



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**ANALISIS KINERJA *SECURITY INFORMATION AND
EVENT MANAGEMENT (SIEM) IBM QRADAR
COMMUNITY EDITION* DALAM MENDETEKSI
ANCAMAN DAN SERANGAN SIBER PADA *SERVER***

LAPORAN SKRIPSI

**POLITEKNIK
NEGERI
JAKARTA**

Gusana Adirosa

4617030017

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2021



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**ANALISIS KINERJA *SECURITY INFORMATION AND
EVENT MANAGEMENT (SIEM) IBM QRADAR
COMMUNITY EDITION* DALAM MENDETEKSI
ANCAMAN DAN SERANGAN SIBER PADA *SERVER***

LAPORAN SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk
Memperoleh Diploma Empat Politeknik**

**POLITEKNIK
NEGERI
Gusana Adirosa
4617030017
JAKARTA**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2021

HALAMAN PERNYATAAN ORISINALITAS

Skripsi/Tesis/Disertasi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Gusana Adirosa
NPM : 4617030017
Tanggal : 4 Juni 2021
Tanda Tangan : 



**POLITEKNIK
NEGERI
JAKARTA**

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Gusana Adirosa
NIM : 4617030017
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Kinerja *Security Information and Event Management (SIEM) IBM QRadar Community Edition* dalam Mendeteksi Ancaman dan Serangan Siber pada *Server*.

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 16, Bulan Juni, Tahun 2021 dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Defiana Arnaldy, S.Tp., M.Si. (.....)
Penguji I : Ayu Rosyida Zain, S.ST., M.T. (.....)
Penguji II : Indra Hermawan, S.Kom., M.Kom. (.....)
Penguji III : Muhammad Yusuf Bagus Rasyiidin, S.Kom., M.TI. (.....)

Mengetahui :
Jurusan Teknik Informatika dan Komputer
Ketua

Mauldy Laya, S.Kom., M.Kom.
NIP. 197802112009121003



KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Skripsi ini. Penulisan Skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik.

Skripsi ini berisi tentang penerapan aplikasi *Security Information and Event Management* dari IBM, yaitu IBM QRadar *Community Edition* dan melakukan analisis terhadap konfigurasi dan pendeteksian ancaman dan serangan siber yang mungkin terjadi terhadap *server*.

Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Defiana Arnaldy, S.Tp., M.Si., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini;
2. Hata Maulana, S.Si, M.TI, selaku kepala laboratorium jurusan Teknik Infomatika dan Komputer yang telah memberikan izin dalam menggunakan *harddisk drive* dan *Graphics Processing Unit (GPU)* komputer untuk melakukan kegiatan skripsi ini;
3. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan material dan moral; dan
4. Sahabat yang telah banyak membantu penulis dalam menyelesaikan skripsi ini.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu

Depok, 4 Juni 2021

Penulis.



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Gusana Adirosa
NIM : 4617030017
Program Studi : Teknik Multimedia dan Jaringan
Jurusan : Teknik Informatika dan Komputer
Jenis karya : Skripsi

demikian demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty- Free Right*)** atas karya ilmiah saya yang berjudul :

Analisis Kinerja *Security Information and Event Management* (SIEM) IBM QRadar *Community Edition* dalam Mendeteksi Ancaman dan Serangan Siber pada *Server* beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok Pada tanggal : 4 Juni 2021

Yang menyatakan

(Gusana Adirosa)

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

*Karya Ilmiah: karya akhir, makalah non seminar, laporan kerja praktek, laporan magang, karya profesi dan karya spesialis



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Analisis Kinerja *Security Information and Event Management (SIEM) IBM QRadar Community Edition* dalam Mendeteksi Ancaman dan Serangan Siber pada *Server*

Abstrak

Sistem keamanan menjadi kebutuhan untuk mendeteksi potensi ancaman dan serangan siber pada server. Kejadian yang berhubungan dengan ancaman dan serangan yang ditargetkan pada server akan menghasilkan log yang dapat dianalisis untuk selanjutnya dijadikan dasar pengambilan keputusan. *Security Information and Event Management (SIEM)* dapat memberikan informasi terhadap ancaman dan serangan keamanan pada server. *IBM QRadar Community Edition (CE)* merupakan produk *SIEM* gratis dengan fitur lengkap dan konfigurasi yang sederhana. Pada penelitian ini dilakukan rancang bangun, konfigurasi, dan analisis terhadap kinerja dari *QRadar CE*. Analisis dilakukan dengan mengevaluasi output *QRadar CE* setelah dilakukan pengujian konfigurasi *flow source* dan *log source*, simulasi *incorrect log in*, *port scanning*, *password cracking*, *denial of service*, dan eksploitasi *Metasploitable 3* dan pengukuran efektivitas berdasarkan identifikasi serangan sebagai *offense* dan deteksi log atau *network activity* sebagai bagian dari serangan. Didapatkan, instalasi *IBM QRadar CE* dilakukan dengan file *OVA* yang disediakan *IBM*. Untuk mendapatkan *network* dan *event activity* masing-masing harus dikonfigurasi *flow* dan *log source*. *Event* dikenal setelah diterima beberapa log. Tingkat efektivitas identifikasi serangan sebesar 20% dan deteksi serangan sebesar 100% dengan *log source Linux OS* dan *Windows Event Log*. Tidak terdapat perbedaan antara *OS* dengan basis yang sama (*Linux* dan *Windows*) dan antara versi lama dan baru.

