

**ANALISIS KOMPARASI KINERJA IBM QRADAR DAN
SNORT UNTUK MELAKUKAN NETWORK FORENSIC
TERHADAP SERANGAN SIBER**

SKRIPSI

Diajukan untuk memenuhi syarat memperoleh gelar Sarjana Teknik S1 Program
Studi Sistem Telekomunikasi di Universitas Pendidikan Indonesia Kampus UPI di
Purwakarta



Oleh

Pramudika Afriza Fahmi

NIM 2009271

**PROGRAM STUDI S1 SISTEM TELEKOMUNIKASI
KAMPUS UPI DI PURWAKARTA
UNIVERSITAS PENDIDIKAN INDONESIA
2024**

**Analisis Komparasi Kinerja IBM QRadar dan Snort untuk
Melakukan *Network Forensic* terhadap Serangan Siber**

Oleh

Pramudika Afriza Fahmi

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Teknik pada Kampus UPI di Purwakarta Program Studi Sistem
Telekomunikasi

© **Pramudika Afriza Fahmi** 2024

Universitas Pendidikan Indonesia

Agustus 2024

Hak cipta dilindungi oleh undang-undang.

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
Dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa izin dari penulis.

LEMBAR PENGESAHAN SKRIPSI

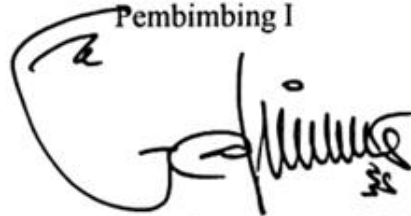
Pramudika Afriza Fahmi

2009271

ANALISIS KOMPARASI KINERJA IBM QRADAR DAN SNORT UNTUK
MELAKUKAN *NETWORK FORENSIC* TERHADAP SERANGAN SIBER

Disetujui dan Disahkan Oleh Pembimbing

Pembimbing I



Galura Muhammad Suranegara, S.Pd., M.T.

NIP. 920190219920111101

Pembimbing II



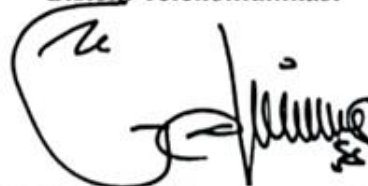
Hafiyyan Putra Pratama, S.ST., M.T.

NIP. 92019021992124101

Mengetahui:

Ketua Program Studi

Sistem Telekomunikasi



Galura Muhammad Suranegara, S.Pd., M.T.

NIP. 920190219920111101

PERNYATAAN ANTI PLAGIARISME

Yang bertandatangan dibawah ini:

Nama : Pramudika Afriza Fahmi
NIM : 2009271
Program Studi : Sistem Telekomunikasi
Fakultas/Kampus Daerah : Kampus UPI di Purwakarta

Dengan ini saya menyatakan bahwa skripsi saya yang berjudul **Analisis Komparasi Kinerja IBM QRadar dan Snort untuk Melakukan *Network Forensic* terhadap Serangan Siber** sepenuhnya merupakan hasil karya diri sendiri.

Di dalamnya saya tidak melakukan penjiplakan atau melakukan pengutipan dengan cara tidak sesuai dengan etika keilmuan yang berlaku pada masyarakat. Dengan pernyataan ini, saya siap menanggung resiko/sanksi yang diberikan kepada saya apabila kemudian ditemukan adanya pelanggaran etika keilmuan atau pihak lain yang mengklaim terhadap keaslian karya saya ini.

Purwakarta, 31 Juli 2024

Yang membuat pernyataan



Pramudika Afriza Fahmi

NIM. 2009271

UCAPAN TERIMA KASIH

Alhamdulillah puji syukur penulis panjatkan kepada Allah SWT. yang senantiasa melimpahkan Rahmat serta anugerah-Nya sehingga penulis dapat menyelesaikan skripsi ini tepat pada waktunya. Shalawat juga penulis junjung kepada nabi Muhammad SAW. selaku umat dan pengikutnya semoga syafaatnya selalu tercurahkan kepada kita semua.

