan informasi tentang sistem operasi target. Informasi yang didapatkan berupa *banner*, *service*, *ports*, dan sistem operasi yang digunakan pada target (Sinha, 2018).

2.2.14 *SQL Injection*

SQL Injection adalah salah satu kerentanan paling merusak yang berdampak pada bisnis, karena dapat menyebabkan paparan semua informasi sensitive yang disimpan dalam *database* aplikasi, termasuk informasi berguna seperti nama pengguna, kata sandi, nama, alamat rumah, nomor telepon, dan detail kartu kredit (Clarke, 2009).

2.2.15 *Denial of Service (DoS)*

Denial of Service (DoS) merupakan serangan jahat yang menolak akses ke sistem, jaringan, aplikasi, atau informasi ke pengguna yang sah. Serangan DoS dapat mengambil banyak bentuk dan dapat diluncurkan dari satu sistem atau dari beberapa sistem. Serangan DoS tidak dapat sepenuhnya dicegah, juga tidak dapat dihentikan sepenuhnya tanpa identifikasi sistem sumber (Maiwald, 2013).

2.2.16 *Port Scanning*

Port Scanning adalah sebuah cara untuk melakukan identifikasi *port* yang terbuka dan menentukan layanan yang tersedia pada sistem. Layanan adalah sebuah pekerjaan spesifik atau tugas dari komputer yang menjalankan seperti *e-mail*, FTP, *printing* atau menjalankan halaman *web*. Salah satu *tools* untuk melakukan *port scanning* adalah Nmap yang ditulis oleh Gordon “Fyodor” Lyon dan banyak dibangun pada distro sistem operasi Linux termasuk Backtrack (Engelbreton, 2011).

2.2.17 *Switch*

Menurut Suryana dan Saputra (2018) *Switch* adalah sebuah alat jaringan yang melakukan penjemputan tak tampak (penghubung atau penyekat (segmentation) banyak jaringan dengan pengalihan berdasarkan alamat MAC. Daripada melewatkan paket ke semua *port*, *switch* meneruskan ke *port* yang dialamatkan. Jadi, *switch* dapat secara drastis mengurangi *traffic network*. *Switch* memelihara daftar MAC address yang dihubungkan ke *port-port* nya yang digunakan untuk menentukan kemana harus mengirimkan paketnya.

2.2.18 *Secure Shell (SSH)*

Menurut Palilingan, dkk (2020) *Secure Shell (SSH)* adalah salah satu *utility* dalam sistem operasi Linux yang digunakan untuk melakukan remote login pada komputer yang berada pada sebuah jaringan. SSH juga dapat dijalankan pada sistem operasi Windows tetapi dengan bantuan *software* tertentu seperti Putty. Perbedaan penggunaan *utility remote login* SSH dan TELNET yaitu SSH mengenkripsi data yang di transmisikan dalam jaringan komputer menjadikan SSH lebih aman untuk digunakan.

2.2.19 *Putty*

Menurut Brades dan Irwansyah (2022) Putty merupakan aplikasi *remote access* yang berbasis open source yang berguna untuk mengendalikan sistem dari jarak jauh atau ditempat yang berbeda dengan memanfaatkan protokol jaringan untuk melakukan *remote* pada komputer maupun *server* dengan menampilkan *command teks* untuk menjalankan perintah tertentu. Adapun fitur-fitur pada Putty seperti mendukung OS Windows, mendukung sistem 32-bit maupun 64-bit dan mendukung layanan *remote* (telnet, ssh, sftp, dan lainnya).

BAB III

METODOLOGI PENELITIAN

3.1 Alat Dan Bahan Penelitian

Untuk melakukan penelitian mengenai SIEM maka diperlukan komponen perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan dalam proses penelitian tersebut, yaitu sebagai berikut :

3.1.1 Spesifikasi Perangkat Keras (*Hardware*)

Spesifikasi perangkat keras (*hardware*) yang dibutuhkan sebagai *client* dan *server* dalam penelitian ini adalah sebagai berikut :

Tabel 3. 1 Spesifikasi Perangkat Keras (*Hardware*)

No	Perangkat Keras	Spesifikasi	Fungsi
1	Laptop	• HP Laptop 15-db0xx • AMD Ryzen 3 2200 • U with Radeon Vega • Mobile Gfx • Ram 8192 MB • Hard disk 1 TB	Digunakan sebagai media pengujian SIEM menggunakan Elastic Stack SIEM dan Splunk

2	Switch	Cisco Catalyst 2960 Series Switch	Digunakan sebagai media penghubung jaringan lokal antara PC yang digunakan sebagai <i>server</i> , <i>client</i> atau <i>attacker</i> dan Laptop sebagai administrator dari SIEM.
3	Kabel UTP (<i>Unshielded Twisted Pair</i>)	Kabel Straight Cat 5e	Digunakan sebagai penghubung jaringan lokal antara PC dan Laptop melalui <i>Switch</i> .
4	PC Labor	Lenovo Intel(R) Core(TM) i5-3470 Ram 4096 MB Hard disk 4540 MB	Digunakan sebagai media untuk server Elastic Stack dan Splunk, serta digunakan juga sebagai <i>client</i> atau <i>attacker</i> dalam melakukan pengujian serangan.

3.1.2 Spesifikasi Perangkat Lunak (*Software*)

Spesifikasi perangkat lunak (*software*) yang dibutuhkan dalam pembuatan penelitian ini adalah sebagai berikut :

Tabel 3. 2 Spesifikasi Perangkat Lunak (*Software*)

No	Perangkat Lunak	Spesifikasi	Fungsi
1	Windows 10	Windows 10 Home Single Language 64-bit	Windows 10 digunakan sebagai administrator yang bertindak untuk melakukan <i>monitoring log</i> menggunakan Elastic Stack SIEM dan Splunk.
2	Ubuntu Server	Versi 20.04	Ubuntu server digunakan untuk pusat meng- <i>install</i> tools SIEM yaitu Elastic Stack SIEM dan Splunk.
3	Kali Linux	Versi 2020.04	Kali Linux digunakan sebagai <i>client</i> atau <i>attacker</i> dalam mengakses <i>web server</i> dan menyerang <i>web server</i> .
4	Elastic Stack SIEM	Versi 7.16	Elastic Stack digunakan sebagai <i>tools</i> untuk <i>monitoring</i> dan analisis <i>log</i> terhadap serangan.

5	Splunk	Splunk Enterprise	Splunk digunakan sebagai <i>tools</i> untuk <i>monitoring</i> dan analisis <i>log</i> terhadap serangan.
6	VirtualBox	Versi 6.1	VirtualBox digunakan sebagai tempat melakukan instalasi virtual server SIEM menggunakan Ubuntu Server dan juga instalasi <i>web server</i> dan Kali Linux.
7	Apache	Apache2	<i>Web server</i> apache digunakan sebagai instalasi dari <i>website vulner</i> yaitu DVWA.
8	Sqlmap	Open Source	Sqlmap digunakan sebagai <i>tools</i> untuk melakukan injeksi <i>database</i> dari <i>vulner</i> sebuah <i>website</i> .
9	Nmap	7.91	Nmap digunakan sebagai <i>tools</i> untuk melakukan <i>port scanning</i> yang

			tersedia dari sebuah <i>website</i> .
10	Nikto	2.1.6	Nikto digunakan sebagai tools untuk melakukan <i>scanning system</i> dari sebuah <i>website</i> .
11	Putty	Versi 0.76	Putty digunakan sebagai media <i>remote</i> akses antara administrator dengan <i>server</i> SIEM.

3.2 Prosedur Penelitian

3.2.1 Teknik Pengumpulan Data

Teknik Pengumpulan data yang dilakukan adalah dengan cara mendapatkan data yang benar dan menyakinkan agar hasil yang diraih tidak menyimpang dari tujuan yang telah diterapkan sebelumnya, penulis melakukan langkah-langkah penelitian sebagai berikut :

1. Perancangan

Tahap ini merancang analisa spesifikasi yang telah di dapat ke dalam bentuk arsitektural perangkat lunak (*software*), untuk diimplementasikan kepada *web server* yang dibangun sebagai bahan pengujian terhadap serangan yang dilakukan.

2. Pengujian

Dalam tahap pengujian kinerja SIEM dilakukan dengan menggunakan *tools* yaitu Elastic Stack SIEM dan Splunk untuk mendapatkan hasil dari pengujian yang sedang berjalan.

3. Analisis

Tahapan analisis digunakan untuk membuktikan bahwa Elastic Stack SIEM dan Splunk dapat menangkap berbagai jenis serangan yang dilakukan seperti *fingerprinting*, *SQL Injection*, *DoS*, dan *Port Scanning*. Dan mampu dalam menganalisa data yang dihasilkan dalam bentuk diagram.

4. Dokumentasi

Pada proses dokumentasi, penulis juga melakukan studi pustaka, membaca dan mempelajari dokumen-dokumen, buku-buku acuan, jurnal, serta sumber lainnya yang berkaitan dengan penelitian untuk dijadikan referensi dalam pembuatan penelitian ini.

3.2.2 Jenis Data

1. Data Primer

Data primer adalah data yang diperoleh secara langsung dari simulasi penelitian yang dilakukan oleh penulis. Dalam penelitian ini, penulis menggunakan satu unit *switch*, empat unit komputer laboratorium di laboratorium jaringan komputer di teknik Informatika UIR dan satu unit laptop. *Switch* digunakan sebagai media penghubung jaringan lokal antara komputer

labor dan laptop. Tiga unit komputer labor digunakan sebagai media *server* yaitu Elastic Stack SIEM, Splunk, dan web server menggunakan Ubuntu Server, dan satu unit digunakan sebagai simulasi serangan yang telah di-*install* Kali Linux. Satu unit laptop digunakan sebagai administrator dalam me-*monitoring* log serangan yang masuk. Data dari penelitian ini diperoleh dari kemampuan Elastic Stack SIEM dan Splunk dalam menganalisa *log* yang masuk kedalam *web server*.

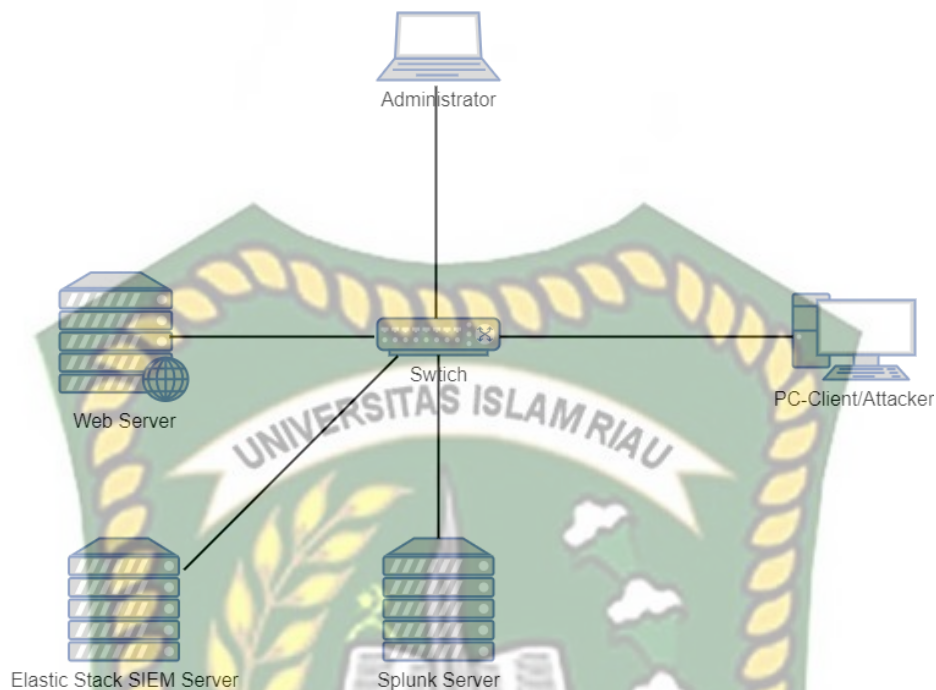
2. Data Sekunder

Yaitu suatu data yang diperoleh melalui daftar pustaka, buku, jurnal, dan literature-literature yang berhubungan dengan masalah yang sedang penulis buat dan diambil dalam bentuk yang sudah jadi atau publikasi. Studi literature adalah melakukan pengumpulan data dengan membaca buku-buku dan jurnal-jurnal yang berkaitan dengan permasalahan yang dibahas.

3.3 Perancangan Dan Pengembangan Topologi Jaringan

3.3.1 Desain Topologi Jaringan

Pada simulasi penelitian ini *dirancang* tiga *server* menggunakan *virtual machine* dengan sistem operasi Ubuntu Server. Topologi yang digunakan terdiri dari dua *server* yang bertindak sebagai SIEM yang masing-masing di-*install* Elastic Stack SIEM dan Splunk, serta terdapat satu *server* sebagai *web server* menggunakan Apache.



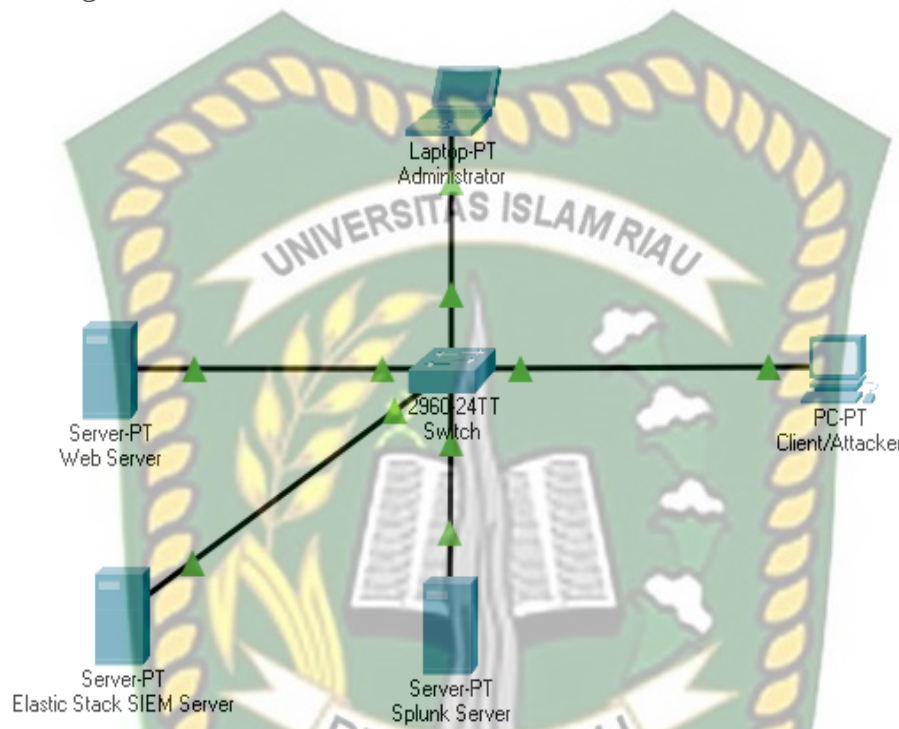
Gambar 3. 1 Desain Topologi Jaringan

Berdasarkan gambar 3.1, simulasi menggunakan jaringan LAN (*Local Area Network*) sederhana untuk mensimulasikan komunikasi yang terjadi antara *host* dan *server* dimana *host* dan *server* terhubung pada satu jaringan yang sama. Pada simulasi ini terdapat satu *host* bertindak sebagai *client* atau *server* yang mengakses *web server* dan melakukan penyerangan dengan menggunakan sistem operasi Kali Linux. Penyerangan yang dilakukan antara lain adalah *Port Scanning*, *SQL Injection*, *Fingerprinting*, dan *DoS*.

3.3.2 Topologi Fisik

Topologi fisik adalah topologi jaringan yang menggabungkan pengabelan dan penempatan berbagai komponen jaringan. Pada topologi fisik penelitian tersebut menggunakan 1 buah PC yang bertindak sebagai *client* atau *attacker*, 1 buah laptop yang bertindak sebagai administrator. Terdapat 3 buah *server* yang

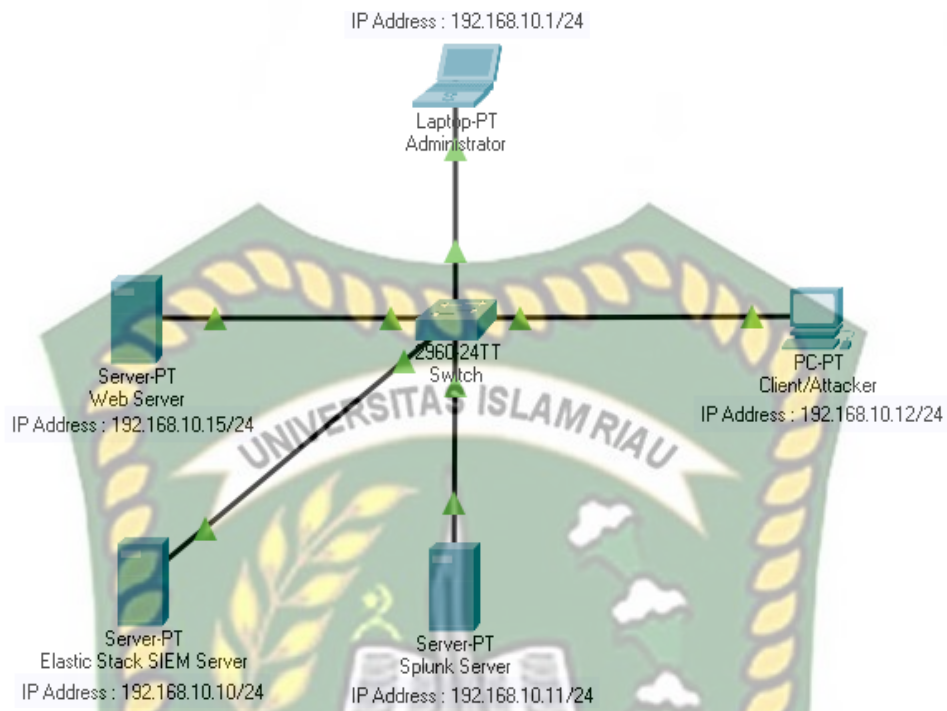
masing-masing digunakan sebagai *web server*, Elastic Stack SIEM *server*, dan Splunk *server*. Berikut adalah topologi fisik dari desain jaringan yang sudah dirancang :



Gambar 3.2 Topologi Fisik

3.3.3 Topologi *Logic*

Topologi *Logic* adalah topologi yang menggambarkan hubungan secara logika yang terjadi pada masing-masing komputer tanpa memperhatikan interkoneksi fisik perangkat. Berikut adalah topologi *logic* dari desain jaringan yang sudah dirancang :



Gambar 3. 3 Topologi Logic

Tabel 3. 3 Tabel Pengalamatan Jaringan

Device	IP Address	Subnet Mask
Administrator	192.168.10.1	255.255.255.0
Elastic Stack SIEM Server	192.168.10.10	255.255.255.0
Splunk Server	192.168.10.11	255.255.255.0
<i>Client/Attacker</i>	192.168.10.12	255.255.255.0
<i>Web Server</i>	192.168.10.15	255.255.255.0

3.4 Metode Pengujian

Pada pengujian ini dilakukan serangan terhadap *web server* yang kemudian *tools* SIEM yaitu Elastic Stack SIEM dan Splunk bertugas untuk melakukan deteksi serangan yang terjadi pada *web server*. Adapun metode pengujian yang dilakukan adalah sebagai berikut :

3.4.1 *Fingerprinting*

Fingerprinting merupakan teknik untuk melakukan pengumpulan informasi seperti sistem operasi, *banner*, *service*, dan *ports* dari target yang diserang. Pengumpulan informasi dapat berdampak buruk dari target dimana terdapat celah keamanan yang bisa digunakan untuk menyerang target.

