RANCANG BANGUN IDS MENGGUNAKAN APLIKASI ZEEK UNTUK MENDETEKSI SERANGAN JARINGAN DAN MALWARE REMOTE ACCESS TROJAN

SKRIPSI

LATIEF MULYARAHIM

2007422002

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

DEPOK

2024

RANCANG BANGUN IDS MENGGUNAKAN APLIKASI ZEEK UNTUK MENDETEKSI SERANGAN JARINGAN DAN MALWARE REMOTE ACCESS TROJAN

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan

untuk Memperoleh Diploma Empat Politeknik

LATIEF MULYARAHIM

2007422002

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

DEPOK

2024

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama	:	Latief Mulyarahim
NIM	:	2007422002
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	:	RANCANG BANGUN IDS MENGGUNAKAN APLIKASI ZEEK UNTUK MENDETEKSI SERANGAN JARINGAN DAN MALWARE REMOTE ACCESS TROJAN

Menyatakan dengan sebenarnya bahwa skripsiini 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 cirri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 28 Agustus 2024

Yang membuat pernyataan

Latief Mulyarahim

NIM 2007422002

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Latief Mulyarahim

NIM : 2007422002

Program Studi : Teknik Multimedia Jaringan

Judul Skripsi : RANCANG BANGUN IDS MENGGUNAKAN APLIKASI ZEEK UNTUK MENDETEKSI SERANGAN JARINGAN DAN MALWARE REMOTE ACCESS TROJAN

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Kamis

Tanggal 19, Bulan Agustus, Tahun 2024. dan dinyatakan **LULUS.**

	Disahkan oleh	Tanda Tangan
Pembimbing I	: Ayu Rosyida Zain, S.ST., M.T.	(.....)
Penguji I	: Maria Agustin, S.Kom., M.Kom.	(.....)
Penguji II	: Asep Kurniawan, S.Pd., M.Kom.	(.....)
Penguji III	: Iik Muhammad Malik Matin, S.Kom., M.T.	(.....)

Mengetahui :

Ketua Jurusan Teknik Informatika dan Komputer

Dr., Anita Hidayati, S.Kom., M.Kom.
NIP. 197802112009121003

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT. karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan skripsi ini dalam rangka memenuhi syarat untuk memperoleh gelar Diploma IV Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer pada Politeknik Negeri Jakarta. Penulisan skripsi ini tidak akan selesai tepat pada waktunya tanpa bantuan, bimbingan dan doa dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Ketua jurusan dan seluruh Dosen serta staf jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta yang telah memberikan ilmu yang sangat bermanfaat kepada penulis;
2. Ibu Ayu Rosyida Zain, S.ST., M.T. selaku Ketua Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta, sekaligus dosen pembimbing yang telah menyediakan waktu, tenaga, pikiran, arahan, dan dorongan yang tiada henti selama proses penyusunan skripsi ini.
3. Orang tua dan keluarga yang selalu memberikan doa, materi, dan dukungan serta kasih sayang kepada penulis selama ini.
4. Adeline Wijaya sebagai tempat untuk refreshing dan penyemangat selama proses penyusunan skripsi ini.
5. Teman-teman Pululan Maut yang sudah memberikan canda tawa, semangat, dan tempat untuk bercerita.
6. Kepada diri sendiri, karena tidak menyerah dalam menempuh Pendidikan dan berhasil menyusun skripsi ini dengan baik.

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan skripsi ini, Oleh karena itu, penulis sangat terbuka terhadap kritik dan saran yang membangun, demi perbaikan dan peningkatan kualitas penulisan di masa mendatang. Semoga skripsi ini mudah dipahami oleh pembaca serta menjadi ilmu yang bermanfaat.

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

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

Nama : Latief Mulyarahim

NIM : 2007422002

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: RANCANG BANGUN IDS MENGGUNAKAN APLIKASI ZEEK UNTUK MENDETEKSI SERANGAN JARINGAN DAN MALWARE REMOTE ACCESS TROJAN Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalih mediakan/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, 28 Agustus 2024

