BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Keamanan jaringan komputer yang lemah dapat memudahkan *hacker* dalam mengeksploitasi data-data penting dengan melakukan berbagai ancaman penyerangan siber (Wijoyo dkk., 2023). Mengemukakan dari pakar keamanan siber dari Cissrec, Pratama Persadha pada bulan Januari 2022 terjadi kebocoran data penting yang terjual bebas oleh para *hacker* (Pudyo P, 2022). Kepala Badan Siber dan Sandi Negara (BSSN) menyatakan pada *annual report* bahwa pada tahun 2023 negara Indonesia akan mengalami ancaman yang besar dalam menghadapi serangan siber ("Terbitkan Annual Report Berisi Prediksi Ancaman Siber 2023, BSSN," 2023).

Hal tersebut menjadi tantangan untuk menerapkan teknologi dalam menganalisis *log* pada jaringan komputer. *Security Information and Event Management* (SIEM) dapat digunakan dalam menganalisis infrastruktur jaringan komputer (Nabil & Yazid, 2023). Dalam melakukan deteksi serangan siber membutuhkan metode ilmiah untuk menemukan fakta dan bukti dalam aktivitas jaringan yang disebut *network forensics* (Wulandari, 2018). Terdapat berbagai jenis aplikasi SIEM gratis yang dapat mendeteksi serangan siber diantaranya adalah IBM QRadar *Community Edition* yang merupakan *tools* dengan teknologi *Artificial Intelligence* (AI) dalam mendeteksi anomali jaringan dan Snort yang populer digunakan oleh para *security analyst* dalam mengatasi ancaman siber (Fauzi, 2018; *IBM Security QRadar SIEM*, 2023).

Pada penelitian ini akan menganalisis serangan *Port Scanning*, Metasploit*/Exploit*, dan *Distributed* / *Denial of Service* (D/DoS) dengan menggunakan aplikasi SIEM gratis, yaitu IBM QRadar SIEM *Community Edition* dan Snort. Penelitian ini diharapkan dapat mengetahui perbandingan efektivitas dari dua aplikasi tersebut dari analisis kinerja deteksi serangan siber sebagai implementasi metode *network forensics* dalam mengatasi ancaman kejahatan siber.

1.2. Identifikasi Masalah Penelitian

Berdasarkan deskripsi latar belakang yang telah dideskripsikan di atas, maka identifikasi masalah dalam penelitian ini adalah sebagai berikut :

1. Ancaman siber yang banyak terjadi di Indonesia pada tahun 2023 mencakup serangan siber, berupa *port scanning*, metasploit/*exploit*, dan *Distributed / Denial of Service* (D/DoS).
2. Potensi serangan siber yang kapan saja bisa terjadi dalam perangkat yang terhubung dengan internet dan menyebabkan perangkat tersebut menjadi tereksploitasi akibat serangan siber.
3. Kejahatan siber yang membutuhkan forensik untuk mengumpulkan data berupa jejak digital sebagai metode mengenali serangan siber.

1.3. Rumusan Masalah Penelitian

Berdasarkan deskripsi latar belakang dan identifikasi masalah penelitian di atas, maka rumusan masalah yang didapatkan dalam peneltitian ini adalah sebagai berikut:

1. Bagaimana analisis terhadap proses menemukan bukti sumber serangan siber dengan metode forensik yang mengancam kerusakan pada jaringan komputer?
2. Bagaimana analisis terhadap implementasi *network forensics* menggunakan *tools* IBM QRadar SIEM *Community Edition* dan Snort agar dapat mendeteksi ancaman serangan siber?
3. Bagaimana analisis perbandingan efektivitas performa dari *tools* IBM QRadar SIEM *Community Edition* dan Snort dalam mendeteksi ancaman dan serangan siber dengan metode *network forensics*?

1.4. Tujuan Penelitian

Adapun tujuan melakukan penelitian ini, antara lain:

1. Melakukan analisis terhadap proses menemukan bukti sumber serangan siber dengan metode forensik yang mengancam kerusakan pada jaringan komputer.

2. Melakukan analisis terhadap implementasi *network forensics* menggunakan *tools* IBM QRadar SIEM *Community Edition* dan Snort agar dapat mendeteksi ancaman serangan siber.
3. Melakukan analisis perbandingan efektivitas performa dari *tools* IBM QRadar SIEM *Community Edition* dan Snort dalam mendeteksi ancaman dan serangan siber dengan metode *network forensics*.

1.5. Batasan Masalah Penelitian

Untuk menentukan arah penelitian terhadap tujuan penelitian, maka batasan terhadap masalah yang ditentukan sebagai berikut:

1. Menggunakan perangkat 1 laptop dengan OS Windows 10.
2. Spesifikasi laptop yang digunakan, yaitu: Intel Core i7-6700HQ (4 cores 8 threads @2.60 GHz), RAM 8GB up to 24GB DDR4, HDD 1TB, SSD 256GB NVME, GPU NVIDIA GeForce GTX 950M.
3. Aplikasi Virtualisasi pada laptop VMWare Workstation Pro 17.0.2 dengan menginstal Windows 10 sebagai *host* yang diserang, CentOS 7 sebagai sistem linux QRadar, Ubuntu 20.04.6 sebagai sistem linux snort, dan Kali Linux 2024.1 sebagai media penyerangan siber.
4. Menggunakan serangan siber *port scanning*, metasploit/*exploit*, dan *Distributed / Denial of Service* (D/DoS).
5. Menggunakan aplikasi Nmap, Metasploit Framework, dan *script* hping3 *Distributed / Denial of Service* (D/DoS) dalam menjalankan serangan.
6. Konfigurasi yang dilakukan pada IBM QRadar *Community Edition* terhadap *rules* sebatas *log source* dan *flow source*.
7. Konfigurasi yang dilakukan pada snort dengan menggunakan *file rules* atau local.rules sebagai deteksi serangan tertentu dan snort.conf sebagai *log source*.
8. *Network Forensics* yang digunakan sebagai metode dalam parameter efektivitas *tools* hanya fokus sebatas tahapan *Preparation*, *Detection*, *Incident Response*, dan *Collection* karena tahapan tersebut termasuk ke dalam lingkup *security analyst* pada *tools*. Sedangkan, tahapan

Preservation, Examination, Investigation, dan *Presentation* adalah bentuk bagian dari forensik yang perlu pengarsipan bukti digital.

9. Deteksi ancaman dan serangan diketahui dengan terlihatnya *event* atau *network activity* pada *tools* IBM QRadar *Community Edition* dan Snort dengan menampilkan informasi terhadap pengujian serangan yang dilakukan.

1.6. Manfaat Penelitian

Terdapat beberapa manfaat di dalam penelitian ini yang manfaatnya adalah sebagai berikut:

1. Pada masyarakat dan mahasiswa, penelitian ini diharapkan dapat memberikan pengetahuan baru mengenai serangan siber yang dapat mengganggu jaringan.
2. Bagi Institusi Universitas Pendidikan Indonesia, penelitian ini dapat dijadikan sebagai referensi ilmiah dalam mengembangkan pengetahuan seputar serangan siber.
3. Sebagai pengetahuan untuk mengembangkan inovasi dalam memperkuat keamanan sistem jaringan yang dapat diimplementasikan ke dalam *security analyst* di berbagai institusi maupun instansi.