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah banyak membantu dalam pelaksanaan dan penyusunan skripsi, diantaranya:

1. Bapak Galura Muhammad Suranegara, S.Pd., M.T. selaku Ketua Program studi Sistem Telekomunikasi Universitas Pendidikan Indonesia sekaligus pembimbing pertama skripsi yang sudah membimbing dengan baik.
2. Bapak Hafiiyan Putra Pratama, S.ST., M.T. selaku pembimbing kedua skripsi yang sudah membantu kepenulisan draft skripsi dengan baik.
3. Orang tua Bapak Jumanto dan Ibu Sriati yang sudah mendukung kinerja dalam membuat penelitian skripsi.
4. Saudari Nuralfa yang sudah membantu memenuhi *resources* dalam melaksanakan penelitian.
5. Teman-teman Sistem Telekomunikasi angkatan 2020 yang sudah saling memberikan semangat satu sama lain.
6. Kepada teman seperjuangan Tryadi, Alpiyan, dan Rahadian yang sudah saling memberikan canda tawa yang membangkitkan semangat.
7. Kepada Drg. Fatimah Juniyanti Assegaf yang selalu *support* dalam membantu dan menemani penulis menyelesaikan skripsi ini.
8. Teman-teman komunitas motor Aesthetic Riders dan Planet Maxxy yang sudah memberikan semangat yang membangun.
9. Seluruh pihak yang tidak dapat disebutkan satu persatu. Penulis hanya bisa mengucapkan banyak terima kasih atas bantuan penyusunan skripsi.

Purwakarta, 31 Juli 2024

Penulis.

Analisis Komparasi Kinerja IBM QRadar dan Snort untuk Melakukan *Network Forensic* terhadap Serangan Siber

Pramudika Afriza Fahmi

NIM: 2009271

ABSTRAK

Keamanan jaringan komputer yang lemah dapat memudahkan *hacker* dalam mengeksploitasi data-data penting. BSSN mengungkapkan pada *annual report* di tahun 2023, Indonesia akan mengalami berbagai kejadian serangan siber. *Security Information and Event Management* (SIEM) termasuk sistem yang dapat mendeteksi ancaman dan serangan siber pada jaringan. Deteksi serangan siber memerlukan metode forensik dalam mengidentifikasi jenis serangan dengan *network forensics*. IBM QRadar *Community Edition* (CE) dan Snort merupakan *tools* dari produk SIEM yang dapat meneteksi ancaman dan serangan siber. Pada penelitian ini dilakukan konfigurasi *log* atau *network activity* dan analisis terhadap kinerja dari QRadar CE dan Snort dalam mendeteksi serangan *Port Scanning*, *Metasploit*, dan *Distributed / Denial of Service* (D/DoS). Penelitian ini menggunakan 4 (empat) tahapan *network forensics*, yaitu *Preparation*, *Detection*, *Incident Response*, dan *Collection* sebagai acuan untuk komparasi *tools*. Hasil dari komparasi tersebut menunjukkan bahwa IBM QRadar lebih efektif dalam konfigurasi *rules*, kecepatan serangan, dan pengumpulan paket data serangan.

Kata kunci: Analisis Deteksi, Siber, QRadar, Snort, *network forensics*

***Comparative Analysis of IBM QRadar and Snort Performance to
Perform Network Forensic against Cyber Attacks***

Pramudika Afriza Fahmi

NIM: 2009271

ABSTRACT

Weak computer network security can make it easier for hackers to exploit important data. BSSN revealed in its annual report that in 2023, Indonesia will experience various cyberattack events. Security Information and Event Management (SIEM) includes systems that can detect threats and cyberattacks on the network. Detection of cyber attacks requires forensic methods in identifying the type of attack with network forensics. IBM QRadar Community Edition (CE) and Snort are tools from SIEM products that can detect cyber threats and attacks. In this research, log or network activity configuration and analysis of the performance of QRadar CE and Snort in detecting Port Scanning, Metasploit, and Distributed / Denial of Service (D/DoS) attacks are carried out. This research uses 4 (four) stages of network forensics, namely Preparation, Detection, Incident Response, and Collection as a reference for tools comparison. The results of the comparison show that IBM QRadar is more effective in configuring rules, attack speed, and collecting attack data packets.

