IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DENGAN WAZUH UNTUK MONITORING KEAMANAN PADA SERVER TIK

SKRIPSI

FADHILRAHMAN

1907422017

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2023

IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DENGAN WAZUH UNTUK MONITORING KEAMANAN PADA SERVER TIK

SKRIPSI

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

FADHILRAHMAN

1907422017

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2023

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	:	Fadhilrahman
NIM	:	1907422017
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	:	Implementasi *Security Information and Event Management* (SIEM) Dengan Wazuh Untuk Monitoring Keamanan Pada Server TIK

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain, kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 06 September 2023

Yang membuat pernyataan

(Fadhilrahman)

NIM. 1907422017

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Fadhilrahman
NIM	:	1907422017
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Implementasi *Security Information and Event Management* (SIEM) Dengan Wazuh Untuk Monitoring Keamanan Pada Server TIK

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Jumat, **Tanggal** 25, **Bulan** Agustus, **Tahun** 2023, **dan dinyatakan LULUS.**

Disahkan oleh

Pembimbing I	:	Iik Muhamad Malik Matin, S.Kom., M.T.	( )
Penguji I	:	Ayu Rosyida Zain, S.ST., M.T.	( )
Penguji II	:	Defiana Arnaldy, S.Tp., M.Si.	
Penguji III	:	Ariawan Andi Suhandana, S.Kom., M.T.I.	( )

Mengetahui:

Ketua Jurusan Teknik Informatika dan Komputer

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP. 197908032003122003

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan Skripsi ini. Penulisan laporan Skripsi ini dilakukan dalam rangka menyelesaikan Pendidikan Diploma IV dan sebagi salah satu syarat untuk mencapai gelar Sarjana Terapan di Politeknik Negeri Jakarta. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan Skripsi, sangatlah sulit bagi penulis untuk menyelesaikan laporan Skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. Bapak Iik Muhamad Malik Matin, S.Kom., M.T. selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan Skripsi ini;
b. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan moral dan material;
c. Sahabat yang telah banyak membantu penulis dalam menyelesaikan laporan Skripsi ini.

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

Depok, 05 Agustus 2023

Penulis

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama	:	Fadhilrahman
NIM	:	1907422017
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Implementasi *Security Information and Event Management* (SIEM) Dengan Wazuh Untuk Monitoring Keamanan Pada Server TIK

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 05 Agustus 2023

Yang Menyatakan

(Fadhilrahman)

NIM. 1907422017

Abstrak

Salah satu kemajuan teknologi yang memiliki manfaat yang besar adalah teknologi virtualisasi. Teknologi virtualisasi merupakan teknologi yang digunakan untuk membuat representasi akan sesuatu, contohnya adalah virtual dari server, penyimpanan ataupun mesin fisik. Server TIK pada Politeknik Negeri Jakarta menggunakan teknologi virtualisasi berupa mesin virtual Proxmox. Server ini sering digunakan oleh mahasiswa untuk melakukan penelitian. Namun, server ini sendiri masih belum memiliki sistem untuk deteksi serangan sehingga jika ada serangan yang masuk maka akan sulit untuk diketahui. Oleh sebab itu, dibutuhkan sebuah solusi untuk memonitor aktivitas pada server ini. Salah satu cara untuk mengamankannya adalah dengan memanfaatkan Security Information and Event Management (SIEM). SIEM dapat mengintegrasikan data dari berbagai sumber seperti log sistem, sensor dan alat keamanan lainnya. Implementasi dari SIEM yang akan diimplementasikan adalah Wazuh yang juga akan diintegrasikan dengan Intrusion Detection System (IDS) yaitu Suricata untuk memantau keamanan pada jaringan. Setelah itu dilakukan beberapa percobaan serangan yaitu port scanning, bruteforce, dan DoS untuk menguji sistem yang diimplementasikan. Dari hasil penelitian yang dilakukan, Implementasi Wazuh dan Suricata berhasil untuk dilakukan pada server TIK, kemudian Wazuh agent dan Suricata berhasil dalam melakukan deteksi atas serangan yang diujikan.