3.4.2 *SQL Injection*

Serangan *SQL Injection* merupakan serangan yang melakukan injeksi terhadap *query database* dari sistem suatu *website*, dalam penelitian ini dilakukan pengujian *SQL Injection* menggunakan *Sqlmap* terhadap *website DVWA*. Serangan *SQL Injection* sangat berdampak buruk karena bisa mendapatkan data rahasia dari *database* yang di injeksi.

3.4.3 *Denial of Service (DoS)*

Denial of Service (DoS) adalah jenis serangan terhadap sebuah *server* di dalam jaringan *internet* dengan cara menghabiskan sumber yang dimiliki oleh *server* tersebut sampai *server* tersebut tidak dapat diakses karena mendapatkan request yang banyak.

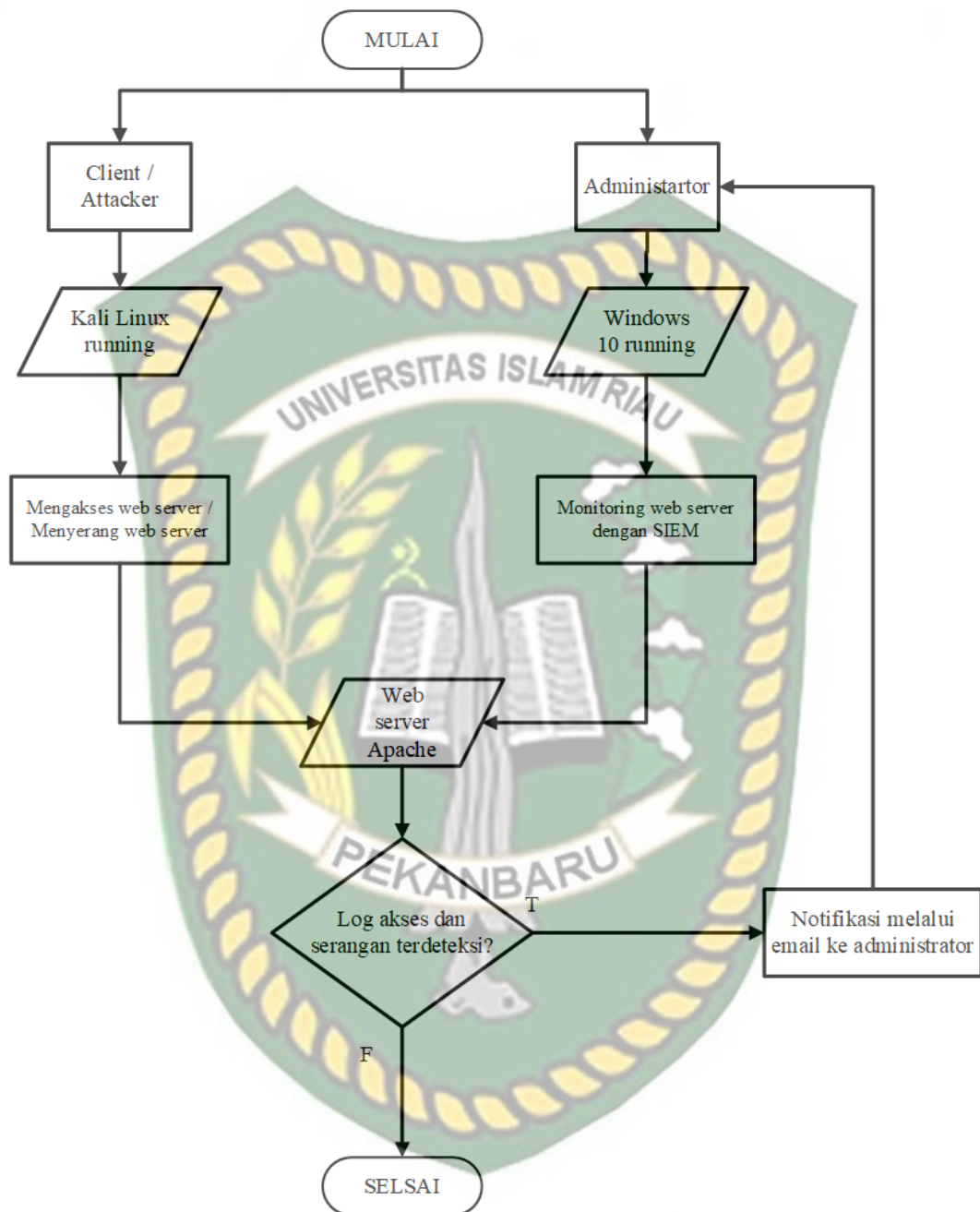
3.4.4 Port Scanning

Port scanning adalah sebuah teknik untuk melakukan identifikasi *port* yang terbuka dan menentukan layanan yang tersedia pada sistem. Layanan adalah sebuah pekerjaan spesifik atau tugas dari komputer yang menjalankan seperti *e-mail*, FTP, *printing* atau menjalankan halaman *web*. Salah satu *tools* untuk melakukan *port scanning* adalah Nmap.

3.5 Skenario Pengujian

Skenario pengujian dilakukan untuk menguji kemampuan deteksi dari Elastic Stack SIEM dan Splunk. Adapun skenario pengujian yang dilakukan sebagai berikut :

1. *Client* mengakses *web server*.
2. *Attacker* melakukan serangan terhadap *web server*.
3. Elastic Stack SIEM dan Splunk mendeteksi serangan yang terjadi pada *web server*.
4. Elastic Stack SIEM dan Splunk mengirimkan notifikasi berupa *e-mail* kepada administrator.



Gambar 3. 4 Skenario Pengujian

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi

Implementasi pada penelitian ini adalah dengan menghubungkan satu unit laptop dan empat unit PC menggunakan *switch* cisco. Satu PC digunakan sebagai *web server* yang di-*install* di dalam sistem operasi Ubuntu Server 20.2 melalui virtual box. Dua PC digunakan sebagai *server* untuk menginstall tools SIEM yaitu Elastic Stack SIEM dan Splunk di dalam sistem operasi Ubuntu Server 20.2 melalui virtualbox. Dan satu PC digunakan sebagai *client* atau *attacker* menggunakan sistem operasi Kali Linux yang di-*install* di dalam virtualbox. Laptop digunakan untuk melakukan *monitoring log* dari *web server* melalui tools SIEM.

4.1.1 Instalasi Perangkat Keras Jaringan

Tahapan instalasi perangkat keras jaringan pada penelitian ini menggunakan *Switch*, laptop, kabel UTP, dan PC labor. *Switch* digunakan sebagai penghubung antara laptop dan PC labor menggunakan kabel UTP. Semua perangkat harus saling terhubung dan terintegrasi sesuai dengan perancangan jaringan. Berikut adalah gambar hasil instalasi perangkat keras jaringan:



Gambar 4. 1 Instalasi Perangkat Keras Jaringan

Pada gambar 4.1 laptop yang digunakan oleh administrator dalam *monitoring web server* menggunakan *tools SIEM*, tiga pc labor yang digunakan sebagai *server* untuk *web server* dan *server SIEM*, serta satu pc labor yang digunakan sebagai *client* atau *attacker* dalam melakukan penyerangan terhadap *web server*. Untuk *port 1* terhubung dengan laptop, *port 2* terhubung dengan *web server*, *port 3* terhubung dengan *elasticstack SIEM*, *port 4* terhubung dengan *Splunk SIEM*, dan *port 5* terhubung dengan *client* atau *attacker*.

4.1.2 Instalasi dan Konfigurasi Elastic Stack SIEM

Proses instalasi dan konfigurasi Elastic Stack SIEM dilakukan oleh administrator dengan *me-remote server elastic stack siem* menggunakan Putty. Sehingga dalam proses instalasi dan konfigurasi nya dapat dilakukan dengan cepat dan terintegrasi.

- a. Instalasi Elasticsearch dan Kibana

Tahapan awal instalasi Elastic Stack SIEM adalah dengan menambahkan sumber repositori dari *website* resmi Elastic Stack dengan perintah pada gambar 4.2 dibawah ini.

```
Last login: Tue Jan 18 05:03:45 2022
root@elasticsiem:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | auto apt-key add -
```

Gambar 4. 2 Penambahan Sumber Elastic Stack

Setelah sumber repositori Elastic Stack ditambahkan, selanjutnya menambahkan *package* Elastic Stack ke dalam repositori Ubuntu Server nya supaya Elastic Stack dapat di instalasi pada server tersebut. Perintah yang dilakukan terdapat pada gambar 4.3 dibawah ini.

```
root@elasticsiem: /etc/apt/sources.list.d
root@elasticsiem:~# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main
root@elasticsiem:~# cd /etc/apt/sources.list.d/
root@elasticsiem:/etc/apt/sources.list.d# ls
elastic-7.x.list
root@elasticsiem:/etc/apt/sources.list.d#
```

Gambar 4. 3 Penambahan *Package* Elastic Stack

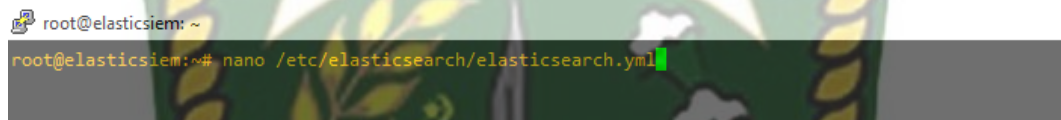
Selanjutnya adalah melakukan instalasi Elastic Stack SIEM, dengan menggunakan perintah *apt install elasticsearch kibana*. Berikut adalah perintah instalasi Elastic Stack SIEM pada gambar 4.4 dibawah ini.

```
root@elasticsiem: ~
root@elasticsiem:~# apt install elasticsearch kibana
```

Gambar 4. 4 Instalasi Elastic Stack SIEM

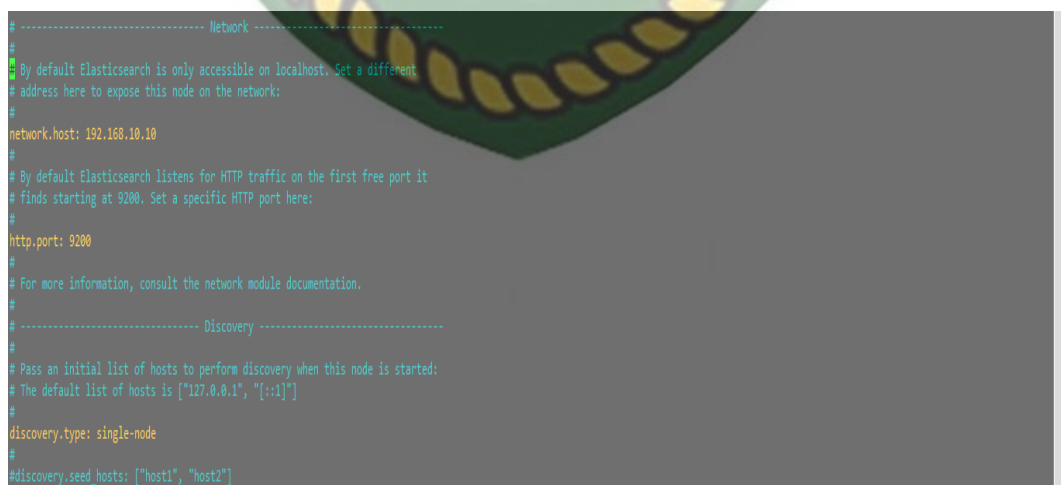
b. Konfigurasi Elasticsearch

Konfigurasi pertama yang dilakukan pada Elastic Stack SIEM adalah dengan mengkonfigurasi *file* Elasticsearch yang digunakan sebagai mesin pencari *log* terhadap *web server*. Perintah konfigurasi Elasticsearch adalah dengan mengetik *nano /etc/elasticsearch/elasticsearch.yml*. Perintah tersebut dapat dilihat pada gambar 4.5 dibawah ini.



Gambar 4. 5 File Konfigurasi Elasticsearch

Di dalam file konfigurasi Elasticsearch tersebut, ubah isi dari *network.host* menjadi alamat IP Address Elastic Stack SIEM yaitu 192.168.10.10 dan ubah isi *http.port* menjadi 9200, serta tambahkan *discovery.type* dengan *single-node*, *discovery.type* digunakan agar Elasticsearch dapat *me-monitoring* satu *node server* yang terhubung.



Gambar 4. 6 Konfigurasi Elasticsearch

Setelah konfigurasi dilakukan, selanjutnya adalah menjalankan Elasticsearch pada server dengan mengetik perintah `systemctl start elasticsearch` dan untuk melihat status apakah Elasticsearch sudah berjalan atau belum ketik perintah `systemctl status elasticsearch`. Hasil dari proses tersebut dapat dilihat pada gambar 4.7 dibawah ini.



```

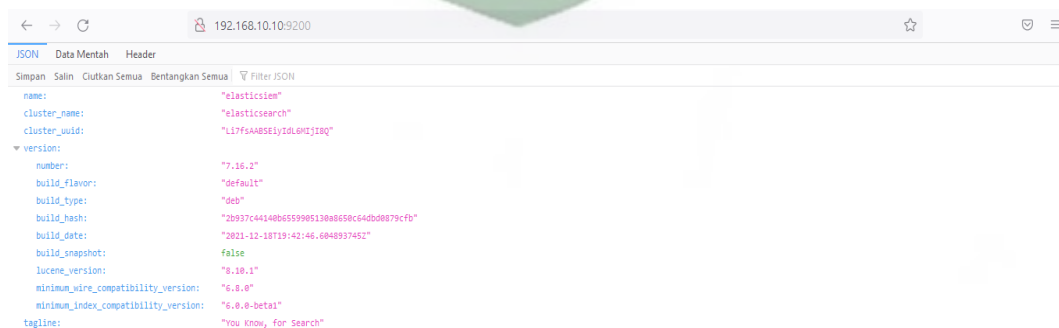
root@elasticsiem:~# systemctl start elasticsearch
root@elasticsiem:~# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-01-18 03:36:03 UTC; 2h 9min ago
     Docs: https://www.elastic.co
   Main PID: 1618 (java)
    Tasks: 61 (limit: 2133)
   Memory: 1.06
   CGroup: /system.slice/elasticsearch.service
           └─1618 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless
           └─1858 /usr/share/elasticsearch/modules/x-pack-m1/platform/linux-x86_64/bin/controller

Jan 18 03:32:58 elasticsiem systemd[1]: Starting Elasticsearch...
Jan 18 03:36:03 elasticsiem systemd[1]: Started Elasticsearch.
root@elasticsiem:~#

```

Gambar 4. 7 Elastcsearch Running

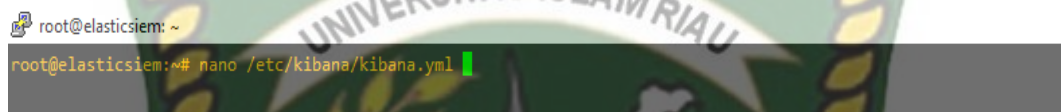
Tampilan *running* Elasticsearch dapat dibuka menggunakan *web browser*, masukkan alamat ip *address* elasticsearch yang sudah dikonfigurasi beserta *port* nya, yaitu 192.168.10.10:9200. Untuk tampilan pada *web browser* dapat dilihat pada gambar 4.8 dibawah ini.



Gambar 4. 8 Tampilan Elasticsearch di Web Browser

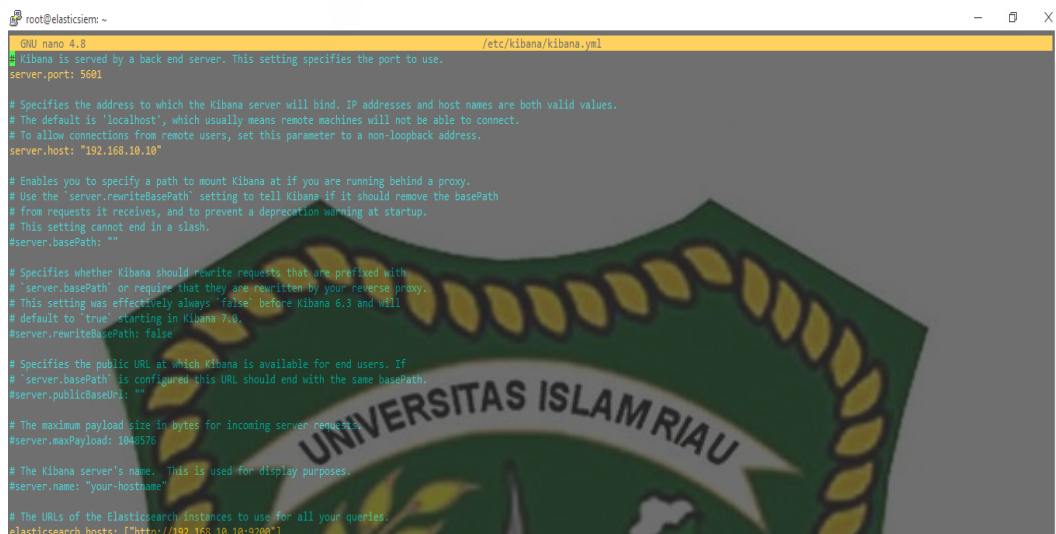
c. Konfigurasi Kibana

Kibana digunakan untuk menampilkan halaman *monitoring* dari Elasticsearch dan juga untuk melihat dashboard beserta *log* yang masuk. Konfigurasi file kibana di dalam file kibana dengan perintah *nano /etc/kibana/kibana.yml*.