Keywords: *Detection Analysis, Cyber, Qradar, Snort, Network Forensics*

DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI	ii
PERNYATAAN ANTI PLAGIARISME	iii
UCAPAN TERIMA KASIH	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Penelitian	1
1.2. Identifikasi Masalah Penelitian	2
1.3. Rumusan Masalah Penelitian	2
1.4. Tujuan Penelitian.....	2
1.5. Batasan Masalah Penelitian.....	3
1.6. Manfaat Penelitian.....	4
BAB II KAJIAN PUSTAKA	5
2.1. Kajian Teori	5
2.2. Penelitian Terdahulu	5
2.3. Penelitian Relevan.....	6
2.4. <i>Security Information and Event Management (SIEM)</i>	7
2.5. Skema Jaringan	8
2.6. Implementasi <i>Network Forensics</i>	8
2.7. Snort	9
2.8. IBM QRadar SIEM Community <i>Edition (CE)</i>	10
2.9. VMWare (Virtual Machine)	10
2.10. <i>Port Scanning</i>	11
2.11. Metasploit Framework	11
2.12. <i>Distributed / Denial of Service (D/DoS)</i>	12
BAB III METODOLOGI PENELITIAN	13
3.1. Desain Penelitian.....	13

3.2. Studi Literatur	13
3.3. Alur Penelitian.....	14
3.4. Skenario Pengujian.....	15
3.5. Spesifikasi Perangkat dan <i>Tools</i> Pengujian	17
3.6. Teknik Pengumpulan Data	18
3.7. Teknik Analisis Data (<i>Network Forensics</i>).....	18
BAB IV TEMUAN DAN PEMBAHASAN	20
4.1. Pengujian.....	20
4.2. Prosedur Tahapan Pengujian	20
4.2.1. <i>Preparation</i>	21
4.2.2. <i>Detection</i>	22
4.2.3. <i>Incident Response</i>	26
4.2.4. <i>Collection</i>	35
4.2.5. <i>Preservation</i>	41
4.2.6. <i>Examination</i>	42
4.2.7. <i>Investigation</i>	42
4.2.8. <i>Presentation</i>	42
4.3. Data Hasil Pengujian	43
4.4. Analisis Komparasi <i>Tools</i> IBM QRadar dan Snort	49
4.4.1. Analisis Penelitian Penulis	49
4.4.2. Analisis dengan Penelitian Terdahulu	50
4.4.3. Hasil Analisis Penelitian Penulis dan Terdahulu.....	52
BAB V KESIMPULAN, IMPLIKASI, DAN REKOMENDASI.....	53
5.1. Kesimpulan.....	53
5.2. Implikasi.....	54
5.3. Rekomendasi	54
DAFTAR PUSTAKA.....	55
LAMPIRAN.....	59

DAFTAR GAMBAR

Gambar 2.1. Konsep SIEM	8
Gambar 2.2. Skema jaringan	8
Gambar 2.3. Implementasi network forensics.....	9
Gambar 2.4. Arsitektur virtual machine	10
Gambar 2.5. Skema port scanning	11
Gambar 2.6. Skema metasploit/exploit	11
Gambar 2.7. Skema D/DoS	12
Gambar 3.1. Alur penelitian	14
Gambar 3.2. Flowchart Pengujian.....	16
Gambar 4.1. Spesifikasi QRadar pada VM	21
Gambar 4.2. Spesifikasi snort pada VM	22
Gambar 4.3. Kondisi CPU setelah serangan DoS	27
Gambar 4.4. Kondisi CPU setelah serangan DDoS	28
Gambar 4.5. Deteksi serangan port scanning	29
Gambar 4.6. Deteksi serangan metasploit/exploit	30
Gambar 4.7. Deteksi serangan DoS	31
Gambar 4.8. Deteksi serangan DDoS	32
Gambar 4.9. Tab Dashboard QRadar	36
Gambar 4.10. Tab Offenses QRadar	37

