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

LAPORAN SKRIPSI

Gusana Adirosa

4617030017

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2021

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

Gusana Adirosa

4617030017

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	**:**	

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 Skipsi 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.

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.

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

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)

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

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 kemanan 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*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

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*).

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

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 teridentifikasinya 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 dikenalinya 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

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.

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.

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.

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.

Frattini, 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].

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

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.

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 Cipayung 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.