BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sangat pesat menuntut meningkatnya kualitas keamanan jaringan. Terutama dengan semakin terbukanya ilmu tentang *hacking* dan *cracking* yang di dukung oleh *tools* yang bisa di dapatkandenganmudah dan gratis. Banyaknya sebuah komunitas group *hacking* dan *cracking* yang di bentuk, menjadi ancaman terhadap sebuah tindak kejahatan pada system keamanan informasi. Karena tidak hanya orang-orang yang menguasai teknologi informasi (TI) saja yang mampu melakukan tindak kejahatan (*cyber crime*) ini. Oleh karena semakin terbukanya ilmu pengetahuan tentang *hacking* dan *cracking* ini maka perlunya untuk membuat perancangan system keamanan yang mampu memantau lalu lintas jaringan dan mem-block aktivitas-aktivitas yang mencurigakan dan dapat dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut.

Selain itu yang menjadi ancaman keamanan jaringan komputer juga datang dari *virus, trojan, DOS, TCP/IP, spoofing, refliying, malicius, spamming,* dan lainnya. Hal inilah yang dapat mengancam system keamanan jaringan dimana data dapat diambil dan dirusak bahkan dihapus oleh para *attacker*. Sebagai contoh, pada tahun 2018 jumlah kasus pencurian data yang dilakukan oleh *hacker* sebanyak 945

kasus. Sementara, pada tahun 2017 kasus pencurian data mencapai 1.162 kasus. Berdasarkan laporan dari perusahaan keamanan Gemalto, jumlah data yang di bobol oleh *hacker* perharinya mencapai 6,9 juta data. Hal ini berdasarkan laporan pencurian data sejak 2013 hingga 2018 yang jumlahnya sebanyak 14,6 miliar. Dari sekian banyak jumlah kehilangan data tersebut, hanya 4 persen dari jumlah tersebut yang dilindungi dengan enkripsi oleh pemiliknya (Aswandi et al., 2020).

Untuk membantu mencegah dari hal-hal yang bersifat membahayakan jaringan tersebut, maka dibutuhkan suatu system keamanan yang bias mendeteksi danmengatasi untuk mencegah serangan-serangan yang akan dilakukan oleh para *attcaker* (penyerang), dan untuk mengatasi hal tersebut penulis memilih menggunakan sebuah *software*/aplikasi yaitu *Intrusion Prevention Sytem* (IPS) yang akan bertindak sebagai *firewall* yang bias menerima atau menolak paket yang masuk, dan akan dimasukan kedalam *IPTables*.

IPTables adalah program aplikasi (berbasislinux) yang memungkinkan administrator system untuk mengkonfigurasi tanel yang disediakan oleh *firewall* kernel *Linux* dan di rantai aturan di tempat itu yang berfungsi sebagai alat untuk melakukan filter (penyaring) terhadap lalu lintas data (*trafic*), dan IPTables mampu dijadikan sebagai metodologi *Intrusion Prevention System* (IPS) yang memiliki kemampuan memeriksa dan mencatat semua paket data, dan menolak akses yang teridentifikasi oleh kemungkinan packet dari seseorang *attacker* misalnya seperti *virus, trojan, DOS/IP Spoofinng, Repliying, Spaming* atau kejahatan lainnya. Di

IPTables juga terdapat beberapa system operasi *Linux* yaitu *Ubuntu, CentOs, Red Hat, Fedora*, dan sebagainya.

Dari penelitian sebelumnya yang dilakukan oleh (Salbani, 2019) berjudul perbandingan *Intrusion Prevention System* (IPS) pada *Linux server* dengan *Mikrotik Router Board*. Mengatakan bahwa dalam mengatasi serangan *DdoS Linux server* lebih baik disbanding *Mikrotik RouterBoard*, dari segi deteksi *Linux Server* dan Mikrotik *RouterBoard* mempunyai keamampuan yang sama, akan tetapi pada persentase CPU *Usage Mikrotik RouterBoard* bekerja lebih keras di banding *Linux Server*, dan juga saat pencatatan Log Mikrotik hanya bertahan 8 menit, sedangkan pada *Linux Server*s selama 10 menit, pengujian *Linux Server* masih bias mencatat log.Mengutip dari hasil penelitian tersebut bahwa *Linux Server* lebih baik dibanding *Mikrotik RouterBoard*. Maka dari ini penulis akan meneliti system operasi *Linux* manakah yang lebih efisien dalam mencegah serangan.