***Kata kunci**: Virtualisasi, SIEM, Wazuh. IDS, Suricata, Port Scanning, Bruteforce, DoS.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi terus mengalami perubahan setiap tahunnya, mulai dari teknologi baru yang tercipta ataupun perkembangan dari teknologi yang sudah ada. Dengan adanya teknologi-teknologi ini dapat mempermudah kehidupan manusia. Salah satu dari teknologi tersebut adalah virtualisasi. Virtualisasi merupakan teknologi yang digunakan untuk membuat representasi akan sesuatu, contohnya adalah virtualisasi dari server, penyimpanan ataupun mesin fisik. Perangkat virtual ini akan meniru perangkat keras fisik untuk menjalankan beberapa mesin virtual secara bersamaan pada satu mesin fisik.

Teknologi virtualisasi memberikan beberapa keuntungan, diantaranya adalah fleksibilitas, efisiensi biaya pada perangkat keras, kegiatan monitoring server menjadi lebih mudah, kemudahan dalam melakukan *backup* dan *recovery*. Karena alasan inilah, banyak perusahaan atau institusi yang mulai beralih menggunakan teknologi virtualisasi. Beberapa contoh dari perangkat lunak virtualisasi yang terkenal dan sering digunakan adalah Virtuabox, VMWare, Proxmox, dan masih banyak lagi.

Jurusan Teknik Informatika di Politeknik Negeri Jakarta memilki sebuah ruang server. Server ini memanfaatkan virtualisasi dari mesin virtual Proxmox dan diberi nama server JTIK2. Proxmox sendiri merupakan sebuah platform virtualisasi yang memfokuskan penggunaannya sebagai server. Server ini sering digunakan oleh mahasiswa untuk melakukan penelitian. Namun, server ini sendiri masih belum memiliki suatu sistem untuk deteksi serangan sehingga jika ada serangan yang masuk maka akan sulit untuk diketahui. Oleh sebab itu, demi menjaga keamanan pada server ini maka harus diimplementasikan suatu sistem yang dapat memantau aktifitas dan memudahkan dalam melakukan monitoring terhadap kejadian-kejadian yang terjadi.

Salah satu cara untuk mengelola keamanan dan mempermudah dalam melakukan monitoring aktivitas yang terjadi adalah dengan menggunakan *Security Information*

and Event Management (SIEM). SIEM adalah sebuah sistem untuk manajemen log dimana SIEM dapat mengintegrasikan data dari berbagai sumber seperti log sistem, sensor dan alat keamanan lainnya seperti IDS. *Intrusion Detection System* (IDS) adalah sebuah sistem yang berguna untuk melakukan monitor terhadap trafik pada jaringan untuk mendeteksi aktivitas mencurigakan yang terjadi.

Pada penelitian terdahulu yang dilakukan oleh (Kamal, 2022) melakukan implementasi *Security Information and Event Management* (SIEM) yaitu Splunk pada jaringan UII untuk mengolah *threat log* yang dihasilkan oleh *firewall* Palo Alto untuk membantu dalam analisis tren ancaman serangan siber. Dengan penggunaan SIEM maka akan mempermudah dalam melakukan pembacaan log. Pada penelitian terdahulu yang dilakukan oleh (Khotimah, et al., 2022) melakukan implementasi SIEM yaitu Wazuh pada salah satu aplikasi SMA Center di Pemerintah Daerah Provinsi NTB. SIEM diimplementasikan dengan tujuan untuk mempermudah tim keamanan Teknologi Informasi pemerintah provinsi NTB dalam melakukan monitoring serangan yang mengancam sistem. Kemudian pada penelitian yang dilakukan oleh (Alpauji, 2021) dengan membuat prototipe dari implementasi *Intrusion Detection System* (IDS) untuk mengamankan jaringan dari Security Operation Center (SOC) PT. ITSEC ASIA dan SIEM Elastic untuk mempermudah melakukan monitoring log. Kemudian penulis melakukan pengujian sistem dengan melakukan percobaan serangan DoS.

Berdasarkan dari referensi diatas, penelitian ini akan melakukan implementasi dari SIEM Wazuh dan IDS Suricata pada server TIK untuk membantu dalam melakukan deteksi dan monitoring keamanan. Kemudian akan dilakukan pengujian beberapa serangan untuk melihat apakah sistem yang telah diimplementasikan dapat mendeteksi serangan dan menampilkan log yang didapat pada Wazuh *dashboard*.

1.2 Perumusan Masalah

Dalam mencapai tujuan dari penelitian ini, terdapat beberapa permasalahan yang dirumuskan sebagai berikut:

a. Bagaimana implementasi *Security Informasi and Event Management* (SIEM) Dengan Wazuh untuk monitoring keamanan pada server TIK?
b. Bagaimana serangan yang terdeteksi dapat dimonitoring dari Wazuh *dashboard*?