Gambar 4. 9 File Konfigurasi Kibana

Konfigurasi dilakukan dengan mengubah isi *server.port* menjadi 5601, mengubah isi *server.host* menjadi 192.168.10.10, dan atur *Elasticsearch.host* sesuai dengan alamat ip dari Elasticsearch yang sudah dikonfigurasi yaitu “http://192.168.10.10:9200”, konfigurasi ini dilakukan agar Elasticsearch dapat terhubung dengan kibana sehingga saat proses pembaca *log* dilakukan dengan Elasticsearch, kibana bertugas untuk menampilkan *log* yang masuk melalui *dashboard*.



```

root@elasticsiem: ~
GNU nano 4.8 /etc/kibana/kibana.yml
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "192.168.10.10"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# 'server.basePath' or require that they are rewritten by your reverse proxy.
# This setting was effectively always 'false' before Kibana 6.3 and will
# default to 'true' starting in Kibana 7.0.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# 'server.basePath' is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.10.10:9200"]

```

Gambar 4. 10 Konfigurasi Kibana

Setelah konfigurasi dilakukan, selanjutnya adalah menjalankan kibana pada server dengan mengetik perintah *systemctl start kibana* dan untuk melihat status apakah kibana sudah berjalan atau belum ketik perintah *systemctl status kibana*. Hasil dari proses tersebut dapat dilihat pada gambar 4.11 dibawah ini.



```

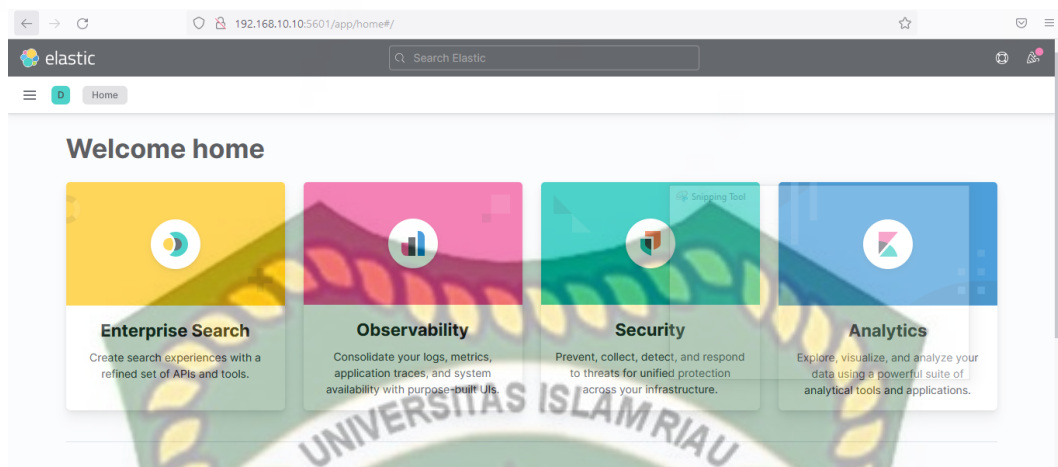
root@elasticsiem:~# systemctl start kibana
root@elasticsiem:~# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-01-18 03:36:46 UTC; 2h 11min ago
     Docs: https://www.elastic.co
    Main PID: 1967 (node)
      Tasks: 11 (limit: 2133)
     Memory: 459.4M
    CGroup: /system.slice/kibana.service
            └─1967 /usr/share/kibana/bin/..node/bin/node /usr/share/kibana/bin/..src/cli/dist --logging.dest=/var/log/kibana/kibana.log --pid.file=/run/kibana/kibana.pid

Jan 18 03:36:46 elasticsiem systemd[1]: Started Kibana.
root@elasticsiem:~#

```

Gambar 4. 11 Kibana Running

Tampilan *running* kibana dapat dibuka menggunakan *web browser*, masukkan alamat ip *address* kibana yang sudah dikonfigurasi beserta *port* nya, yaitu 192.168.10.10:5601. Untuk tampilan kibana pada *web browser* dapat dilihat pada gambar 4.12 dibawah ini.



Gambar 4. 12 Tampilan Kibana di Web Browser

4.1.3 Instalasi dan Konfigurasi Splunk

a. Instalasi Splunk

Instalasi dan Konfigurasi Splunk dilakukan oleh administrator dengan *remote server* Splunk menggunakan Putty. *Download package* Splunk pada website resmi nya <https://www.splunk.com>. Pada penelitian ini penulis melakukan *download* melalui cli (*command line interface*) dengan perintah *wget*. Perintah *download* Splunk melalui cli dapat dilihat pada gambar 4.13 dibawah ini.

```

root@splunksiem: ~
root@splunksiem:~# wget -O splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb 'https://download.splunk.com/products/splunk/releases/8.2.4/linux/splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb'
--2022-01-18 06:09:08-- https://download.splunk.com/products/splunk/releases/8.2.4/linux/splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 13.227.230.125, 13.227.230.71, 13.227.230.106, ...
Connecting to download.splunk.com (download.splunk.com)|13.227.230.125|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 434892008 (415M) [binary/octet-stream]
Saving to: 'splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb'

splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb 1%> ] 6.95M 4.95MB/s

```

Gambar 4. 13 Download Package Splunk

Setelah *package* Splunk berhasil di download, selanjutnya adalah proses instalasi *package* Splunk. Untuk proses instalasi *package* Splunk perintah yang dilakukan dapat dilihat pada gambar 4.14 dibawah ini.



Gambar 4. 14 Instalasi *Package* Splunk

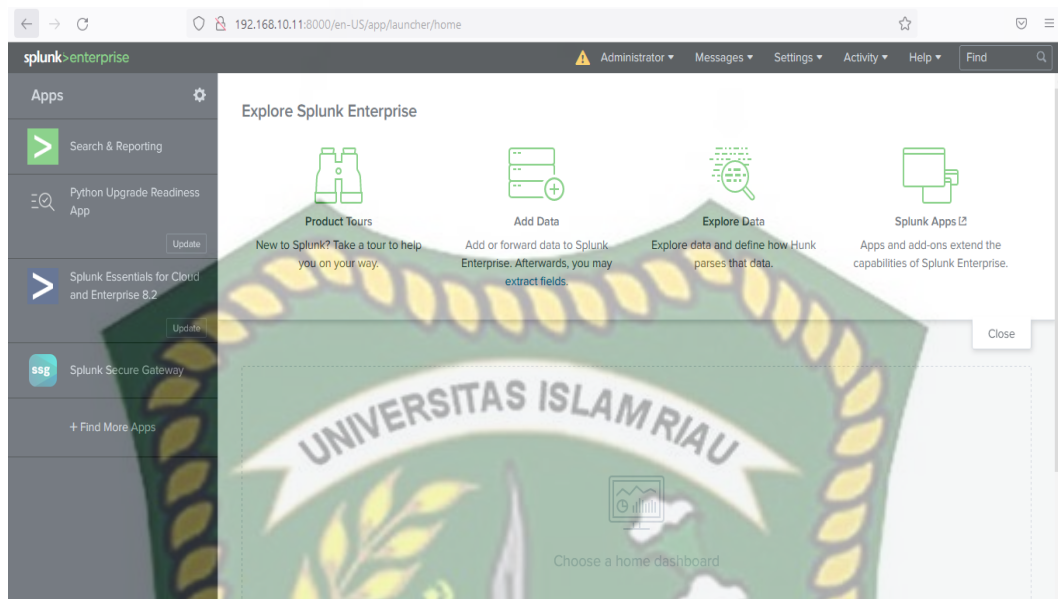
b. Konfigurasi Splunk

Konfigurasi Splunk dilakukan di dalam *folder package* Splunk yaitu */opt/splunk/bin*. Di dalam *folder* ini ketik perintah *./splunk start --accpet-license*. Splunk otomatis berjalan saat perintah tersebut sudah dijalankan.



Gambar 4. 15 Konfigurasi Splunk

Pada gambar 4.15 diatas, Splunk otomatis berjalan pada alamat ip dari *server* Splunk tersebut dengan port 8000. Untuk menampilkan tampilan Splunk pada *web browser*, masukkan alamat ip dan *port* Splunk tersebut yaitu 192.168.10.11.8000. Tampilan Splunk dapat dilihat pada gambar 4.16 dibawah ini.

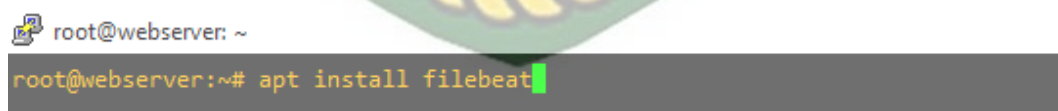


Gambar 4. 16 Tampilan Splunk di Web Browser

4.1.4 Menghubungkan SIEM dengan Web Server

a. Menghubungkan Elastic Stack SIEM dengan Web Server

Untuk menghubungkan Elastic Stack SIEM dan web server maka diperlukan *package* tambahan yang bernama filebeat yang dipasang pada web browser. Filebeat digunakan sebagai *monitoring log* apache dari web server. Instal filebeat pada web server yang sudah di remote dengan perintah *apt install filebeat*.



Gambar 4. 17 Instalasi Filebeat di Web Server

Konfigurasi *file* dari filebeat dengan perintah *nano /etc/filebeat/filebeat.yml*.

Gambar 4.18 adalah perintah dari konfigurasi filebeat.

```
root@webserver: ~
```

```
root@webserver:~# nano /etc/filebeat/filebeat.yml
```

Gambar 4. 18 File Konfigurasi Filebeat

Selanjutnya konfigurasi kibana di dalam filebeat dengan mengubah isi *host* kibana menjadi IP Address kibana yang sudah di konfigurasi yaitu `http://192.168.10.10:5601`.

```
GNU nano 4.8 /etc/filebeat/filebeat.yml
# ===== Kibana =====
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "http://192.168.10.10:5601"
```

Gambar 4. 19 Konfigurasi Kibana didalam Filebeat

Selanjutnya konfigurasi elasticsearch di dalam filebeat dengan mengubah isi *hosts* elasticsearch menjadi IP Address elasticsearch yang sudah dikonfigurasi yaitu `192.168.10.10:9200`.

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.10.10:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"
```

Gambar 4. 20 Konfigurasi Elasticsearch di dalam Filebeat

Filebeat yang sudah dikonfigurasi kemudian dijalankan dengan perintah `service filebeat start`, untuk melihat status filebeat berhasil berjalan dan terhubung

dengan elastic stack siem adalah dengan perintah *service filebeat status*. Tampilan *running* filebeat dapat dilihat pada gambar 4.21 dibawah ini.



```

root@webserver:~# service filebeat start
root@webserver:~# service filebeat status
• filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-01-20 11:20:49 WIB; 4min 27s ago
     Docs: https://www.elastic.co/beats/filebeat
   Main PID: 1433 (filebeat)
    Tasks: 6 (limit: 2133)
   Memory: 43.5M
   CGroup: /system.slice/filebeat.service
           └─1433 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc/filebeat --path.data /var/lib/filebeat

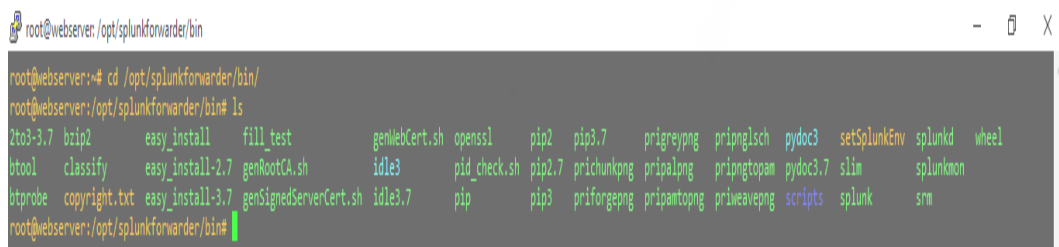
Jan 20 11:20:57 webserver filebeat[1433]: 2022-01-20T11:20:57.613+0700      INFO    [index-management ilm] ilm/std.go:126      Index Alias filebeat-7.16.3 exists already.
Jan 20 11:20:57 webserver filebeat[1433]: 2022-01-20T11:20:57.645+0700      INFO    [publisher pipeline output] pipeline/output.go:151      Connection to backoff(elasticsearch)
Jan 20 11:21:23 webserver filebeat[1433]: 2022-01-20T11:21:23.423+0700      INFO    [monitoring] log/log.go:184      Non-zero metrics in the last 30s      ("monitoring": {"web
Jan 20 11:21:53 webserver filebeat[1433]: 2022-01-20T11:21:53.417+0700      INFO    [monitoring] log/log.go:184      Non-zero metrics in the last 30s      ("monitoring": {"web
Jan 20 11:22:23 webserver filebeat[1433]: 2022-01-20T11:22:23.428+0700      INFO    [monitoring] log/log.go:184      Non-zero metrics in the last 30s      ("monitoring": {"web
Jan 20 11:23:53 webserver filebeat[1433]: 2022-01-20T11:23:53.427+0700      INFO    [monitoring] log/log.go:184      Non-zero metrics in the last 30s      ("monitoring": {"web
Jan 20 11:23:53 webserver filebeat[1433]: 2022-01-20T11:23:53.419+0700      INFO    [monitoring] log/log.go:184      Non-zero metrics in the last 30s      ("monitoring": {"web
Jan 20 11:24:23 webserver filebeat[1433]: 2022-01-20T11:24:23.419+0700      INFO    [monitoring] log/log.go:184      Non-zero metrics in the last 30s      ("monitoring": {"web
Jan 20 11:24:53 webserver filebeat[1433]: 2022-01-20T11:24:53.417+0700      INFO    [monitoring] log/log.go:184      Non-zero metrics in the last 30s      ("monitoring": {"web
lines 1-20/20 (END)

```

Gambar 4. 21 Filebeat Running

b. Menghubungkan Splunk dengan Web Server

Untuk menghubungkan Splunk dengan Web Server, diperlukan *package* dari Splunk yaitu Splunk Forwarder. Download Splunk Forwarder dari *website* resmi Splunk, lalu ekstrak pada *web server*. Kemudian masuk ke dalam *folder* Splunk Forwarder dengan perintah *cd /opt/splunkforwarder/bin*. Untuk tampilan *folder* Splunk Forwarder dapat dilihat pada gambar 4. 22 dibawah ini.



```

root@webserver:/opt/splunkforwarder/bin
root@webserver:/opt/splunkforwarder/bin# ls
2to3-3.7  bzr2          easy_install  fill_test      genWebCert.sh  openssl      pip2      pip3.7      prigraypng  pringlsch  pydoc3      setSplunkEnv  splunkd  wheel
bttool    classify       easy_install-2.7  genRootCA.sh  idle3          pid_check.sh  pip2.7    prichunkpng  pripalpng  pringtopam  pydoc3.7     slim       splunkmon
btprobe   copyright.txt  easy_install-3.7  genSignedServerCert.sh  idle3.7       pip           pip3      priforgepng  pripantopng  priweavepng  scripts     splunk    srm
root@webserver:/opt/splunkforwarder/bin#

```

Gambar 4. 22 Folder Splunk Forwarder

Selanjutnya, jalankan Splunk Forwarder yang sudah di install pada *web server* agar dapat terhubung dengan Splunk. Perintah menjalankan Splunk forwarder dapat dilihat pada gambar 4. 23 dibawah ini.



```

root@webserver:/opt/splunkforwarder/bin# ./splunk start
splunkd 2202 was not running.
Stopping splunk helpers...

Done.
Stopped helpers.
Removing stale pid file... done.

Splunk> CSI: Logfiles.

Checking prerequisites...
  Checking mgmt port [8083]: open
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
  All installed files intact.
  Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

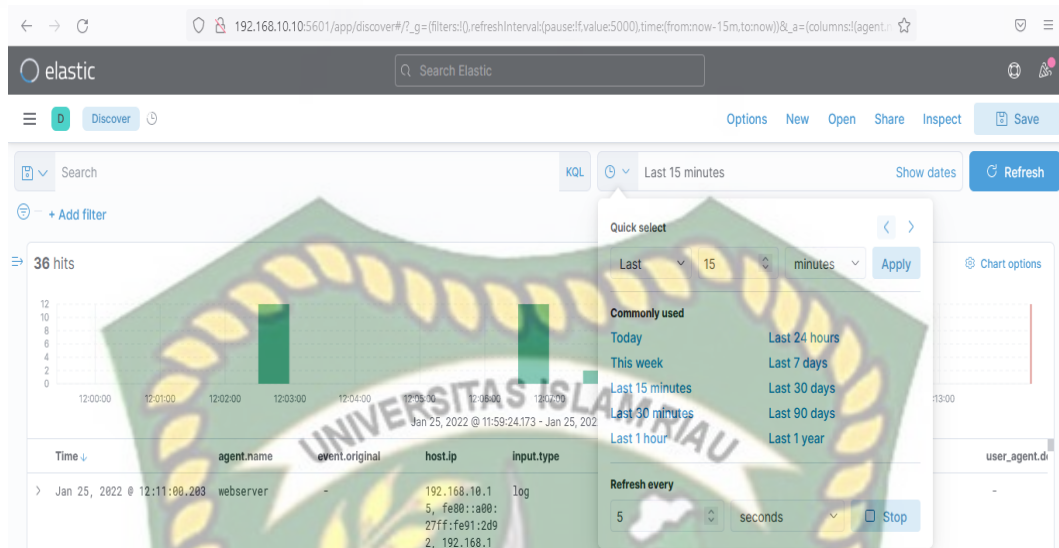
root@webserver:/opt/splunkforwarder/bin# ./splunk add forward-server 192.168.10.11:9997
Your session is invalid. Please login.
Splunk username: admin
Password:
Login failed
root@webserver:/opt/splunkforwarder/bin# ./splunk add forward-server 192.168.10.11:9997
Your session is invalid. Please login.
Splunk username: admin
Password:
192.168.10.11:9997 forwarded-server already present

```

Gambar 4. 23 Splunk Forwarder Running

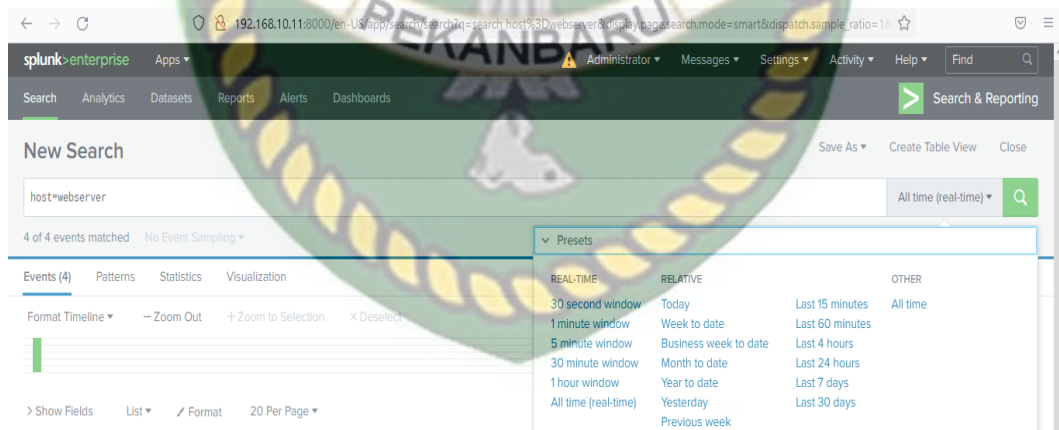
4.2 Pengujian

Setelah penginstalan dan konfigurasi *web server* dan SIEM selesai, selanjutnya dilakukan tahap pengujian dimana Elastic Stack SIEM dan Splunk diatur secara *realtime* untuk *me-monitoring* aktifitas pada *web server*. Pengujian dilakukan selama tiga hari untuk mendapatkan perbandingan dari pengujian.



Gambar 4. 24 Elastic Stack SIEM Diatur Secara *Realtime*

Pada gambar 4.24 diatas, elastic stack siem diatur secara *realtime* dan setiap *log* yang masuk di *refresh* setiap 5 detik. Sehingga dalam 5 detik tersebut dapat dilihat aktifitas yang terjadi pada *web server*.



Gambar 4. 25 Splunk Yang Diatur Secara *Realtime*

Pada gambar 4.25 diatas, Splunk diatur secara *realtime* sehingga setiap aktifitas yang terjadi pada *web server* dapat dilihat secara langsung melalui Splunk.

4.2.1 Pengujian *Client* atau *Attacker* Mengakses *Web Server* Hari Ke 1

Pada pengujian pertama hari ke 1, *client* atau *attacker* melakukan akses terhadap *website* DVWA yang diinstall di dalam *web server*. Tampilan *website* DVWA yang diakses oleh *client* atau *attacker*, dapat dilihat pada gambar 4.26 dibawah ini.



Gambar 4. 26 *Client* atau *Attacker* Mengakses *Web Server* Hari Ke 1

Elastic Stack SIEM dan Splunk berhasil mendeteksi data *log* akses *client* atau *attacker* secara *realtime* saat mengakses *website* DVWA pada hari ke 1.

Time ↓	Document
> Feb 22, 2022 @ 12:52:33.449	@timestamp: Feb 22, 2022 @ 12:52:33.449 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [22/Feb/2022:12:52:28 +0700] \"GET /login.php HTTP/1.1\" 200 1161 \"-\" \"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\"] event.dataset: system.syslog event.ingested: Feb 22, 2022 @ 12:52:34.460 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver
> Feb 22, 2022 @ 12:52:33.449	@timestamp: Feb 22, 2022 @ 12:52:33.449 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [22/Feb/2022:12:52:28 +0700] \"GET /dwa/css/login.css HTTP/1.1\" 200 741 \"http://192.168.10.15/login.php\" \"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\"] event.dataset: system.syslog event.ingested: Feb 22, 2022 @ 12:52:34.462 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64
> Feb 22, 2022 @ 12:52:33.449	@timestamp: Feb 22, 2022 @ 12:52:33.449 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [22/Feb/2022:12:52:28 +0700] \"GET /dwa/images/login_logo.png HTTP/1.1\" 304 181

Gambar 4. 27 Hasil *Monitoring Log* Akses Elastic Stack SIEM Hari Ke 1

i	Time	Event
>	2/22/22 5:52:28.000 AM	192.168.10.12 - - [22/Feb/2022:12:52:28 +0700] "GET /dvwa/images/login_logo.png HTTP/1.1" 304 181 "http://192.168.10.15/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	2/22/22 5:52:28.000 AM	192.168.10.12 - - [22/Feb/2022:12:52:28 +0700] "GET /dvwa/css/login.css HTTP/1.1" 200 741 "http://192.168.10.15/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	2/22/22 5:52:28.000 AM	192.168.10.12 - - [22/Feb/2022:12:52:28 +0700] "GET /login.php HTTP/1.1" 200 1161 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	2/22/22 5:26:21.000 AM	192.168.10.1 - - [22/Feb/2022:12:26:21 +0700] "GET /dvwa/images/login_logo.png HTTP/1.1" 304 181 "http://192.168.10.15/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 28 Hasil Monitoring Log Akses Splunk Hari Ke 1

Hasil *monitoring* Splunk berhasil dikirim melalui *e-mail notification* administrator sedangkan Elastic Stack SIEM gagal dalam mengirimkan *e-mail notification*. Dengan adanya *e-mail notification* dari Splunk, administrator dapat melihat informasi mengenai serangan atau *log* yang masuk ke dalam *web server*. Untuk notifikasi melalui *e-mail* dapat dilihat pada gambar 4.29 dibawah ini.



Gambar 4. 29 Notifikasi Log Masuk di Splunk Melalui E-mail Hari Ke 1

4.2.2 Pengujian *Fingerprinting* Hari Ke 1

Pengujian *fingerprinting* dilakukan untuk mendapatkan informasi khusus terhadap target serangan. Informasi yang didapatkan berupa *service*, *banner*, direktori sistem, dan lokasi *root* sistem. *Tools* yang digunakan untuk melakukan *fingerprinting* yaitu Nikto. Pengujian *fingerprinting* menggunakan Nikto dapat dilihat pada gambar 4.30 dibawah ini.

