



**IMPLEMENTASI IBM QRADAR *COMMUNITY EDITION*
SEBAGAI *SECURITY INFORMATION AND EVENT
MANAGEMENT (SIEM)* UNTUK DETEKSI ANCAMAN
DAN SERANGAN SIBER**

LAPORAN TUGAS AKHIR

**UNIVERSITAS
MERCU BUANA**
MOHAMAD REZA AL FATAH
41520010183

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA 2024**



**IMPLEMENTASI IBM QRADAR *COMMUNITY EDITION*
SEBAGAI *SECURITY INFORMATION AND EVENT
MANAGEMENT* (SIEM) UNTUK DETEKSI ANCAMAN
DAN SERANGAN SIBER**

LAPORAN TUGAS AKHIR

MOHAMAD REZA AL FATAH

41520010183

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA 2024**

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Mohamad Reza Al Fatah
NIM : 41520010183
Program Studi : Teknik Informatika
Judul Proposal Penelitian : Implementasi IBM QRadar *Community Edition*
Sebagai *Security Information and Event Management* (SIEM) Untuk Deteksi Ancaman dan Serangan Siber

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.



Jakarta, 14 Juli 2024



Mohamad Reza Al Fatah

UNIVERSITAS
MERCU BUANA

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh :

Nama : Mohamad Reza Al Fatah

NIM : 41520010183

Program Studi : Teknik Informatika

Judul Laporan Skripsi : Implementasi IBM QRadar Community Edition Sebagai Security Information and Event Management (SIEM) Untuk Deteksi Ancaman dan Serangan Siber

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar sarjana Strata I pada Program Studin Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Disahkan oleh:

Pembimbing : Lukman Hakim, ST., M. Kom

NIDN : 327107701

Ketua Penguji : Prastika Indriyanti, S.Kom., M.Cs

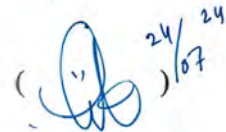
NIDN : 312089401

Penguji 1 : Muhammad Rifqi, S.Kom., M.Kom

NIDN : 301067101

Penguji 2 : Dr. Misbahul Fajri, M.TI

NIDN : 306077203



Jakarta, 22 Juli 2024

Mengetahui,

Dekan

Ketua Program Studi



Dr.Bambang Jokonowo, S.Si.,M.T.I

NIDN 320037002



Dr.Hadi Santoso, S.Kom, M.Kom

NIDN 225067701

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT, Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Laporan Skripsi ini. Penulisan Laporan Skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer pada Fakultas Ilmu Komputer Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan Laporan Skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof.Dr.Ir. Andi Adriansyah, M/Eng selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom sebagai Ketua Program Studi Teknik Informatika.
4. Bapak Lukman Hakim, ST., M.Kom selaku Dosen Pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.
5. Kepada orang tua yang telah memberikan dukungan serta motivasi agar saya bisa menjadi sarjana yang terbaik.

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

Jakarta, 14 Juli 2023


Mohamad Reza Al Fatah

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama : Mohamad Reza Al Fatah
NIM : 415200100183
Program Studi : Teknik Informatika
Judul Proposal Penelitian : Implementasi Ibm Qradar Community Edition
Sebagai Security Information And Event
Management (Siem) Untuk Deteksi Ancaman Dan
Serangan Siber

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 14 Juli 2024

Yang Menyatakan,



Mohamad Reza Al Fatah

ABSTRAK

Nama : Mohamad Reza Al Fatah
NIM : 41520010183
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Implementasi IBM QRadar Community Edition Sebagai Security Information and Event Management (SIEM) Untuk Deteksi Ancaman dan Serangan Siber
Pembimbing : Lukman Hakim, ST., M. Kom

Keamanan siber adalah elemen penting dalam manajemen infrastruktur teknologi informasi, terutama dengan meningkatnya frekuensi dan kompleksitas serangan siber. Penelitian ini bertujuan untuk mengaplikasikan IBM QRadar *Community Edition* sebagai platform *Security Information and Event Management* (SIEM) untuk mendeteksi ancaman dan serangan siber pada server. IBM QRadar *Community Edition* menawarkan solusi yang terintegrasi untuk mengumpulkan, menganalisis, dan mengkorelasikan data log dari berbagai sumber guna mengidentifikasi aktivitas mencurigakan dan memberikan peringatan dini. Metode penelitian ini meliputi instalasi dan konfigurasi IBM QRadar *Community Edition* pada mesin virtual, pengaturan sumber aliran data untuk mengumpulkan data dari server Linux, serta pembuatan aturan untuk mendeteksi ancaman tertentu. Pengujian dilakukan dengan mensimulasikan serangan siber untuk menilai efektivitas deteksi dan respons SIEM. Hasil penelitian menunjukkan bahwa IBM QRadar *Community Edition* dapat mendeteksi berbagai jenis serangan siber secara *real-time* dan memberikan peringatan yang dapat digunakan oleh administrator untuk mengambil tindakan mitigasi. Implementasi SIEM menggunakan IBM QRadar *Community Edition* terbukti meningkatkan visibilitas dan respons terhadap ancaman siber, serta membantu organisasi dalam mengelola keamanan jaringan dengan lebih proaktif dan efisien. Penelitian ini memberikan kontribusi yang signifikan dalam bidang keamanan siber, khususnya dalam penerapan solusi SIEM untuk mendeteksi dan merespons ancaman di lingkungan server.