1.3 Batasan Masalah

Pada penelitian ini, ruang lingkup penelitian ini meliputi:

a. Implementasi SIEM Wazuh dan IDS Suricata.
b. Log yang didapat berasal dari Wazuh *agent* dan Suricata.
c. Pengujian menggunakan metode serangan *port scanning*m, *bruteforce*, dan DoS (*Denial of Service*).
d. Pengujian *port scanning* menggunakan *tools* Zenmap dan NetScanTools demo.
e. Pengujian *bruteforce* menggunakan *tools* Hydra dan Metasploit.
f. Pengujian DoS (*Denial of Service*) menggunakan *tools* LOIC dan Hping3.
g. Penelitian dilakukan menggunakan server JTIK2 pada ruang server TIK.
h. Serangan dilakukan secara lokal.

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari penelitian ini sebagai berikut:

1.4.1 Tujuan

a. Melakukan implementasi *Security Informasi and Event Management* (SIEM) Dengan Wazuh untuk monitoring keamanan pada server TIK.
b. Menganalisis serangan yang terdeteksi dan dimonitoring dari Wazuh *dashboard*.

1.4.2 Manfaat

a. Membantu pengguna dalam melakukan monitoring keamanan dengan lebih efisien dan efektif.
b. Mempermudah pengguna mendeteksi serangan yang diujikan.

c. Mempermudah pengguna dalam melakukan pembacaan log dari Wazuh *agent* dan Suricata melalui Wazuh *dashboard*.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan laporan ini, sebagai berikut :

1. BAB I PENDAHULUAN

   Pada Bab ini membahas tentang latar belakang dari penelitian, rumusan masalah dari penelitian yang dilakukan, batasan masalah yang ada pada penelitian, tujuan dan manfaat dari penelitian yang dilakukan serta sistematika penulisan.
2. BAB II TINJAUAN PUSTAKA

   Pada Bab ini membahas tentang landasan teori yang berhubungan dengan topik penelitian dan penelitian terdahulu yang telah dilakukan berkaitan dengan topik yang dibahas.
3. BAB III RANCANGAN DAN REALISASI

   Pada Bab ini membahas tentang rancangan penelitian, tahapan penelitian, objek penelitian, framework yang akan digunakan, serta teknik pengumpulan dan analisis data.
4. BAB IV HASIL DAN PEMBAHASAN

   Pada Bab ini akan membahas mengenai hasil dan pembahasan dari pengujian terhadap sistem yang telah diimplementasikan pada penelitian yang telah dilakukan.
5. BAB V PENUTUP

   Pada Bab ini akan membahas mengenai kesimpulan yang didapat dari penelitian yang telah dilakukan dan memberikan saran untuk pengembangan terhadap penelitian selanjutnya berdasarkan hasil dari penelitian.
6. DAFTAR PUSTAKA

   Pada bagian ini berisi tentang referensi dalam pembentukan laporan ini.

BAB V
PENUTUP

5.1 Simpulan

Berdasarkan hasil dari penelitian yang telah dilakukan oleh penulis, maka dapat ditarik kesimpulan sebagai berikut:

1. Implementasi *Security Information and Event Management* (SIEM) dengan Wazuh untuk monitoring keamanan pada server JTIK2 berhasil untuk dilakukan.
2. Percobaan serangan yang dilakukan dengan menggunakan metode serangan *port scanning*, *bruteforce*, dan *denial of service* (DoS) berhasil untuk dideteksi oleh Wazuh *agent* dan Suricata. Serangan *port scanning* menggunakan *tools* Zenmap dan NetScanTools demo. Untuk serangan *bruteforce* menggunakan tools Hydra dan Metasploit. Kemudian untuk serangan *denial of service* (DoS) menggunakan *tools* LOIC dan Hping3.

5.2 Saran

Saran yang dapat diusulkan pada penelitian ini adalah:

1. Menggunakan metode serangan lainnya untuk melihat apakah serangan yang diujikan dapat dideteksi oleh Wazuh *agent* dan Suricata dan ditampilkan pada Wazuh *dashboard*.
2. Menggunakan *tools* lainnya untuk mendeteksi serangan dan diintegrasikan dengan Wazuh. Ini bertujuan untuk mendapatkan log serangan yang lebih banyak untuk dianalisis.

