BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem adalah suatu sekumpulan elemen atau unsur yang saling berkaitan dan memiliki tujuan yang sama. Keamanan adalah suatu kondisi yang terbebas dari resiko. Komputer adalah suatu perangkat yang terdiri dari *software* dan *hardware* serta dikendalikan oleh *brainware* (manusia) Dan jika ketiga kata ini dirangkai maka akan memiliki arti suatu sistem yang mengkondisikan komputer terhindar dari berbagai resiko, itulah sistem keamanan komputer.

Keamanan jaringan sangat diperlukan untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Keamanan yang kuat dapat menjamin dan mengurangi kerugian yang didapat dari serangan terhadap jaringan komputer oleh orang yang tidak bertanggung jawab. Suatu serangan terhadap suatu jaringan dapat terjadi kapan saja , banyak cara untuk melakukan penyusupan pada jaringan. Berawal sekedar tes pada jaringan hingga mencoba merusak atau mencuri informasi penting. Untuk membantu dalam pemantauan paket data pada jaringan dan menganalisa paket – paket tersebut untuk mencegah dari hal – hal yang bersifat membahayakan jaringan, dibutuhkan *Intrusion Detection System* (IDS) . Salah satu tugas IDS adalah untuk mendeteksi trafik jaringan yang mencurigakan dan menyimpan di Log catatan IDS tersebut , dengan begitu dapat membantu administrator jaringan agar dapat mencegah kejahatan terhadap suatu jaringan. IDS

Intrusion Detection System (IDS) adalah tool, metode atau sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap suatu aktivitas jaringan komputer. Suricata adalah salah satu perangkat lunak pendeteksi dan pencegah gangguan atau *Intrusion Detection System* yang dikeluarkan oleh *Open Information System Foundation* (OISF) organisasi non-profit yang didukung oleh Amerika Serikat. Penggunaan terhadap suricata dapat dibilang sangat mudah karena dapat digunakan menggunakan *command lines* dan juga *Berkeley Packet Filter*.

Universitas Muhammadiyah Palembang adalah salah satu institusi yang memiliki jaringan internet yang cukup besar. Jaringan komputer yang hanya mengandalkan *firewall* untuk mengamankan komputer , perlu pengaman lebih untuk mengamankan data – data untuk terhindar dari pencurian data dari orang yang tidak bertanggung jawab. Dikarenakan pada era ini sangat mudah untuk mendapatkan informasi melalui desktop ataupun smartphone. Untuk Universitas Muhammadiyah Palembang sendiri menggunakan *Internet Service Provider* (ISP) untuk terkoneksi ke internet , dimana bercampur dengan jutaan pengguna lainya yang rentan terhadap hal yang tidak di inginkan .

Berdasarkan uraian diatas maka peneliti tertarik untuk melakukan penelitian, serta tujuan akhir penelitian ini untuk menganalisis Log IDS Suricata yang terdapat di Universitas Muhammadiyah Palembang agar dapat membantu administrator jaringan untuk mengamankan jaringan komputer di Lab tersebut, maka penelitian skripsi ini diberi judul **“ANALISIS LOG SURICATA STUDI KASUS UNIVERSITAS MUHAMMADIYAH PALEMBANG”.**

1.2 Perumusan Masalah

Berdasarkan latar belakang pada bab ini, maka peneliti merumuskan permasalahan dalam mengamankan jaringan lab komputer di Universitas Muhammadiyah Palembang adalah bagaimana menganalisis Log IDS Suricata ?

1.3 Batasan Masalah

Agar penelitiaan ini terarah dan sesuai tujuan, maka peneliti membatasi ruang lingkup pembahasan sebagai berikut :

1. Penyerangan hanya menggunakan DDOS Attack dan Zenmap
2. Penelitian ini hanya dilakukan di lab fakultas pertanian Universitas Muhammadiyah Palembang
3. Scenario penyerangan ini memanfaatkan Wi-Fi pada lab komputer fakultas pertanian Universitas Muhammadiyah Palembang

3.4 Tujuan dan Manfaat Penelitian

3.4.1 Tujuan

Adapun tujuan dari penelitian ini adalah mencari bukti digital melalui Log Suricata di Universitas Muhammadiyah Palembang serta menganalisis Log Suricata

3.4.2 Manfaat

Pada penilitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Memberikan solusi pengamanan jaringan komputer di Lab Universitas Muhammadiyah Palembang
2. Sebagai penerapan ilmu yang didapat selama peneliti menempuh kuliah di Universitas Muhammadiyah Palembang.