Kata Kunci: Keamanan Siber, IBM QRadar *Community Edition*, *Security Information and Event Management* (SIEM), Deteksi Ancaman, Serangan Siber, Analisis Keamanan.

ABSTRACT

Nama : Mohamad Reza Al Fatah
NIM : 41520010183
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Implementasi IBM QRadar Community Edition Sebagai Security Information and Event Management (SIEM) Untuk Deteksi Ancaman dan Serangan Siber
Pembimbing : Lukman Hakim, ST., M. Kom

Cybersecurity is a crucial element in managing information technology infrastructure, especially with the increasing frequency and complexity of cyberattacks. This study aims to apply IBM QRadar Community Edition as a Security Information and Event Management (SIEM) platform to detect threats and cyberattacks on servers. IBM QRadar Community Edition offers an integrated solution to collect, analyze, and correlate log data from various sources to identify suspicious activity and provide early warnings. The research methodology includes the installation and configuration of IBM QRadar Community Edition on a virtual machine, setting up data flow sources to collect data from Linux servers, and creating rules to detect specific threats. Testing was conducted by simulating cyberattacks to evaluate the effectiveness of SIEM's detection and response capabilities. The study results show that IBM QRadar Community Edition can detect various types of cyberattacks in real-time and provide alerts that administrators can use to take mitigation actions. Implementing SIEM using IBM QRadar Community Edition has proven to enhance visibility and response to cyber threats, helping organizations manage network security more proactively and efficiently. This study makes a significant contribution to the field of cybersecurity, particularly in the application of SIEM solutions to detect and respond to threats in server environments.

Keywords: *Cybersecurity, IBM QRadar Community Edition, Security Information and Event Management (SIEM), Threat Detection, Cyber Attacks, Security Analysis.*

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERNYATAAN KARYA SENDIRI	ii
HALAMAN PENGESAHAN	iii
KATA PENGANTAR.....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian	3
1.4 Manfaat Penelitian	3
1.5 Batasan Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	5
2.1 Penelitian Terdahulu.....	5
2.2 Teori Pendukung	24
2.2.1 Security Information and Event Management (SIEM)	24
2.2.2 IBM QRadar Community Edition	24
2.2.3 Port Scanning.....	25
2.2.4 Distributed Denial of Service (DDoS).....	25
2.2.5 SSH BruteForce	25
2.2.6 Keamanan Siber	25
BAB III METODE PENELITIAN	27
3.1 Jenis Penelitian	27
3.2 Tahapan Penelitian.....	27
3.2.1 Studi Literatur	28

3.2.2 Analisis Sistem	28
3.2.3 Analisa Kebutuhan.....	29
3.2.4 Perancangan Jaringan	29
3.2.5 Instalasi IBM QRadar Community Edition	30
3.2.6 Pengujian.....	31
3.2.7 Hasil Pengujian.....	32
3.2.8 Analisis Hasil Pengujian	32
3.2.9 Pembuatan Laporan Akhir	33
BAB IV HASIL DAN PEMBAHASAN.....	34
4.1 Konfigurasi	34
4.1.1 Konfigurasi VMware	34
4.1.2 Instalasi IBM QRadar Community Edition	34
4.1.3 Instalasi PC Target.....	45
4.1.4 Instalasi PC Penyerang.....	50
4.2 Hasil Pengujian	53
4.2.1 Port Scanning	53
4.2.2 Distributed Denial of Service (DDoS).....	56
4.2.3 SSH BruteForce.....	61
BAB V PENUTUP	65
5.1 Kesimpulan	65
5.2 Saran	65
DAFTAR PUSTAKA.....	66
LAMPIRAN.....	69



