BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini memungkinkan orang untuk mengakses internet secara terus-menerus. Ketika sebuah komputer, baik secara lokal maupun melalui internet, komputer tersebut berpotensi untuk disusupi. Melihat begitu berharganya suatu informasi, tidaklah heran jika bermunculan serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Pihak-pihak tersebut dapat melakukan penyusupan dengan tujuan mencuri, mengubah dan merusak informasi yang ada pada suatu komputer[1].

Berdasarkan laporan Indonesia Honeynet Project Badan Siber dan Sandi Negara 2021 serangan siber mencapai 266.741.784 dan serangan malware mencapai 393.851 dengan target port tertinggi yaitu pada port 445 dengan jumlah serangan sebanyak 182.716.385[2]. Port 445 adalah salah satu port yang digunakan dalam jaringan samba.

Samba adalah komponen penting untuk mengintegrasikan server dan desktop linux/unix dengan mulus ke dalam lingkungan active directory. Sejak tahun 1992, Samba telah menyediakan layanan file dan cetak yang aman, stabil dan cepat untuk semua klien yang menggunakan protokol SMB/CIFS, seperti semua versi DOS dan Windows, OS/2, Linux dan banyak lainnya[3]. Menurut National Institute of Standards and Technology pada bagian National Vulnerability Database samba dari versi 3.5.0 dan sebelum versi 4.6.4 memiliki kerentanan *remote code execution*, yang mana kerentanan tersebut memungkinkan penyerang mendapatkan hak akses istimewa (privilege escalation)[4]. Pada laporan CVE Details serangan code execution masih menjadi trend pada tahun 2022 seperti pada Gambar 1.1


Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2002	1														
2003	1		1	1											
2004	1		1												
2005	1														
2006	9	3	2	3	1										
2007	1	1													
2008	1		1												
2009	7	1	2	1							1				
2010	14	3	1	2	1						1				
2011	12	3						1							
2012	11	1		1											
2013	4														
2014	11		1							1					
Total	76	14	8	8	1			1		1	2				
% Total		18.4	11.8	10.5	1.3	0.0	0.0	1.3	0.0	1.3	2.6	0.0	0.0	0.0	

Gambar 1. 1 Vulnerability Trends Over Time

Sambacry merupakan serangan *remote code execution* terbaru yang menyerang port server message block untuk mendapatkan hak akses istimewa (privilege escalation). Kerentanan sambacry memiliki cvss score dengan level critical yaitu pada score 10 yang mana cvss score tersebut dipublish pada tanggal 30 Mei 2017 dan diupdate pada tanggal 16 Agustus 2022 [5][6]. Server Message Block (SMB) adalah protokol yang digunakan untuk berbagi file jaringan pada sistem operasi Microsoft Windows untuk membaca dan menulis ke file[7]. Protokol SMB dapat digunakan diatas protokol TCP/IP atau protokol jaringan lainnya. Menggunakan protokol SMB, aplikasi (atau pengguna aplikasi) dapat mengakses file atau sumber data lain di server jauh. Itu juga dapat berkomunikasi dengan program server apapun yang diatur untuk menerima permintaan klien SMB.

Oleh sebab itu, pentingnya untuk menjaga dan memperkuat keamanan jaringan dengan memberikan perlindungan dari potensi bahaya menggunakan instruction detection system seperti snort, yang dapat menganalisis lalu lintas jaringan dengan mendeteksi aktivitas serangan malware sambacry dan memberikan peringatan serangan tersebut dengan bantuan bot telegram untuk mengirimkan hasil log serangan malware sambacry pada snort ke administrator pada media telegram.

Atas dasar-dasar masalah diatas maka peneliti memuat sebuah topik yang berjudul **"Analisis Intrusion Detection System Menggunakan Snort Dalam Mendeteksi Serangan Malware Sambacry"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah maka peneliti merumuskan masalah yaitu sebagai berikut;

1. Bagaimana intrusion detection system pada snort dapat mendeteksi serangan malware sambacry?
2. Berapa waktu durasi yang dibutuhkan snort untuk mengirim log peringatan serangan malware sambacry pada bot telegram?

1.3 Batasan Masalah

Adapun batasan masalah yang bertujuan untuk memfokuskan pembahasan dalam penelitian ini adalah:

a. Penelitian ini berfokus mendeteksi malware sambacry pada server message block.
b. Penelitian ini berfokus menganalisis rules snort.
c. Penelitian ini menggunakan snort sebagai intrusion detection system.
d. Notifikasi deteksi serangan sambacry pada snort dikirimkan pada media telegram.
e. Penelitian ini berfokus melakukan serangan malware sambacry.
f. Serangan yang digunakan terbatas pada celah port server message block.
g. Penelitian ini hanya dilakukan menggunakan virtual environment dengan 2 sistem operasi; Debian 11.4.0 (sebagai server dan snort), dan Debian 11.4.0 (sebagai attacker).

1.4 Tujuan Penelitian

Adapaun Tujuan dari penelitian ini adalah sebagai berikut:

1. Mendeteksi serangan malware sambacry pada port server message block menggunakan snort.
2. Mengetahui waktu durasi yang dibutuhkan snort untuk mengirimkan peringatan log serangan pada bot telegram.

1.5 Manfaat Penelitian

Manfaat penelitian ini yaitu untuk menjaga kemanan sistem dari serangan anomaly-anomaly khususnya malware sambacry dengan mengirimkan notifikasi peringatan serangan pada media telegram. Penelitian ini bisa digunakan dalam menjaga sistem oraganisasi, kampus, dan lain-lain.

1.6 Sistematika Penulisan

Dalam penelitian ini, penulis disajikan dalam lima bab dengan sistematika pembahasan sebagai berikut:

Bab I Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Bab ini berisi tentang teori-teori pemecahan masalah yang berhubungan dan digunakan untuk mendukung penulisan penelitian ini.

Bab III Metodologi Penelitian

Bab ini berisi metode penelitian, objek penelitin, alur penelitian, serta alat dan bahan yang digunakan untuk penelitian.

Bab IV Pembahasan

Bab ini berisi tentang rancangan sistem, instalasi environment server, instalasi environment attacker, pengujian sistem, dan hasil penelitian.

Bab V Penutup

Bab ini berisi tentang kesimpulan dari pembahasan penelitian, hasil akhir penelitian dan saran.