BAB I
PENDAHULUAN

1.1 Latar Belakang

Semakin berkembangnya dunia digital dewasa ini semakin pesat pula penyebaran informasi melalui berbagai platform khususnya platform digital, penyebaran informasi yang semakin tinggi membutuhkan sebuah wadah yang dapat menampung segala sesuatu yang berkaitan dengan informasi yang ingin disebarluaskan. Berangkat dari hal tersebut terciptalah sebuah *Web*. *Web* diciptakan khusus sebagai wadah dan alat untuk menyebarluaskan informasi digital. Namun dari sisi keamanan, platform web dapat dibilang sebagai platform yang sangat rentan dari berbagai ancaman keamanan, hal ini tentu saja dapat membuat pengguna mengalami kerugian akibat dari serangan – serangan atau malware yang terdapat pada laman web. Salah satu serangan yang terdapat pada web yang mempunyai dampak langsung pada pengguna adalah *cryptojacking*. *Cryptojacking* adalah suatu tindakan yang dilakukan oleh orang yang tidak bertanggung jawab yang memakai *resource* dari komputer korban untuk menambang *cryptocurrency* seperti *coinhive* [1], *cryptojacking* mungkin masih asing ditelinga para pengguna internet khususnya pengguna *web*, karena *cryptojacking* dapat dijalankan secara otomatis dan tanpa disadari oleh korban, tercatat terdapat 33.000 website yang sudah tersisipi oleh skrip cryptojacking [2], selain itu tidak adanya sistem yang memberikan peringatan tentang *cryptojacking* menjadi masalah lain untuk pengguna *web*.

Berangkat dari masalah tersebut diatas, diperlukan sebuah *tool* untuk melakukan deteksi pada *server* untuk mendeteksi dan memberikan peringatan jika *cryptojacking* sedang dijalankan di *web* yang sedang diakses, salah satunya adalah menggunakan IDS *Snort*, yaitu sebuah *tool* untuk melakukan pendeteksian aktifitas mencurigakan atau tidak normal

yang terjadi pada sebuah sistem. Tool *snort* dipilih karena bersifat real time monitor yaitu dimana semua paket yang masuk ataupun keluar dari dan ke dalam jaringan akan disaring dan dianalisa secara langsung pada saat itu juga [3], selain itu sifat lain dari tool *snort* adalah fleksibel terhadap kebutuhan dari pengguna, selain itu keudahan dalam konfigurasi juga menjadi poin tambahan mengapa tool snort dipilih sebagai tool untuk melakukan deteksi terhadap serangan cryptojacking. Selain dari sisi kemudahan, kecepatan deteksi snort juga menjadi poin tambahan mengapa snort dipilih menjadi tool utama dalam penelitian ini.

1.2 Rumusan Masalah

Dari latar belakang yang sudah diuraikan, dapat di simpulkan masalah pada tugas akhir ini sebagai berikut :

1. Apakah tool snort dapat mendeteksi serangan cryptojacking?

1.3 Batasan masalah

Batasan masalah pada penelitian ini adalah :

1. Instalasi dan implementasi IDS Snort pada jaringan lokal.
2. Pengujian *Snort* dengan mengakses halaman *web "mixbelgorod.ru"* yang terdapat skrip *cryptojacking*.

1.4 Maksud dan Tujuan Penelitian

Tujuan dari tugas akhir ini adalah melakukan instalasi dan implementasi *Snort* pada sebuah jaringan lokal untuk melakukan deteksi terhadap *cryptojacking*.

1.5 Manfaat Penelitian

Manfaat yang didapatkan dari penelitian ini adalah para pengguna *internet* khususnya *web* dapat menghindari terjadinya *cryptojacking*.

1.6 Metode Penelitian

Penulis menjabarkan cara-cara memperoleh data-data yang digunakan untuk kebutuhan penelitian. Metode penelitian yang penulis gunakan dalam penyusunan skripsi ini adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

Penulis menggunakan metode studi Pustaka dalam pengumpulan data yang dimaksudkan untuk mendapatkan data teoritis menggunakan buku, jurnal dan sumber lainnya yang berhubungan dengan masalah yang diteliti. Metode pengumpulan data yang digunakan dalam penelitian antara lain :

1.6.1.1 Metode Observasi

Penulis mengamati dan mendapatkan hasil bahwa IDS snort mempunyai fungsi yang sangat berguna untuk mendeteksi serangan cryptojacking.

1.6.2 Metode Analisis

Metode analisis menggunakan analisis Eksperimen. Dimana terdapat beberapa langkah yang harus dilakukan dalam metode ini, yaitu Tahap Persiapan, Pelaksanaan Penelitian dan Pengolahan Data.

1.6.3 Metode Perancangan

Metode perancangan yang diaplikasikan oleh penulis yaitu menggunakan flowchart untuk membangun sistem keamanan berbasis snort.

1.7 Sistematika Penulisan

Sistematika penulisan yang dilakukan dalam skripsi ini akan dijelaskan dalam garis besar per-bab, yaitu sebagai berikut :

BAB I : PENDAHULUAN

Bab ini merupakan pengantar dari pokok permasalahan yang dibahas dalam skripsi ini, yaitu tentang latar belakang masalah, rumusan masalah, Batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas landasan teori tentang intrusion detection system (IDS) yang digunakan sebagai system keamanan pada sebuah server jaringan komputer beserta dengan tool dari IDS tersebut.

BAB III : METODE PENELITIAN

Bab ini menjelaskan tentang alat dan bahan dan alur penelitian yang digunakan dalam melakukan penelitian dan perancangan sistem keamanan berbasis IDS.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini adalah penjabaran tentang hasil dan pembahasan yang diperoleh dalam penelitian.

BAB V : PENUTUP

Bab ini membahas tentang kesimpulan dari implementasi IDS pada server jaringan komputer dalam mendeteksi serangan cryptojacking dan beberapa saran yang mungkin diperlukan untuk masa yang akan datang.

DAFTAR PUSTAKA

LAMPIRAN