BAB I
PENDAHULUAN

1.1 Latar Belakang

Analisis keamanan jaringan pada web merupakan hal yang sangat penting bagi organisasi dan perusahaan yang mengandalkan teknologi informasi untuk menjalankan bisnis mereka. Hal ini sangat krusial mengingat bahwa jaringan web merupakan bagian dari infrastruktur teknologi informasi yang paling rentan terhadap serangan. Salah satu jenis serangan yang dapat mengancam keamanan jaringan web adalah serangan DDoS (*Distributed Denial of Service*).

Serangan DDoS adalah jenis serangan yang dilakukan dengan membanjiri jaringan dengan permintaan yang tidak sah sehingga mengakibatkan kerusakan atau gangguan pada sistem. Serangan ini dilakukan dengan memanfaatkan ribuan komputer yang terinfeksi virus atau *malware* dan digunakan sebagai bot untuk melakukan serangan. Serangan DDoS dapat menyebabkan kerugian besar bagi perusahaan, termasuk kerusakan pada infrastruktur jaringan, kehilangan produktivitas, dan kerugian finansial. [1]

Untuk mengatasi masalah ini, metode *live forensics* digunakan untuk menganalisis serangan DDoS secara *real-time. Live forensics* adalah proses mengumpulkan dan menganalisis data yang dikumpulkan saat serangan sedang berlangsung. Proses ini memungkinkan untuk mengidentifikasi sumber serangan dan memastikan bahwa data yang dikumpulkan tidak terpengaruh oleh serangan. Setelah sumber serangan teridentifikasi, tim keamanan dapat mengambil tindakan untuk memblokir serangan dan mencegah serangan berulang.

Analisis keamanan jaringan pada web saat terjadi serangan DDoS sangat penting untuk memastikan bahwa jaringan tetap aman dan memastikan bahwa serangan tidak akan berulang. Proses ini juga membantu untuk memastikan bahwa perusahaan dapat melanjutkan bisnis mereka tanpa gangguan dan bahwa data dan informasi klien tetap aman.

Secara keseluruhan, analisis keamanan jaringan pada web saat terjadi serangan DDoS dan penggunaan metode *live forensics* merupakan hal yang penting untuk memastikan keamanan jaringan dan melindungi organisasi dari serangan yang merugikan.

1.2 Rumusan Masalah

Rumusan masalah dari proyek akhir ini adalah:

1. Bagaimana cara mengidentifikasi tanda-tanda serangan DDoS yang sedang terjadi pada jaringan web?
2. Bagaimana cara menganalisis data yang telah diperoleh untuk mencari tahu sumber serangan DDoS?
3. Bagaimana cara mencari tahu cara terbaik untuk menangani serangan DDoS yang sedang terjadi?

1.3 Batasan Masalah

Batasan masalah dari proyek akhir ini adalah:

1. Penelitian ini hanya memfokuskan pada analisis keamanan jaringan web yang menggunakan metode *live forensics*. Sehingga, penelitian ini tidak mencakup analisis keamanan jaringan web dengan menggunakan metode lain.
2. Penelitian ini hanya membahas serangan DDoS sebagai ancaman keamanan jaringan web. Sehingga, penelitian ini tidak mencakup ancaman keamanan jaringan web lainnya.
3. Penelitian ini hanya menggunakan perangkat lunak yaitu
    a) Suricata sebagai IDS
    b) Firewall sebagai keamanan
    c) Putty sebagai perangkat lunak untuk mengakses SSH
    d) Python untuk menjalankan perangkat lunak penyerangan dan
    e) GoldenEye sebagai perangkat lunak untuk melakukan penyerangan.
4. Penelitian ini hanya menggunakan VPS untuk membuat target penyerangan dan penyerang serta menggunakan *Personal Computer* (PC) untuk mengontrol atau mengatur VPS serta digunakan untuk menganalisis dan mengolah data.
5. Pada Penelitian ini sudah terpasang website dan aapanel pada VPS, sehingga penelitian ini tidak mencakup cara pemasangan website dan aapanel
6. Penelitian ini hanya dapat digunakan untuk yang memiliki akses *superuser* atau *root* pada server. Sehingga, penelitian ini tidak mencakup *user* biasa pada server.

7. Pada penelitian ini tidak membahas cara mengkoneksikan domain dengan DNS Cloudflare.

1.4 Tujuan Penelitian

Tujuan penelitian dari proyek akhir ini adalah:

1. Menggunakan metode *live forensics* untuk mengidentifikasi dan menganalisis tanda-tanda serangan DDoS pada jaringan web secara *real-time.*
2. Menghadapi dan mitigasi serangan DDoS pada situs web dengan pendekatan *live forensics* guna menjaga kinerja dan ketersediaan.
3. Meningkatkan keamanan jaringan web terhadap serangan DDoS dengan mengetahui cara terbaik untuk menangani serangan DDoS yang sedang terjadi.