Kata kunci: *Security Information and Event Management (SIEM)*, *IBM QRadar Community Edition*, ancaman siber, serangan siber, server

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS.....	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xviii
DAFTAR LAMPIRAN.....	xix
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan dan Manfaat.....	3
1.4.1 Tujuan.....	3
1.4.2 Manfaat.....	4
1.5 Metode Pelaksanaan Skripsi.....	4
BAB II.....	6
TINJAUAN PUSTAKA	6
2.1 Tinjauan Pustaka	6
2.1.1 Security Information and Event Management (SIEM).....	6

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.1.2 IBM QRadar dan IBM QRadar <i>Community Edition</i> (QRadar CE)	6
2.1.3 <i>Port Scanning</i>	8
2.1.4 <i>Password Cracking</i>	8
2.1.5 Serangan <i>Denial of Service</i> (DoS)	10
2.1.6 Metasploitable 3	10
2.1.7 Keamanan, Ancaman, dan Serangan Siber	11
2.1.8 <i>Server</i>	11
2.1.9 <i>Virtual Machine</i> (VM)	11
2.1.10 Hypervisor	12
2.1.11 Linux	12
2.1.12 <i>Windows Server</i>	13
2.2 Penelitian Terdahulu	13
BAB III	16
PERENCANAAN DAN REALISASI	16
3.1 Perancangan Infrastruktur	16
3.1.1 Deskripsi Infrastruktur	16
3.1.2 Topologi Jaringan	17
3.1.3 Spesifikasi Perangkat dan Software/Tools	17
3.3 Realisasi Infrastruktur	18
3.3.1 Instalasi IBM QRadar <i>Community Edition</i>	18
3.3.2 Konfigurasi <i>Flow Source</i> IBM QRadar <i>Community Edition</i>	25
3.3.3 Konfigurasi <i>Log Source</i> IBM QRadar <i>Community Edition</i>	28
BAB IV	36
PEMBAHASAN	36
4.1 Pengujian	36



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.2 Deskripsi Pengujian.....	36
4.3 Prosedur Pengujian.....	36
4.3.1 Pengamatan Hasil Konfigurasi <i>Flow Source</i> dan <i>Log Source</i>	37
4.3.2 <i>Incorrect Log In</i>	37
4.3.3 <i>Port Scanning</i>	38
4.3.4 <i>Password Cracking</i>	44
4.3.5 <i>Denial of Service (DoS)</i>	46
4.3.6 Eksploitasi Metasploitable 3.....	48
4.4 Data Hasil Pengujian.....	50
4.4.1 Data Pengujian Hasil Konfigurasi <i>Flow Source</i> dan <i>Log Source</i>	51
4.4.2 Data Pengujian <i>Incorrect Log In</i>	56
4.4.3 Data Pengujian <i>Port Scanning</i>	61
4.4.4 Data Pengujian <i>Password Cracking</i>	66
4.4.5 Data Pengujian <i>Denial of Service (DoS)</i>	78
4.4.6 Data Pengujian Eksploitasi Metasploitable 3.....	84
4.5 Analisis Data.....	86
4.5.1 Analisis Data Hasil Konfigurasi <i>Flow Source</i> dan <i>Log Source</i>	86
4.5.2 Analisis Data Pengujian Skenario Ancaman dan Penyerangan.....	89
BAB V.....	99
PENUTUP.....	99
5.1 Kesimpulan.....	99
5.2 Saran.....	100
DAFTAR PUSTAKA.....	101



DAFTAR GAMBAR

Gambar 2.1	Arsitektur SIEM	6
Gambar 2.2	Arsitektur QRadar	7
Gambar 2.3	Pemindaian Aktif Jaringan LAN	8
Gambar 2.4	Kemungkinan Alur Password Cracking	9
Gambar 2.5	Virtual Machine.....	12
Gambar 3.1	Topologi Jaringan.....	17
Gambar 3.2	Tampilan EULA CentOS 7	19
Gambar 3.3	Tampilan EULA IBM QRadar CE.....	20
Gambar 3.4	Persetujuan EULA IBM QRadar CE	20
Gambar 3.5	Konfigurasi Password Antarmuka Web IBM QRadar CE.....	21
Gambar 3.6	Tampilan Antarmuka Halaman Login Web IBM QRadar CE.....	21
Gambar 3.7	Persyaratan Lisensi IBM QRadar CE	21
Gambar 3.8	Tampilan Menu Dashboard IBM QRadar CE.....	22
Gambar 3.9	Tampilan Menu Dashboard IBM QRadar CE.....	22
Gambar 3.10	Tampilan Menu System and License Management IBM QRadar CE	23
Gambar 3.11	Tampilan Menu Admin	24
Gambar 3.12	Tampilan Menu System and License Management	24
Gambar 3.13	Tampilan Menu System Time pada Menu View and Manage System	25
Gambar 3.14	Tampilan Konfirmasi Menyimpan Konfigurasi Waktu	25
Gambar 3.15	Isi Konfigurasi File /etc/sysconfig/network-scripts/ifcfg-ens36	26
Gambar 3.16	Tampilan Isi dari File Konfigurasi Jaringan pada IBM QRadar CE.....	27
Gambar 3.17	Menu Admin, Flow Sources.....	27
Gambar 3.18	Konfigurasi Flow Source	28
Gambar 3.19	Pilihan Deploy Changes pada Menu Admin	28
Gambar 3.20	Tampilan Menu Admin	30
Gambar 3.21	Tampilan Menu Log Sources	30
Gambar 3.22	Konfigurasi Log Source Ubuntu 14.04 pada IBM QRadar CE	30

