1 PENDAHULUAN

1.1 Latar Belakang

Pusat Penelitian dan Pengembangan Tanaman Pangan merupakan sebuah badan penelitian yang meneliti dan mengembangkan hasil produksi tanaman pangan. Pusat Penilitian dan Pengembangan Tanaman Pangan (Puslitbangtan) memberikan kontribusi nyata dalam pembangunan pertanian. Hal ini tercermin dari inovasi teknologi dan kelembagaan yang dihasilkan melalui berbagai penelitian antara lain varietas unggul, benih sumber varietas unggul baru berdasarkan SMM-ISO 9001-2008, teknologi budi daya, panen dan pascapanen primer, model bioindustri berbasis tanaman pangan, Sekolah Lapang Kedaulatan Pangan (SL-KP) yang terintegrasi dengan 1.000 Desa Mandiri Benih mendukung Swasembada Pangan, rekomendasi kebijakan pengembangan tanaman pangan serta Taman Sains Pertanian.

Pada jaringan Puslitbangtan yang menggunakan satu router dan tiga switch yang saling terhubung secara linear. Selain itu, keamanan jaringan yang dipakai di Puslitbangtan hanya berupa konfigurasi router mikrotik yang diperkuat tanpa ada bantuan dari tools keamanan jaringan lainnya. Hal ini dapat menyebabkan beberapa masalah seperti jika router mikrotik diretas maka keamanan jaringan di Puslitbangtan jadi tidak aman, server menjadi terbuka dan data-data instansi menjadi rentan untuk dicuri. Untuk itu diperlukan suatu sistem tambahan untuk keamanan jaringan di Puslitbangtan.

Intrusion Prevention System (IPS) atau Sistem Pencegahan Intrusi adalah sistem yang dapat memblokir percobaan serangan dari peretas dan dapat membantu monitoring keamanan jaringan. “Pencegahan intrusi adalah proses melakukan deteksi intrusi dan berusaha menghentikan kemungkinan insiden yang terdeteksi” (Kumar et al. 2013). “Sistem ini adalah sistem yang realtime untuk memblok atau mencegah suatu aktivitas yang membahayakan jaringan” (Kristanto 2010). Salah satu tools yang dapat menerapkan Intrusion Prevention System (IPS) adalah Snort.

Snort merupakan *tools* yang dapat mendeteksi adanya intrusi pada jaringan. Untuk mendeteksi atau memblok percobaan intrusi tergantung dari yang telah didaftarkan. Snort dapat diubah ke mode IPS dengan bantuan *library* tambahan, salah satunya adalah *Netfilter-queue* (NFQ). NFQ bekerja dengan cara memasukkan paket ke dalam antrian. Kemudian paket yang dialihkan ke antrian dicek oleh Snort.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah dalam Implementasi *Network Intrusion Prevention System* Menggunakan Snort di Pusat Penelitian dan Pengembangan Tanaman Pangan adalah sebagai berikut:

1. Bagaimana cara melindungi jaringan di Pusat Penelitian dan Pengembangan Tanaman Pangan yang hanya menggunakan satu buah router sebagai sistem keamanan jaringannya?
2. Apakah ada sebuah sistem yang dapat melindungi dan memantau keamanan jaringan di Pusat Penelitian dan Pengembangan Tanaman Pangan?

1.3 Tujuan

Berdasarkan latar belakang yang telah dipaparkan, tujuan dari tugas akhir ini adalah membuat simulasi penerapan Network Intrusion Prevention System menggunakan Snort dalam mencegah serangan peretas dan memonitoring keamanan jaringan di Puslitbangtan.

.

1.4 Manfaat

Manfaat dari Implementasi Network Intrusion Prevention System Menggunakan Snort di Pusat Penelitian dan Pengembangan Tanaman Pangan adalah sebagai berikut:

1. Sistem ini diharapkan dapat menjadi lapis kedua keamanan jaringan setelah *firewall* router di Pusat Penelitian dan Pengembangan Tanaman Pangan.
2. Sistem ini diharapkan dapat membantu admin jaringan yang ada di Pusat Penelitian dan Pengembangan Tanaman Pangan dalam memantau keamanan jaringan.

1.5 Ruang Lingkup

Ruang lingkup dari Implementasi *Network Intrusion Prevention System* (NIPS) Menggunakan Snort di Pusat Penelitian dan Pengembangan Tanaman Pangan adalah:

1. Sistem yang dibuat bersifat virtual dengan menggunakan Virtualbox.
2. *Rules* yang ada pada sistem adalah untuk mendeteksi dan memblokir PING dari network lain dan mendeteksi dan memblokir *port scanning* dari network lainnya.
3. *Firewall* yang digunakan adalah Iptables.
4. Paket yang dapat diperiksa oleh sistem IPS ini adalah paket yang melewati sistem saja.
5. Tampilan GUI di *browser* hanya bisa menampilkan *action alert.*