1. PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, keamanan *website* dan *server* menjadi sangat penting. *Website* berkembang pesat dan mampu memenuhi kebutuhan penggunanya, seperti mengakses informasi, berbelanja, berkomunikasi, dan banyak lagi. Namun, kemajuan teknologi juga membuka celah bagi para penjahat *cyber* untuk melakukan serangan yang lebih kompleks dan bervariasi. Kemanan *website* dan *server* menjadi semakin penting untuk melindungi data pengguna dan menjaga kelancaran operasi.

Serangan terhadap *website* dan *server* dapat menimbulkan berbagai konsekuensi serius, seperti pencurian data, kerugian finansial, gangguan operasi, membuat para pengguna kehilangan kepercayaan pada perusahaan terkait, dan masih banyak lagi. Untuk jenis-jenis serangan yang umum terjadi pada *website* dan *server*, yaitu serangan *malware*, serangan *SQL injection*, serangan *Denial of Service (DoS)*, serangan *cross-site scripting (XSS)*, dan jenis serangan lainnya.

Salah satu metode yang biasa dilakukan untuk menguji keamanan dari sebuah *website* maupun *server* adalah *Distributed Denial of Service* (DDoS) *attack*, dimana penguji akan mengirimkan *fake traffic* pada server atau sistem yang akan diuji secara terus menerus hingga server atau sistem tidak mampu mengatur *traffic* dan dapat menyebabkan server atau sistem *down*. (Napizahni, M., 2022)

Dalam penelitian ini, target akan diserang dengan metode serangan *DDoS*. Penelitian ini menggunakan metode penyerangan tersebut karena berfokus pada ketahanan sistem yang akan diuji terhadap serangan *DDoS*.

Untuk melakukan *DDoS attack*, studi ini akan menggunakan *GoldenEye*. *GoldenEye* merupakan sebuah *tools open-source* yang dibuat untuk melakukan pengujian pada keamanan suatu sistem atau jaringan. *GoldenEye* dapat melakukan simulasi serangan *Denial of Service* (*DoS)* pada sistem atau jaringan yang ingin diuji agar dapat memahami bagaimana sistem atau jaringan yang diuji akan bereaksi. (Johan, 2023)

Selain akan dilakukan penyerangan terhadap sistem, penelitian ini juga akan menerapkan solusi tentang bagaimana cara bertahan atau melindungi dan mencegah sistem yang dimiliki dari *DDoS attack*. Terdapat beberapa cara yang diketahui secara umum mengenai bagaimana cara mencegah serangan *DDoS*, seperti menggunakan *hardware* dan *software* anti-*DDoS*, melakukan konfigurasi *hardware* yang dimiliki terhadap serangan *DDoS*, menggunakan alat perlindungan *DDoS* (*NetScout Arbor, Fortinet, Cisco,* dll.) dan masih ada beberapa cara lainnya. (Ramadhan, H. G., 2020)

Di luar pembahasan mengenai metode penyerangan yang akan dilakukan dalam penelitian ini sendiri, terdapat suatu *website* yang akan diuji. *Website* yang akan diuji merupakan *website* yang melakukan jual beli beragam jenis atau tipe mobil untuk para pengguna-nya yang sedang mencari atau ingin membeli mobil. Selain itu, terdapat salah satu fitur yang cukup banyak digunakan oleh para pengguna-nya yaitu tukar tambah mobil. Mobil yang di jual atau disediakan dalam *website* dijamin memiliki kualitas mesin yang dapat diandalkan dan dipercaya karena bagi pengguna yang ingin melakukan transaksi baik dalam tukar tambah maupun jual beli mobil akan diberikan garansi dari perusahaan terkait yang memiliki *website* tersebut.

Oleh karena itu, penting untuk memastikan bahwa sistem atau jaringan yang akan diuji dapat dikatakan aman dari serangan *Denial of Service* (*DoS*). Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan dan pemahaman yang lebih baik tentang cara mengevaluasi sebuah sistem dengan melakukan penyerangan seperti *Distributed Denial of Service* (*DDoS*) *Attack* pada *website* dan *server* XYZ dengan menggunakan *GoldenEye*, serta bagaimana hasilnya dapat digunakan untuk meningkatkan keamanan *website* maupun *server XYZ* dan mencegah sistem *down* akibat serangan *DDoS*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang ada, maka dapat dirumuskan masalah untuk proyek akhir ini sebagai berikut:

1. Apa saja kerentanan yang dapat ditemukan dalam *server* maupun *website* XYZ melalui proses *DDoS attack*?

2. Apa saja yang dapat dilakukan untuk melindungi sebuah sistem dari *DDoS attack*?

1.3 Tujuan Penelitian

Berdasarkan perumusan masalah di atas, dapat disimpulkan bahwa tujuan proyek akhir untuk menemukan dan memahami kerentanan yang terdapat dari sistem yang diuji, serta cara untuk melindungi sistem tersebut dari *DDoS attack*.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat bermanfaat bagi :

