BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan informasi semakin pesat. Kemajuan sistem informasi memberikan banyak keuntungan bagi kehidupan manusia. Meski begitu aspek negatifnya juga banyak, seperti kejahatan komputer atau penyerangan yang berupa penyadapan data di jaringan komputer oleh pihak-pihak yang tidak bertanggungjawab. Hal itu terjadi karena kurang pengamanan yang tepat maupun ketidaktahuan masyarakat awam. Bahkan korban penyadapan ini pun tidak sadar bahwa ada seseorang yang sedang menyadapnya. Tidak hanya itu, penyadap juga melakukan penyerangan dengan berpura-pura memalsukan bahwa mereka adalah *host* yang dapat dipercaya. Pada kenyataannya, masih sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas penyadapan ini. [1]

Serangan yang paling sering terjadi di keamanan jaringan adalah *Port Scanning* dan *DOS (Denial Of Service)*. [2]

Keberadaan ilmu komputer forensik ini sangat dibutuhkan saat sekarang apalagi dimasa mendatang, karena banyaknya kejahatan-kejahatan berbasis komputer/digital yang tidak dapat dibuktikan secara nyata, sehingga terkadang tidak diakui sebagai alat bukti di pengadilan untuk kasus-kasus seperti ini. [3]

Oleh karena itu, penulis mengadakan penelitian dan penulisan skripsi tentang Digital Forensik dengan judul **"Analisis dan Perancangan**

Traceback Network Based Attack Menggunakan Metode ICMP Traceback".

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dapat didefinisikan rumusan masalah adalah : "Apakah metode ICMP Traceback dapat membantu dalam sistem *Traceback Network Based Attack* dengan baik untuk mendeteksi serangan DoS?"

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang diuraikan diatas, maka untuk mempermudah penelitian dibuat suatu masalah, meliputi :

1. Hanya melakukan penelitian dengan metode ICMP Traceback.
2. Tidak membahas tentang cara serangan DoS.
3. Analisa dan perancangan ICMP Traceback hanya pada 1 website, 2 sistem penyerangan berbeda dan 3 topologi.
4. Tidak membahas cara konfigurasi topologi jaringan.
5. Website tidak menggunakan sistem keamanan.
6. Hanya melakukan analisa serangan DoS.
7. Serangan menggunakan DoS.
8. Webserver menggunakan sistem operasi Debian 8.
9. Penyerang menggunakan sistem operasi Backbox.
10. Analisa menggunakan aplikasi Wireshark.
11. Website menggunakan *localhost*.
12. Penyerangan menggunakan Hping3 dan Loic.

13. Pengujian 1 topologi secara langsung (tanpa simulator), sedangkan 2 topologi dengan simulator GNS3.

1.4 Tujuan Penelitian

Tujuan penulisan penelitian yang ingin dicapai dari analisis dan perancangan Traceback network based attack menggunakan metode ICMP Traceback adalah sebagai berikut :

1. Dapat menganalisa dan merancangan serangan DoS dengan metode ICMP Traceback.
2. Dapat membandingkan hasil ICMP Traceback dari setiap topologi.
3. Membantu mengembangkan digital forensik di Universitas Amikom Yogyakarta.

1.5 Manfaat Penelitian

Adapun manfaat yang akan diperoleh oleh penelitian ini sebagai berikut :

1. Penelitian ini dapat memberikan informasi tentang cara analisis dan perancangan keamanan jaringan khususnya menggunakan metode ICMP Traceback.
2. Diharapkan dapat membantu dalam identifikasi terhadap serangan DoS.

1.6 Metode Penelitian

Penelitian ini menggunakan metode The Security Policy Development Life Cycle (SPDLC) sebagai acuan dalam membuat skripsi. [12]

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian.

BAB II LANDASAN TEORI

Pada bab ini akan dibahas mengenai landasan teori atau konsep dasar serta metode yang mendukung dalam penyusunan skripsi, seperti Tinjauan Pustaka, Pengertian Network Forensics, Konsep Dasar Serangan (Attack), DoS, Teknik Serangan DoS, Tools DoS, Teknik Bertahan Dari Serangan DoS, ICMP Traceback, Wireshark, Metode penelitian, serta berbagai teori lain yang berhubungan dengan pembahasan dan penyelesaian skripsi.

BAB III ANALISIS DAN PERANCANGAN

Bab ini akan menguraikan analisa dan perancangan Traceback network based attack menggunkana metode ICMP traceback ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menjelaskan tentang implementasi hasil analisis dan perancangang ICMP Traceback yang dibuat serta pembahasannya.

BAB V PENUTUP

Pada bab ini berisi kesimpulan dan saran yang dapat diambil dalam pembuatan skripsi ini.

DAFTAR PUSTAKA