DAFTAR GAMBAR

GAMBAR 1. TAHAPAN PENELITIAN	28
GAMBAR 2. CONTOH ARSITEKTUR JARINGAN	30
GAMBAR 3. ALUR PENYERANGAN	31
GAMBAR 4. HASIL SIMULASI YANG TERBACA DI LOG ACTIVITY	32
GAMBAR 5. HASIL SIMULASI YANG TERBACA DI NETWORK ACTIVITY	32
GAMBAR 6. DOWNLOAD FILE ISO QRADAR COMMUNITY EDITION	35
GAMBAR 7. MEMBUAT VIRTUAL MACHINE YANG BARU.....	35
GAMBAR 8. PILIH FILE ISO	36
GAMBAR 9. MASUKAN NAMA UNTUK VIRTUAL MACHINE	37
GAMBAR 10. PILIH KAPASITAS PENYIMPANAN.....	38
GAMBAR 11. TAMPILAN SPESIFIKASI VIRTUAL MACHINE	39
GAMBAR 12. TAMPILAN SETELAH MEMBUAT VIRTUAL MACHINE	39
GAMBAR 13. TAMPILAN PILIHAN BOOT OS.....	40
GAMBAR 14. MENGATUR LOGIN MENJADI ROOT DAN	40
GAMBAR 15. MELAKUKAN INSTALASI PACKAGE YANG SUDAH DI SEDIAKAN	40
GAMBAR 16. TAMPILAN KEBIJAKAN DAN LISENSI.....	41
GAMBAR 17. PILIHAN UNTUK MENGINSTALL PACKAGE	41
GAMBAR 18. MASUKAN KATA SANDI UNTUK PERGI KE KONSOL QRADAR.....	42
GAMBAR 19. PERINGATAN SETELAH PERGI KE KONSOL QRADAR	43
GAMBAR 20. MASUKAN NAMA PENGGUNA DAN KATA SANDI	43
GAMBAR 21. TAMPILAN KONSOL QRADAR COMMUNITY EDITION	44
GAMBAR 22. MEMBUAT ATURAN BARU	44
GAMBAR 23. MEMBUAT DAN MEMILIH EVENT UNTUK RULE	45
GAMBAR 24. UNTUK MEMUNCULKAN NOTIFIKASI BAHWA ADA TERJADI SERANGAN.....	45
GAMBAR 25. FILE QRADAR.....	46
GAMBAR 26. MEMBUAT NAMA VIRTUAL MACHINE.....	46
GAMBAR 27. TAMPILAN UNTUK MENJALANKAN VIRTUAL MACHINE.....	47
GAMBAR 28. MENGATUR LOGIN MENJADI ROOT DAN KATA SANDI	47
GAMBAR 29. MENGUBAH HOSTNAME MENJADI TARGET	47
GAMBAR 30. MENGINSTALL AUDIT	48
GAMBAR 31. MERUBAH FILE SYSLOG	49
GAMBAR 32. MASUKKAN IP ADDRESS	49
GAMBAR 33. INSTALL NGROK.....	50
GAMBAR 34. HASIL INSTALL NGROK	50
GAMBAR 35. FILE QRADAR.....	50
GAMBAR 36. MEMBUAT NAMA VIRTUAL MACHINE.....	51
GAMBAR 37. TAMPILAN UNTUK MENJALANKAN VIRTUAL MACHINE.....	51
GAMBAR 38. MENGATUR LOGIN MENJADI ROOT DAN KATA SANDI	52
GAMBAR 39. MENGUBAH HOSTNAME MENJADI ATTACKER	52
GAMBAR 40. INSTALL NGROK.....	52
GAMBAR 41. HASIL INSTALL NGROK	53
GAMBAR 42. PORT SCANNING NMAP -PN	53

GAMBAR 43. PORT SCANNING NMAP -SN	54
GAMBAR 44. PORT SCANNING NMAP -V -A	55
GAMBAR 45. HASIL PORT SCANNING	55
GAMBAR 46. HASIL PORT SCANNING	55
GAMBAR 47. SERANGAN MENGGUNAKAN NGROK	59
GAMBAR 48. PENGUJIAN GAGAL	59
GAMBAR 49. SERANGAN DDOS MENGGUNAKAN SCRIPT MHDDOS	60
GAMBAR 50. MEMULAI PENYERANGAN	60
GAMBAR 51. HASIL PENYERANGAN MHDDOS	61
GAMBAR 52. MENYERANG MENGGUNAKAN NGROK	63
GAMBAR 53. HASIL MENYERANG MENGGUNAKAN NGROK	64



DAFTAR TABEL

TABLE 1. ANOMALI TRAFFIC 2022 [1].....	1
TABLE 2. PERANGKAT KERAS.....	29
TABLE 3. PERANGKAT LUNAK.....	29

