



UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

**ANALISIS PADA WAZUH SEBAGAI IMPLEMENTASI
SECURITY INFORMATION AND EVENT MANAGEMENT
(SIEM) TERHADAP SERANGAN MALWARE DI SISTEM
OPERASI DEBIAN**

SKRIPSI

MICHAEL AURELIO NUGRAHA

1910511077

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN
JAKARTA**

2023



UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

**ANALISIS PADA WAZUH SEBAGAI IMPLEMENTASI
SECURITY INFORMATION AND EVENT MANAGEMENT
(SIEM) TERHADAP SERANGAN MALWARE DI SISTEM
OPERASI DEBIAN**

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer

MICHAEL AURELIO NUGRAHA

1910511077

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN
JAKARTA**

2023

**PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Michael Aurelio Nugraha

NIM : 1910511077

Fakultas : Ilmu Komputer

Program Studi : S1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

Analisis Pada Wazuh Sebagai Implementasi Security Information and Event Management (SIEM) Terhadap Serangan Malware di Sistem Operasi Debian

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih- media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Bogor

Pada tanggal: 16 Juli 2023

Yang menyatakan,



(Michael Aurelio Nugraha)

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama : Michael Aurelio Nugraha
NIM : 1910511077
Program Studi : S1 Informatika
Judul : Analisis Pada Wazuh Sebagai Implementasi *Security Information, and Event Management* (SIEM) Terhadap Serangan Malware di Sistem Operasi Debian.

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.



(Henki Bayu Seta, S.Kom, MTL)
Penguji I




(Rio Wirawan, S.Kom, M.M.S.I.)
Penguji II



(Bayu Hananto, S.Kom, M.Kom.)
Dosen Pembimbing



(Dr. Ermatita, M.Kom.)
Dekan Fakultas Ilmu Komputer



(Dr. Widya Cholil, M.I.T)
Ketua Program Studi

Ditetapkan di : Jakarta
Tanggal Persetujuan : 6 Juli 2023



LEMBAR PERSETUJUAN

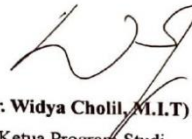
LEMBAR PERSETUJUAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama : Michael Aurelio Nugraha
NIM : 1910511077
Program Studi : S1 - Informatika
Judul : Analisis Pada Wazuh Sebagai Implementasi Security Information and Event Management (SIEM) Terhadap Serangan Malware di Sistem Operasi Debian

Sebagai bagian persyaratan yang diperlukan untuk mengikuti ujian Sidang Skripsi pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.

Mengetahui,



(Dr. Widya Cholil, M.I.T)
Ketua Program Studi

Menyetujui,



(Bayu Hananto, S.Kom., M.Kom.)
Dosen Pembimbing

Ditetapkan di : Jakarta
Tanggal Persetujuan : 06 Juni 2023

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun ditujuk telah saya nyatakan dengan benar.

Nama : Michael Aurelio Nugraha

NIM : 1910511077

Program Studi : S1 – Informatika

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 06 Juni 2023

Yang Menyatakan,



(Michael Aurelio Nugraha)

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan yang Mahakuasa atas segala karunianya, sehingga Skripsi (Tugas Akhir) ini berhasil diselesaikan. Skripsi ini disusun sebagai syarat kelulusan Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta. Penulis ingin mengucapkan terima kasih kepada:

1. Orang tua, Bapak Andreas Teguh Nugroho dan Ibu Maria Esti Darmayanti.
2. Bapak Dr. Anter Venus, M.A., Comm selaku rektor Universitas Pembangunan Nasional Veteran Jakarta.
3. Ibu Dr. Ermatita, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
4. Ibu Dr. Widya Cholil, M.I.T. selaku Ketua Program Studi Sarjana Jurusan S1 Informatika.
5. Bapak Bayu Hananto, S.Kom., M.Kom., selaku Dosen Pembimbing yang telah memberikan saran yang bermanfaat.
6. Bapak Henki Bayu Seta, S.Kom., MTI., selaku Dosen Penguji I yang telah memberikan revisi terhadap skripsi saya.
7. Bapak Rio Wirawan, S.Kom., M.M.S.I., selaku Dosen Penguji II yang telah memberikan revisi terhadap skripsi saya.
8. Bapak Hamonangan Kinantan Prabu, M.T., selaku Dosen Pembimbing Akademik yang telah membantu saya dalam membimbing segala urusan perkuliahan dan juga skripsi.
9. Teman – teman satu angkatan, khususnya kelompok Pejuang yang selalu memberikan semangat setiap harinya.
10. Seluruh pihak yang terlibat dalam kelancaran pembuatan makalah karya ilmiah ini dan yang tidak mungkin disebutkan satu per satu di atas, saya ucapkan terima kasih.

Penulis sadar bahwa laporan ini masih jauh dari kata sempurna, baik materi maupun teknik penyajiannya. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun.

Bogor, 06 Juni 2023

A handwritten signature in black ink, appearing to read 'M. Aurelio Nugraha', with a horizontal line underlining the bottom part of the signature.