1. Bagi Pengguna Website:
    a. Meningkatkan loyalitas dari pengguna.
    b. Meminimalisir kehilangan atau pencurian pada data yang bersifat sensitif.
    c. Meningkatkan kepercayaan pengguna terhadap *website* perusahaan terkait
2. Bagi Pengembang Website:
    a. Membantu dalam proses pembuatan dan pengembangan *website* agar *website* menjadi lebih aman dan terpercaya.
    b. Memberikan pemahaman mengenai strategi untuk meningkatkan keamanan dari sebuah *website*.
3. Bagi Ilmu Pengetahuan:
    a. Menjadi referensi bagi peneliti lainnya yang ingin melakukan penelitian dengan topik serupa.
    b. Memperkaya informasi di bidang teknologi informasi, terutama pada pengembangan *website*.

1.5 Ruang Lingkup

Ruang lingkup penelitian ini dibatasi pada :

1. Menggunakan *GoldenEye*, *Hping3*, *Slowloris*, dan *TOR Proxychains* sebagai *tools* untuk melakukan serangan *DDoS* pada target.
2. Target yang menjadi uji percobaan serangan *DDoS* adalah *website* XYZ.
3. Menggunakan *Nmap* dan *Zenmap* untuk melakukan *Reconnaissance* dan *Scanning*.
4. Menggunakan *Kali Linux* dan *Ubuntu* sebagai media untuk menggunakan *tools* yang diperlukan untuk melakukan serangan terhadap target.
5. Metode serangan yang akan dilakukan adalah *Distributed Denial of Service (DDoS) attack*, dimana *website* dan *server* XYZ akan dibanjiri dengan *fake traffic* yang berlebih hingga *website* maupun *server* XYZ tidak dapat menampung *traffic* yang ada dan membuat *server* mati.
6. Terdapat 2 jenis serangan yang akan dilakukan dengan metode *DDoS*, yaitu serangan protokol dan serangan layer aplikasi.
7. Melakukan pemantauan terhadap target setelah serangan dilakukan untuk melihat dampak serangan yang ada pada target.
8. Melakukan evaluasi terhadap sistem keamanan yang dimiliki *website* dan *server* XYZ agar bisa memberikan rekomendasi cara bertahan dari serangan *DDoS* yang sudah dilakukan oleh peneliti.
9. Hasil penelitian akan berupa cara untuk melakukan serangan *DDoS* dan cara meningkatkan keamanan dari sistem yang sudah atau akan diserang dengan metode *DDoS*.
10. Hasil dari penelitian juga berupa laporan dari hasil analisis secara keseluruhan mengenai bagaimana *DDoS attack* dilakukan dan cara melindungi sistem dari *DDoS attack*. Beberapa hal terkait hasil penelitian yang akan dimasukkan ke dalam laporan penelitian adalah sebagai berikut :
    a. Kondisi *website* XYZ setelah dilakukan penyerangan.
    b. Akumulasi *traffic* pada saat dilakukan penyerangan.
    c. Pengaruh serangan *DDoS* yang telah dilakukan terhadap pengguna *website* XYZ.
    d. Tools yang bisa digunakan untuk melindungi sistem dari serangan *DDoS*.
    e. Strategi atau langkah proaktif yang dapat diterapkan untuk mencegah serangan *DDoS*.

1.6 Metodologi Penelitian

Langkah-langkah dalam pengerjaan skripsi :

1. Persiapan & *Planning*
2. Implementasi *Distributed Denial of Service* (*DDoS*) *Attack*
3. Strategi Bertahan dan Perbaikan Sesuai Rekomendasi Oleh Perusahaan
4. Membuat Laporan Akhir Kesimpulan Pengujian

1.7 Sistematika Penulisan

Penulisan pada skripsi ini dibagi menjadi beberapa bab, seperti sebagai berikut :

- Bab I : Pendahuluan

  Bab ini berisikan judul penelitian, latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup penelitian, dan metodologi penelitian.
- Bab II : Teori Penunjang

  Bab ini berisikan teori yang mendasari metode dan implementasi pada penelitian ini.
- Bab III : Metodologi Penelitian

  Bab ini berisikan pembahasan mengenai desain dari sistem pengerjaan yang akan dilakukan.
- Bab IV : Implementasi Sistem

  Bab ini berisikan implementasi dari metodologi penelitian yang dimiliki.
- Bab V : Pengujian

  Bab ini berisikan hasil uji dari serangan dengan metode *DDoS* dengan menggunakan *tools* yang diperlukan.
- Bab VI : Kesimpulan dan Saran

  Bab ini berisikan kesimpulan dari segala hasil selama penelitian dilakukan dan saran bagi instansi atau perusahaan terkait.