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 3.23 Konfigurasi Log Source Ubuntu 20.04 LTS pada IBM QRadar CE	31
Gambar 3.24 Konfigurasi Log Source CentOS 8 pada IBM QRadar CE.....	31
Gambar 3.25 Konfigurasi Log Source Debian 10 pada IBM QRadar CE.....	31
Gambar 3.26 Tipe Setup WinCollect	32
Gambar 3.27 Konfigurasi Log Source Windows pada WinCollect.....	33
Gambar 3.28 Konfigurasi Info Tujuan Koneksi WinCollect.....	33
Gambar 3.29 Instalasi WinCollect	34
Gambar 3.30 Konfigurasi Instalasi Patch WinCollect	34
Gambar 3.31 Instalasi Console Konfigurasi WinCollect.....	35
Gambar 3.32 Tampilan Console Konfigurasi WinCollect.....	35
Gambar 4.1 Flowchart Skenario Pengujian Pengamatan Hasil Konfigurasi	37
Gambar 4.2 Flowchart Skenario Pengujian Incorrect Log In	38
Gambar 4.3 Flowchart Skenario Pengujian Port Scanning	44
Gambar 4.4 Flowchart Skenario Pengujian Password Cracking	46
Gambar 4.5 Flowchart Skenario Pengujian Denial of Service	48
Gambar 4.6 Flowchart Skenario Pengujian Eksploitasi Metasploitable 3.....	50
Gambar 4.7 Tampilan Menu Dashboard.....	51
Gambar 4.8 Tampilan Menu Offenses.....	51
Gambar 4.9 Tampilan Menu Log Activity.....	52
Gambar 4.10 Tampilan Log yang Pertama Kali Masuk pada IBM QRadar CE... 52	
Gambar 4.11 Tampilan Menu Network Activity.....	52
Gambar 4.12 Grafik Jumlah Network Activity yang Masuk Setelah Konfigurasi Flow Source	52
Gambar 4.13 Tampilan Menu Network Activity	53
Gambar 4.14 Grafik Jumlah Network Activity yang Masuk Setelah Konfigurasi Log Source	53
Gambar 4.15 Log Activity Host 192.168.1.101 Setelah Konfigurasi Log Source 54	
Gambar 4.16 Event Log Activity Pertama Host 192.168.1.102 Setelah Konfigurasi Log Source	54

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.17 Log Activity Kedua Host 192.168.1.102 Setelah Konfigurasi Log Source.....	54
Gambar 4.18 Log Activity Pertama Host 192.168.1.103 Setelah Konfigurasi Log Source.....	54
Gambar 4.19 Log Activity Kedua Host 192.168.1.103 Setelah Konfigurasi Log Source.....	55
Gambar 4.20 Log Activity Pertama Host 192.168.1.104 Setelah Konfigurasi Log Source.....	55
Gambar 4.21 Log Activity Kedua Host 192.168.1.104 Setelah Konfigurasi Log Source.....	55
Gambar 4.22 Log Activity Host 192.168.1.105 Setelah Konfigurasi Log Source	55
Gambar 4.23 Log Activity Pertama Host 192.168.1.106 Setelah Konfigurasi Log Source.....	56
Gambar 4.24 Log Activity Kedua Host 192.168.1.106 Setelah Konfigurasi Log Source.....	56
Gambar 4.25 Tampilan Menu Dashboard Setelah Pengujian Incorrect Log In....	56
Gambar 4.26 Tampilan Menu Offenses Setelah Pengujian Incorrect Log In.....	57
Gambar 4.27 Log Activity Host 192.168.1.101 Setelah Pengujian Incorrect Log In.....	57
Gambar 4.28 Informasi Event Pertama Host 192.168.1.101 Setelah Pengujian Incorrect Log In.....	57
Gambar 4.29 Log Activity Host 192.168.1.102 Setelah Pengujian Incorrect Log In.....	58
Gambar 4.30 Informasi Event Pertama Host 192.168.1.102 Setelah Pengujian Incorrect Log In.....	58
Gambar 4.31 Log Activity Host 192.168.1.103 Setelah Pengujian Incorrect Log In.....	58
Gambar 4.32 Informasi Event Pertama Host 192.168.1.103 Setelah Pengujian Incorrect Log In.....	59



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.33 Log Activity Host 192.168.1.104 Setelah Pengujian Incorrect Log In 59

Gambar 4.34 Informasi Event Pertama Host 192.168.1.104 Setelah Pengujian Incorrect Log In..... 59