DAFTAR TABEL

Tabel 3.1. Parameter network forensics	15
Tabel 3.2. Spesifikasi Perangkat Keras Laptop.....	17
Tabel 4.1. IP address perangkat.....	20
Tabel 4.2. Konfigurasi rules QRadar.....	23
Tabel 4.3. Konfigurasi rules snort	25
Tabel 4.4. Contoh log port scanning pada snort.....	33
Tabel 4.5. Contoh log metasploit/exploit pada snort.....	34
Tabel 4.6. Contoh log DoS pada snort	34
Tabel 4.7. Contoh log DDoS pada snort	35
Tabel 4.8. Log result pada snort	37
Tabel 4.9. Spesifikasi pada IBM QRadar	43
Tabel 4.10. Spesifikasi pada Snort	43
Tabel 4.11. Aspek konfigurasi pada QRadar	44
Tabel 4.12. Aspek konfigurasi pada snort	45
Tabel 4.13. Waktu serangan siber QRadar	46
Tabel 4.14. Waktu serangan siber snort.....	46
Tabel 4.15. Selisih waktu IBM QRadar dan Snort.....	47
Tabel 4.16. Hasil data serangan QRadar	48
Tabel 4.17. Hasil data serangan Snort	48

DAFTAR PUSTAKA

- I Wayan Ardiyasa, & Ni Luh Gede Pivin Suwirmayanti. (2021). Investigasi Serangan Remote Exploit menggunakan Metode Live Forensic Investigation. *Jurnal Sistem Dan Informatika (JSI)*, 16(1), 11-16. <https://doi.org/10.30864/jsi.v16i1.342>
- Afif, Z., Azhari, D. S., Kustati, M., & Sepriyanti, N. (2023). Penelitian Ilmiah (Kuantitatif) Beserta Paradigma, Pendekatan, Asumsi Dasar, Karakteristik, Metode Analisis Data Dan Outputnya. *Innovative: Journal Of Social Science Research*, 3(3), 682–693. <https://doi.org/10.31004/innovative.v3i3.2260>
- Abdullah, M. S., & Ikasari, I. H. (2023). *Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan*. 1(1), 96–98.
- Achmad, R., Manullang, E. V., & Sanmas, E. R. (2020). RANCANG BANGUN APLIKASI DETEKSI DAN PENANGANAN SERANGAN DDOS DAN PORT SCANNING MEMANFAATKAN SNORT PADA JARINGAN KOMPUTER. 8(1), 1–10.
- Adam Zukhruf, Bagus Fatkhurrozi, & Andriyatna Agung Kurniawan. (2023). COMPARATIVE STUDY OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK DETECTION IN COMPUTER NETWORKS. *Jurnal Teknik Informatika (Jutif)*, 4(5), 1033–1039. <https://doi.org/10.52436/1.jutif.2023.4.5.756>
- Adirosa, G. (2021). ANALISIS KINERJA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IBM QRADAR COMMUNITY EDITION DALAM MENDETEKSI ANCAMAN DAN SERANGAN SIBER PADA SERVER. *EVENT MANAGEMENT*.
- Amin, A. S., & Arnesia, P. D. (2023). Pengembangan Sistem Keamanan Jaringan Menggunakan Network Forensics. *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, 20(1), 50. <https://doi.org/10.36080/bit.v20i1.2180>

- Ardiyasa, I. W. (2021). *Analisa Serangan Remote Exploit pada Jaringan Komputer dengan menggunakan Metode Network Forensic*. 11(2), 46–52.
- Elan Maulani, I., & Faisal Umam, A. (2023). Evaluasi Efektivitas Sistem Deteksi Intrusi Dalam Menjamin Keamanan Jaringan. *Jurnal Sosial Teknologi*, 3(8), 662–667. <https://doi.org/10.59188/jurnalsostech.v3i8.907>
- Fauzi, A. R. (2018). *MONITORING JARINGAN WIRELESS TERHADAP SERANGAN PACKET SNIFFING DENGAN MENGGUNAKAN IDS*. 8(2), 11–17.
- Fitri Nova, Pratama, M. D., & 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), 1–7. <https://doi.org/10.30630/jitsi.3.1.59>
- González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, 21(14), 4759. <https://doi.org/10.3390/s21144759>
- Gunawan, G. B., Sukarno, P., & Putrada, A. G. (2018). *Pendeteksian Serangan Denial of Service (DoS) pada Perangkat Smartlock Berbasis Wifi Menggunakan SNORT IDS*. 5(3), 7875–7884.
- IBM Security QRadar SIEM*. (2023). <https://www.ibm.com/products/qradar-siem>
- Mahendra, D. D., & Mukti, F. S. (2022). Sistem Deteksi dan Pengendalian Serangan Denial of Service pada Server Berbasis Snort dan Telegram-API. *Techno.Com*, 21(3), 511–522. <https://doi.org/10.33633/tc.v21i3.6466>
- Nabil, M. F., & Yazid, S. (2023). *Perancangan Kapabilitas Security Operations Center (SOC): Studi Kasus PT XYZ*. 2(9), 751–777.
- Pandari, J. L. J., & Sulistyono, W. (2023). *IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) UNTUK MENDETEKSI SERANGAN METASPLOIT EXPLOIT MENGGUNAKAN SNORT DAN WIRESHARK*. 6(1), 41–50.