Yang Menyatakan

Latief Mulyarahim
NIM 2007422002

RANCANG BANGUN IDS MENGGUNAKAN APLIKASI ZEEK UNTUK MENDETEKSI SERANGAN JARINGAN DAN MALWARE REMOTE ACCESS TROJAN

Abstrak

Perkembangan pesat teknologi internet membawa dampak positif namun juga menghadirkan ancaman keamanan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem Intrusion Detection System (IDS) menggunakan Zeek untuk mendeteksi serangan jaringan dan malware, serta mengirim notifikasi otomatis melalui Telegram. Pengujian ini dilakukan dengan 3 jenis serangan, yaitu *Port Scanning*, DDoS , dan malware *Remote Access Trojan*. Hasil menunjukkan bahwa IDS Zeek mampu mendeteksi ketiga jenis serangan tersebut dengan tingkat keberhasilan 100% dalam 10 kali pengujian. Zeek berhasil mencatat serangan dalam notice.log dan mengirimkan notifikasi melalui Telegram, memungkinkan tim keamanan merespons secara cepat. Waktu rata-rata yang dibutuhkan untuk mendeteksi dan mengirim notifikasi adalah 4.80 detik untuk *Port Scanning*, 3.978 detik untuk DDoS, dan 1.832 detik untuk malware *Remote Access Trojan*. Dengan hasil ini, Zeek menunjukkan tingkat efektivitas tinggi dan responsivitas yang baik, serta penelitian ini berpotensi dapat dikembangkan lebih lanjut untuk menghadapi berbagai jenis ancaman keamanan jaringan.

Kata kunci : DDoS, Telegram, *Port Scanning, Remote Access Trojan* (RAT), Zeek

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada zaman sekarang, teknologi berkembang dengan sangat pesat yang semakin mempermudah penggunanya untuk melakukan kegiatan sehari-hari dengan memanfaatkan teknologi internet. Setiap hari banyak orang yang mengakses internet untuk melakukan kegiatan. Namun seiring berjalannya waktu, perkembangan teknologi ini tidak selalu berdampak positif, tetapi juga dihadapkan dengan munculnya berbagai kejahatan berbasis siber yang memanfaatkan kelemahan sistem dan kesadaran pengguna informasi.

Mengingat ancaman seperti pencurian data, kerusakan sistem, dan gangguan operasional, keamanan siber telah menjadi prioritas utama bagi organisasi dan individu. Serangan jaringan, seperti Port Scanning dan Distributed Denial of Service (DDoS), dan malware seperti Remote Access Trojan (RAT) semakin sering terjadi dan memiliki potensi untuk melakukan dampak besar. Untuk menangani dari ancaman ini, penggunaan Intrusion Detection System (IDS) menjadi penting. IDS dirancang untuk memantau aktivitas jaringan dan sistem, mengidentifikasi potensi ancaman, dan memberikan peringatan jika terjadi perilaku mencurigakan. IDS memiliki peran krusial dalam mendeteksi anomali atau aktivitas yang mencurigakan pada jaringan, sehingga dapat memberikan respons cepat terhadap serangan yang terdeteksi. Intrusion Detection System atau IDS adalah sebuah software yang ditujukan menjadi pemantau aktivitas jaringan atau sistem dan dapat mendeteksi jika terjadi aktivitas yang berbahaya (Suci, 2020).

Zeek adalah salah satu tools penganalisis lalu lintas jaringan sumber terbuka dan pasif. Tools ini biasanya digunakan sebagai pemantau keamanan jaringan untuk menyelidiki kemungkinan aktivitas jahat yang terjadi dalam lalu lintas jaringan. Alat ini dapat menangkap lalu lintas sebagai paket yang dikirim ke antrian yang kemudian akan diproses. Zeek juga mampu melakukan tugas analisis lalu lintas yang berbeda di luar domain keamanan, termasuk pengukuran kinerja dan pemecahan masalah. Zeek juga sepenuhnya dapat disesuaikan dan diperluas berkat bahasa Zeek Scripting. Dengan memanfaatkan script pada zeek, dapat

memungkinkan pengguna untuk memodifikasi kode dan fungsi khusus, seperti membuat parameter pendeteksian, mengenali jenis serangan, dan integrasi ke telegram. Sehingga bahasa zeek script ini cukup fleksibel karena dapat disesuaikan dengan kebutuhan (Basile, Cardiello and Smorti, 2022).

Penelitian ini bertujuan untuk membangun sistem IDS menggunakan Zeek yang berfokus pada deteksi serangan Port Scanning, DDoS, dan malware RAT. Selain itu, sistem ini dilengkapi dengan notifikasi otomatis melalui Telegram untuk meningkatkan respons terhadap potensi ancaman. Dengan mengintegrasikan Zeek ke Telegram, dapat meningkatkan kemampuan deteksi Zeek dalam mengirim proses pemberitahuan ketika terjadi serangan. Dengan adanya penelitian ini diharapkan dapat memberikan kontribusi positif dalam meningkatkan keamanan terhadap berbagai serangan yang melalui jaringan, serta memberikan solusi yang baik dalam melawan ancaman tersebut.