```
(kali@kali)-[~]
$ nikto -h 192.168.10.15
- Nikto v2.1.6

+ Target IP: 192.168.10.15
+ Target Hostname: 192.168.10.15
+ Target Port: 80
+ Start Time: 2022-02-22 02:05:45 (GMT-5)

+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /tests/: Directory indexing found.
+ OSVDB-3092: /tests/: This might be interesting ...
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfi/nc.txt: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /.git/index: Git index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /.git/config: Git config file found. Infos about repo details may be present.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ 7915 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time: 2022-02-22 02:06:47 (GMT-5) (62 seconds)

+ 1 host(s) tested
```

Gambar 4. 30 Pengujian *Fingerprinting* Menggunakan Nikto Hari Ke 1

Pengujian dengan metode *fingerprinting* berhasil dideteksi secara *realtime* oleh Elastic Stack SIEM dan Splunk saat pengujian tersebut langsung dilakukan. *Log* serangan *fingerprinting* yang berhasil dideteksi berupa informasi terkait dengan *tools* serangan yang digunakan dan waktu serangan berlangsung.

Time	Document
> Feb 22, 2022 @ 14:08:01.569	@timestamp: Feb 22, 2022 @ 14:08:01.569 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /util/xmlrpc/Handler.ashx HTTP/1.1" 404 491 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:007245)] event.dataset: system.syslog event.ingested: Feb 22, 2022 @ 14:08:10.244 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver
> Feb 22, 2022 @ 14:08:01.569	@timestamp: Feb 22, 2022 @ 14:08:01.569 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /cgi-bin/config.exp HTTP/1.1" 404 491 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:007246)] event.dataset: system.syslog event.ingested: Feb 22, 2022 @ 14:08:10.244 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver
> Feb 22, 2022 @ 14:08:01.568	@timestamp: Feb 22, 2022 @ 14:08:01.568 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /currentsetting.htm HTTP/1.1" 404 491 "-"

Gambar 4. 31 Hasil Monitoring Serangan Fingerprinting Elastic Stack SIEM

Hari Ke 1

> 2/22/22 7:06:47.000 AM	192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /util/xmlrpc/Handler.ashx HTTP/1.1" 404 491 "-" "Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:007245)"
host = webserver	source = /var/log/apache2/access.log ; sourcetype = access-too_small
> 2/22/22 7:06:47.000 AM	192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /ibm/console/Logon.jsp HTTP/1.1" 404 491 "-" "Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:007244)"
host = webserver	source = /var/log/apache2/access.log ; sourcetype = access-too_small
> 2/22/22 7:06:47.000 AM	192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /.well-known/oauth-authorization-server HTTP/1.1" 404 491 "-" "Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:007243)"
host = webserver	source = /var/log/apache2/access.log ; sourcetype = access-too_small
> 2/22/22 7:06:47.000 AM	192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /.well-known/openid-configuration HTTP/1.1" 404 491 "-" "Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:007242)"
host = webserver	source = /var/log/apache2/access.log ; sourcetype = access-too_small
> 2/22/22 7:06:47.000 AM	192.168.10.12 - - [22/Feb/2022:14:06:47 +0700] "GET /util/xmlrpc/Handler.ashx HTTP/1.1" 404 491 "-" "Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:007241)"
host = webserver	source = /var/log/apache2/access.log ; sourcetype = access-too_small

Gambar 4. 32 Hasil Monitoring Serangan Fingerprinting Splunk Hari Ke 1

Hasil serangan *fingerprinting* yang berhasil di deteksi oleh Splunk, kemudian dikirim melalui *e-mail notification* administrator sedangkan Elastic Stack SIEM gagal dalam mengirimkan notifikasi *e-mail*. Administrator dapat melihat informasi serangan *fingerprinting* tersebut mulai dari *tools* yang digunakan hingga waktu serangan terjadi. *E-mail notification* serangan *fingerprinting* dapat dilihat pada gambar 4.33 dibawah ini.

Splunk Alert Inbox x

admsiem.elksplunk2022@gmail.com
to me ▾

2:05 PM (2 minutes ago) ☆ ↶ ⋮

Alert Has Detection

```
192.168.10.12 -- [22/Feb/2022:14:05:45 +0700] "GET / HTTP/1.1" 302 505 "-" "Mozilla/5.0 (Nikto/2.1.6) (Evasion
s:None) (Test:map_codes)"
```

```
192.168.10.12 -- [22/Feb/2022:14:05:45 +0700] "GET /Wiga8aYK.access HTTP/1.1" 404 491 "-" "Mozilla/5.0 (Nikto/
2.1.6) (Evasions:None) (Test:map_codes)"
```

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data

Gambar 4. 33 Notifikasi Serangan *Fingerprinting* di Splunk Melalui *E-mail* Hari

Ke 1

4.2.3 Pengujian SQL Injection Hari Ke 1

Pengujian SQL Injection pada website DVWA bertujuan untuk mendapatkan informasi *database*. Pengujian ini menggunakan *tools* yang bernama Sqlmap, *tools* ini yang digunakan dalam melakukan injeksi *database* terhadap website DVWA. Untuk pengujian menggunakan Sqlmap dapat dilihat pada gambar 4.34 dibawah ini.

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.10.15/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=impossible; PHPSESSID=s3serrac14r6jc4ib0jcf1l19" --dbs

{1.4.11#stable}
[+] fetching database names
available databases [7]:
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 01:21:43 /2022-02-22/
[+] database schema
[01:21:43] [INFO] resuming back-end DBMS 'mysql'
[01:21:43] [INFO] testing connection to the target URL
```

Gambar 4. 34 Pengujian SQL Injection Menggunakan Sqlmap Hari Ke 1

Serangan Sqlmap yang dilakukan, menghasilkan informasi mengenai *database* yang digunakan pada *website* DVWA, dengan informasi yang di dapatkan tersebut. *Attacker* dapat mengambil data penting seperti data *user* yang terdaftar dalam *website* tersebut dan dapat masuk ke dalam *website* tersebut secara ilegal. Hasil dari serangan tersebut dapat dilihat pada gambar 4.35 dibawah ini.

```
[01:21:48] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[01:21:48] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[01:21:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.10.15'
[01:21:48] [WARNING] your sqlmap version is outdated

[*] ending @ 01:21:48 /2022-02-22/
```

Gambar 4. 35 Informasi *Database* Yang Didapatkan Oleh *Attacker* Menggunakan Sqlmap Hari Ke 1

```
Database: dvwa
Table: users
[5 entries]
```

	user_id	user	avatar	password	last_name	first_name	last_login	failed_login
1	admin	/DVWA/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	2022-01-16 15:35:30	0	
2	gordonb	/DVWA/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	2022-01-13 14:42:08	0	
3	1337	/DVWA/hackable/users/1337.jpg	8d353d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	2022-01-13 14:42:08	0	
4	pablo	/DVWA/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2022-01-13 14:42:08	0	
5	smithy	/DVWA/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	2022-01-13 14:42:08	0	

```
[01:52:10] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.10.15/dump/dvwa/users.csv'
[01:52:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.10.15'
[01:52:10] [WARNING] your sqlmap version is outdated

[*] ending @ 01:52:10 /2022-02-22/
```

Gambar 4. 36 Data *User* DVWA Yang Didapatkan Oleh *Attacker* Hari Ke 1

Elastic Stack SIEM dan Splunk berhasil mendeteksi serangan *SQL Injection* yang dilakukan oleh *Attacker*, serangan yang di deteksi berupa informasi dari *query* yang digunakan dalam melakukan injeksi terhadap *website* DVWA.

Gambar 4. 37 Hasil *Monitoring* SQL Injection Elastic Stack SIEM Hari Ke 1

Gambar 4. 38 Hasil *Monitoring SQL Injection* Splunk Hari Ke 1

Hasil serangan *SQL Injection* yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan notifikasi *e-mail* serangan *SQL Injection*. Tampilan notifikasi serangan *SQL Injection* dapat dilihat pada gambar 4.39 dibawah ini.

Serangan *Denial of Service* (DoS) menggunakan Slowhttptest berhasil di deteksi oleh Elastic Stack SIEM dan Splunk. Informasi *log* yang di dapatkan dalam serangan ini berupa *traffic* yang banyak dari berbagai *browser* yang sudah di atur pada *tools* Slowhttptest tersebut. Hasil deteksi serangan DoS dapat dilihat pada gambar 4.41 pada Elastic Stack SIEM dan gambar 4.42 pada Splunk dibawah ini.



Gambar 4. 41 Hasil Monitoring Serangan DoS Elastic Stack SIEM Hari Ke 1

i	Time	Event
>	2/22/22 7:26:27.000 AM	192.168.10.12 - - [22/Feb/2022:14:26:27 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	2/22/22 7:26:27.000 AM	192.168.10.12 - - [22/Feb/2022:14:26:27 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	2/22/22 7:26:27.000 AM	192.168.10.12 - - [22/Feb/2022:14:26:27 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	2/22/22 7:26:27.000 AM	192.168.10.12 - - [22/Feb/2022:14:26:27 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	2/22/22 7:26:47.000 AM	:::1 - - [22/Feb/2022:14:26:47 +0700] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.41 (Ubuntu) (internal dummy connection)" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 42 Hasil Monitoring Serangan DoS Splunk Hari Ke 1

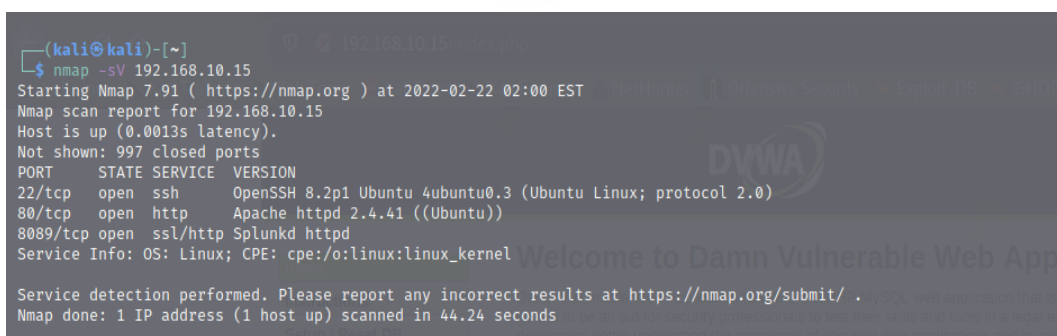
Hasil serangan *Denial of Service* (DoS) yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan notifikasi *e-mail* serangan DoS. Tampilan notifikasi serangan DoS dapat dilihat pada gambar 4.43 dibawah ini.



Gambar 4. 43 Notifikasi Serangan DoS di Splunk Melalui *E-mail* Hari Ke 1

4.2.5 Pengujian Port Scanning Hari Ke 1

Port scanning dilakukan oleh *attacker* untuk mendapatkan informasi mengenai *port* yang terbuka di dalam *website* DVWA yang menjadi target serangan *port scanning*. *Tools* yang digunakan dalam *port scanning* ini adalah Nmap. Pengujian Nmap dapat dilihat pada gambar 4.44 dibawah ini.



Gambar 4. 44 Pengujian Port Scanning Menggunakan Nmap Hari Ke 1

Serangan *port scanning* berhasil dideteksi oleh Elastic Stack SIEM dan Splunk, hasil *monitoring* dari kedua *tools* tersebut dapat mendeteksi informasi terkait penggunaan *tools* yang digunakan dalam serangan *port scanning*, ip address attacker, dan waktu penyerangan. Hasil deteksi serangan dari Elastic Stack SIEM dapat dilihat pada gambar 4.45, dan hasil deteksi serangan splunk dapat dilihat pada gambar 4.46 dibawah ini.



> Feb 22, 2022 @ 14:00:45.000	@timestamp: Feb 22, 2022 @ 14:00:45.000 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Feb 22, 2022 @ 14:00:48.772 event.dataset: apache.access event.ingested: Feb 22, 2022 @ 14:00:49.788 event.kind: event event.module: apache event.original: 192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" event.outcome: failure fileset.name: access host.architecture: x86_64
> Feb 22, 2022 @ 14:00:45.000	@timestamp: Feb 22, 2022 @ 14:00:45.000 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Feb 22, 2022 @ 14:00:48.772 event.dataset: apache.access event.ingested: Feb 22, 2022 @ 14:00:50.038 event.kind: event event.module: apache event.original: 192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "GET /nmaplowercheck1645513245 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" event.outcome: failure fileset.name: access
> Feb 22, 2022 @ 14:00:45.000	@timestamp: Feb 22, 2022 @ 14:00:45.000 agent.ephemeral_id: f66321c6-4303-4569-b390-6ecde75a330a agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Feb 22, 2022 @ 14:00:48.772 event.dataset: apache.access event.ingested: Feb 22, 2022 @ 14:00:50.038 event.kind: event event.module: apache event.original: 192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "GET / HTTP/1.0" 302 469 "-" "-" event.outcome: success

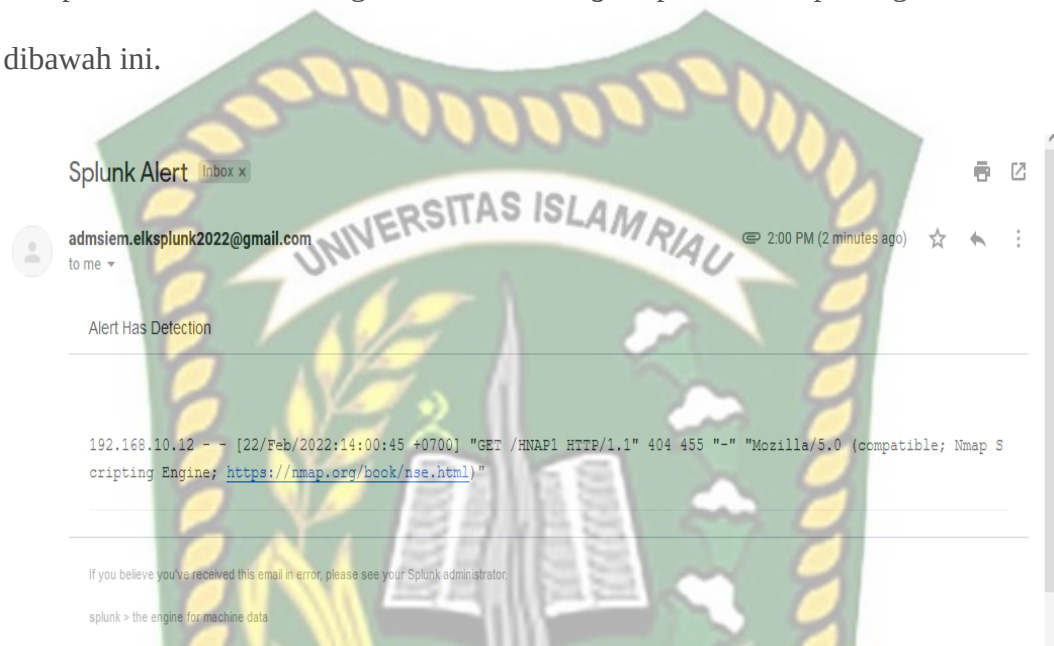
Gambar 4. 45 Hasil Monitoring Serangan Port Scanning Elastic Stack SIEM

Hari Ke 1

> 2/22/22 7:00:45.000 AM	192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "GET /evox/about HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 2/22/22 7:00:45.000 AM	192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "GET /HNAP1 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 2/22/22 7:00:45.000 AM	192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "GET / HTTP/1.0" 302 469 "-" "-"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 2/22/22 7:00:45.000 AM	192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "GET /nmaplowercheck1645513245 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 2/22/22 7:00:45.000 AM	192.168.10.12 - - [22/Feb/2022:14:00:45 +0700] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 2/22/22 7:00:21.000 AM	192.168.10.12 - - [22/Feb/2022:14:00:21 +0700] "GET / HTTP/1.0" 302 469 "-" "-"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 46 Hasil Monitoring Serangan Port Scanning Splunk Hari Ke 1

Hasil serangan *Port Scanning* yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan notifikasi *e-mail* serangan *Port Scanning*. Tampilan notifikasi serangan *Port Scanning* dapat dilihat pada gambar 4.47 dibawah ini.



Gambar 4. 47 Notifikasi Serangan Port Scanning di Splunk Melalui E-mail Hari Ke 1

4.2.6 Pengujian *Client* atau *Attacker* Mengakses *Web Server* Hari Ke 2

Pengujian pada hari ke-2 *client* atau *attacker* mengakses halaman *website* DVWA. Pada pengujian ini hanya dilakukan untuk mengakses *website* saja tanpa melakukan penyerangan terhadap *website*. Tampilan halaman *website* DVWA yang diakses oleh *client* atau *attacker* dapat dilihat pada gambar 4.48 dibawah ini.



