BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era modern saat ini teknologi informasi dan sistem informasi sudah berkembang sangat pesat. Perkembangan tersebut berpengaruh pada berbagai bidang yang menggunakan IT untuk memperoleh informasi-informasi penting seperti data diri, informasi rahasia suatu instansi atau perusahaan (Wijatmoko, 2020). Informasi tersebut rawan dengan kejahatan siber yang dilakukan oleh individu atau kelompok orang yang lebih sering disebut *hacker. Hacker* ini menjadi salah satu pelaku kejahatan siber yang berkemungkinan untuk mengancam keamanan informasi.

Keamanan informasi sangat rentan terhadap pengguna jahat dan perangkat lunak yang dirancang untuk membahayakan server atau sistem web. Serangan siber dapat berupa serangan aktif dan pasif. Ketika serangan aktif memodifikasi data sistem dengan maksud membahayakan sistem operasi, serangan pasif di mana peretas menggunakan data sistem tetapi tidak membahayakan sistem operasi (Nurwa et al., 2023). Dalam melancarkan serangannya para penyerang (*attacker*) mencari internet yang terhubung ke server agar mereka dapat melancarkan serangannya ke server tersebut. Salah satu target yang paling sering diserang yaitu layanan akses jarak jauh, misalnya *Scure Shell* (SSH) (Jamaludding et al., 2023).

Secure Shell (SSH) adalah protokol jaringan yang berada di lapisan aplikasi protokol TCP/IP dan memungkinkan komunikasi yang aman antara dua sistem menggunakan arsitektur klien-server yang menyediakan kerahasiaan dan integritas data melalui teknik enkripsi dan dekripsi yang dapat diterapkan. Secara otomatis dalam koneksi, menggunakan SSH membutuhkan otentikasi pengguna dalam bentuk kunci publik dan kata sandi terenkripsi. Para penyerang sering menyerang port ssh ini menggunakan metode *brute force attack* yang mana presentase serangannaya bisa mencapai 25% dibawah serangan *Denial of Service* (Dos) (Hardjianto, 2022).

Pada serangan *brute force*, penyerang menggunakan protocol SSH dan

telnet untuk mengetahui *password login*. Protocol yang digunakan ini memungkinkan dapat bertukarnya data antara dua perangkat jaringan yang berbasisi linux dan unix (Fachri, 2023). Adapun salah satu cara yang dilakukan untuk mengatasi serangan brute force adalah menggunakan *honeypot*.

Honeypot adalah salah satu aplikasi untuk membaca serangan yang dilakukan oleh *attacker*. *Honeypot* adalah layanan palsu yang berfungsi menjebak penyerang yang bertujuan untuk melakukan pencurian atau perusakan data yang dapat merugikan sistem. Aplikasi honeypot bekerja dengan cara menyembunyikan service port ssh yang asli. Kemudian dibuat service port ssh palsu yang akan di akses oleh penyerang. Sehingga dengan aplikasi honeypot ini diharapkan dapat terhindar dari serangan dan bisa memantau pola serangan untuk meningkatkan keamanan (Arkaan & Sakti, 2019).

Dalam melakukan pencegahan dan perlindungan keamanan informasi terhadap suatu serangan siber misalnya seperti pada *brute force attack*, penggunaan *honeypot* dilakukan dengan mengumpulkan data *honeypot* dan menganalisisnya. Data yang dikumpulkan *honeypot* berupa data-data seperti log waktu (upaya login gagal yang dicatat), alamat IP penyerang, informasi pengguna yang diserang, metode otentifikasi yang digunakan dan kredensial yang digunakan. Pada umumnya, tahapan dalam menganalisisnya antara lain mengidentifikasi log waktu serangan *brute force* yang lebih sering dilakukan pada jam dan waktu kapan saja, menganalisis alamat IP dari penyerang dan alamat IP yang mencurigakan, mengidentifikasi kredensial (*username* dan *password*) yang sering diserang dan melakukan evaluasi (Rupiat et al., 2020).

Pengetahuan tentang *honeypot* dan cara melakukan analisis terhadap serangan siber seperti *brute force attack* perlu untuk diketahui agar dapat meningkatkan pemahaman tentang keamanan informasi. *Brute force attack* sendiri menjadi suatu serangan siber yang dilakukan dengan cara masuk ke suatu sistem menggunakan kombinasi *username* dan *password* yang berbeda-beda. Tujuan dilakukannya *brute force attack* ini sendiri untuk mencuri data-data pribadi pengguna, mengambil alih akun dan menyusup ke sistem. Maka dari itu, perlu dilakukannya pencegahan dini terhadap *brute force attack* dan

perlindungan keamanan informasi. Melalui permasalahan tersebut, peneliti tertarik untuk melakukan penelitian yang berjudul "**ANALISA POLA SERANGAN BRUTE FORCE ATTACK PADA PORT SSH**".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dibuat sebelumnya maka rumusan masalah dari penelitian ini sebagai berikut:

1. Apa faktor-faktor yang mempengaruhi frekuensi dan intensitas serangan brute force attack pada port ssh?
2. Bagaimana dampak serangan brute force attack pada port ssh terhadap keamanan dan kinerja sistem?
3. Apa strategi pencegahan dan mitigasi serangan brute force attack pada port ssh yang efektif dan efisien?

1.3 Tujuan penelitian

Adapun tujuan untuk mengidentifikasi pola serangan *brute force* attack pada port SSH sehingga dapat dianalisis cara pencegahan serangan dengan cara Penerapan Kebijakan Kata Sandi yang Kuat.

1.4 Batasan Masalah

Batasan masalah pada penelitian ialah sebagai berikut:

1. Penelitian ini hanya menganalisis pola serangan brute force attack pada port ssh yang tercatat di server log selama periode juni-agustus 2023.
2. Penelitian ini hanya menggunakan metode analisis data kuantitatif dengan bantuan perangkat lunak statistik.
3. Penelitian ini hanya menguji pengaruh variabel waktu, lokasi, dan sumber serangan terhadap frekuensi dan intensitas serangan brute force attack pada port ssh.
4. Penelitian ini hanya mengukur dampak serangan brute force attack pada port ssh berdasarkan indikator downtime, bandwidth, dan kerugian finansial.
5. Penelitian ini hanya merekomendasikan strategi pencegahan

1.5 Manfaat Penelitian

Pada penelitian ini diharapkan dapat memberi manfaat sebagai berikut :

1. Dengan menganalisa pola serangan *brute force attack* pada port SSH, penelitian ini dapat membantu pengamanan sistem untuk menemukan celah keamanan dan mengambil tindakan pencegahan yang tepat, sehingga meningkatkan keamanan sistem secara keseluruhan.
2. Dapat mengetahui waktu dan jam tertentu yang digunakan oleh penyerang (*attacker*) dalam melakukan *brute force attack* pada port SSH sehingga penyerangan yang akan dilakukan dapat diantisipasi.
3. Dapat mengetahui strategi penyerangan yang dilakukan oleh penyerang (*attacker*) ketika melakukan *brute force attack* pada port SSH. Dengan adanya pengetahuan tentang strategi penyerangan oleh penyerang, maka *counter* dari strategi yang akan digunakan oleh *attacker* dapat disesuaikan dan diatur ulang