1.2 Rumusan Masalah

Dari latar belakang tersebut adapun perumusan masalahnya sebagai berikut :

1. Bagaimana membangun sistem untuk mendeteksi serangan dari dalam jaringan?
2. Bagaimana penerapan zeek dalam mendeteksi serangan malware Remote Access Trojan, Port Scanning, DDoS?
3. Bagaimana zeek dapat diintegrasikan dengan notifikasi telegram ketika terjadi serangan?

1.3 Batasan Masalah

Terdapat batasan masalah yang bertujuan agar pembahasan menjadi lebih terarah. Adapun batasan masalah dapat dijelaskan sebagai berikut :

1. Penelitian ini menerapkan Intrusion Detection System (IDS) dengan implementasi aplikasi Zeek sebagai alat untuk mendeteksi serangan.
2. Penelitian ini melakukan pembuatan rules agar zeek dapat mengenali jenis serangan dan terbatas pada pendeteksian tiga jenis serangan Port Scanning, DDoS, dan malware Remote Access Trojan (RAT)..
3. Penelitian ini membuat notifikasi telegram ketika terjadi serangan.

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dengan dilakukannya penelitian ini adalah sebagai berikut:

1.4.1 Tujuan

1. Merancang dan menerapkan Intrution Detection System (IDS) dengan menggunakan Zeek
2. Tools ini mampu untuk mendeteksi berbagai serangan jaringan dan malware, terutama jenis serangan seperti Port Scanning, DDoS, dan Remote Access Trojan (RAT) yang terintegrasi dengan Telegram
3. Untuk mengevaluasi kemampuan Zeek dalam mendeteksi dan mengidentifikasi jenis serangan

1.4.2 Manfaat

1. Meningkatkan keamanan jaringan dengan sistem IDS yang efektif dan responsif.
2. Dengan adanya notifikasi otomatis melalui Telegram, dapat merespons dan melakukan tindakan mitigasi terhadap serangan dengan lebih cepat, sehingga risiko kerusakan dan downtime dapat diminimalisir.
3. Penelitian ini memberikan pemahaman yang lebih tentang penggunaan Zeek sebagai IDS dan bagaimana sistem ini dapat dioptimalkan untuk berbagai kondisi jaringan.

1.5 Sistematika Penulisan

Sistimatika Penulisan Penelitian ini dilakukan dengan Sistimatika Penulisan sebagai berikut:

a. BAB I PENDAHULUAN

   Pada bab ini membahas tentang latar belakang, perumusan masalah, perumusan masalah, tujuan dan manfaat pada penelitian ini.

b. BAB II TINJAUAN PUSTAKA

   Pada bab ini membahas tentang materi-materi yang mendukung dan membantu penelitian ini.

c. BAB III PERANCANGAN DAN REALISASI

   Pada bab ini membahas metode pengerjaan, rancangan penelitian, tahapan penelitian dan objek penelitian.

d. BAB IV PEMBAHASAN

Pada bab ini berisi mengenai pengujian dan hasil dari analisis pengujian IDS seperti deskripsi pengujian, prosedur pengujian, data hasil pengujian dan analisis data/evaluasi.

e. BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dan saran dari keseluruhan penelitian.

BAB V
PENUTUP

1.1 Kesimpulan

Setelah melakukan rancang bangun IDS menggunakan Zeek untuk mendeteksi serangan jaringan dan malware, yang kemudian akan mengirim notifikasi otomatis melalui telegram, dapat disimpulkan :

a. IDS Zeek mampu mendeteksi serangan *Port Scanning,* DDoS, dan malware *Remote Access Trojan* dengan tingkat keberhasilan 100% dalam melakukan 10 kali percobaan.
b. Zeek mampu menampilkan jenis serangan pada *notice.log* dan mengirim log ke telegram yang akan memberikan notifikasi jika terjadi serangan *Port Scanning*, DDoS, dan *Remote Access Trojan*.
c. Pada 10 percobaan serangan *port scanning* membutuhkan waktu rata-rata 4.80 detik untuk zeek mendeteksi dan telegram mengirim notifikasi. Kemudian, Pada 10 percobaan serangan DDoS membutuhkan waktu rata-rata 3.978 detik untuk zeek mendeteksi dan telegram mengirim notifikasi. Lalu, Pada 10 percobaan serangan *Remote Access Trojan* membutuhkan waktu rata-rata 1.832 detik untuk zeek mendeteksi dan telegram mengirim notifikasi.

1.2 Saran

Untuk pengembangan dari sistem ini dapat menambahkan beberapa pembaharuan terhadap fitur atau rules pada Zeek, yaitu :

a. Melakukan pengujian dengan menggunakan jenis serangan lain yang lebih bervariasi agar sistem dapat memberikan kinerja yang lebih baik dan mampu beradaptasi dengan berbagai situasi.
b. Melakukan integrasi untuk membuat notifikasi menggunakan aplikasi lain, selain telegram dan juga integrasi dengan tools yang dapat memvisualisasikan data.

