BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan internet pada era saat ini sudah menjadi kebutuhan utama dalam aktivitas sehari-hari. Sehingga keamanan suatu jaringan komputer yang terhubung dengan layanan internet sangat penting. Sehingga apabila terjadi ancaman dari tindak *hacker* dapat mencuri informasi data dan serangan tersebut dapat merusak jaringan komputer. Jenis serangan yang sering digunakan oleh *hacker* adalah *Denial of Services (DOS)* yang bersifat mengirimkan sejumlah paket melalui *internet protocol (IP)* secara terus menerus yang dapat mengganggu organisasi dari jaringan komputer dengan tujuan melumpuhkan *server*.

Kejahatan siber (*cybercrime*) dan jaringan sangat penting dalam dunia yang semakin terhubung secara digital. Di mana teknologi informasi dan jaringan memainkan peran sentral dalam kehidupan sehari-hari. Adanya kejahatan siber menjadi ancaman dalam kehidupan manusia, sehingga menyulitkanm organisasi dan pemerintah untuk mengatasi kejahatan yang dilakukan dalam teknologi komputer. Kejahatan ini berdampak buruk pada masyarakat, perusahaan, perbankan, dan lainnya. Salah satu *cybercrime* yang sering terjadi pada suatu jaringan dan sistem yaitu *Denial of Service (DOS) Attack* dan *Brute force Attack.*

Dari beberapa serangan *cybercrime* salah satunya adalah metode *brute force*, dimana metode *brute force* adalah metode yang bertujuan untuk mendapatkan hak akses masuk ke suatu sistem secara paksa dengan mencoba semua kemungkinan *username* dan *password* yang sudah disiapkan *attacker* dalam sebuah wordlist

dengan bantuan *software* seperti THC Hydra, Medusa dan lain-lain (Syaputera A, Riska, Yessi Mardiana., 2023). *Brute force attack* adalah metode peretasan yang dilakukan menggunakan cara *trial* and *error* untuk memecahkan kata sandi, kredensial *login*, maupun kunci enkripsi. Peretas mencoba mengirimkan banyak kata sandi atau frasa sandi dengan tujuan dapat menebak dengan benar.

Jaringan internet pada era saat ini sudah menjadi kebutuhan utama dalam aktivitas sehari-hari. Sehingga keamanan suatu jaringan komputer yang terhubung dengan layanan internet sangat penting. Sehingga apabila terjadi ancaman dari tindak *hacker* dapat mencuri informasi data dan serangan tersebut dapat merusak jaringan komputer. Jenis serangan yang sering digunakan oleh *hacker* adalah *(Denial of Services) DOS* yang bersifat mengirimkan sejumlah paket melalui *internet protocol (IP)* secara terus menerus yang dapat mengganggu organisasi dari jaringan komputer dengan tujuan melumpuhkan *server* (Fanani dan Riadi, 2020).

Denial of Service atau *DOS* merupakan serangan yang terbilang cukup kuat untuk melukai sebuah infrastruktur dari suatu organisasi. Serangan *Denial of Service (DOS)* bertujuan untuk mencegah pengguna menikmati layanan yang diberikan suatu *server* dan pada akhirnya *server* tersebut akan down. Serangan *Denial of Service (DOS)* memiliki sifat satu lawan satu, sehingga dibutuhkan *host* yang dapat membanjiri lalu lintas sebuah *host* target sehingga mencegah klien untuk mengakses layanan jaringan pada *server* yang dijadikan target oleh penyerang.

Untuk mengurangi dan mencegah dampak serangan kejahatan *cyber* pada dunia digital, maka dibutuhkanlah *cyber security* atau kemananan siber yang bertugas untuk mencegah dan melindungi sistem komputer maupun data.

Keamanan siber mempunyai kedudukan berarti dalam melindungi keamanan data sebab jadi perihal yang krusial buat melindungi informasi dalam media penyimpanan serta menjamin data yang dikirim dalam kondisi nyaman dan proteksi sistem data terhadap ancaman siber (Sudarmadi, Runturambi., 2019).

1.2 Rumusan Masalah

Berdasarkan uraian dari latar belakang yang ada maka perumuasan masalah dari penelitian ini adalah apakah penindakan serangan *Denial of Service* (DOS) berbasis *brute force* menggunakan Wireshark dapat dicegah?

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah mengaplikasikan serangan *Denial of Service* berbasis *brute force* menggunakan Wireshark.

Adapun tujuan khusus pada penelitian ini, yaitu:

1. Mencari cara penindakan serangan *Denial of Service (DOS)* melalui Wireshark.
2. Mengetahui *lateral movement* pelaku dalam melakukan serangan *Denial of Service (DOS)* berbasis *brute force*.

1.4 Ruang Lingkup

Pada penelitian ini membahas:

1. Analisa serangan *Denial of Service (DOS)* berbasis *brute force* dan mencakup*: sniffing tools,* analisa *traffic capture, lateral movement, pivoting, network share, backdoor.*
2. Pembahasan tentang *cyber security* terkait *cyber blue team* (*defender*).
3. Aplikasi yang digunakan dalam penelitian ini adalah Wireshark.

Pada penelitian ini tidak membahas dan tidak mencakup:

1. Bagaimana cara untuk mengoperasikan *cybercrime.*
2. *Cyber Security* lainnya *(Red Team, Green Team, Purple Team, Yellow Team, Orange Team). Cyber Team* mempunyai tugasnya masing-masing sesuai dengan *role* nya. *Yellow Team (Software Coders and Architects, "The Builders"), Orange Team (Facilitate Education), Red Team (Offensive Security, "The Breakers"), Purple Team (Integration Defensive TacticsS with Offensive Result), Blue Team (Defensive Security, "The Defenders"), Green Team (Enhance Security Automation with Design Code).* Pada penelitian ini hanya mencakup *Cyber Blue Team* atau yang dikenal dengan *The Defender* dikarenakan membahas seputar melindungi sistem komputer, jaringan, dan data dari serangan atau akses ilegal.
3. Penelitian ini hanya menggunakan *port* 445 dan tidak membahas detail *port* lain selain *port* 445.