DAFTAR PUSTAKA

Abdurrahman, Soni & Hafid, A., 2019. OPTIMALISASI SUMBER DAYA KOMPUTER DENGAN VIRTUALISASI SERVER MENGGUNAKAN PROXMOX VE. *JURNAL FASILKOM*, 9(2), pp. 369-376.

Alfiansyah, F., 2022. *Implementasi Security Information and Event Management (SIEM) pada lingkungan ITSEC Asia Menggunakan Elastic SIEM.* s.l.:s.n.

Alpauji, A., 2021. *Implementasi Security Information and Event Management Menggunakan Tools Elastic Serta Suricata Sebagai Sistem Pendeteksi Intrusi Pada Sistem Operasi Linux Ubuntu di Perusahaan PT. ITSEC ASIA.* s.l.:s.n.

Fachri, F., 2023. OPTIMASI KEAMANAN WEB SERVER TERHADAP SERANGAN BRUTE-FORCE MENGGUNAKAN PENETRATION TESTING. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 10(1), pp. 51-58.

Fadhlillah, A. S., Bogi, N. & Irawan, A. I., 2019. ANALISIS PERFORMANSI IDS MENGGUNAKAN METODE DETEKSI ANOMALY-BASED TERHADAP SERANGAN DOS. *e-Proceeding of Engineering*, 6(2), p. 3398.

Fahrudi, M. A. & Suartana, M., 2023. Integrasi End-point Security Berbasis Agent dan Bot Messenger untuk Deteksi dan Monitoring Serangan pada Web Server secara Real-time. *Journal of Informatics and Computer Science*, 4(3).

gen_too, 2022. *Integrate Suricata with Wazuh for Log Processing.* [Online] Available at: https://kifarunix.com/integrate-suricata-with-wazuh-for-log-processing/
[Diakses 21 Juni 2023].

Harjono, E. B., 2016. Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *SinkrOn: Jurnal & Penelitian Teknik Informatika*, 1(1).

Huda, N., 2022. *Apa itu Intrusion Detection System (IDS)? Jenis dan Cara Kerjanya.* [Online] Available at: https://www.dewaweb.com/blog/ids-adalah/ [Diakses 3 Agustus 2023].

Huda, N., 2022. *SIEM: Pengertian, Cara Kerja, serta Perbedaannya dengan SOAR.* [Online] Available at: https://www.dewaweb.com/blog/pengertian-siem/ [Diakses 7 Juli 2023].

Intern, D., 2020. *Apa itu Server ? Berikut Pengertian, Jenis dan Fungsinya.* [Online] Available at: https://www.dicoding.com/blog/apa-itu-server/ [Diakses 14 Agustus 2023].

Kali, 2023. *What is Kali Linux & Kali's features.* [Online] Available at: https://www.kali.org/docs/introduction/ [Diakses 17 Juli 2023].

Kamal, M. R., 2022. *IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DENGAN SPLUNK UNTUK ANALISIS TREN ANCAMAN SIBER PADA JARINGAN UII.* [Online] Available at: https://dspace.uii.ac.id/handle/123456789/40786 [Diakses 16 Februari 2023].

Khotimah, H., Bimantoro, F., Kabanga, R. S. & Widiartha, I. B. K., 2022. IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PADA APLIKASI SMS CENTER PEMERINTAH DAERAH PROVINSI NUSA TENGGARA BARAT. *JBegaTI.*

Pratama, M. D., Nova, F. & Prayama, D., 2022. Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1), pp. 1-7.

Rendro, D. B., N. & Aji, W. N., 2020. ANALISIS MONITORING SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SOFTWARE

NMAP (STUDI KASUS DI SMK NEGERI 1 KOTA SERANG). *Jurnal PROSISKO*, 7(2).

Shah, M. et al., 2019. Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool. *International Conference on Computing, Mathematics and Engineering Technologies – iCoMET*, p. 6.

Suricata, 2023. *Suricata User Guide.* [Online] Available at: https://docs.suricata.io/en/latest/index.html [Diakses 5 Juli 2023].

Wazuh, 2023. *Getting started with Wazuh.* [Online] Available at: https://documentation.wazuh.com/current/getting-started/index.html [Diakses 26 Juni 2023].

