ANALISIS INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT DALAM MENDETEKSI SERANGAN MALWARE SAMBACRY

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh:

CADIPA SIDIQ

17.83.0105

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

ANALISIS INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT DALAM MENDETEKSI SERANGAN MALWARE SAMBACRY

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh:

CADIPA SIDIQ

17.83.0105

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT DALAM MENDETEKSI SERANGAN MALWARE SAMBACRY

yang disusun dan diajukan oleh

Cadipa Sidiq

17.83.0105

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 24 Agustus 2022

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng
NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT DALAM MENDETEKSI SERANGAN MALWARE SAMBACRY

yang disusun dan diajukan oleh

Cadipa Sidiq

17.83.0105

Telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Agustus 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Banu Santoso, S.T., M.Eng **NIK. 190302327**	
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 24 Agustus 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Cadipa Sidiq
NIM : 17.83.0105

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Intrusion Detection System Menggunakan Snort Dalam Mendeteksi Serangan Malware Sambacry

Dosen Pembimbing: Banu Santoso, S.T., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 24 Agustus 2022

Yang Menyatakan,

Cadipa Sidiq

HALAMAN PERSEMBAHAN

Dengan mengucapkan Alhamdulillah segala puji dan syukur saya panjatkan kehadirat ALLAH SWT atas segala rahmat dan hidayah-Nya dan atas dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia saya khaturkan rasa syukur dan terimakasih saya kepada :

1. Allah SWT, Tuhan Yang Maha Esa karena hanya atas izin dan karunia-Nyalah, maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan semesta alam yang meridhoi dan mengabulkan segala doa.
2. Orang tua saya, yang tidak pernah lelah memberikan saya dukungan dan doa. Untuk Ibu yang tidak pernah lelah dalam memberikan semangat supaya saya bisa menyelesaikan skripsi ini dan untuk Bapak yang telah banyak memberikan begitu banyak pengorbanan yang tidak bisa saya balaskan. Terimakasih banyak saya ucapkan untuk keduanya.
3. Dosen Pembimbing skripsi bapak Banu Santoso S.T., M.Eng. selaku dosen pembimbing saya, saya sangat berterimakasih atas bimbingannya selama ini yang telah memberikan masukan, kritik dan saran yang membangun agar menjadi lebih baik lagi untuk kedepannya. serta seluruh jajaran dosen Universitas Amikom Yogyakarta yang sudah membagikan ilmunya saya mengucapkan terimakasih, semoga ilmu dari bapak dan ibu dosen bisa saya amalkan ke yang lain juga.
4. Seluruh teman dan keluarga besar kelas 17 Teknik Komputer khususnya Ahmad Ristanto, Fakhrizal Asshiddiq, Ipung Ardiansyah, Kumara Prayoga, Misbachul Munir, dan Muhammad Rasyid Maulana yang telah memberikan dukungan dan semangat.
5. Perda Ristika Sari sebagai *best partner* yang telah memberikan saya dukungan dan kasih sayang serta motivasi untuk menjadi pribadi yang lebih baik.

KATA PENGANTAR

Dengan mengucapkan Alhamdulillah segala puji dan syukur penulis panjatkan atas kehadirat Allah SWT, karena berkat rahmat dan hidayah-Nya penyusunan skripsi yang berjudul "Analisis Instrusion Detection System Menggunakan Snort Dalam Mendeteksi Serangan Malware Sambacry" ini dapat diselesaikan guna memenuhi salah satu persyaratan dalam menyelesaikan pendidikan pada Jurusan Teknik Komputer Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

Perjalanan panjang telah penulis lalui dalam rangka menyelesaikan penulisan skripsi ini. Banyak hambatan yang dihadapi dalam penyusunannya, namun berkat kehendak-Nyalah sehingga penulis berhasil menyelesaikan penulisan skripsi ini. Oleh karena itu, dengan penuh kerendahan hati, pada kesempatan ini patutlah kiranya penulis mengucapkan terima kasih kepada :

1. Allah SWT atas rahmat, hidayah, serta karunia-Nya yang telah diberikan kepada penulis sehingga skripsi ini dapat terselesaikan.
2. Prof. Dr. M. Suyanto, MM selaku rektor Universitas AMIKOM Yogyakarta
3. Bapak Hanif Al Fatta,S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer.
4. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta
5. Kedua orang tua, yang selalu memberikan dukungan baik materi maupun doa.
6. Bapak Banu Santoso S.T., M.Eng. selaku dosen pembimbing yang tidak bosan memberikan arahan, saran dan motivasi agar penulis bisa mengerjakan naskah ini dengan baik dan benar.
7. Bapak dan Ibu Universitas AMIKOM Yogyakarta yang telah memberikan ilmunya selama penulis kuliah.

8. Keluarga besar kelas S1 Teknik Komputer 02 angkatan 2017.
9. Serta semua pihak yang telah membantu dalam proses penyusunan skripsi ini yang tidak dapat disebutkan satu per satu.

Akhirnya dengan kerendahan hati penulis mengucapkan terimakasih dan semoga skripsi ini dapat bermanfaat bagi penulis maupun pembaca.

Yogyakarta, 22 Agustus 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Perkembangan teknologi saat ini memungkinkan orang untuk mengakses internet secara terus-menerus. Ketika menggunakan sebuah komputer, baik secara lokal ataupun melalui internet, komputer tersebut berisiko un-tuk disusupi. Mengingat pentingnya nilai informasi tersebut, tidak heran jika adanya penyerangan yang dil-akukan oleh pihak-pihak yang tidak bertanggung jawab. Salah satu serangan yang digunakan adalah sambacry. Serangan sambacry menyerang port server message block (SMB) untuk mendapat hak akses istimewa (privilege escala-tion). Oleh sebab itu, pentingnya untuk menjaga dan memperkuat keamanan jaringan dengan memberikan perlindungan dari potensi bahaya dengan menggunakan instruction detection system (IDS) seperti snort, yang dapat menganalisis lalu lintas jaringan dengan mendeteksi aktifitas yang berbahaya dan memberikan peringatan. Pada penelitian ini, penulis bertujuan untuk mengkonfigurasi rule snort dalam mendeteksi serangan malware sambacry pada port SMB dengan mengirimkan peringatan tersebut melalui media telegram. Hasil dari penelitian ini menunjukkan bahwa snort dapat mendeteksi serangan malware sambacry setelah melakukan penambahan rule serta snort bisa diintegrasikan dengan media telegram didapatkan rata rata delay adalah 0,677527µs.

Kata kunci: Keamanan Jaringan, Sambacry, IDS, Snort, Telegram

ABSTRACT

Current technological developments allow people to access the internet continuously. When using a computer, either locally or via the internet, the computer is at risk of being compromised. Given the importance of the value of this information, it is not surprising that there are attacks carried out by irresponsible parties. One of the attacks used is sambacry. The sambacry attack attacks the server message block (SMB) port for privilege escalation. Therefore, it is important to maintain and strengthen network security by providing protection from potential hazards by using an instruction detection system (IDS) such as snort, which can analyze network traffic by detecting malicious activity and providing warnings. In this study, the author aims to configure snort rule malware attacks sambacry on port by sending the warning via telegram media. The results of this study indicate that snort malware attacks sambacry after adding rules and snort can be integrated with telegram media, the average delay is 0.677527µs.

Keywoards: Network Security, Sambacry, IDS, Snort, Telegram