BAB I
PENDAHULUAN

1.1 Latar Belakang

Berkembangnya jaringan internet di Indonesia mempunyai banyak manfaat dan mencakup banyak aspek seperti pendidikan, perbankan, bahkan dalam aspek militer. Menurut data dari APJII sendiri pada tahun 2019 penetrasi internet di Indonesia sebanyak 73,3% dengan pengguna internet di Indonesia hingga 196.714.070,3. Oleh sebab itu, internet dalam kehidupan sehari-hari pada masa sekarang sangat dibutuhkan.

Semakin berkembang dan pesat internet di Indonesia memunculkan banyak celah pada keamanan jaringan internet pada setiap pengguna internet di Indonesia. Celah keamanan ini dapat digunakan untuk melakukan kejahatan jaringan seperti meretas jaringan, mengambil data pengguna jaringan, dan mengirimkan paket serangan malware atau virus ke pengguna jaringan internet. Beberapa kejahatan dari kejahatan jaringan yaitu DDOS (*Distributed Denial of Service*), *Sniffing*, *Spoofing*, dan *Phising*. Serta aktivitas kejahatan lainnya yang dapat mengganggu kinerja dari perangkat jaringan kabel maupun nirkabel.

Untuk memberikan rasa aman pada pengguna jaringan internet serta mencegah serangan yang dapat mengganggu kinerja dari perangkat jaringan, salah satu cara mendeteksi serangan pada jaringan internet nirkabel dan kabel yaitu dengan menerapkan sistem yang dapat mendeteksi serangan serta penyusupan pada jaringan internet salah satunya adalah dengan menggunakan IDS *(Intrusion Detection System)*. IDS atau Sistem Pendeteksian Penyusupan adalah sebuah sistem keamanan jaringan yang ditujukan untuk memantau setiap aktivitas jaringan. IDS akan melakukan pendeteksian pada setiap pengguna yang terhubung dan setiap lalu lintas paket data yang melewati jaringan. Kemudian, Sistem IDS akan memberikan *Alert* pada administrator jaringan saat terjadi aktivitas yang mencurigakan pada jaringan [1]. Pada penelitian ini, penulis menggunakan jaringan internet nirkabel LAN *(Local Area Network)*, jaringan internet yang nirkabel LAN adalah jaringan nirkabel frekuensi radio yang

memungkinkan perangkat komputer untuk berkomunikasi satu sama lain dan, akhirnya, titik akses yang berfungsi sebagai dasar untuk transceiver radio dua arah yang biasanya beroperasi di *bandwith* 2,4 GHz (802.11b, 802.11g) atau 5 GHz (802.11a) [2].

Beberapa *software* IDS yang dapat digunakan antara lain Snort, OSSEC, Sagan, Bro, Suricata, dan Security Onion. Pada penelitian ini, penulis menggunakan *software* Security Onion. Security Onion adalah *software* IDS yang bersifat *open-source* yang dapat digunakan untuk memantau keamanan jaringan dan manajemen log. Untuk metode penelitian, penulis menggunakan metode penelitian *Live Forensic*. Metode *Live forensic* bekerja dengan mengidentifikasi serangan berdasarkan tipe serangan. Tipe serangan yang digunakan penulis untuk penelitian ini adalah DDOS. DDOS merupakan serangan memadati lalu lintas paket data dengan paket yang ilegal kemudian dikirimkan dengan serempak, tujuan dari DDOS ini adalah mematikan target dan mengganggu kinerja dari router [3].

Tujuan dari penelitian ini adalah untuk mengimplementasikan serta menganalisa sistem IDS pada sebuah jaringan internet. *Software* IDS atau NSM (*Network Security Monitoring*) yang digunakan pada penelitian ini adalah Security Onion. Security Onion dapat memantau serta menganalisa lalu lintas paket data yang melewati router. Sedangkan untuk pengujian, menggunakan *software* LOIC (*Low Orbit Ion Cannon*) untuk melakukan serangan terhadap jaringan internet yang telah di implementasikan Security Onion. Diharapkan, penelitian ini dapat membantu Administrator Jaringan untuk mendeteksi, menganalisa, serta mengambil tindakan selanjutnya pada saat serangan terjadi pada jaringan internet.