3.5 Metodologi Penelitian

3.5.1 Tempat dan Waktu Penelitian

1. Tempat

   Tempat penelitian berlokasi di Lab Fakultas Pertanian Universitas Muhammadiyah Palembang

2. Waktu

   Waktu penelitiaan ini dilakukan mulai pada November 2019 sampai dengan February 2020.

3.5.2 Alat dan Bahan

Dalam penelitian Analisis Log Suricata studi kasus Universitas Muhammadiyah Palembang, alat dan bahan yang menjadi penunjang dari penelitian ini meliputi perangkat keras (hardware) dan perangkat lunak (software) sebagai berikut :

1. Perangkat keras (hardware)
   a. Laptop Lenovo Ideapad 110
   b. Processor AMD A9
   c. Ram 4 GB
   d. Hardisk 1 TB
   e. Printer

f. Switch

g. smartphone

2. Perangkat Lunak (software)

a. Windows 10 sebagai sistem operasi

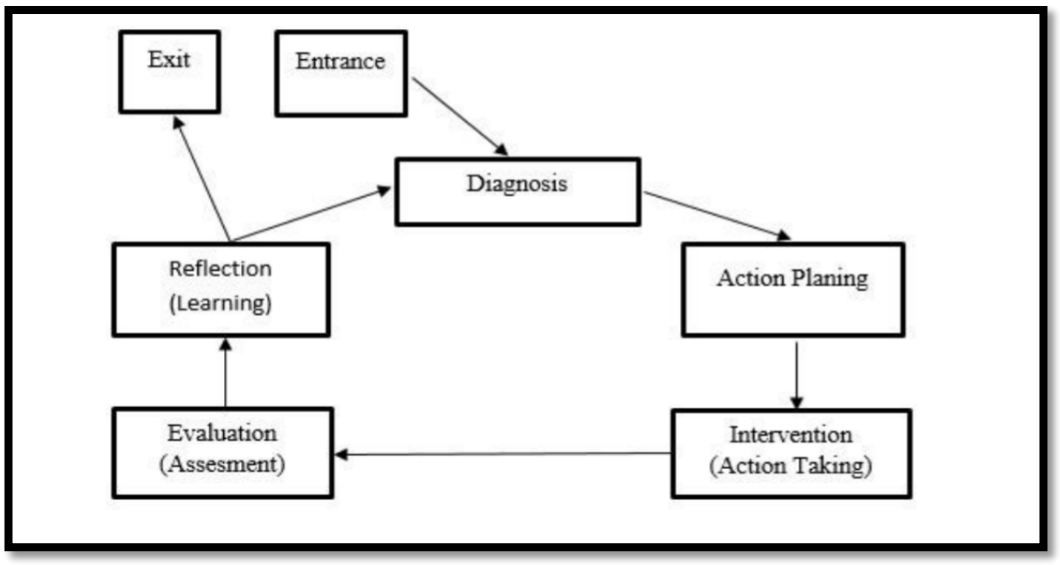
b. Ubuntu 18.04 sebagai sitem operasi

c. Suricata

d. Termux

3.5.3 Metode Penelitian

Metodologi adalah ilmu yang digunakan untuk memperoleh kebenaran menggunakan penelusuran dengan tata cara tertentu dalam menemukan kebenaran, tergantung dari realitas yang sedang di kaji. Dalam penelitian ini metode penelitian yang di gunakan dalam penelitian ini adalah penelitian tindakan (action research), dalam penelitian tindakan mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial pada waktu yang bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi. Adapun tahapan dalam melakukan penelitian *Action Research* menurut Davison, Martinsons, dan Kock (2004) yaitu penelitian tindakan yang mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau interversi dengan tujuan perbaikan atau partisipasi. Penelitian tindakan merupakan penelitian yang bertujuan mengembangkan metode kerja yang paling efisien, sehingga biaya produksi dapat ditekan dan prokdutivitas lembaga dapat meningkat. (Sugiyono, 2007:9). Adapun tahapan penelitian yang merupakan bagian dari action research ini, yaitu sebagai berikut :