1.5 Manfaat Penelitian

Manfaat penelitian dari proyek akhir ini adalah:

1. Penelitian ini dapat membantu perusahaan atau organisasi untuk lebih memahami tanda-tanda serangan DDoS dan mengambil tindakan pencegahan serta respons yang lebih cepat dan efektif. Hal ini akan meningkatkan kesadaran staf terhadap ancaman tersebut dan membantu melindungi kinerja dan ketersediaan layanan.
2. Penelitian ini dapat diintegrasikan ke dalam kurikulum pendidikan di kampus, memberikan pelajar akses ke studi kasus nyata tentang serangan DDoS dan metode *Live Forensics*. Ini akan memperkaya pengalaman belajar mereka dalam bidang keamanan jaringan dan teknologi informasi

1.6 Metodelogi Penelitian

Tahapan-tahapan yang dilakukan dalam pengerjaan tugas akhir ini adalah sebagai berikut:

1. Penyusunan Proposal Tugas Akhir

   Tahap awal dalam penelitian ini adalah menyusun proposal tugas akhir yang berisi deskripsi tentang analisis keamanan jaringan pada web saat terjadi serangan DDoS dan penggunaan metode *live forensics*. Dalam proposal, akan dibahas tentang gambaran umum dari tugas akhir, termasuk garis besar dari proses analisis yang akan dilakukan. Tujuan dari penelitian ini adalah untuk mengatasi serangan DDoS dengan menganalisis jaringan web secara *real-time* dan mengidentifikasi sumber serangan.

2. Studi Literatur

   Pada tahap ini dilakukan untuk mencari informasi dan studi literatur apa saja yang dapat dijadikan sebagai referensi untuk membantu pengerjaan tugas akhir ini. Tahap ini merupakan tahap untuk memahami semua metode yang akan dikerjakan, sehingga memberi gambaran selama pengerjaan tugas akhir. Informasi didapatkan dari buku dan literatur yang berhubungan dengan metode yang digunakan.

3. Implementasi

   Implementasi merupakan tahap untuk mengimplementasikan metode-metode yang sudah diajukan pada proposal Tugas Akhir. Dalam tahap ini, data yang dikumpulkan akan dianalisis dan diterapkan metode *live forensics* untuk mengidentifikasi sumber serangan DDoS. Tahap ini meliputi tiga tahap utama, yaitu melakukan uji coba, mengumpulkan data hasil uji coba, dan melakukan analisa terhadap data hasil uji coba.

4. Evaluasi

   Tahap ini bertujuan untuk mengukur efektivitas metode yang telah diterapkan dan mengevaluasi keberhasilan dari analisa dan solusi yang telah diajukan. Evaluasi yang dilakukan akan membantu dalam menentukan apakah metode analisa dan solusi yang diterapkan efektif dalam mengatasi serangan DDoS pada jaringan.

5. Penyusunan Buku

   Pada tahap ini disusun buku sebagai dokumentasi dari pelaksanaan tugas akhir yang mencangkup seluruh konsep, teori, implementasi, serta hasil yang telah dikerjakan.

1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini akan membahas tentang latar belakang, permasalahan, tujuan, manfaat, metodologi dan sistematika penulisan penelitian. Hal ini akan membantu memberikan pemahaman pada pembaca mengenai masalah yang akan dibahas dan bagaimana hasil penelitian ini dapat berguna bagi pembaca. Bab ini akan memaparkan secara singkat apa yang akan dibahas pada penelitian ini.

BAB II LANDASAN TEORI

Bab ini membahas teori-teori yang terkait dengan penelitian ini, seperti definisi serangan DDoS, metode *live forensics*, keamanan jaringan, dan

lainnya. Bab ini akan memperkaya pemahaman pembaca mengenai hal-hal yang berhubungan dengan penelitian ini, dan menjadi dasar untuk analisa dan pembahasan pada bab berikutnya

BAB III PERANCANGAN DAN ANALISA

Bab ini membahas analisa dari penelitian yang dilakukan. Analisa ini akan memaparkan bagaimana metode *live forensics* dapat membantu dalam mengatasi serangan DDoS dan memperkuat keamanan jaringan web.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas hasil dari analisa yang dilakukan dan pembahasan mengenai hasil tersebut. Pembahasan ini akan memaparkan bagaimana hasil analisa dapat menjawab permasalahan yang diajukan dalam penelitian ini.

BAB V PENUTUP

Bab ini membahas kesimpulan dan rekomendasi dari penelitian yang dilakukan. Kesimpulan ini akan memaparkan hasil dari analisa dan pembahasan pada bab sebelumnya, dan memberikan rekomendasi bagi pembaca mengenai hal-hal yang dapat dilakukan untuk mengatasi serangan DDoS dan memperkuat keamanan jaringan web.