Gambar 4. 48 Client Atau Attacker Mengakses Website Hari Ke 2

Elastic Stack SIEM dan Splunk berhasil mendeteksi data *log* akses *client* atau *attacker* secara *realtime* saat mengakses *website* DVWA di hari ke 2.

Time	Document
> Mar 1, 2022 @ 10:27:59.754	@timestamp: Mar 1, 2022 @ 10:27:59.754 agent.ephemeral_id: c952fc91-833b-4d07-9772-90b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:10:27:56 +0700] "GET / HTTP/1.1" 302 506 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"] event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 10:28:00.498 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver
> Mar 1, 2022 @ 10:27:59.754	@timestamp: Mar 1, 2022 @ 10:27:59.754 agent.ephemeral_id: c952fc91-833b-4d07-9772-90b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:10:27:56 +0700] "GET /login.php HTTP/1.1" 200 993 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"] event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 10:28:05.498 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver
> Mar 1, 2022 @ 10:27:56.000	@timestamp: Mar 1, 2022 @ 10:27:56.000 agent.ephemeral_id: c952fc91-833b-4d07-9772-90b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 1, 2022 @ 10:27:57.431 event.dataset: apache.access event.ingested: Mar 1, 2022 @ 10:27:58.198 event.kind: event

Gambar 4. 49 Hasil *Monitoring Log* Akses Elastic Stack SIEM Hari Ke 2

i	Time	Event
>	3/1/22 3:27:56.000 AM	192.168.10.12 - - [01/Mar/2022:10:27:56 +0700] "GET /login.php HTTP/1.1" 200 993 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/1/22 3:27:56.000 AM	192.168.10.12 - - [01/Mar/2022:10:27:56 +0700] "GET / HTTP/1.1" 302 506 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 50 Hasil *Monitoring Log* Akses Splunk Hari Ke 2

Hasil *monitoring* Splunk berhasil dikirim melalui *e-mail notification* ke administrator sedangkan Elastic Stack SIEM gagal dalam mengirimkan *e-mail notification*. Dengan adanya *e-mail notification* dari Splunk, administrator dapat mengetahui informasi mengenai serangan atau *log* yang masuk ke dalam *web server*. Tampilan *e-mail notification* Splunk dapat dilihat pada gambar 4.51 dibawah ini.



Gambar 4. 51 Notifikasi *Log* Masuk di Splunk Melalui *E-mail* Hari Ke 2

4.2.7 Pengujian *Fingerprinting* Hari Ke 2

Pengujian *fingerprinting* pada hari ke 2 menggunakan *tools* yang bernama Nikto. Pengujian ini dilakukan untuk mendapatkan informasi khusus dari *website* yang menjadi target yaitu berupa *service*, *banner*, direktori sistem, dan lokasi *root* sistem. Pengujian *fingerprinting* menggunakan Nikto dapat dilihat pada gambar 4.52 dibawah ini.

```

(kali@kali)~$ nikto -h 192.168.10.15
Nikto v2.1.6

+ Target IP: 192.168.10.15
+ Target Hostname: 192.168.10.15
+ Target Port: 80
+ Start Time: 2022-02-28 23:23:47 (GMT-5)

+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /tests/: Directory indexing found.
+ OSVDB-3092: /tests/: This might be interesting...
+ /info.php: Output from the phpinfo() Function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://hackers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /git/Andex: Git index file may contain directory listing information.
+ /git/HEAD: Git HEAD file found. Full repo details may be present.
+ /git/config: Git config file found. Infos about repo details may be present.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ 7915 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time: 2022-02-28 23:24:51 (GMT-5) (64 seconds)

+ 1 host(s) tested

```

Gambar 4. 52 Pengujian *Fingerprinting* Menggunakan Nikto Hari Ke 2

Pengujian dengan metode *fingerprinting* pada hari ke 2, berhasil dideteksi oleh Elastic Stack SIEM dan Splunk secara *realtime*. Log serangan yang terdeteksi berupa *tools* yang digunakan untuk penyerangan *fingerprinting* dan waktu serangan terjadi.

```

> Mar 1, 2022 @ 11:24:53.130 @timestamp: Mar 1, 2022 @ 11:24:53.130 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:11:24:51 +0700] \"GET /redis_config.json HTTP/1.1\" 404 491 \"-\" \"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007217)\"] event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 11:24:54.826 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver

> Mar 1, 2022 @ 11:24:53.130 @timestamp: Mar 1, 2022 @ 11:24:53.130 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:11:24:51 +0700] \"GET /redis_config.json HTTP/1.1\" 404 491 \"-\" \"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007218)\"] event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 11:24:54.826 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver

> Mar 1, 2022 @ 11:24:53.130 @timestamp: Mar 1, 2022 @ 11:24:53.130 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:11:24:51 +0700] \"GET /redis_config.json HTTP/1.1\" 404 491 \"-\" \"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007219)\"] event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 11:24:54.826 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver

```

Gambar 4. 53 Hasil *Monitoring* Serangan *Fingerprinting* Elastic Stack SIEM

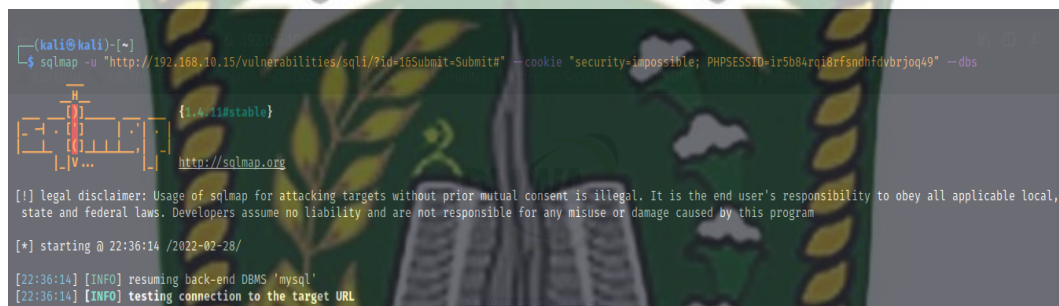
Hari Ke 2

Gambar 4. 54 Hasil *Monitoring* Serangan *Fingerprinting* Splunk Hari Ke 2

ke 2

4.2.8 Pengujian SQL Injection Hari Ke 2

Pengujian SQL Injection pada website DVWA pada hari ke 2 menggunakan tools yang bernama Sqlmap. Tools ini digunakan untuk melakukan injeksi query database terhadap website DVWA agar mendapatkan data seperti user dari website DVWA tersebut. Pengujian menggunakan Sqlmap dapat dilihat pada gambar 4.56 dibawah ini.



```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.10.15/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=impossible; PHPSESSID=1r5b84rq18rfsndhfdvbrjq49" --dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:36:14 /2022-02-28/

[22:36:14] [INFO] resuming back-end DBMS 'mysql'
[22:36:14] [INFO] testing connection to the target URL
```

Gambar 4. 56 Pengujian SQL Injection Menggunakan Sqlmap Hari Ke 2

Serangan SQL Injection yang dilakukan, menghasilkan informasi mengenai database yang digunakan pada website DVWA, dengan informasi yang di dapatkan oleh attacker tersebut, attacker dapat mengambil data penting seperti data user yang terdaftar dalam website tersebut dan masuk secara illegal. Hasil serangan mendapatkan informasi database website dapat dilihat pada gambar 4.56, dan informasi tentang data user yang di dapatkan oleh attacker dapat dilihat pada gambar 4.57 dibawah ini.

```

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x717a7a71,0x4a494354534a764b6e5247734c6769646d50476f4a437046506d6e
Submit
[22:36:17] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:36:17] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

```

Gambar 4. 57 Informasi Database Yang Didapatkan Oleh Attacker

Menggunakan Sqlmap Hari Ke 2

```

Database: dvwa
Table: users
[5 entries]

```

user_id	user	avatar	password	last_name	first_name	last_login	failed_login
1	admin	/DVWA/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	2022-01-16 15:35:30	0
2	gordonb	/DVWA/hackable/users/gordonb.jpg	e99a18c428cb38d5f268853678922e03 (abc123)	Brown	Gordon	2022-01-13 14:42:08	0
3	1337	/DVWA/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	2022-01-13 14:42:08	0
4	pablo	/DVWA/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2022-01-13 14:42:08	0
5	smithy	/DVWA/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	2022-01-13 14:42:08	0

```

[22:44:07] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.10.15/dump/dvwa/users.csv'
[22:44:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.10.15'
[22:44:07] [WARNING] your sqlmap version is outdated
[*] ending @ 22:44:06 /2022-02-28/

```

Gambar 4. 58 Informasi Data User DVWA Yang Didapatkan Oleh Attacker Hari Ke 2

Elastic Stack SIEM dan Splunk berhasil mendeteksi serangan SQL Injection pada hari ke 2, serangan yang di deteksi berupa informasi mengenai URL website DVWA yang rentan sehingga *attacker* dapat melakukan pengujian SQL injection.

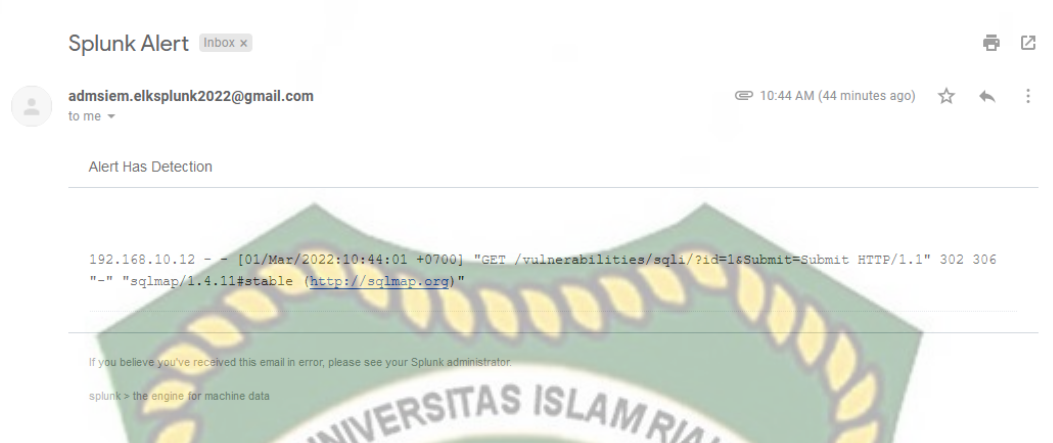
Time	Document
> Mar 1, 2022 @ 10:36:24.800	@timestamp: Mar 1, 2022 @ 10:36:24.800 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:10:36:15 +0700] \"GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1\" 302 306 \"-\" \"sqli/1.4.11#stable (http://sqli.org)\"] event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 10:36:25.776 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver
> Mar 1, 2022 @ 10:36:24.800	@timestamp: Mar 1, 2022 @ 10:36:24.800 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:10:36:17 +0700] \"GET /login.php HTTP/1.1\" 200 956 \"-\" \"sqli/1.4.11#stable (http://sqli.org)\"] event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 10:36:30.790 event.module: system event.timezone: +07:00 fileset.name: syslog host.architecture: x86_64 host.containerized: false host.hostname: webserver

Gambar 4. 59 Hasil *Monitoring SQL Injection Elastic Stack SIEM* Hari Ke 2

i	Time	Event
>	3/1/22 3:36:17.000 AM	192.168.10.12 - - [01/Mar/2022:10:36:17 +0700] "GET /login.php HTTP/1.1" 200 956 "-" "sqli/1.4.11#stable (http://sqli.org)" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/1/22 3:36:15.000 AM	192.168.10.12 - - [01/Mar/2022:10:36:15 +0700] "GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1" 302 306 "-" "sqli/1.4.11#stable (http://sqli.org)" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/1/22 3:33:40.000 AM	192.168.10.12 - - [01/Mar/2022:10:33:40 +0700] "GET /dwa/images/login_logo.png HTTP/1.1" 304 181 "http://192.168.10.15/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/1/22 3:33:40.000 AM	192.168.10.12 - - [01/Mar/2022:10:33:40 +0700] "GET /dwa/css/login.css HTTP/1.1" 200 741 "http://192.168.10.15/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 60 Hasil *Monitoring SQL Injection Splunk* Hari Ke 2

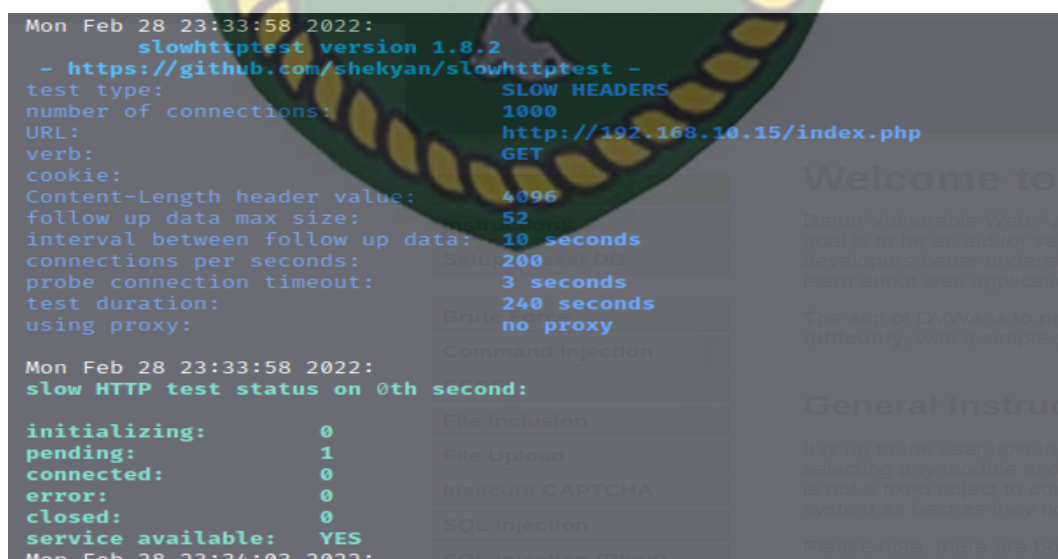
Hasil serangan *SQL Injection* yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan notifikasi *e-mail* serangan *SQL Injection*. Tampilan notifikasi *e-mail* serangan *SQL Injection* dapat dilihat pada gambar 4.61 dibawah ini.



Gambar 4. 61 Hasil Notifikasi SQL Injection di Splunk Melalui E-mail Hari Ke 2

4.2.9 Pengujian Denial of Service (DoS) Hari Ke 2

Pengujian *Denial of Service* (DoS) dilakukan menggunakan *tools* yang bernama Slowhttptest. Pengujian ini menyebabkan *website* tidak dapat di akses karena mendapatkan banyak *traffic* yang disebabkan oleh *tools* Slowhttptest. Pengujian menggunakan *tools* Slowhttptest dapat dilihat pada gambar 4.62 dibawah ini.



Gambar 4. 62 Pengujian Denial of Service (DoS) Menggunakan Slowhttptest

Hari Ke 2

Serangan *Denial of Service* (DoS) menggunakan Slowhttptest berhasil di deteksi oleh Elastic Stack SIEM dan Splunk. Hasil deteksi serangan DoS oleh Elastic Stack SIEM dapat dilihat pada gambar 4.63 dibawah ini. Dan hasil deteksi serangan DoS Splunk dapat dilihat pada gambar 4.64 dibawah ini.

"'." data-bbox="188 270 849 444"/>

Time	Document
> Mar 1, 2022 @ 11:35:36.388	@timestamp: Mar 1, 2022 @ 11:35:36.388 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:11:35:14 +0700] \"/>" event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 11:35:37.429 event.module: system
> Mar 1, 2022 @ 11:35:36.388	@timestamp: Mar 1, 2022 @ 11:35:36.388 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:11:35:14 +0700] \"/>" event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 11:35:37.429 event.module: system
> Mar 1, 2022 @ 11:35:36.388	@timestamp: Mar 1, 2022 @ 11:35:36.388 agent.ephemeral_id: c952fc91-833b-4d07-9772-30b3e825eab2 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 error.message: Provided Grok expressions do not match field value: [192.168.10.12 - - [01/Mar/2022:11:35:14 +0700] \"/>" event.dataset: system.syslog event.ingested: Mar 1, 2022 @ 11:35:37.429 event.module: system

Gambar 4. 63 Hasil Monitoring Serangan DoS Elastic Stack SIEM Hari Ke 2

"'." data-bbox="186 499 849 668"/>

i	Time	Event
>	3/1/22 4:34:54.000 AM	192.168.10.12 - - [01/Mar/2022:11:34:54 +0700] "GET /index.php HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition Mac AppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host= webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/1/22 4:34:54.000 AM	192.168.10.12 - - [01/Mar/2022:11:34:54 +0700] "GET /index.php HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition Mac AppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host= webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/1/22 4:34:54.000 AM	192.168.10.12 - - [01/Mar/2022:11:34:54 +0700] "GET /index.php HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition Mac AppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host= webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/1/22 4:34:54.000 AM	192.168.10.12 - - [01/Mar/2022:11:34:54 +0700] "GET /index.php HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Opera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition Mac AppStore; en) Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34" host= webserver source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 64 Hasil Monitoring Serangan DoS Splunk Hari Ke 2

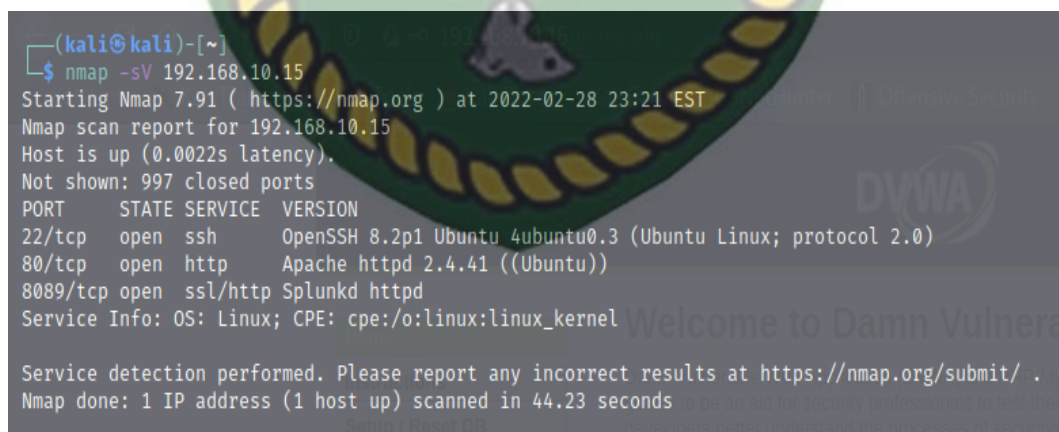
Hasil serangan DoS yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan notifikasi *e-mail* ke administrator. Tampilan notifikasi serangan DoS dapat dilihat pada gambar 4.65 dibawah ini.