DAFTAR RIWAYAT HIDUP

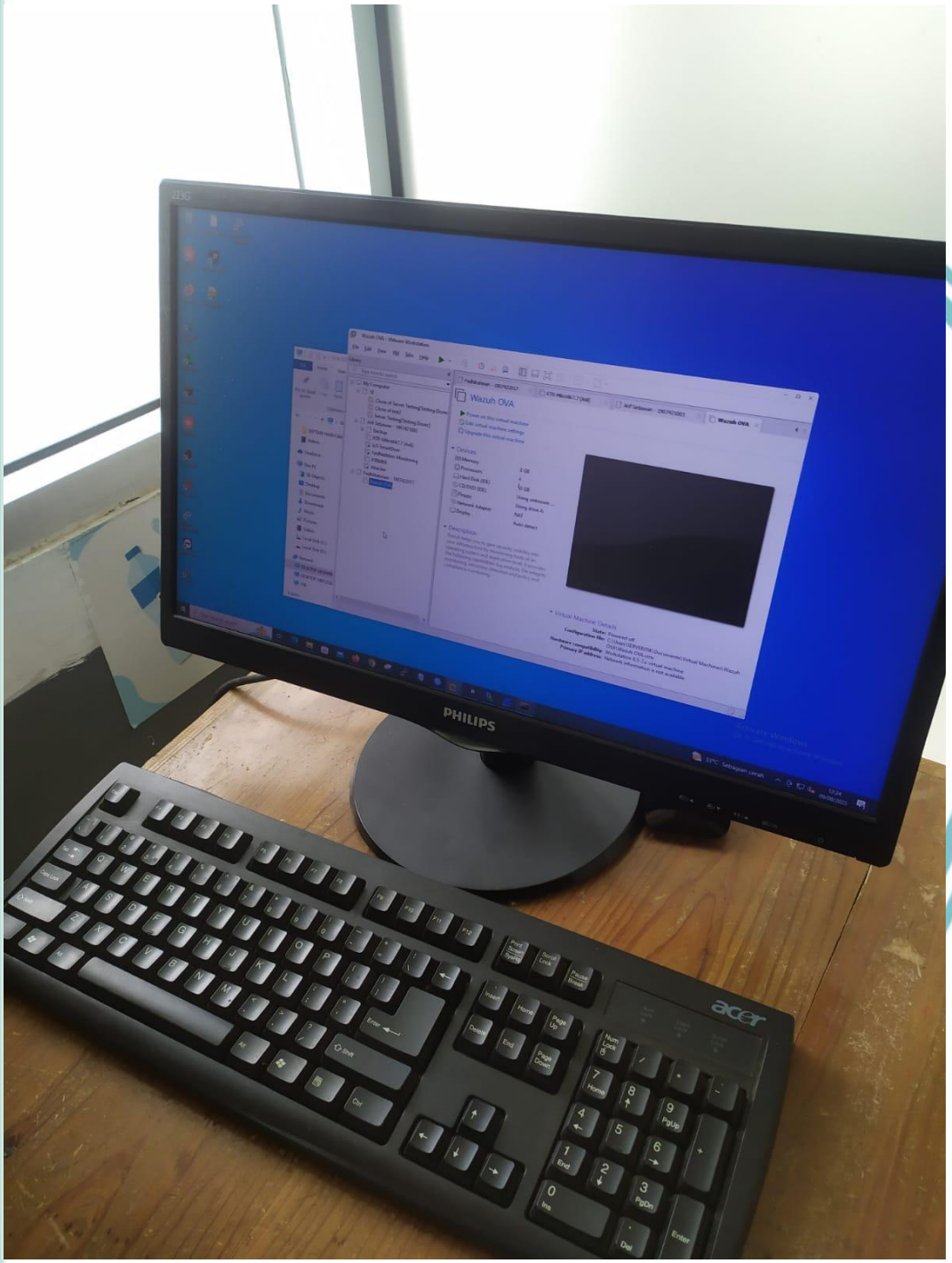
Fadhilrahman

Lahir di Bukittinggi, 05 Januari 2000. Lulus dari SDN 29 Kotohilalang pada tahun 2012, SMPN 1 Ampek Angkek pada tahun 2015, SMAN 1 Ampek Angkek pada tahun 2018 dan Diploma II program studi Network Administrator Profesional di CEP-CCIT FTUI pada tahun 2021. Saat ini sedang menempuh Pendidikan Diploma IV Jurusan Teknik Informatika dan Komputer Program Studi Teknik Multimedia dan Jaringan di Politeknik Negeri Jakarta.

LAMPIRAN-LAMPIRAN

Lampiran 1: Server TIK

1. Perangkat PC Windows 10



“lanjutan”

2. Perangkat Server JTIK2

Lampiran 2: *Agent Deployment*