Oleh karena itu dari latar belakang diatas maka penulis akan melakukan penelitian sekaligus untuk menyususn skripsi yang berjudul **"ANALISIS DAMPAK PENERAPAN INTRUSION PREVENTION SYSTEM (IPS) TERHADAP KEAMANAN JARINGAN PADA SISTEM OPERASI LINUX UBUNTU DAN LINUX CENTOS"**. Penulis membatasi penelitian ini pada keamanan jaringan menggunakan *system* keamanan *Intrusion Prevention Sytem* (IPS) dengan tujuanuntuk meningkatkan dan menagamati system keamanan jaringan manakah yang lebih aman, dan melakukan analisis *IPTables* yang di implementasikan pada *Linux Ubuntu* dan *Linux CentOs*.

1.2 Perumasan Masalah

Dari latar belakang yang telah di paparkan diatas maka rumusan msalah yang akan dikaji adalah bagaimana perbandingan diantara *IPtables* pada *Linux Ubuntu* dan *Linux CentOs*.

1.3 Batasan Masalah

Hal-hal yang akan dilakukan dalam skripsi ini dibatasi pada pembatsan masalah yang akan dibahas yaitu :

1. Proses pengujian serangan yang dilakukan adalah serangan *Brute Force*.
2. Sistem operasi yang digunaka adalah *Linux Ubuntu* dan *Linux CentOs*.
3. Akan melakukan perbandingan sebuah system keamanan dari *IPtables* pada sistem operasi *Linux Ubuntu* dan *Linux CentOs*.

1.4 Tujuan dan MafaatPenelitian

1.4.1 Tujuan Penelitian

Pada penelitian ini penulis memiliki tujuan seperti berikut :

1. Merancang keamanan jaringan yang aman menggunakan *IPTables* pada sistem operasi *Linux Ubuntu* dan *CentOs*.
2. Menganalisa dampak penerapan dari *Intrusion Prevention System* pada sistem operasi *linux ubuntu* dan *linux centos* terhadap keamanan sistem.
3. Mengetahui tingkat keamanan yang manakah yang lebih baik pada jarinngan untuk mengatasi serangan.

1.4.2 Manfaat Penelitian

Adapun dari penelitian ini diharapkan dapat memberikan manfaat berikut :

1. Merancang jaringan keamanan yang lebih baik dengan menggunakan *IPTables* yang ada di sistem operasi *Linux Ubuntu* dan *Linux CentOs*.
2. Mengetahui celah kelemahan sistem keamanan antara sistem operasi *Linux Ubuntu* dan *Linux CentOs.*
3. Mengetahui cara kerja dari *Intrusion Prevention System* (IPS) saat diterapkan antara sistem operasi *Linux Ubuntu* dan *Linux CentOs*.
4. Sebagai sumber informasi dan juga dapat di jadikan bahan rujukan atau masukan untuk penelitian-penelitian berikutnya.

1.5 Waktu Penelitian

Penelitian ini dilakukan pada tanggal 07 Januari 2022 sampai dengan 15 maret 2022.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Merupakan bab pendahuluan yang menguraikan tentang latar rumusan masalah, pembatasan masalah, tujuan dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menguraikan tentang landasan teori yang didapat dari studi pustaka.

BAB III ANALIS DAN PERANCANGAN

Pada bab ini akan menjabarkan mengenai tahapan yang digunakan dalam penelitian ini, yang meliputi pengujian *intrusion Prevention Ssytem* (IPS) dari *IPTables* pada *Linux Ubuntu* dan *Linux CentOs*.

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang hasil penelitian yang kita lakukan dan pembahasan dari apa yang telah kita kerjakan serta penyelesaian dari apa yang telah kita kerjakan serta penyelesaian dari masalah-masalah yang ada dalam penelitian. Agar sistematis, pada bab ini dibagi menjadi beberapa bagian seperti berikut ini :

1. Hasil dari Penelitian
2. Analisis Pembahsan

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dari hasil penelitian yang telah dilakukan, serta berisi tentang saran yang dikemukakan oleh penulis untuk mengatasi kelemahan yang ada.