1.2 Rumusan Masalah

Berdasarkan judul penelitian serta penjelasan pada latar belakang tentang monitoring jaringan dengan Security Onion, yaitu :

1. Bagaimana cara melakukan pemantauan serangan DDOS serta melakukan pemantauan lalu lintas jaringan dengan menggunakan Security Onion ?

2. Bagaimana cara melakukan deteksi serangan DDOS dengan menggunakan Security Onion sebagai *Intrussion Detection System* (IDS) dan *Network Security Monitoring* (NSM) ?
3. Metode analisis apa yang digunakan pada penelitian IDS dan NSM dengan menggunakan Software Security Onion ?

1.3 Batasan Masalah

Berikut ini adalah beberapa batasan masalah yang ditetapkan dalam penelitian ini:

1. Penelitian ini dilakukan pada area jaringan internet nirkabel LAN milik penulis dengan skenario serangan dari luar jaringan
2. Mendeteksi serangan DDOS menggunakan sistem Security Onion pada jaringan internet dengan router Mikrotik
3. Proses investigasi menggunakan metode *live forensic*, investigasi dilakukan saat sistem hidup.
4. Perangkat keras yang digunakan dalam penelitian Laptop ASUS A442UR serta Mikrotik hAP lite RB941-2nD-TC untuk pemasangan Security Onion menggunakan Virtual Machine dari *software* VirtualBox, sedangkan perangkat lunak yang digunakan pada peneltian ini yaitu Winbox, LOIC (*Low Orbit Ion Cannon*), Virtual Box.

1.4 Maksud dan Tujuan Penelitian

Tujuan penelitian ini didasarkan pada beberapa pertimbangan yang telah penulis dipertimbangkan dengan matang, tujuannya antara lain :

1. Meningkatkan sistem keamanan jaringan dari adanya serangan DDOS menggunakan Security Onion pada router Mikrotik.
2. Menganalisis keamanan jaringan internet lokal terhadap serangan *Distributed Denial of Service*

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat menghasilkan manfaat penelitian tentang serangan DDOS pada Router Mikrotik. Selanjutnya diharapkan dapat menjadi

acuan bagi administrator jaringan dalam menganalisa setiap serangan DDOS pada jaringan internet lokal.

1.6 Metode Penelitian

Metode dalam penelitian yang digunakan oleh penulis adalah *Live Forensic*. Metode *Live Forensic* merupakan metode untuk mengumpulkan setiap data dan informasi untuk dijadikan barang bukti data yang berbentuk elektronik pada suattu jaringan internet [4]. Metode *Live Forensic* mengumpulkan setiap data, informasi, dan barang bukti pada saat sistem jaringan internet hidup. Dengan harapan pelaku serangan jaringan internet dapat segera teridentifikasi, maka administrator akan melakukan tindakan pencegahan terhadap serangan tersebut. Tahapan yang dilakukan pada penelitian ditunjukkan pada Gambar 1.3

Gambar 1. 1 Metode Live Forensic

1.7 Sistematika Penulisan

Pada bagian ini dituliskan urut-urutan dan sistematika penulisan yang dilakukan. Berikan ringkasan mengenai isi masing-masing bab.

1. BAB I : PENDAHULUAN

   Bab ini membahas tentang latar belakang masalah, definisi masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

2. BAB II : LANDASAN TEORI

Bab ini akan membahas teori fundamental yang mendasari penelitian sebelumnya dan dijadikan sebagai landasan pemecahan masalah dalam penelitian.

3. BAB III : METODOLOGI PENELITIAN

   Dalam bab ini, membahas metode penelitian yang digunakan dalam penelitian Analisis dan Implementasi Security Onion untuk mendeteksi serangan Distributed Denial of Service pada router Mikrotik.

4. BAB IV : HASIL DAN PEMBAHASAN

   Bab ini akan membahas bagaimana menghitung setiap parameter yang diuji secara matematis dan kemudian dianalisis berdasarkan standar yang telah ditentukan.

5. BAB V : PENUTUP

   Bab ini berisi kesimpulan akhir dan saran untuk penelitian selanjutnya..