Michael Aurelio Nugraha

ABSTRAK

Salah satu teknologi yang berkembang pesat hingga saat ini adalah *Internet*. Pesatnya perkembangan *Internet* ini disebabkan oleh kebutuhan manusia yang semakin beragam juga. Berkembang pesatnya *Internet* tidak hanya menimbulkan efek positif, namun negatifnya juga. Salah satu efek negatif dari *Internet* yaitu serangan *Malware*. Dalam penelitian ini akan dilakukan analisis terhadap serangan *malware* menggunakan konsep SIEM (*Security Information and Event Management*) dengan tujuan untuk mengidentifikasi suatu serangan *malware*, menganalisa kemampuan SIEM dalam menangani serangan *malware*, dan tentu mencari solusi untuk menangani suatu serangan *malware* pada sistem. Penelitian ini akan dilakukan menggunakan sistem operasi Windows 10, Debian 11 dan disertai juga dengan *tools* seperti VirusTotal dan Wazuh. Wazuh di sini adalah sebagai implementasi dari konsep SIEM yang digunakan dalam penelitian ini. Dengan dilakukannya konfigurasi antara Wazuh dengan VirusTotal, maka hasil yang diharapkan adalah dapat dihasilkan otomatis berupa *alert* ke Wazuh dan *auto remove file* terhadap *file* yang terdeteksi sebagai *malware*.

Kata Kunci: SIEM, *Malware*, Wazuh.

ABSTRACT

One of the technologies that has developed rapidly until now is the Internet. The rapid development of the Internet is due to the increasingly diverse human needs as well. The rapid development of the Internet not only has a positive effect, but also a negative one. One of the negative effects of the Internet is malware attacks. In this study, analysis of malware attacks will be carried out using the concept of SIEM (Security Information and Event Management) with the aim of identifying a malware attack, analyzing the ability of SIEM to handle malware attacks, and of course finding solutions to deal with a malware attack on the system. This research will be conducted using the Windows 10 operating system, Debian 11 and also accompanied by tools such as VirusTotal and Wazuh. Wazuh is an application that is used as an implementation of the SIEM concept in this study. With the configuration between Wazuh and VirusTotal, the expected result is that an automation can be generated in the form of alerts to Wazuh and an auto remove file against the file that detected as malware.

Keyword: SIEM, Malware, Wazuh.

DAFTAR ISI

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	iii
LEMBAR PENGESAHAN	iv
LEMBAR PERSETUJUAN	v
PERNYATAAN ORISINALITAS	vi
KATA PENGANTAR	vii
ABSTRAK.....	ix
ABSTRACT.....	x
DAFTAR ISI.....	xi
DAFTAR GAMBAR	xiii
DAFTAR TABEL.....	xiv
BAB 1	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	2
1.3 Rumusan Masalah	3
1.4 Batasan Masalah.....	3
1.5 Tujuan Penelitian	3
1.6 Manfaat Penelitian	3
1.7 Sistematika Penulisan	4
BAB 2	6
LANDASAN TEORI.....	6
2.1 Malware (Malicious Software).....	6
2.2 Log	7
2.3 Log Management	7
2.4 Hash	8
2.5 SIEM (Security Information and Event Management).....	8
2.6 Wazuh	8
2.7 VirusTotal	9

2.8	Penelitian Terkait	9
BAB 3		12
METODOLOGI PENELITIAN.....		12
3.1	Tahapan Penelitian.....	12
3.1.1	<i>Identifikasi Masalah</i>	12
3.1.2	<i>Studi Literatur</i>	13
3.1.3	<i>Perancangan Sistem</i>	13
3.1.4	<i>Implementasi</i>	14
3.1.5	<i>Hasil.....</i>	17
3.2	Perangkat Penelitian	17
3.3	Jadwal Penelitian.....	18
BAB 4		19
HASIL DAN PEMBAHASAN.....		19
4.1	Sistem Pemantauan	19
4.2	Sistem Penyerangan	25
4.3	Pengujian.....	28
BAB 5		37
KESIMPULAN DAN SARAN.....		37
5.1	Kesimpulan	37
5.2	Saran.....	38
DAFTAR PUSTAKA		39
RIWAYAT HIDUP		41
LAMPIRAN.....		43

DAFTAR GAMBAR

Gambar 1. 1 Windows Malware Detection 2019 - 2021 dikutip dari sumber: (MalwareBytes cyberprotection, 2022).....	2
Gambar 2. 1 Taksonomi Malware.....	6
Gambar 3. 1 Kerangka Berpikir.....	12
Gambar 3. 2 Sistem Penyerangan	13
Gambar 3. 3 Sistem Pemantauan	14
Gambar 3. 4 Topologi	15
Gambar 3. 5 Pengujian Sistem.....	16
Gambar 4. 1 API Key Dari VirusTotal	20
Gambar 4. 2 Flowchart Rules 1.....	22
Gambar 4. 3 Flowchart Rules 2.....	24
Gambar 4. 4 Wazuh server via desktop	25
Gambar 4. 5 Laman wazuh agent.....	25
Gambar 4. 6 Deploy agent (1).....	26
Gambar 4. 7 Deploy agent (2).....	26
Gambar 4. 8 Deploy agent (3).....	27
Gambar 4. 9 Bukti agent aktif	27
Gambar 4. 10 Website Das Malwerk	28
Gambar 4. 11 Unduh file malware	29
Gambar 4. 12 Bukti file dihapus	29
Gambar 4. 13 File terdeteksi oleh VirusTotal.....	29
Gambar 4. 14 Karakteristik malware	29

DAFTAR TABEL

Tabel 3. 1 Jadwal Pelaksanaan September 2022 - Januari 2023.....	18
Tabel 3. 2 Jadwal Pelaksanaan Februari - Juni 2023	18
Tabel 4. 1 Tabel Hasil Uji Coba Malware (9 Juli 2023).....	31
Tabel 4. 2 Tabel Bukti Malware Terdeteksi	34