Gambar 4.35 Log Activity Host 192.168.1.105 Setelah Pengujian Incorrect Log In 60

Gambar 4.36 Informasi Event Pertama Host 192.168.1.105 Setelah Pengujian Incorrect Log In..... 60

Gambar 4.37 Log Activity Host 192.168.1.106 Setelah Pengujian Incorrect Log In 60

Gambar 4.38 Informasi Event Pertama Host 192.168.1.106 Setelah Pengujian Incorrect Log In..... 61

Gambar 4.39 Tampilan Menu Dashboard Setelah Pengujian Port Scanning..... 61

Gambar 4.40 Tampilan Menu Offenses Setelah Pengujian Port Scanning..... 61

Gambar 4.41 Log Activity Semua Host Setelah Pengujian Port Scanning Tipe 1 62

Gambar 4.42 Log Activity Host 192.168.1.101 Setelah Pengujian Port Scanning Tipe 2 62

Gambar 4.43 Informasi Event Pertama Host 192.168.1.101 Setelah Pengujian Port Scanning Tipe 2..... 62

Gambar 4.46 Log Activity Host 192.168.1.102 Setelah Pengujian Port Scanning Tipe 2 63

Gambar 4.45 Informasi Event Pertama Host 192.168.1.102 Setelah Pengujian Port Scanning Tipe 2..... 63

Gambar 4.46 Log Activity Host 192.168.1.103 Setelah Pengujian Port Scanning Tipe 2 63

Gambar 4.47 Informasi Event Pertama Host 192.168.1.103 Setelah Pengujian Port Scanning Tipe 2..... 64

Gambar 4.48 Log Activity Host 192.168.1.104 Setelah Pengujian Port Scanning Tipe 2 64



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.49 Informasi Event Pertama Host 192.168.1.104 Setelah Pengujian Port Scanning Tipe 2.....	65
Gambar 4.50 Log Activity Host 192.168.1.105 Setelah Pengujian Port Scanning Tipe 2	65
Gambar 4.51 Informasi Event Pertama Host 192.168.1.105 Setelah Pengujian Port Scanning Tipe 2.....	65
Gambar 4.52 Log Activity Host 192.168.1.106 Setelah Pengujian Port Scanning Tipe 2	65
Gambar 4.53 Informasi Event Pertama Host 192.168.1.106 Setelah Pengujian Port Scanning Tipe 2.....	66
Gambar 4.54 Event Log Semua Host Setelah Pengujian Port Scanning Tipe 3 ...	66
Gambar 4.55 Tampilan Menu Dashboard Setelah Pengujian Password Cracking	67
Gambar 4.56 Tampilan 2 Menu Dashboard Setelah Pengujian Password Cracking	67
Gambar 4.57 Tampilan Menu Offenses Setelah Pengujian Password Cracking ..	68
Gambar 4.58 Log Activity Host 192.168.1.101 Setelah Pengujian Password Cracking	68
Gambar 4.59 Informasi Event Pertama Host 192.168.1.101 Setelah Pengujian Password Cracking.....	69
Gambar 4.60 Informasi Custom Rule Engine Pertama Host 192.168.1.101 Setelah Pengujian Password Cracking.....	69
Gambar 4.61 Log Activity Host 192.168.1.102 Setelah Pengujian Password Cracking	70
Gambar 4.62 Informasi Event Pertama Host 192.168.1.102 Setelah Pengujian Password Cracking.....	70
Gambar 4.63 Informasi Custom Rule Engine Pertama Host 192.168.1.102 Setelah Pengujian Password Cracking.....	70
Gambar 4.64 Log Activity Host 192.168.1.103 Setelah Pengujian Password Cracking	71



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.65 Informasi Event Pertama Host 192.168.1.103 Setelah Pengujian Password Cracking.....	71
Gambar 4.66 Informasi Custom Rule Engine Pertama Host 192.168.1.103 Setelah Pengujian Password Cracking.....	72
Gambar 4.67 Log Activity Host 192.168.1.104 Setelah Pengujian Password Cracking.....	73
Gambar 4.68 Informasi Event Pertama Host 192.168.1.104 Setelah Pengujian Password Cracking.....	73
Gambar 4.69 Informasi Custom Rule Engine Pertama Host 192.168.1.104 Setelah Pengujian Password Cracking.....	74
Gambar 4.70 Log Activity Host 192.168.1.105 Setelah Pengujian Password Cracking.....	75
Gambar 4.71 Informasi Event Pertama Host 192.168.1.105 Setelah Pengujian Password Cracking.....	75
Gambar 4.72 Informasi Custom Rule Engine Pertama Host 192.168.1.105 Setelah Pengujian Password Cracking.....	76
Gambar 4.73 Log Activity Host 192.168.1.106 Setelah Pengujian Password Cracking.....	77
Gambar 4.74 Informasi Event Pertama Host 192.168.1.106 Setelah Pengujian Password Cracking.....	77
Gambar 4.75 Informasi Custom Rule Engine Pertama Host 192.168.1.106 Setelah Pengujian Password Cracking.....	78
Gambar 4.76 Network Activity Host 192.168.1.101 Setelah Pengujian Denial of Service (DoS).....	79
Gambar 4.77 Informasi Network Activity Pertama Host 192.168.1.101 Setelah Pengujian Denial of Service (DoS).....	79
Gambar 4.78 Network Activity Host 192.168.1.102 Setelah Pengujian Denial of Service (DoS).....	80
Gambar 4.79 Informasi Network Activity Pertama Host 192.168.1.102 Setelah Pengujian Denial of Service (DoS).....	80