- Prasetyo, S. M., Agusti, M. B., Mahesa, D. A., Maulana, F., & Rafly, A. (2024). *Mesin Virtual (Virtual Machine): Sekilas Tentang Tujuan, Fungsi, Keuntungan, Dan Pengelolaan Dari Mesin Virtual*. 1(6), 743–749.
- Pudyo P, W. (2022). Analisis Intelijen Atas Potensi Ancaman Serangan Siber pada Presidensi KTT G20 Tahun 2022 di Indonesia. *Edunity: Kajian Ilmu Sosial dan Pendidikan*, 1(03), 81–94. <https://doi.org/10.57096/edunity.v1i03.15>
- Putra, R. D., & Mardianto, I. (2019). Exploitation with Reverse_tcp Method on Android Device using Metasploit. *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, 5(1), 106. <https://doi.org/10.26418/jp.v5i1.26893>
- Rahman, R., & Akmal, G. L. (2024). *FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER*. 1(3), 70–76. <https://doi.org/10.69714/zxrv9q19>
- Riza, F. (2023). *ANALISIS SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) ELASTIC SEARCH MENGGUNAKAN METODE NIST 800-61 REV2 PADA DATACENTER PT. SEMBILAN PILAR SEMESTA*. 16(2), 63–66.
- Rizal, R. (2018). *NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT)*. <https://dspace.uui.ac.id/handle/123456789/8455>
- Santoso, D., Noertjahyana, A., & Andjarwirawan, J. (2022). *Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS*. 10(1), 136–141.
- Suskalo, D., Moric, Z., Redzepagic, J., & Regvart, D. (2023). Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management. Dalam B. Katalinic (Ed.), *DAAAM Proceedings* (1 ed., Vol. 1, hlm. 0096–0102). DAAAM International Vienna. <https://doi.org/10.2507/34th.daaam.proceedings.014>
- Syahrizal, H., & Jailani, M. S. (2023). Jenis-Jenis Penelitian Dalam Penelitian Kuantitatif dan Kualitatif. *Jurnal QOSIM: Jurnal Pendidikan, Sosial & Humaniora*, 1(1), 13–23. <https://doi.org/10.61104/jq.v1i1.49>

- Tasmi, T., Antony, F., & Ubaidillah, U. (2022). NETWORK FORENSIK UNTUK MENGANALISA TRAFIK DATA GAME ONLINE. *Klik - Jurnal Ilmu Komputer*, 3(1), 50–58. <https://doi.org/10.56869/klik.v3i1.352>
- Terbitkan Annual Report Berisi Prediksi Ancaman Siber 2023, BSSN: Materi Literasi Budaya Keamanan Siber dan Buktikan Akuntabilitas Kinerja | www.bssn.go.id. (2023, Februari 20). *Annual Report 2022*. <https://www.bssn.go.id/annualreport2022/>
- Wahyusesa, A. S., Hidayanto, P. W., & Ramdayani, E. A. (2023). *Solusi Cerdas: Meningkatkan Keamanan dan Kinerja Jaringan pada Warnet dengan Mengatasi Kelemahan Sistem*. 1(2), 62–66.
- Wijoyo, A., Rosadi, A., Hakim, F. I., Hanafi, M., & Sidik, R. (2023). *Keamanan Jaringan Melindungi Sistem dari Serangan Luar*. 1(3), 1–3.
- Wulandari, W. A. (2018). *ANALISIS NETWORK FORENSICS MENGGUNAKAN HONEYPOT PADA JARINGAN LAYANAN PUBLIC CLOUD COMPUTING ANALYSIS NETWORK FORENSICS USING HONEYPOT ON PUBLIC CLOUD COMPUTING SERVICE NETWORK*. 3(1), 18–25.