Gambar 4. 65 Notifikasi Serangan DoS di Splunk Melalui *E-mail* Hari Ke 2

4.2.10 Pengujian *Port Scanning* Hari Ke 2

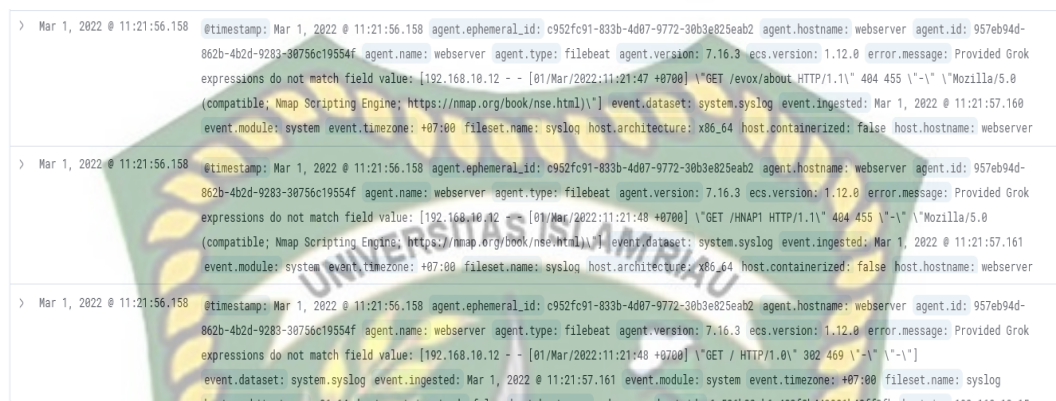
Pengujian *port scanning* digunakan untuk mendapatkan informasi mengenai *port* yang terbuka dari website DVWA. *Tools* yang digunakan pada pengujian *port scanning* ini adalah Nmap. Pengujian nmap dapat dilihat pada gambar 4.66 dibawah ini.



Gambar 4. 66 Pengujian *Port Scanning* Menggunakan Nmap Hari Ke 2

Serangan *port scanning* berhasil di deteksi oleh Elastic Stack SIEM dan Splunk, hasil deteksi serangan Elastic Stack SIEM dapat dilihat pada gambar 4.67

dibawah ini. Dan hasil deteksi serangan Splunk dapat dilihat pada gambar 4.68 dibawah ini.



Gambar 4. 67 Hasil Monitoring Serangan Port Scanning Elastic Stack SIEM
Hari Ke 2



Gambar 4. 68 Hasil Monitoring Serangan Port Scanning Splunk Hari Ke 2

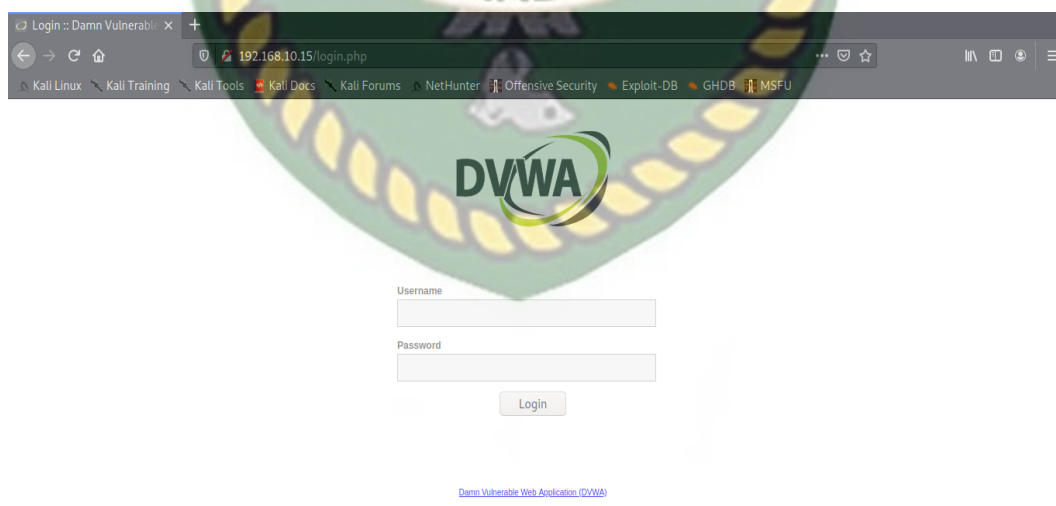
Hasil serangan *Port Scanning* yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan notifikasi *e-mail* ke administrator. Tampilan notifikasi serangan *Port Scanning* dapat dilihat pada gambar 4.69 dibawah ini.



Gambar 4. 69 Notifikasi Serangan *Port Scanning* di Splunk Melalui *E-mail* Hari Ke 2

4.2.11 Pengujian *Client* atau *Attacker* Mengakses *Web Server* Hari Ke 3

Pada pengujian ini *client* atau *attacker* melakukan akses terhadap website DVWA. Tampilan website DVWA yang diakses oleh *client* atau *attacker* dapat dilihat pada gambar 4.70 dibawah ini.



Gambar 4. 70 *Client* atau *Attacker* Mengakse *Web Server* Hari Ke 3

Elastic Stack SIEM dan Splunk berhasil mendeteksi data *log* akses *client* atau *attacker* secara *realtime*. Tampilan deteksi *log* akses pada Elastic Stack SIEM

dapat dilihat pada gambar 4.71 dibawah ini. Dan tampilan deteksi *log* akses Splunk dapat dilihat pada gambar 4.72 dibawah ini.

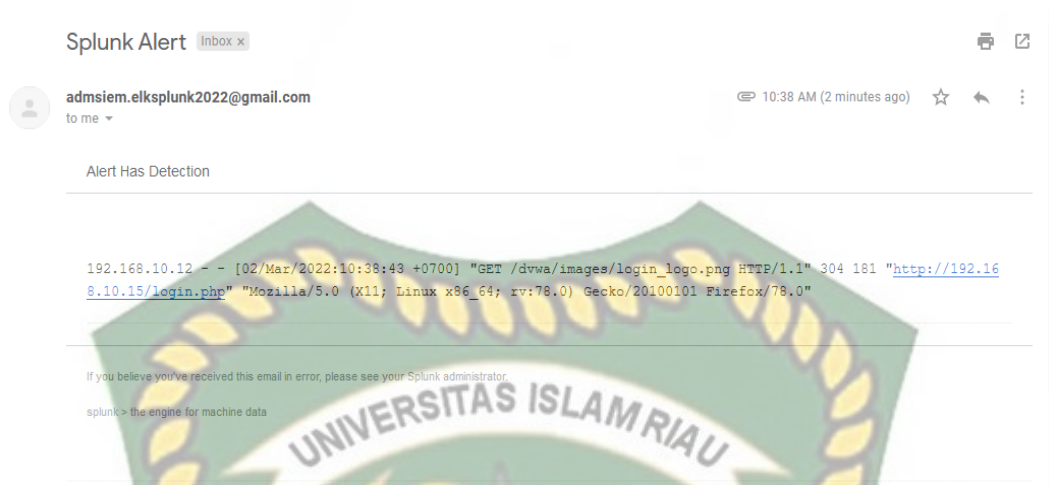
Time	Document
> Mar 2, 2022 @ 10:32:12.000	@timestamp: Mar 2, 2022 @ 10:32:12.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efce3294 agent.hostname: webservier agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webservier agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:32:20.058 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:32:21.134 event.kind: event event.module: apache event.original: 192.168.10.12 -- [02/Mar/2022:10:32:12 +0700] "GET / HTTP/1.1" 302 506 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" event.outcome: success fileset.name: access host.architecture: x86_64 host.containerized: false
> Mar 2, 2022 @ 10:32:12.000	@timestamp: Mar 2, 2022 @ 10:32:12.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efce3294 agent.hostname: webservier agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webservier agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:32:20.060 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:32:24.953 event.kind: event event.module: apache event.original: 192.168.10.12 -- [02/Mar/2022:10:32:12 +0700] "GET /login.php HTTP/1.1" 200 992 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" event.outcome: success fileset.name: access host.architecture: x86_64 host.containerized: false

Gambar 4. 71 Hasil Monitoring Log Akses Elastict Stack SIEM Hari Ke 3

i	Time	Event
>	3/2/22 3:32:12.000 AM	192.168.10.12 -- [02/Mar/2022:10:32:12 +0700] "GET /login.php HTTP/1.1" 200 992 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webservier source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/2/22 3:32:12.000 AM	192.168.10.12 -- [02/Mar/2022:10:32:12 +0700] "GET / HTTP/1.1" 302 506 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webservier source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 72 Hasil Monitoring Log Akses Splunk Hari Ke 3

Hasil *monitoring* Splunk berhasil dikirim melalui *e-mail notification* ke administrator sedangkan Elastic Stack SIEM gagal dalam mengirimkan *e-mail notification*. Tampilan *e-mail notification* Splunk dapat dilihat pada gambar 4.73 dibawah ini.



Gambar 4. 73 Notifikasi *Log* Masuk di Splunk Melalui *E-mail* Hari Ke 3

4.2.12 Pengujian *Fingerprinting* Hari Ke 3

Pengujian *fingerprinting* dilakukan dengan menggunakan *tools* yang bernama Nikto. Tampilan pengujian *fingerprinting* menggunakan Nikto dapat dilihat pada gambar 4.74 dibawah ini.



Gambar 4. 74 Pengujian *Fingerprinting* Menggunakan Nikto Hari Ke 3

Pengujian dengan metode *fingerprinting* berhasil di deteksi oleh Elastis Stack SIEM dan Splunk secara *realtime*. Tampilan deteksi Elastic Stack SIEM

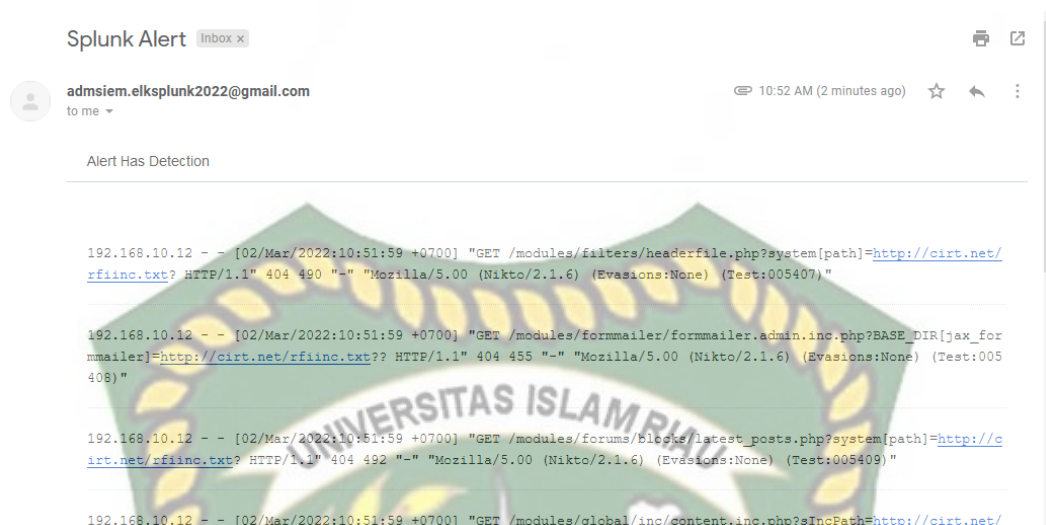
```
> Mar 2, 2022 @ 10:52:22.773 @timestamp: Mar 2, 2022 @ 10:52:22.773 agent.ephemeral_id: 659cc67f-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 apache.error.module: php7 ecs.version: 1.12.0 event.category: web event.dataset: apache.error event.ingested: Mar 2, 2022 @ 10:53:16.992 event.kind: event event.module: apache event.original: [Wed Mar 02 10:52:22.773398 2022] [php7:error] [pid 921] [client 192.168.10.12:57096] script '/var/www/html/ad.php' not found or unable to stat event.timezone: +07:00 event.type: error fileset.name: error host.architecture: x86_64 host.containerized: false

> Mar 2, 2022 @ 10:52:22.764 @timestamp: Mar 2, 2022 @ 10:52:22.764 agent.ephemeral_id: 659cc67f-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.dataset: apache.error event.ingested: Mar 2, 2022 @ 10:53:16.991 event.kind: event event.module: apache event.original: [Wed Mar 02 10:52:22.764587 2022] [php7:error] [pid 921] [client 192.168.10.12:57096] script '/var/www/html/_adminer.php' not found or unable to stat event.timezone: +07:00 event.type: error fileset.name: error host.architecture: x86_64 host.containerized: false

> Mar 2, 2022 @ 10:52:22.000 @timestamp: Mar 2, 2022 @ 10:52:22.000 agent.ephemeral_id: 659cc67f-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:52:24.503 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:53:14.445 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:10:52:22 +0700] "GET /README.markdown HTTP/1.1" 404 492 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0" output_type: failure fileset.name: error host.architecture: x86_64 host.containerized: false
```

Gambar 4. 76 Hasil *Monitoring Serangan Fingerprinting* Splunk Hari Ke 3

Pengujian dengan metode *fingerprinting* berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan *e-mail notification* ke administrator mengenai informasi serangan *fingerprinting* yang terjadi. Tampilan notifikasi serangan dari Splunk dapat dilihat pada gambar 4.77 dibawah ini.



Gambar 4. 77 Notifikasi Serangan *Fingerprinting* di Splunk Melalui *E-mail* Hari Ke 3

4.2.13 Pengujian SQL Injection Hari Ke 3

Pengujian SQL *Injection* menggunakan *tools* yang bernama Sqlmap, *tools* ini digunakan untuk melakukan injeksi *query database* dari *website* DVWA sehingga *attacker* dapat mengetahui informasi *database* yang digunakan dan melakukan pencurian data. Pengujian menggunakan Sqlmap dapat dilihat pada gambar 4.78 dibawah ini.



Gambar 4. 78 Pengujian SQL *Injection* Menggunakan Sqlmap Hari Ke 3

Hasil serangan menggunakan Sqlmap dapat dilihat pada gambar 4.79 dibawah ini. Dan *attacker* juga berhasil mendapatkan data *user* dengan melakukan

injeksi *query database*. Data *user* yang berhasil di dapatkan oleh *attacker* dapat dilihat pada gambar 4.80 dibawah ini.

```

Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x717a7a71,0x4a494354534a/64b6e5247734c6/69646d504/6f4a43/046506d6e48
Submit
-----
[22:39:13] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:39:13] [INFO] fetching database names
available databases [2]:
[*] dwwa
[*] information_schema

[22:39:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.10.15'
[22:39:13] [WARNING] your sqlmap version is outdated

[*] ending @ 22:39:13 /2022-03-01/

```

Gambar 4. 79 Informasi *Database* Yang Didapatkan Oleh *Attacker* Menggunakan *Sqlmap* Hari Ke 3

Database: dwwa
Table: users
[5 entries]

user_id	user	avatar	password	last_name	first_name	last_login	failed_login
1	admin	/DVWA/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	2022-01-16 15:35:30	0
2	gordonb	/DVWA/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	2022-01-13 14:42:08	0
3	1337	/DVWA/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	2022-01-13 14:42:08	0
4	pablo	/DVWA/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2022-01-13 14:42:08	0
5	smithy	/DVWA/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	2022-01-13 14:42:08	0

[22:43:37] [INFO] table 'dwwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.10.15/dump/dwwa/users.csv'
[22:43:37] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.10.15'
[22:43:37] [WARNING] your sqlmap version is outdated

[*] ending @ 22:43:37 /2022-03-01/

Gambar 4. 80 Data *User DVWA* Yang Didapatkan Oleh *Attacker* Hari Ke 3

Elastic Stack SIEM dan Splunk berhasil mendeteksi serangan *SQL Injection* menggunakan *Sqlmap*. Tampilan deteksi Elastic Stack SIEM dapat dilihat pada gambar 4.81 dibawah ini. Dan tampilan deteksi Splunk dapat dilihat pada gambar 4.82 dibawah ini.

Time	Document
> Mar 2, 2022 @ 10:39:14.000	@timestamp: Mar 2, 2022 @ 10:39:14.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:39:15.127 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:39:16.166 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:10:39:14 +0700] "GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1" 302 306 "-" "sqlmap/1.4.11#stable (http://sqlmap.org)" event.outcome: success fileset.name: access host.architecture: x86_64
> Mar 2, 2022 @ 10:39:14.000	@timestamp: Mar 2, 2022 @ 10:39:14.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:39:15.129 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:39:16.181 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:10:39:14 +0700] "GET /login.php HTTP/1.1" 200 956 "-" "sqlmap/1.4.11#stable (http://sqlmap.org)" event.outcome: success fileset.name: access host.architecture: x86_64 host.containerized: false host.hostname: webserver
> Mar 2, 2022 @ 10:39:10.000	@timestamp: Mar 2, 2022 @ 10:39:10.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:39:15.127 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:39:16.126 event.kind: event

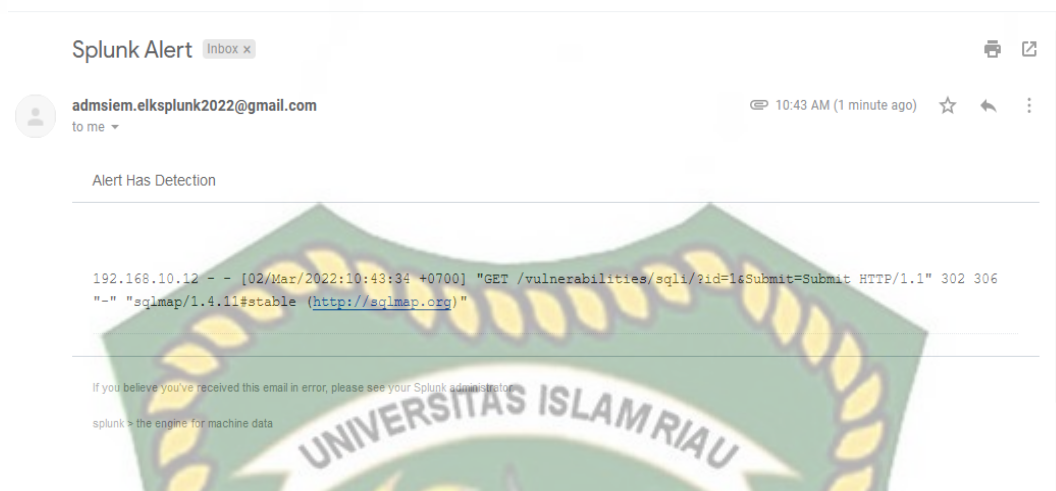
Gambar 4. 81 Hasil *Monitoring Serangan SQL Injection Elastic Stack SIEM* Hari

Ke 3

i	Time	Event
>	3/2/22 3:39:14.000 AM	192.168.10.12 - - [02/Mar/2022:10:39:14 +0700] "GET /login.php HTTP/1.1" 200 956 "-" "sqlmap/1.4.11#stable (http://sqlmap.org)" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/2/22 3:39:14.000 AM	192.168.10.12 - - [02/Mar/2022:10:39:14 +0700] "GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1" 302 306 "-" "sqlmap/1.4.11#stable (http://sqlmap.org)" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/2/22 3:39:10.000 AM	192.168.10.12 - - [02/Mar/2022:10:39:10 +0700] "GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1" 302 417 "-" "sqlmap/1.4.11#stable (http://sqlmap.org)" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/2/22 3:38:43.000 AM	192.168.10.12 - - [02/Mar/2022:10:38:43 +0700] "GET /dwa/images/login_logo.png HTTP/1.1" 304 181 "http://192.168.10.15/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/2/22 3:38:43.000 AM	192.168.10.12 - - [02/Mar/2022:10:38:43 +0700] "GET /dwa/css/login.css HTTP/1.1" 200 741 "http://192.168.10.15/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
>	3/2/22 3:38:43.000 AM	192.168.10.12 - - [02/Mar/2022:10:38:43 +0700] "GET /login.php HTTP/1.1" 200 993 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 82 Hasil *Monitoring Serangan SQL Injection Splunk* Hari Ke 3

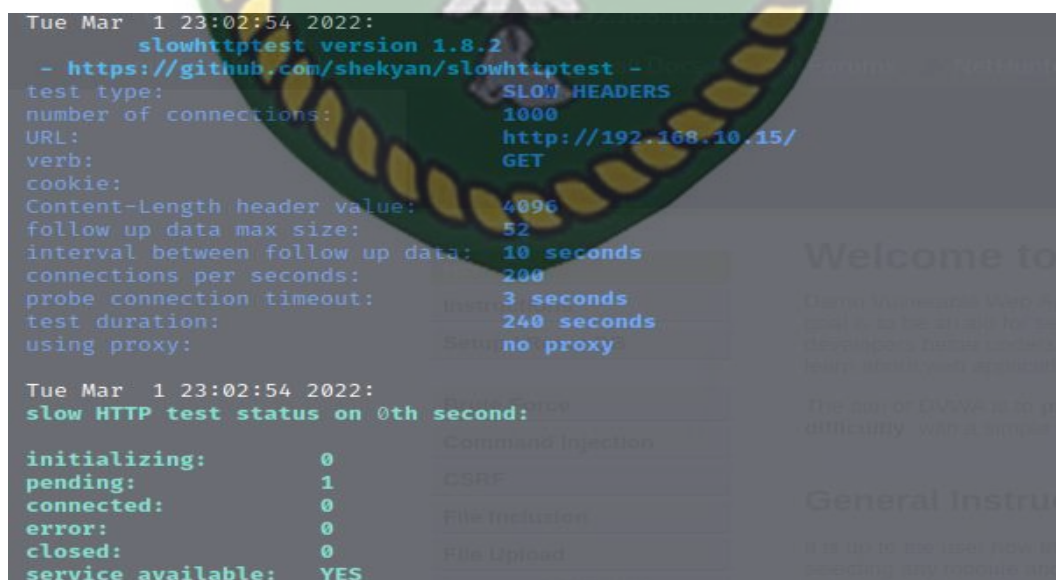
Hasil serangan *SQL Injection* yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan *e-mail notification* ke administrator. Tampilan notifikasi serangan *SQL Injection* dapat dilihat pada gambar 4.83 dibawah ini.