Gambar 4.80 Network Activity Host 192.168.1.103 Setelah Pengujian Denial of Service (DoS).....	81
Gambar 4.81 Informasi Network Activity Pertama Host 192.168.1.103 Setelah Pengujian Denial of Service (DoS).....	81
Gambar 4.82 Network Activity Host 192.168.1.104 Setelah Pengujian Denial of Service (DoS).....	82
Gambar 4.83 Informasi Network Activity Pertama Host 192.168.1.104 Setelah Pengujian Denial of Service (DoS).....	82
Gambar 4.84 Network Activity Host 192.168.1.105 Setelah Pengujian Denial of Service (DoS).....	83
Gambar 4.85 Informasi Network Activity Pertama Host 192.168.1.105 Setelah Pengujian Denial of Service (DoS).....	83
Gambar 4.86 Network Activity Host 192.168.1.106 Setelah Pengujian Denial of Service (DoS).....	84
Gambar 4.87 Informasi Network Activity Pertama Host 192.168.1.106 Setelah Pengujian Denial of Service (DoS).....	84
Gambar 4.88 Log Activity Host 192.168.1.101 Setelah Pengujian Eksploitasi Metasploitable 3.....	85
Gambar 4.89 Informasi Network Activity Pertama Host 192.168.1.101 Setelah Pengujian Eksploitasi Metasploitable 3.....	85
Gambar 4.90 Informasi Network Activity Kedua Host 192.168.1.101 Setelah Pengujian Eksploitasi Metasploitable 3.....	85
Gambar 4.91 Log Activity Host 192.168.1.102 Setelah Pengujian Eksploitasi Metasploitable 3.....	86
Gambar 4.92 Informasi Event Pertama Host 192.168.1.102 Setelah Pengujian Eksploitasi Metasploitable 3.....	86

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR TABEL

Tabel 1. Shell Script Pengujian Port Scanning	39
Tabel 2. Shell Script Pengujian Password Cracking	44
Tabel 3. Shell Script Pengujian Denial of Service	47
Tabel 4. Perintah Pengujian Metasploitable 3 - Ubuntu 14.04	49
Tabel 5. Perintah Pengujian Metasploitable 3 - Windows Server 2008	49
Tabel 6. Pengamatan Hasil Konfigurasi Flow Source	87
Tabel 7. Pengamatan Hasil Konfigurasi Log Source	88
Tabel 8. Output IBM QRadar CE pada Tiap Skenario Pengujian Serangan	89
Tabel 9. Perbandingan Output IBM QRadar CE pada Skenario Pengujian Incorrect Log In	90
Tabel 10. Perbandingan Output IBM QRadar CE pada Skenario Pengujian Port Scanning Tipe 2	92
Tabel 11. Perbandingan Output IBM QRadar CE pada Skenario Pengujian Password Cracking	93
Tabel 12. Perbandingan Output IBM QRadar CE pada Skenario Pengujian Denial of Service (DoS)	95
Tabel 13. Perbandingan Output IBM QRadar CE pada Skenario Pengujian Eksploitasi Metasploitable 3	97

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

DAFTAR LAMPIRAN

L-1 Daftar Riwayat Hidup Penulis.....	104
---------------------------------------	-----



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang

Penggunaan komputer dan teknologi internet terus bertambah pada abad ke-21 dan dalam penggunaannya pun banyak sistem server dan komputer yang menyimpan dan memproses data yang sensitif dan sangat penting bagi suatu organisasi atau individu. Banyaknya jumlah data yang sensitif ini menyebabkan bertambahnya serangan siber. Pada bulan September 2020 jumlah pembobolan data dan serangan siber menyentuh rekor jumlah serangan tertinggi dengan angka 267 juta serangan (IT Governance, 2020).

Untuk melindungi *server* dan perangkat komputer dibutuhkan sistem keamanan yang dapat mendeteksi adanya aktifitas mencurigakan yang memiliki potensi sebagai bentuk dari ancaman dan serangan siber (Goodall, et al., 2018). Isu utama dalam mendeteksi serangan siber ini adalah infrastruktur teknologi informasi (TI) yang harus dilindungi biasanya berjumlah sangat banyak sehingga proses analisis *log* yang dihasilkan oleh infrastruktur TI untuk mendapatkan kesimpulan atau keputusan yang tepat sangatlah rumit.

SIEM (*Security Information and Event Management*) dapat digunakan untuk mengatasi masalah tersebut. SIEM dapat mengumpulkan data yang dihasilkan oleh infrastruktur TI dan melakukan *profiling* berdasarkan data tersebut untuk memudahkan dalam melakukan pendeteksian ancaman dan serangan dengan mencocokkan dengan pola yang ada (Lee, et al., 2017). Penggunaan SIEM membutuhkan keterampilan untuk melakukan analisis lebih lanjut terhadap data dari SIEM. Oleh karena itu pada perusahaan – perusahaan besar, data yang dihasilkan SIEM selanjutnya diproses oleh *security analyst* yang berada pada sebuah SOC (*Security Operations Centre*).