Daftar Pustaka

Anendya Aorinka (2023) *Mencegah Serangan Jaringan Komputer Ilegal Dengan Nmap*. Available At: Https://Www.Dewaweb.Com/Blog/Nmap-Mencegah-Jaringan-Ilegal/#Apa_Itu_Nmap (Accessed: 29 August 2024).

Arifin, R.D. (2022) *Apa Itu Telegram? Pengertian Telegram Adalah, Sejarah, Fitur, Kelebihan*. Available At: Https://Dianisa.Com/Pengertian-Telegram/ (Accessed: 22 February 2024).

Basile, C., Cardiello, R. And Smorti, M. (2022) *Politecnico Di Torino Analysis And Improvement Of Ransomware Detection Techniques Supervisor: Company Supervisor: Candidate*.

Dar, M.H. *Et Al.* (2018) 'Implementasi Snort Intrusion Detection System (Ids) Pada Sistem Jaringan Komputer', *Muhammad Halmi Dar*, 1(3).

Haniyah, W. *Et Al.* (2024) 'Simulasi Serangan Denial Of Service (Dos) Menggunakan Hping3 Melalui Kali Linux', *Journal Of Internet And Software Engineering*, 1(2), P. 8. Available At: Https://Doi.Org/10.47134/Pjise.V1i2.2654.

Huda, N. (2022) *Network Security: Pengertian, Manfaat, Dan Jenis-Jenisnya*. Available At: Https://Www.Dewaweb.Com/Blog/Pengertian-Network-Security/#Apa_Itu_Network_Security (Accessed: 20 February 2024).

Jiang, W. *Et Al.* (2019) 'A Highly Efficient Remote Access Trojan Detection Method', *International Journal Of Digital Crime And Forensics*, 11(4), Pp. 1–13. Available At: Https://Doi.Org/10.4018/Ijdcf.2019100101.

Lin, C. (2024) *Scrubcrypt Deploys Venomrat With An Arsenal Of Plugins | Fortiguard Labs*. Available At: Https://Www.Fortinet.Com/Blog/Threat-Research/Scrubcrypt-Deploys-Venomrat-With-Arsenal-Of-Plugins (Accessed: 29 August 2024).

Linknet (2023) *Apa Itu Penetration Testing? Pengertian, Fungsi, Dan Tahapannya - Link Net*. Available At: Https://Www.Linknet.Id/Article/Penetration-Testing (Accessed: 30 August 2024).

Made, I. *Et Al.* (2020) *Network Security Monitoring System On Snort With Bot Telegram As A Notification*, *International Journal Of Computer Applications Technology And Research*. Available At: Www.Ijcat.Com.

Nissim, K. And Wood, A. (2018) 'Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya', *Philosophical Transactions Of The Royal Society A: Mathematical, Physical And Engineering Sciences*, 376(2128). Available At: Https://Doi.Org/10.1098/Rsta.2017.0358.

Renondo Sianipar, V. (2023) *Program Studi Teknik Informatika Fakultas Teknik Dan Komputer Universitas Putera Batam Tahun 2023*.

Syani, M. (2020) *Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps)*, *Jurnal Inkofar* *. Online.

What Is Port Scanning And How Does It Work? | Avast (2024). Available At: Https://Www.Avast.Com/Business/Resources/What-Is-Port-Scanning#Pc (Accessed: 26 August 2024).

Yasin, A. And Mohidin, I. (2018) 'Dampak Serangan Ddos Pada Software Based Openfow Switch Di Perangkat Hg553', *Jurnal Technopreneur (Jtech)*, 6(2), P. 72. Available At: Https://Doi.Org/10.30869/Jtech.V6i2.206.

Zeek (2024) *About Zeek — Book Of Zeek (Git/Master)*. Available At: Https://Docs.Zeek.Org/En/Master/About.Html (Accessed: 20 February 2024).

DAFTAR RIWAYAT HIDUP

Latief Mulyarahim, lahir di Jakarta, 6 September 2001. Merupakan anak pertama dari dua bersaudara. Saat ini penulis bertempat tinggal di Depok, Jawa Barat. Penulis telah menempuh pendidikan Sekolah Menengah Atas di SMK PKP 2 Jakarta (2016-2019). Penulis juga telah menempuh pendidikan professi CEP-CCIT Fakultas Teknik Universitas Indonesia (2019-2021) konsentrasi Network Administrator Professional dan meneruskan pendidikan di Perguruan Tinggi Politeknik Negeri Jakarta Jurusan Teknik Informatika dan Komputer Program Studi Teknik Multimedia dan Jaringan.