Gambar 1.1 Alur Metode Action Research

1. Melakukan Diagnosa (Diagnosis)

   Pada tahap pertama ini peneliti melakukan identifikasi masalah pokok yang ada guna menjadi dasar penelitian pada jaringan Lab Fakultas Pertanian Universitas Muhammadiyah Palembang. Pada langkah ini peneliti menganalisis dengan cara mengumpulkan data dari infrastruktur kerja Teknologi Informasi lab.

2. Membuat Rencana Tindakan (Action Planning)

   Pada tahap ini peneliti telah memahami pokok masalah yang ada kemudian menyusun rencana tindakan untuk menyelesaikan masalah yang ada pada Lab Fakultas Pertanian Universitas Muhammadiyah Palembang.

3. Melakukan Tindakan (Action Taking)

Pada tahap ini peneliti telah menyusun rencana yaitu, membuat sistem Intrusion Detection System (IDS) pada jaringan Lab Muhammadiyah Palembang, kemudian membuat scenario penyerangan terhadap IDS menggunakan teknik DDOS Attack, Ip Spoofing dan SYN Flood. Setelah dilakukan penyerangan lalu peneliti menganalisis Log IDS tersebut guna mentrace pelaku penyerangan tersebut.

4. Melakukan Evaluasi (Evaluation)

   Setelah tahap Action Taking peneliti melakukan evaluasi terhadap hasil penelitian yang telah didapat.

5. Pembelajaran (Learning)

   Pada tahap ini peneliti melaksanakan review tahap demi tahap kemudian penelitian ini dapat berakhir.

3.5.4 Metode Pengumpulan Data

Adapun metode pengumpulan data adalah sebagi berikut :

1. Observasi

   Yaitu pengumpulan data dengan melakukan suatu pengamatan terhadap Lab Fakultas Pertanian Universitas Muhammadiyah Palembang lalu mencatat hal – hal yang berhubungan dengan penelitian yang akan dijadikan rujukan untuk penelitian ini.

2. Wawancara

   Yaitu pengumpulan data dengan cara mengadakan Tanya jawab dengan pihak – pihak yg terkai tentang permasalahan yg diangkat dalam penelitian ini.

3. Studi dokumen

   Yaitu data yang diperoleh melalui literature, melakukan studi kepustakaan dalam mencari bahan di internet dan membaca Jurnal – jurnal yang sesuai dengan objek yang diteliti.

3.6 Sistematika Penulisan

Dalam bagian ini, peneliti membuat alur pembahasan laporan supaya sesuai dengan tujuan dan dapat mudah di mengerti.

BAB I Pendahuluan

Dalam bab ini peneliti menjelaskan mengenai latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodelogi penelitian dan sitematika penulisan dalam penyusunan skripsi.

BAB II Tinjauan Pustaka

Dalam bab ini peneliti menjelaskan secara singkat mengenai tinjauan umum dari objek penelitian serta pengertian dan istilah - istilah yang digunakan dalam penelitian.

BAB III Analisis dan Perancangan

Dalam bab ini, peneliti menguraikan tentang langkah – langkah penelitian yang akan dilakukan dengan metode Action Research yang memiliki tahap Diagnosis, Action Planning, Action Taking, Evaluation, Learning.

BAB IV Hasil dan Pembahasan

Dalam bab ini peneliti menjelaskan hasil dari penelitian yang telah dilakukan.

BAB V Kesimpulan dan Saran

Dalam bab ini peneliti memberikan kesimpulan dan saran yang dapat bermanfaat bagi semua pihak.