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Terdapat banyak jenis aplikasi SIEM yang tersedia dan menawarkan fitur yang berbeda-beda sesuai dengan kebutuhan penggunanya. Penelitian ini akan menggunakan salah satu aplikasi SIEM gratis, yaitu IBM QRadar *Community Edition* dikarenakan banyaknya fitur yang membuat aplikasi ini menjadi sangat *powerful* dan juga dokumentasi yang terdapat dari *website* IBM. Penelitian ini memiliki tujuan untuk menerapkan IBM QRadar *Community Edition* dan juga melakukan analisis kinerja dengan menentukan pengaturan yang ada untuk melakukan pendeteksian ancaman dan serangan siber secara *real-time*.

1.2 Perumusan Masalah

Rumusan masalah yang terdapat pada Analisis Kinerja *Security Information and Event Management (SIEM) IBM QRadar Community Edition* dalam Mendeteksi Ancaman dan Serangan Siber pada *Server* adalah:

- a. Bagaimana proses rancang bangun aplikasi SIEM IBM QRadar *Community Edition*;
- b. Bagaimana konfigurasi yang harus dilakukan agar aplikasi SIEM IBM QRadar *Community Edition* dapat memulai pendeteksian ancaman dan serangan siber;
- c. Bagaimana efektivitas aplikasi SIEM IBM QRadar *Community Edition* dalam mendeteksi dan mengidentifikasi ancaman dan serangan siber pada *server* dengan sistem operasi *Windows Server* dan *Linux*.

1.3 Batasan Masalah

Dalam realisasi, penelitian ini dibatasi beberapa hal sebagai berikut:

- a. Menggunakan 1 *router*, 1 perangkat komputer, dan 2 laptop.
- b. Aplikasi virtualisasi pada komputer dan laptop 1 menggunakan VMWare Workstation Pro versi 15.5 dan laptop 2 menggunakan Oracle VM Virtual Box versi 6.1.16 dengan *Windows 10* sebagai *host* sistem operasinya.
- c. Menggunakan masing-masing 1 sistem operasi jaringan dari Metasploitable 3 berbasis *Ubuntu 14.04* dan Metasploitable 3 berbasis *Windows Server 2008*, *Ubuntu 20.04 LTS*, *CentOS 8*, *Debian 10*, *Windows Server 2012 R2*



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- yang dipasang sebagai *virtual machine* pada komputer dan laptop 2 yang digunakan sebagai *host* yang diserang.
- d. *Service firewall* pada semua sistem operasi dinonaktifkan dan terdapat *service SSH* atau *remote desktop* dan *Web Service* pada setiap sistem operasi jaringan.
 - e. Menggunakan sistem operasi Kali Linux versi 2018.2 untuk penyerang yang dipasang sebagai *virtual machine* pada laptop.
 - f. Konfigurasi yang dilakukan pada IBM QRadar *Community Edition* hanya sebatas *flow source* dan *log source*-nya.
 - g. Konfigurasi *flow source* sebatas konfigurasi *internal flow source* untuk mengumpulkan paket data lalu lintas jaringan pada jaringan lokal (LAN).
 - h. Konfigurasi *log source* sebatas konfigurasi *log source* Linux OS dengan menggunakan Rsyslog pada sistem operasi berbasis Linux dan Microsoft Windows *Security Event Log* dengan menggunakan WinCollect v7.3.0-41 pada sistem operasi berbasis Windows.
 - i. *Data network activity* hanya dianalisis jika tidak ada data atau sedikitnya *log source* yang masuk pada IBM QRadar *Community Edition*.
 - j. Tingkat efektivitas diukur dengan parameter terdeteksi dan teridentifikasi ancaman dan serangan pada IBM QRadar *Community Edition* setelah pengujian dilakukan.
 - k. Deteksi ancaman dan serangan diketahui dengan munculnya *event* atau *network activity* dengan informasi yang berkaitan dengan pengujian yang dilakukan.
 - l. Identifikasi ancaman diketahui dengan dikenalnya pengujian sebagai *offense* oleh IBM QRadar *Community Edition*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dilakukannya kegiatan ini adalah untuk melakukan rancang bangun, konfigurasi, dan analisis kinerja aplikasi SIEM IBM QRadar *Community Edition* dalam mendeteksi dan mengidentifikasi ancaman dan serangan siber yang ditargetkan pada *server* dengan sistem operasi berbasis Windows Server dan Linux.



1.4.2 Manfaat

Manfaat dari analisis aplikasi SIEM IBM QRadar *Community Edition* adalah untuk mengetahui bagaimana cara konfigurasi yang harus dilakukan agar IBM QRadar *Community Edition* dapat melakukan pendeteksian ancaman dan serangan siber pada *server* dan seberapa efektif aplikasi IBM QRadar *Community Edition* dalam melakukan pendeteksian dan pengidentifikasian ancaman dan serangan pada *server* dengan sistem operasi Windows *Server* dan Linux.