Gambar 4. 83 Hasil Notifikasi SQL Injection di Splunk Melalui E-mail Hari Ke 3

4.2.14 Pengujian *Denial of Service* (DoS) Hari Ke 3

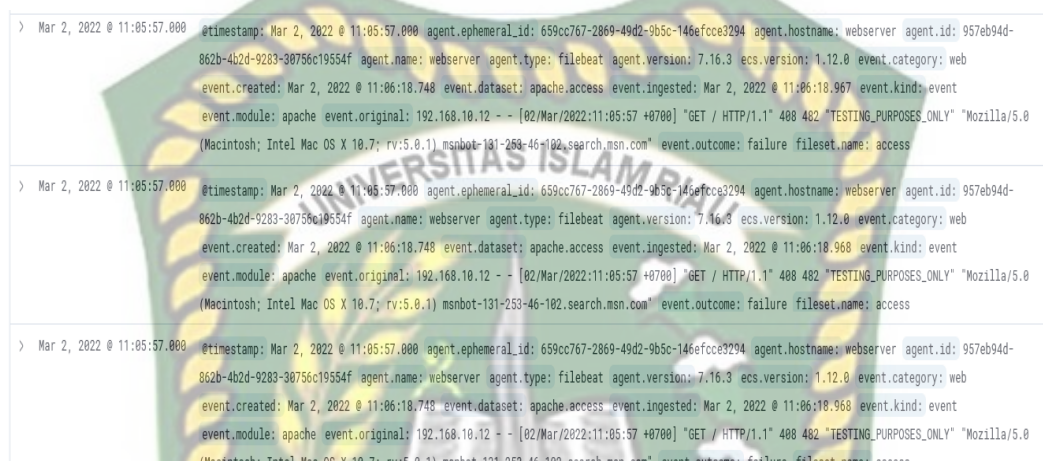
Pengujian DoS bertujuan untuk membuat *traffic* yang banyak kepada *web server* hingga *website* DVWA tidak dapat di akses. *Tools* yang digunakan untuk melakukan serangan DoS adalah Slowhttptest. Tampilan serangan DoS menggunakan Slowhttptest dapat dilihat pada gambar 4.84 dibawah ini.



Gambar 4. 84 Pengujian *Denial of Service* (DoS) Menggunakan Slowhttptest

Hari Ke 3

Serangan DoS berhasil di deteksi oleh Elastic Stack SIEM dan Splunk secara *realtime*. Hasil deteksi Elastic Stack SIEM dapat dilihat pada gambar 4.85 dibawah ini. Dan hasil deteksi Splunk dapat dilihat pada gambar 4.86 dibawah ini.



> Mar 2, 2022 @ 11:05:57.000	@timestamp: Mar 2, 2022 @ 11:05:57.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 11:06:18.748 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 11:06:18.967 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:11:05:57 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com" event.outcome: failure fileset.name: access
> Mar 2, 2022 @ 11:05:57.000	@timestamp: Mar 2, 2022 @ 11:05:57.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 11:06:18.748 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 11:06:18.968 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:11:05:57 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com" event.outcome: failure fileset.name: access
> Mar 2, 2022 @ 11:05:57.000	@timestamp: Mar 2, 2022 @ 11:05:57.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 11:06:18.748 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 11:06:18.968 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:11:05:57 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com" event.outcome: failure fileset.name: access

Gambar 4. 85 Hasil Monitoring Serangan DoS Elastic Stack SIEM Hari Ke 3



> 3/2/22 4:05:55.000 AM	192.168.10.12 - - [02/Mar/2022:11:05:55 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 4:05:55.000 AM	192.168.10.12 - - [02/Mar/2022:11:05:55 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 4:05:55.000 AM	192.168.10.12 - - [02/Mar/2022:11:05:55 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 4:05:55.000 AM	192.168.10.12 - - [02/Mar/2022:11:05:55 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 4:05:55.000 AM	192.168.10.12 - - [02/Mar/2022:11:05:55 +0700] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1) msbot-131-253-46-102.search.msn.com"
host = webserver	source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 86 Hasil Monitoring Serangan DoS Splunk Hari Ke 3

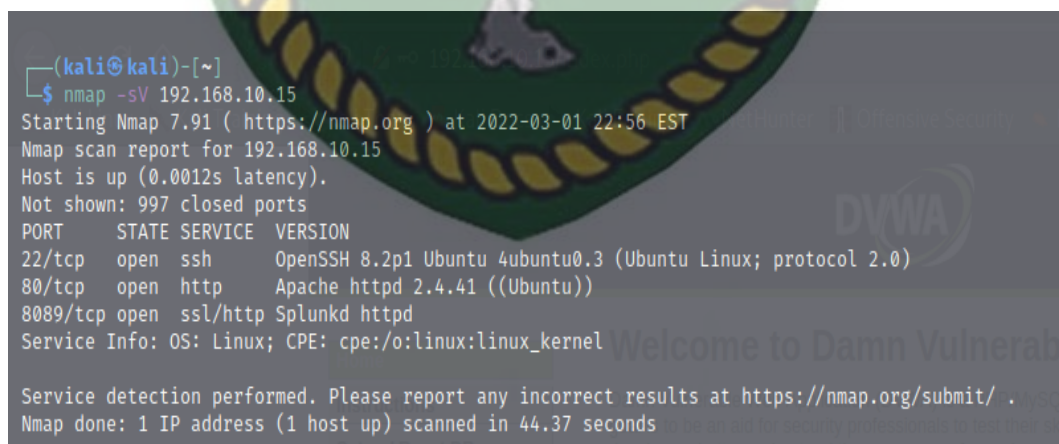
Hasil serangan DoS yang di deteksi oleh Splunk, selanjutnya Splunk mengirimkan *e-mail notification* ke administrator. Tampilan notifikasi serangan DoS dapat dilihat pada gambar 4.87 dibawah ini.



Gambar 4. 87 Notifikasi Serangan DoS di Splunk Melalui *E-mail* Hari Ke 3

4.2.15 Pengujian *Port Scanning* Hari Ke 3

Pengujian *Port Scanning* menggunakan *tools* yang bernama Nmap. Nmap digunakan untuk melakukan *scanning* terhadap *port* yang terbuka dari website DVWA. Tampilan serangan menggunakan Nmap dapat dilihat pada gambar 4.88 dibawah ini.



Gambar 4. 88 Pengujian *Port Scanning* Menggunakan Nmap Hari Ke 3

Serangan *port scanning* berhasil di deteksi oleh Elastic Stack SIEM dan Splunk secara *realtime*. Hasil deteksi Elastic Stack SIEM dapat dilihat pada gambar

4.89 dibawah ini. Dan hasil deteksi Splunk dapat dilihat pada gambar 4.90 dibawah ini.

Time ↓	Document
> Mar 2, 2022 @ 10:57:03.000	@timestamp: Mar 2, 2022 @ 10:57:03.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:57:08.858 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:57:09.875 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:10:57:03 +0700] "GET /nmaplowercheck1646193422 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" event.outcome: failure fileset.name: access
> Mar 2, 2022 @ 10:57:03.000	@timestamp: Mar 2, 2022 @ 10:57:03.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:57:08.860 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:57:09.907 event.kind: event event.module: apache event.original: 192.168.10.12 - - [02/Mar/2022:10:57:03 +0700] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" event.outcome: failure fileset.name: access host.architecture: x86_64
> Mar 2, 2022 @ 10:57:03.000	@timestamp: Mar 2, 2022 @ 10:57:03.000 agent.ephemeral_id: 659cc767-2869-49d2-9b5c-146efcce3294 agent.hostname: webserver agent.id: 957eb94d-862b-4b2d-9283-30756c19554f agent.name: webserver agent.type: filebeat agent.version: 7.16.3 ecs.version: 1.12.0 event.category: web event.created: Mar 2, 2022 @ 10:57:08.860 event.dataset: apache.access event.ingested: Mar 2, 2022 @ 10:57:09.907 event.kind: event

Gambar 4. 89 Hasil Monitoring Serangan Port Scanning Elastic Stack SIEM

Hari Ke 3

> 3/2/22 3:57:03.000 AM	192.168.10.12 - - [02/Mar/2022:10:57:03 +0700] "GET /evox/about HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
	host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 3:57:03.000 AM	192.168.10.12 - - [02/Mar/2022:10:57:03 +0700] "GET /HAPI HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
	host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 3:57:03.000 AM	192.168.10.12 - - [02/Mar/2022:10:57:03 +0700] "GET / HTTP/1.0" 302 469 "-" "-"
	host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 3:57:03.000 AM	192.168.10.12 - - [02/Mar/2022:10:57:03 +0700] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
	host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small
> 3/2/22 3:57:03.000 AM	192.168.10.12 - - [02/Mar/2022:10:57:03 +0700] "GET /nmaplowercheck1646193422 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
	host = webserver source = /var/log/apache2/access.log sourcetype = access-too_small

Gambar 4. 90 Hasil Monitoring Serangan Port Scanning Splunk Hari Ke 3

Hasil serangan *port scanning* yang berhasil di deteksi oleh Splunk, selanjutnya Splunk mengirimkan *e-mail notification* ke administrator. Tampilan notifikasi serangan *Port Scanning* yang berhasil dikirim dapat dilihat pada gambar 4.91 dibawah ini.



Gambar 4. 91 Notifikasi Serangan *Port Scanning* di Splunk Melalui *E-mail* Hari Ke 3

4.3 Analisa

Berdasarkan hasil pengujian yang telah dilakukan oleh *attacker* terhadap *web server*, maka dilakukan analisa dari Elastic Stack SIEM dan Splunk yang digunakan untuk *me-monitoring* aktifitas *web server*.

4.3.1 Analisa *Client* atau *Attacker* Mengakses *Web Server*

Pengujian pertama yang dilakukan dengan cara *client* atau *attacker* mengakses *web server*. Pada pengujian ini *client* atau *attacker* tidak melakukan serangan apapun, *client* hanya mengakses *web server* saja. Dan *log akses* dari *client* dapat di deteksi oleh Elastic Stack SIEM dan Splunk secara *realtime*. Informasi yang didapatkan dari *log masuk* tersebut, berupa IP Address, URL yang diakses, Host dari *web server*, *browser* yang digunakan dan waktu akses dari *client*. Data *log* yang berhasil di deteksi tersebut selanjutnya dikirim melalui *e-mail* notifikasi

kepada administrator, sehingga administrator dapat melihat siapa yang mengakses *web server* tersebut.

4.3.2 Analisa Pengujian *Fingerprinting* Menggunakan Nikto

Pengujian menggunakan *fingerprinting* dapat dideteksi secara *realtime* oleh Elastic Stack SIEM dan Splunk. Dari serangan yang dilakukan, Elastic Stack SIEM dan Splunk mampu mengumpulkan informasi mengenai serangan tersebut, mulai dari IP Address *attacker*, *tools* yang digunakan, *browser* yang digunakan untuk menyerang, mengenali *tools* yang digunakan dalam melakukan serangan *Fingerprinting* yaitu Nikto beserta versi dari Nikto tersebut, dan waktu serangan terjadi. Splunk berhasil mengirimkan informasi dari serangan *Fingerprinting* yang terjadi melalui *e-mail* notifikasi kepada administrator, sedangkan Elastic Stack SIEM gagal dalam mengirimkan *e-mail* notifikasi. Dengan Splunk mengirimkan *e-mail* notifikasi tersebut, administrator dapat melihat serangan terhadap *web server*.

4.3.3 Analisa Pengujian SQL Injection Menggunakan Sqlmap

Pengujian menggunakan SQL Injection, merupakan jenis serangan yang sangat berbahaya karena dapat membocorkan data penting dari *website* DVWA yang diserang. Pada pengujian SQL Injection ini, *attacker* menggunakan *tools* yang bernama Sqlmap. *Attacker* menggunakan *query* yang rentan dari *website* tersebut untuk dapat melakukan injeksi *query database*, sehingga *attacker* dapat mendapatkan informasi *database* dan data pengguna dari *website* DVWA yang diserang. Serangan SQL Injection ini dapat di deteksi oleh Elastic Stack SIEM dan Splunk secara *realtime*. Informasi yang di dapatkan dari serangan tersebut berupa IP address *attacker*, proses injeksi *query database*, *tools* yang digunakan, dan waktu

serangan. Dan Splunk berhasil mengirimkan notifikasi *e-mail* serangan SQL *Injection* kepada administrator, sehingga administrator dapat melakukan tindakan dalam menangani serangan SQL *Injection*.

4.3.4 Analisa Pengujian *Denial of Service (DoS)* Menggunakan *Slowhttptest*

Serangan DoS bertujuan untuk membuat *web server* tidak dapat diakses dengan memberikan *traffic* yang banyak terhadap *web server* tersebut. Pada pengujian ini Elastic Stack SIEM dan Splunk dapat mendeteksi serangan DoS secara *realtime*. Penyerangan ini membuat *traffic* yang banyak sehingga data yang didapatkan berupa jenis *browser* yang digunakan dalam serangan DoS, waktu serangan, dan IP address *attacker*. Splunk dapat mengirimkan *e-mail* notifikasi serangan DoS kepada administrator, sedangkan Elastic Stack SIEM gagal dalam mengirimkan *e-mail* notifikasi kepada administrator.

4.3.5 Analisa Pengujian *Port Scanning* Menggunakan *Nmap*

Serangan *Port Scanning* dilakukan oleh *attacker* untuk mendapatkan *port* yang terbuka dari *website* DVWA. Dengan adanya informasi *port* yang terbuka, *attacker* dapat melakukan serangan terhadap *port* yang terbuka tersebut. Pada pengujian yang telah dilakukan, Elastic Stack SIEM dan Splunk dapat mendeteksi serangan *Port Scanning* yang dilakukan oleh *attacker*. Informasi yang didapatkan berupa IP address penyerang, *tools* yang digunakan untuk melakukan serangan *port scanning* yaitu Nmap, *browser* yang digunakan *attacker*, dan waktu serangan terjadi. Dalam serangan ini, Splunk berhasil mengirimkan *e-mail* notifikasi kepada Administrator, sedangkan Elastic Stack SIEM gagal dalam mengirimkan *e-mail* notifikasi kepada administrator.

4.3.6 Penjelasan Output Monitoring

Hasil *monitoring* menggunakan Elastic Stack SIEM yaitu berupa log yang berisikan data-data mengenai serangan yang terjadi. Untuk mempermudah dalam memahami data-data *log* yang berhasil di-*monitoring* maka dibuat penjelasan mengenai data-data tersebut.

Tabel 4. 1 Penjelasan Output Elastic Stack SIEM

Serangan	Output	Penjelasan
<i>Fingerprinting</i>	<i>event.dataset</i>	Jika terdapat satu sumber satu atau lebih <i>log</i> yang masuk, <i>dataset</i> digunakan untuk mengklasifikasi dari mana sumber <i>log</i> itu berasal. Misalnya, <i>apache.access</i>
	<i>event.ingested</i>	Ketika serangan terjadi, <i>event.ingested</i> yang pertama kali menangkap data waktu serangan, dan disimpan di dalam <i>timestamp</i> .
	<i>event.module</i>	Untuk mengetahui nama sistem dari sumber yang dimonitoring. Misalnya, <i>apache</i> .
	<i>event.timezone</i>	Untuk mengetahui zona waktu berdasarkan lokasi dari <i>agent</i> yang di- <i>monitoring</i> .

	<i>fileset.name</i>	Kumpulan <i>log</i> yang dibaca oleh <i>filebeat</i> dan disimpan dalam satu <i>file system</i> yaitu <i>syslog</i> .
	<i>host.architecture</i>	Data arsitektur komputer yang di- <i>monitoring</i> oleh Elastic Stack SIEM. Misalnya <i>x86_64</i> .
	<i>host.containerized</i>	Jika <i>host</i> (<i>web server</i>) menggunakan <i>container</i> misalnya seperti <i>docker</i> maka nilai nya akan menjadi <i>true</i> , jika tidak maka akan bernilai <i>false</i> (tidak menggunakan <i>container</i>).
	<i>host.hostname</i>	Nama dari <i>host</i> yang berhasil terhubung antara <i>filebeat</i> dengan Elastic Stack SIEM.
SQL Injection	<i>event.dataset</i>	Untuk mengklasifikasi dari mana sumber <i>log</i> berasal.
	<i>event.ingested</i>	<i>event.ingested</i> yang pertama kali menangkap data waktu serangan.
	<i>event.module</i>	Nama sistem dari sumber yang di- <i>monitoring</i>
	<i>event.timezone</i>	Untuk mengetahui zona waktu dari <i>agent</i> yang di- <i>monitoring</i> .

	<i>fileset.name</i>	Kumpulan <i>log</i> yang dikirimkan dari <i>agent</i> filebeat ke Elastic Stack SIEM
	<i>host.architecture</i>	Data arsitektur dari <i>host</i> yang di- <i>monitoring</i> .
	<i>host.containerized</i>	Data <i>container</i> dari <i>host</i> yang di- <i>monitoring</i> . Jika menggunakan <i>container</i> maka bernilai <i>true</i> , jika tidak maka bernilai <i>false</i> .
	<i>host.hostname</i>	Nama <i>host</i> yang di- <i>monitoring</i> oleh Elastic Stack SIEM.
DoS (<i>Denial Of Service</i>)	<i>event.dataset</i>	Klasifikasi serangan berdasarkan sumber dari <i>log</i> yang masuk.
	<i>event.ingested</i>	Menangkap waktu serangan pertama kali terjadi dan disimpan pada <i>timestamp</i> .
	<i>event.kind</i>	Memberikan informasi tentang tipe dari serangan yang masuk. Dan serangan informasinya juga berupa apakah serangan ini hanya dilakukan sekali atau berulang kali dalam satu serangan yang sama.

