BAB I
PENDAHULUAN

1. Latar Belakang

Teknologi informasi merupakan ilmu pengetahuan yang sekarang ini sedang berkembang dengan pesat. Seiring dengan perkembangan zaman, Teknologi Informasi memberikan pengaruh yang luar biasa bagi kemajuan ilmu pengetahuan yang bisa dimanfaatkan bagi setiap orang. Teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Karena banyak kemudahan yang ditawarkan, teknologi informasi hampir tidak dapat dilepaskan dari berbagai aspek kehidupan manusia. Seorang dapat dengan mudah mendapatkan informasi, referensi, pengetahuan, wawasan dan lain – lain yang didapat melalui TI. [1]

Dengan mudahnya pengaksesan terhadap teknologi informasi tersebut menyebabkan timbulnya masalah baru yaitu informasi atau data – data penting dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri. Sehingga sebuah sistem keamanan jaringan menjadi salah satu aspek yang sangat penting untuk diterapkan di jaringan internet. [2]

Pola keamanan jaringan yang sudah banyak diketahui tentunya menjadi masalah bagi seorang administrator untuk mengamankan sistem yang dikelolanya. Munculnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan pemerintah nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan *Telecom Act* menjadi angin segar bagi pengelola sistem karena pelaku dapat dijerat hukum. Untuk menjerat pelaku administrator perlu membuktikan pelaku bersalah. *Digital*

forensics dan *Network forensic* merupakan *alternative* untuk membuktikan pelaku kejahatan *cyber*. [3]

Berdasarkan penelitian sebelumya salah satu jenis serangan yang bisa terjadi adalah *sniffing*, dengan melakukan *sniffing*, *intruder* dapat membaca paket data yang lewat pada jaringan sehingga dapat mengakibatkan terjadinya kebocoran informasi penting seperti data pribadi, *username*, *password* dan lain-lain. [4]

Untuk itu dibutuhkan sebuah metode untuk mendeteksi terjadinya serangan *sniffing* agar dapat di analisa dan dijadikan sebagai bukti kejahatan digital. Berdasarkan penjabaran latar belakang di atas maka penulis akan melakukan penelitian berkaitan dengan "Analisis Forensik Pada *Snort* IDS Terhadap Serangan *Sniffing* Berbasis *Arp Spoofing*" penelitian ini bertujuan untuk melakukan analisa forensik saat terjadi serangan *sniffing* berbasis *arp spoofing / poisoning* dengan memanfaatkan *software Intrusion Detection System* (IDS) *Snort* untuk mengumpulkan bukti digital dan menemukan pelaku serangan.

1.2 Rumusan Masalah

1. Bagaimana proses analisis forensik, untuk mengetahui pelaku dan asal serangan saat terjadi serangan *sniffing*?
2. Apakah proses analisis forensik yang dilakukan berhasil menemukan asal serangan dan pelakunya?

1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini sebagai berikut:

1. Penelitian hanya membahas tentang serangan paket *sniffing* pada suatu server.

2. Serangan menggunakan metode *arp spoffing / poisoning* menggunakan aplikasi Ettercap.
3. Fokus penelitian pada bukti forensik terjadinya serangan *sniffing* dengan indikasi *arp spoffing*.
4. *Software* pendukung yang akan digunakan dalam penelitian kali ini adalah Ettercap, Snort IDS, Virtual Box, dan Linux.
5. Penelitian ini dilakukan dengan membangun jaringan virtual menggunakan Virtual Box.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Berdasarkan latar belang masalah di atas, maka maksud dari penelitian ini adalah mempelajari serangan yang terjadi pada suatu jaringan komputer, Khususnya pada serangan paket *sniffing*.

1.4.2 Tujuan Penelitian

Adapun tujuan penelitian ini sebagai berikut:

1. Sebagai syarat untuk mencapai gelar sarjana program studi informaatika Universitas AMIKOM Yogyakarta
2. Mengumpulkan bukti *forensic* terjadinya serangan.
3. Melakukan analisa fotensik untuk mengetahui asal dan pelaku serangan paket *sniffing*.

1.4.3 Manfaat Penelitian

Manfaat penelitian yang ingin dicapai dalam penelitian kali ini adalah:

1. Universitas Amikom Yogyakarta

   Arsip dan refrensi untuk mahasiswa angkatan selanjutnya dalam menyusun tugas perkuliahan, matrai perkuliahan, tugas akhir dan skripsi.

2. Peneliti

   a. Meningkatkan pengetahuan dan pemahaman terhadap jaringan computer, khususnya di bidang keamanan jaringan.

   b. Sebagai pengalaman dalam menganalisa, perancangan dan membuat sebuah jaringan, sehinggsa nantinya berguna di dunia kerja.

   c. Peneliti mengetahui tahapan – tahapan apa saja yang harus dilakukan dalam membuat suatu penelitian dan metode apa saja yang digunakan untuk mengatasi sebuah kasus.

3. Pembaca

   Memberikan pengetahuan kepada pembaca pada serangan yang terjdi pada suatu jaringan, khususnya serangan paket *sniffing*.

1.5 Metode Penelitian

1.5.1 Metode Pengumpulan Data

Pada tahap ini melakukan pencarian data dan informasi terkait permasalahn yang dianalisis melalui jurnal,buku,artikel dan internet untuk mendapatkan konsep teoritis dalam menanalisa data yang ada pada penelitian ini.

1.5.2 Metode Analisis

Pada tahap ini dilakukan analisis untuk menentukan kebutuhan yang diperlukan dalam penelitian. Perangkat tersebut terbagi dua yaitu perangkat lunak *(software)* dan perangkat keras (*hardware*).

1.6 Sistematika Penulisan

Sesuai dengan petunjuk penulisan laporan skripsi yang berlaku di Universitas Amikom Yogyakarta, sistematika penulisan laporan ini adalah sebagai berikut:

1.6.1 Bab I Pendahuluan

Bab ini menjelaskan latar belakang, rumusan masalah, batasan masalah, maksut dan tujuan penelitian, manfaat penelitian, metode penelitian yang dilakukan serta sistematika penulisan karya ini.

1.6.2 Bab II Landasan Teori

Bab ini menjelaskan landasan teori yang mendasari pemilihan parameter – parameter yang digunakan dalam penelitian ini serta *hardware* dan *Software* yang mendukung penelitian ini. Memaparkan sejumlah teori yang berkaitan dengan penelitian.

1.6.3 Bab III Metode Penelitian

Bab ini akan membahas secara lengkap alur penelitian yang dilakukan, metode pengambilan data, serta perancangan *hardware* dan *software* yang digunakan di penelitian ini.

1.6.4 Bab IV Hasil dan Pembahasan

Bab ini berisi tentang pemaparan hasil perancangan jaringan yang telah dibuat beserta konfigurasinya. Selain itu, dipaparkan pula cara pengujian penelitian menggunakan variabel pengujian yang telah ditentukan untuk merumumuskan hasil penelitian.

1.6.5 Bab V Kesimpulan dan Saran

Bab ini memaparkan kesimpulan dari penelitian yang dilakukan serta saran – saran untuk mengembangan penelitian ini lebih lanjut.