1.5 Metode Pelaksanaan Skripsi

Penelitian ini dilakukan dengan melakukan rancang bangun dari aplikasi dan juga meneliti hubungan sebab akibat dari variabel yang ada untuk mendapatkan hasil yang akurat. Tahapan penelitian yang dilakukan adalah sebagai berikut:

1. Studi Literatur
Studi literatur dilakukan untuk mengumpulkan data dari buku, jurnal penelitian, dan jurnal prosiding konferensi tentang informasi yang terkait dengan masalah pada topik penelitian.
2. Perancangan infrastruktur
Infrastruktur yang dirancang terdiri atas jaringan, komputer, laptop, dan *virtual machine*.
3. Rancang bangun infrastruktur
Dibuat *virtual machine* dengan OS Linux dan Windows *Server* pada komputer yang disiapkan untuk *server* yang diuji.
4. Rancang bangun aplikasi
Aplikasi IBM QRadar *Community Edition* di-*install* sebagai *virtual machine* menggunakan VMWare Workstation Pro yang di-*install* pada laptop 1 sesuai dengan topologi yang disiapkan.
5. Pengujian
Pengujian dilakukan dengan cara melakukan pengamatan sebelum dan sesudah konfigurasi *flow source* dan *log source*, serta dilakukan penyerangan terhadap semua *server* yang berada pada jaringan.
6. Analisis Hasil Pengujian

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Data yang didapat dari pengujian dicatat dan dilakukan analisis untuk mendapatkan kesimpulan dari penelitian yang dilakukan.

7. Penyusunan Laporan Penelitian

Laporan penelitian dilakukan setelah seluruh penelitian selesai dengan mengikuti pedoman yang ditetapkan oleh panitia skripsi Jurusan Teknik Informatika dan Komputer. Pembuatan laporan penelitian akan dibimbing oleh dosen pembimbing dan juga pakar serta kegiatan pengerjaan didokumentasikan dalam bentuk foto, video, maupun media lain.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang sudah dilakukan dapat diambil kesimpulan sebagai berikut:

- a. Aplikasi SIEM IBM QRadar *Community Edition* dapat di-*install* dengan melakukan instalasi menggunakan *file* OVA yang merupakan sistem operasi CentOS 7 berisi *file* instalasi QRadar yang terdapat pada *website* IBM.
- b. Konfigurasi *flow source* diperlukan untuk menangkap *network activity* pada jaringan.
- c. Konfigurasi *log source* diperlukan untuk menangkap *log* dari perangkat *server*.
- d. *Event* dari *log source* dapat diproses oleh IBM QRadar CE setelah terdapat cukup *log* yang dikirimkan oleh *host*, sehingga membuat waktu kemunculan *event* (yang diketahui isinya oleh IBM QRadar CE) memiliki waktu yang bervariasi.
- e. Konfigurasi *internal flow source*, *log source* Linux OS, dan Windows *Event Log* hanya memberikan tingkat efektivitas 20% dalam mengidentifikasi serangan karena hanya serangan *password cracking* yang dapat dikenali oleh IBM QRadar CE, sedangkan tingkat efektivitas dari pendeteksian serangan adalah 100%.
- f. Dua jenis *log source* yang digunakan hanya dapat mengidentifikasi ancaman dan serangan yang berbasis otentikasi *user*.
- g. Tidak ada perbedaan *output* IBM QRadar CE pada versi Linux yang berbeda (Ubuntu, CentOS, dan Debian) dan pada sistem operasi yang memiliki versi lebih tua seperti Metasploitable 3 Ubuntu 14.04 dan Metasploitable 3 Windows *Server* 2008, dengan sistem operasi dengan versi yang lebih baru seperti Ubuntu 20.04 LTS, CentOS 8, Debian 10, dan Windows *Server* 2012 R2.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- h. IBM QRadar CE dapat mendeteksi dan mengidentifikasi dengan cepat ancaman dan serangan yang terjadi pada *server* dengan waktu di bawah 1 sampai 2 menit dari penyerangan dimulai.

5.2 Saran

Penelitian ini dilakukan dengan kondisi perangkat keras dan waktu yang terbatas sehingga terdapat saran yang dapat diterapkan, yaitu:

- a. Dilakukan penelitian lebih lanjut untuk melihat data yang didapat apabila ditambahkan skenario pengujian dimana penyerang dan *host* yang diserang berada pada jaringan yang berbeda.
- b. Penelitian terhadap IBM QRadar CE dengan menggunakan atau menambahkan *log source* lainnya seperti IDPS ataupun perangkat *firewall* dapat dilakukan untuk mengukur tingkat kinerja dari IBM QRadar CE dalam mendeteksi ancaman dan serangan.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR PUSTAKA