	<i>event.module</i>	Nama sistem dari sumber yang di- <i>monitoring</i> .
	<i>event.original</i>	Pesan mentah (<i>raw text</i>) dari <i>log</i> yang berhasil ditangkap.
	<i>event.outcome</i>	Untuk menangkap satu jenis serangan yang dilakukan secara berulang. Jika Elastic Stack SIEM berhasil mendeteksi serangan tersebut maka akan bernilai <i>success</i> , dan jika tidak maka akan bernilai <i>failure</i> .
	<i>filename.set</i>	Kumpulan <i>log</i> dari <i>agent</i> yang dikirim ke Elastic Stack SIEM.
	<i>host.architecture</i>	Data arsitektur dari <i>host</i> yang di- <i>monitoring</i> .
	<i>host.containerized</i>	Data <i>container</i> dari <i>host</i> yang di- <i>monitoring</i> .
	<i>host.hostname</i>	Nama <i>host</i> yang di- <i>monitoring</i> .
<i>Port Scanning</i>	<i>event.dataset</i>	Klasifikasi sumber <i>log</i> yang di- <i>monitoring</i> .
	<i>event.ingested</i>	Data waktu yang ditangkap pertama kali saat serangan terjadi.

	<i>event.kind</i>	Informasi mengenai tipe serangan yang masuk, dan apakah serangan tersebut dilakukan sekali atau berkali-kali dalam satu serangan yang sama.
	<i>event.module</i>	Nama sistem dari sumber yang di-monitoring.
	<i>event.original</i>	Raw text dari serangan yang berhasil di deteksi.
	<i>event.outcome</i>	Untuk mengetahui apakah serangan tersebut dalam satu serangan yang sama atau tidak. Jika berhasil ditangkap maka akan bernilai <i>success</i> , jika tidak akan bernilai <i>failure</i> .
	<i>fileset.name</i>	Kumpulan <i>log agent</i> yang dikirim ke Elastic Stack SIEM.
	<i>host.architecture</i>	Data arsitektur <i>host</i> yang di-monitoring.

Dengan adanya serangan yang terjadi, maka dibuat tabel perbandingan untuk mengetahui kemampuan deteksi serangan dari Elastic Stack SIEM dan Splunk yang

dilakukan selama tiga hari. Tabel perbandingan hasil pengujian dapat dilihat pada tabel 4.2 dibawah ini.

Tabel 4. 2 Tabel Perbandingan Hasil *Monitoring*

Serangan	Elastic Stack SIEM	Splunk
<i>Client</i> atau <i>Attacker</i> Mengakses <i>website</i>	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi <i>raw text</i> dari serangan yang ditangkap yang informasinya mengenai <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i> atau <i>client</i>, serta <i>tools</i> yang digunakan. • Mendeteksi informasi tentang <i>agent</i> yang terhubung yaitu <i>web server</i>.	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i> atau <i>client</i>, serta <i>tools</i> yang digunakan. • Mendeteksi nama <i>host</i> yang terhubung. • Mendeteksi lokasi <i>log</i> yang di-<i>monitoring</i>. • Menyimpan data <i>log</i> berdasarkan <i>path</i> serangan yang terjadi.

	• Mendeteksi nama sistem yang terhubung. • Mendeteksi zona waktu dari <i>host</i> yang terhubung. • Mendeteksi arsitektur dari <i>host</i> yang terhubung.	
<i>Fingerprinting</i>	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi data mengenai <i>agent</i> yang terhubung ke Elastic Stack SIEM. • Mendeteksi <i>raw text</i> yang berisi data <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i>, serta <i>tools</i> yang digunakan.	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i> atau <i>client</i>, serta <i>tools</i> yang digunakan. • Mendeteksi nama <i>host</i> yang terhubung. • Mendeteksi lokasi <i>log</i> yang di-monitoring.

	• Mendeteksi zona waktu dari <i>agent</i> yang terhubung. • Mendeteksi arsitektur dari <i>host</i> yang terhubung. • Mendeteksi nama <i>host</i> yang terhubung.	• Menyimpan data <i>log</i> berdasarkan <i>path</i> serangan yang terjadi.
SQL Injection	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi data mengenai <i>agent</i> yang terhubung ke Elastic Stack SIEM. • Mendeteksi <i>raw text</i> yang berisi data <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i>, dan <i>tools</i> yang digunakan.	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i> atau <i>client</i>, serta <i>tools</i> yang digunakan. • Mendeteksi nama <i>host</i> yang terhubung. • Mendeteksi lokasi <i>log</i> yang di-monitoring.

	• Mendeteksi nama sistem yang di-<i>monitoring</i>. • Mendeteksi arsitektur <i>host</i> yang terhubung. • Mendeteksi <i>containter</i> dari <i>host</i>, namun pada hasil pengujian tidak menggunakan <i>containter</i> dan hasilnya menjadi <i>false</i>. • Mendeteksi nama <i>host</i> yang terhubung.	• Menyimpan data <i>log</i> berdasarkan <i>path</i> serangan yang terjadi.
<i>Denial of Service</i> (DoS)	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi data mengenai <i>agent</i> yang terhubung ke Elastic Stack SIEM. • Mendeteksi <i>raw text</i> yang berisi data <i>ip</i>	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i> atau <i>client</i>. • Mendeteksi nama <i>host</i> yang terhubung.

	<i>address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i>. • Berhasil mendeteksi serangan DoS dengan mengumpulkan <i>log</i> serangan yang sama. Dan <i>output</i> serangan disimpan pada <i>event.outcome</i> dengan hasil <i>success</i>. • Mendeteksi arsitektur dari <i>host</i> yang terhubung. • Mendeteksi <i>containter</i> dari <i>host</i>. • Mendeteksi nama <i>host</i> yang terhubung.	• Mendeteksi lokasi <i>log</i> yang di-monitoring.
<i>Port Scanning</i>	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi data mengenai <i>agent</i> yang	• Mendeteksi waktu serangan yang terjadi. • Mendeteksi <i>ip address</i> dan <i>web browser</i> yang

	terhubung ke Elastic Stack SIEM. • Mendeteksi <i>raw text</i> yang berisi data <i>ip address</i> dan <i>web browser</i> yang digunakan oleh <i>attacker</i>, dan <i>tools</i> yang digunakan. • Mendeteksi arsitektur dari <i>host</i> yang terhubung. • Mendeteksi <i>containter</i> dari <i>host</i>. • Mendeteksi nama <i>host</i> yang terhubung.	digunakan oleh <i>attacker</i> atau <i>client</i>, serta <i>tools</i> yang digunakan. • Mendeteksi nama <i>host</i> yang terhubung. • Mendeteksi lokasi <i>log</i> yang di-<i>monitoring</i>. • Menyimpan data <i>log</i> berdasarkan <i>path</i> serangan yang terjadi.
--	---	---

Berdasarkan tabel 4.2 diatas, Elastic Stack SIEM dan Splunk berhasil mendeteksi semua serangan yang terjadi selama tiga hari pengujian. Dengan hasil deteksi yang memiliki persamaan dan perbedaan, hal ini dapat membantu administrator dalam melakukan tindakan untuk mengatasi serangan yang terjadi.

Pemberitahuan serangan yang terjadi, dikirim oleh Elastic Stack SIEM dan Splunk melalui *e-mail* notifikasi kepada administrator, kemampuan dalam mengirimkan notifikasi *e-mail* dapat dilihat pada tabel 4.3 dibawah ini.

Tabel 4. 3 Tabel Hasil Mengirim Notifikasi Serangan

Serangan	Elastic Stack SIEM	Splunk
<i>Client</i> atau <i>attacker</i> mengakses <i>webstie</i>	Tidak Berhasil	Berhasil
<i>Fingerprinting</i>	Tidak Berhasil	Berhasil
SQL <i>Injection</i>	Tidak Berhasil	Berhasil
<i>Denial of Service</i> (DoS)	Tidak Berhasil	Berhasil
<i>Port Scanning</i>	Tidak Berhasil	Berhasil

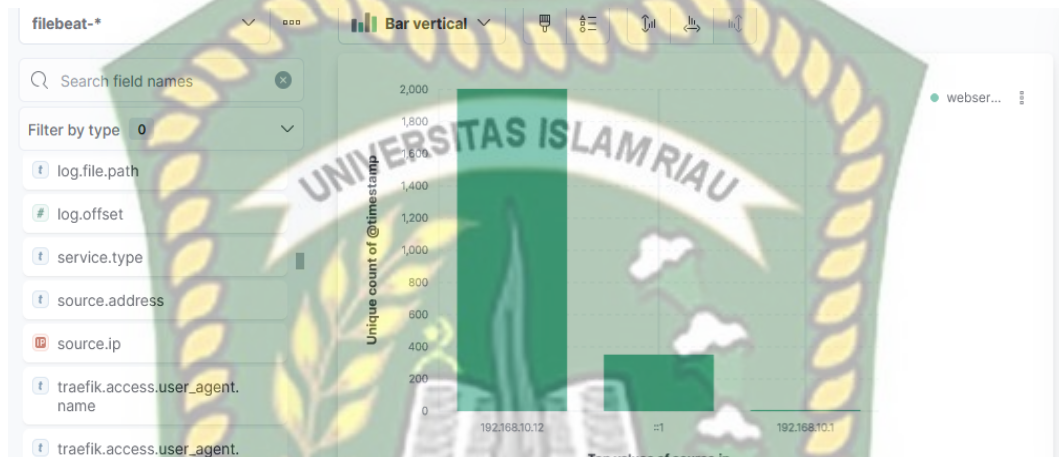
Berdasarkan tabel 4.3 diatas, Splunk berhasil mengirimkan notifikasi semua serangan yang terjadi selama tiga hari pengujian melalui *e-mail* ke administrator, sedangkan Elastic Stack SIEM gagal dalam mengirimkan notifikasi ke administrator. Dalam hal ini Splunk unggul dalam melakukan pengiriman notifikasi serangan yang terjadi.

4.3.7 Visualisasi Hasil Serangan

Elastic Stack SIEM dan Splunk memiliki fitur untuk memvisualisasi hasil serangan dalam bentuk diagram. Pada penelitian ini penulis menggunakan diagram batang supaya mempermudah dalam memahami waktu dan jumlah serangan yang

terjadi terhadap *web server*. Berikut adalah visualiasasi hasil serangan dalam bentuk diagram batang dari Elastic Stack SIEM dan Splunk.

a. Visualisasi Hasil Serangan Pada Elastic Stack SIEM



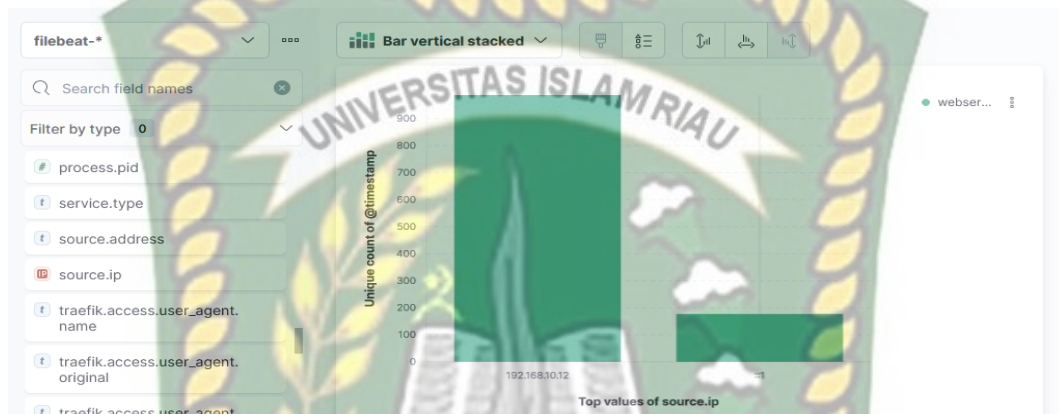
Gambar 4. 92 Diagram Batang Hasil Monitoring Elastic Stack SIEM Hari Ke 1

Pada gambar 4.92 diatas, diagram batang tersebut menunjukkan jumlah serangan yang dilakukan oleh *attacker* pada hari ke 1. IP address attacker yaitu 192.168.10.12, pada diagram tersebut *attacker* melakukan serangan dengan total yang terhitung yaitu 2000, angka 2000 merupakan akumulasi dari *log* yang terbaca.



Gambar 4. 93 Diagram Batang Hasil Monitoring Elastic Stack SIEM Hari Ke 2

Pada gambar 4.93 diatas, diagram batang tersebut menunjukkan jumlah serangan yang dilakukan oleh *attacker* pada hari ke 2. IP address attacker yaitu 192.168.10.12, pada diagram tersebut *attacker* melakukan serangan dengan total yang terhitung yaitu 1800, angka 1800 merupakan akumulasi dari *log* yang terbaca.



Gambar 4. 94 Diagram Batang Hasil Monitoring Elastic Stack SIEM Hari Ke 3

Pada gambar 4.94 diatas, diagram batang tersebut menunjukkan jumlah serangan yang dilakukan oleh *attacker* pada hari ke 3. IP address attacker yaitu 192.168.10.12, pada diagram tersebut *attacker* melakukan serangan dengan total yang terhitung yaitu 987, angka 987 merupakan akumulasi dari *log* yang terbaca.

b. Visualisasi Hasil Serangan Pada Splunk

[illegible]

Gambar 4. 96 *Diagram Batang Hasil Monitoring Splunk Hari Ke 2*

Sum of date_in day

month

Gambar 4. 97 *Diagram Batang Hasil Monitoring Splunk Hari Ke 3*

Pada gambar 4.97 diatas, diagram batang dari Splunk menampilkan banyaknya serangan yang terjadi pada hari ke 3.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisa dari penelitian ini dapat diambil kesimpulan sebagai berikut :

1. Implementasi yang dilakukan menggunakan Elastic Stack SIEM dan Splunk dalam mengumpulkan informasi serangan berhasil dilakukan. Kedua *tools* tersebut dapat mendeteksi semua serangan yang terjadi selama tiga hari pengujian. Dalam notifikasi serangan melalui *e-mail*, Splunk mampu mengirimkan semua notifikasi saat serangan terjadi, sementara Elastic Stack SIEM gagal dalam mengirimkan notifikasi melalui *e-mail*.
2. Semua *log* serangan yang dilakukan selama tiga hari, dapat di rekam oleh kedua *tools* SIEM yang digunakan yaitu Elastic Stack SIEM dan Splunk. Hasil deteksi serangan yang telah terjadi, akan disimpan oleh Elastic Stack SIEM dan Splunk, sehingga administrator dapat melakukan analisa dan visualisasi serangan yang terjadi.
3. Komponen yang digunakan untuk menganalisa *log* yaitu Filebeat dan Splunk forwarder. Filebeat merupakan komponen yang bertugas sebagai *agent* yang menghubungkan aktifitas *log* dari *web server* ke Elastic Stack SIEM. Splunk forwarder merupakan komponen dari Splunk yang di install di dalam *web server* supaya *web server* dapat terhubung ke dalam Splunk, dan Splunk dapat *me-monitoring log* dari *web server*.

5.2 Saran

Adapun saran yang dapat digunakan untuk pengembangan lanjutan penelitian ini, yaitu sebagai berikut :

1. Analisa *Log* dapat dilakukan menggunakan *Tools* SIEM lainnya.
2. Melakukan jenis serangan yang lainnya dengan tujuan untuk mengetahui kemampuan deteksi dari SIEM.
3. Melakukan pengujian menggunakan *server* yang lainnya untuk di *monitoring*.



DAFTAR PUSTAKA

- Akmal, M. D., Kusuma, K. D., & Ridha, M. A. F. (2018). Jurnal Aksara Komputer Terapan Politeknik Caltex Riau Impelementasi Security Information And Event Management (SIEM). *Jurnal Aksara Komputer Terapan*, 7(2), 1–10.
- Brades, T., & Irwansyah. (2022). *PEMANFAATAN METODE PORT KNOCKING DAN BLOCKING UNTUK KEAMANAN JARINGAN BPKAD PROVINSI SUMSEL*. 99–107.
- Clarke, J. (2009). SQL Injection Attacks and Defense. In *SQL Injection Attacks and Defense*. ELSEVIER.
- DVWA. (n.d.). *Damn Vulnerable Web Application (DVWA)*. <https://Dvwa.Co.Uk/>.
Diakses pada 20 September 2021, dari <https://dvwa.co.uk/>
- Engelbreton, P. (2011). *The Basics of Hacking and Penetration Testing* (J. Broad (ed.); Vol. 148). ELSEVIER.
- Hae, Y., & Sulisty, W. (2021). *Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen*. 8(4), 2095–2105.
- Kamal, M. R., & Setiawan, M. A. (2021). Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *AUTOMATA*, 4.
- Krawetz, N. (2010). *Ubuntu Powerful Hacks and Customizations*. Wiley Publishing.

Lukman, A. M., & Bachtiar, Y. (2018). Analisis Sistem Pengelolaan, Pemeliharaan dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto. *Evolusi : Jurnal Sains Dan Manajemen*, 6(2), 49–56.

Maiwald, E. (2013). *Network Security A Beginner's Guide, Third Edition* (A. Brandt (ed.)). The McGraw-Hill Companies.

Muakhori, I., Sunardi, S.T, M.T, Phd, D., & Abdul Fadlil, M. . (2018). Membangun Web Server Menggunakan Dynamic Domain Name System (Dns) Berbasis Berkeley Internet Name Domain (Bind9) Pada Ip Dinamis. *Jurnal Sistem Informasi (JSI) Universitas Dirgantara Marsekal Suryadarma*, 5(2), 1–8.

Palilingan, A. G., Najooan, M. E. I., & Sompie, S. R. U. . (2020). Sistem Komunikasi Darurat Bencana Dengan Teknologi Mobile Ad-Hoc Network (MANET). *Jurnal Teknik Elektro Dan Komputer*, 9(2), 49–60.

Sampurno, D. S., Noertjahyana, A., & Setiawan, A. (2019). Implementasi Pembuatan Distro Linux Untuk Keperluan Laboratorium Informatika. *Jurnal Infra Petra*, II(1), 2.

Satwika, I. K. S., & Semadi, K. N. (2020). Perbandingan Performansi Web Server Apache Dan Nginx Dengan Menggunakan Ipv6. *SCAN - Jurnal Teknologi Informasi Dan Komunikasi*, 15(1), 10–15.

Sholihah, W., Pripambudi, S., & Mardiyono, A. (2020). Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack). *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, 2(1), 12–20.

Sinha, S. (2018). Beginning Ethical Hacking with Kali Linux. In *Beginning Ethical Hacking with Kali Linux*. Apress.

Suryana, N., & Saputra, D. D. (2018). Perancangan Penggunaan Firewall Dan Proxy Server Untuk. *Jurnal Sutet*, 8(1), International Research Jurnal of Microbiologi.

Tarigan, C., Engel, V. J. L., & Angela, D. (2018). Sistem Pengawasan Kinerja Jaringan Server Web Apache dengan Log Management System ELK (Elasticsearch, Logstash, Kibana). *Jurnal Telematika*, 7–14.