- Arfanudin, C., Sugiantoro, B. & Prayudi, Y., 2019. "Analisis Serangan Router dengan Security Information and Event Management (SIEM) dan Implikasinya pada Indeks Keamanan Informasi". *CyberSecurity dan Forensik Digital*, 2(1), 1-7.
- Aziz, A. & Tarkono, A., 2016. "Teknologi Virtualisasi Openvz dan Kernel-Based Virtual Machine sebagai Layanan IaaS pada Jaringan Enterprise". *Jurnal Multitenics*, 2(1), 24-30.
- Birkinshaw, C., Rouka, E. & Vassilakis, V. G., 2019. "Implementing an Intrusion Detection and Prevention System Using Software-Defined Networking: Defending Against Port-Scanning and Denial-of-Service Attacks". *Journal of Network and Computer Applications*, 136(1), 71-85.
- Dauti, B., 2019. *Windows Server 2019 Administration Fundamentals*. 2nd ed. Birmingham: Packt Publishing Ltd.
- Fratini, F., Giordano, U. & Conti, V., 2019, September. *Facing Cyber-Physical Security Threats by PSIM-SIEM Integration*. Paper presented at the 2019 15th European Dependable Computing Conference (EDCC), Naples, Italia.
- Goodall, J. R. et al., 2018. "Situ: Identifying and Explaining Suspicious Behavior in Networks". *IEEE Transactions on Visualization and Computer Graphics*, 25(1), 204-214.
- Gupta, S., Chaudhari, B. S. & Chakrabarty, B., 2016, Agustus. *Vulnerable network analysis using war driving and security intelligence*. Paper presented at the 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India.
- Hasani, S. & Dode, A., 2016, Desember. *Network Security Through Vulnerability Analysis*. Paper presented at the Eleventh International Scientific Conference, Bansko, Bulgaria.
- Humayun, M. et al., 2020. "Cyber Security Threats and Vulnerabilities: A Systematic Mapping". *Arabian Journal for Science and Engineering*, 45(1), 3171-3189.
- IBM, 2020. IBM Security QRadar Community Edition. <https://www.ibm.com/community/qradar/ce>. [13 Januari 2021].

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumikan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- IBM, 2020. IBM Support. <https://www.ibm.com/support/pages/node/6395080>. [12 Mei 2021].
- IBM, 2021. IBM Configuring System Time Documentation. <https://www.ibm.com/docs/en/qsip/7.3.3?topic=time-configuring-system>. [12 Mei 2021].
- IBM, 2021. IBM QRadar on Cloud Documentation. <https://www.ibm.com/docs/en/qradar-on-cloud?topic=wincollect-overview>. [16 Mei 2021].
- IBM, 2021. IBM Types of Flow Sources Documentation. <https://www.ibm.com/docs/en/qsip/7.3.3?topic=sources-types-flow>. [14 Mei 2021].
- IT Governance, 2020. IT Governance. <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-september-2020>. [8 Oktober 2020].
- Kakarla, T., Mairaj, A. & Javaid, A. Y., 2018, May. *A Real-world Password Cracking Demonstration Using Open Source Tools for Instructional Use*. Paper presented at the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA.
- Lee, J., Kim, Y. S., Kim, J. H. & Kim, I. K., 2017, Oktober. *Toward the SIEM Architecture for Cloud-Based Security Services*. Paper presented at the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA.
- Lulu, L., Kai, Z., Qiankun, S. & Xin, H., 2016, Desember. *A Denial of Service Attack Method for an IoT System*. Paper presented at the 2016 8th International Conference on Information Technology in Medicine and Education (ITME), Fuzhou, China.
- Murari, G., 2020, Desember. *Exploiting the Vulnerabilities on Metasploit 3(Ubuntu) Machine Using Metasploit Framework and Methodologies*, Edmonton: Faculty of Graduate Studies, Concordia University of Edmonton.
- Prakoso, R. D. & Asmunin, 2018. "Implementasi dan Perbandingan Performa Proxmox dalam Virtualisasi dengan Tiga Virtual Server". *Jurnal Manajemen Informatika*, 8(1), 79-85.
- Shah, M. et al., 2019, Januari. *Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool*. Paper presented at the 2019 2nd



© Hak Cipta milik Politeknik Negeri Jakarta

International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan.

Sharma, H., 2020. Desember. *Exploiting Vulnerabilities of Metasploitable 3 (Windows) Using Metasploit Framework*, Edmonton: Faculty of Graduate Studies, Concordia University of Edmonton.

Sornalakshmi, K., 2017, Juni. *Detection of DoS Attack and Zero Day Threat with SIEM*. Paper presented at the 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India.

Wang, P. S., 2018. *Mastering Modern Linux Second Edition*. 2nd ed. Boca Raton: CRC Press Taylor & Francis Group.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 1 L-1 Daftar Riwayat Hidup Penulis

DAFTAR RIWAYAT HIDUP



Penulis bernama Gusana Adirosa lahir di Jakarta, 3 Agustus 1999. Merupakan anak kedua dari dua bersaudara. Penulis bertempat tinggal di Jalan Kenari 1 Perumahan Bojong Depok Baru 2, Kelurahan Sukahati, Kecamatan Cibinong, Kabupaten Bogor. Penulis menyelesaikan sekolah dasar di SD Negeri Cipayang 1 pada tahun 2011. Menyelesaikan pendidikan sekolah menengah pertama di SMP Negeri 19 Bogor pada tahun 2014 dan pendidikan sekolah menengah atas di SMA Negeri 2 Bogor pada tahun 2017. Hingga sampai penulisan skripsi ini, penulis masih terdaftar sebagai mahasiswa aktif program Diploma 4 di Politeknik Negeri Jakarta.

**POLITEKNIK
NEGERI
JAKARTA**