# 1 PENDAHULUAN

## 1.1 Latar Belakang

Badan Pengkajian dan Penerapan Teknologi (BPPT) adalah Lembaga Pemerintah Non-Kementerian yang berada dibawah koordinasi Kementerian Riset, Teknologi dan Pendidikan Tinggi yang mempunyai tugas melaksanakan tugas pemerintahan di bidang pengkajian dan penerapan teknologi. Badan Pengkajian dan Penerapan Teknologi mempunyai Pusat Teknologi Informasi dan Komunikasi (PTIK) yang berfungsi melakukan pengkajian mengenai penerapan teknologi informasi dan komunikasi. PTIK terdiri atas beberapa subbagian dan masing-masing subbagian memiliki tugas pokok yang berbeda-beda. PTIK mengendalikan segala pusat data dan sistem teknologi informasi dan komunikasi.

PTIK terdapat Lab *Development* yang fungsinya memegang peranan penting untuk menjaga stabilitas jaringan serta mengelola data-data yang terdapat pada server BPPT. Untuk menjaga data-data tersebut sistem keamanan di Lab *Development* BPPT hanya dapat mendeteksi serangan yang masuk tetapi tidak dapat mencegah terjadinya serangan, oleh karena itu diperlukan perimeter yang dapat melakukan pencegahan dari serangan *hacking* berbasis *open source* yang membuat data pada server menjadi aman terhadap serangan.

Salah satu sistem keamanan jaringan yang dapat mencegah terjadinya serangan dari peretas adalah *Instrusion Prevention System* (IPS). Sistem IPS dapat digunakan untuk mencegah serangan yang masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat serangan telah teridentifikasi, IPS akan menolak akses dan mencatat semua paket data yang telah teridentifikasi. “IPS melakukan kontrol dari suatu jaringan berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan *port* atau IP *address* seperti firewall pada umumnya”(Kuswanto D. 2014). IPS tidak akan memberikan *alert* pada administrator tetapi langsung merespon pada aktivitas ilegal tersebut.

Salah satu perangkat lunak yang dapat menerapkan *Intrusion Prevention System* (IPS) adalah Snort. Snort merupakan perangkat lunak yang dapat mendeteksi adanya serangan pada jaringan. Untuk mendeteksi atau memblok percobaan serangan pada jaringan tergantung dari aturan yang telah dibuat atau yang sudah ada. Berdasarkan hal tersebut untuk mengatasi masalah keamanan jaringan yang ada di Lab *Development* BPPT diperlukan Implementasi *Intrusion Prevention System* menggunakan Snort di Lab *Development* BPPT.

## 1.2 Tujuan

Tujuan dari Implementasi *Intrusion Prevention System* (IPS) Menggunakan Snort di Lab *Development* BPPT adalah :

1 Menerapkan *Intrusion Prevension System* (IPS) menggunakan Snort di Lab *Development* BPPT

2 Menerapkan barnyard2 sebagai penghubung antara *database* Snort dengan BASE
3 Menerapkan BASE sebagai *Graphical User Interfaces* (GUI) dari *Intrusion Prevension System* (IPS)

### 1.3 Manfaat

Manfaat yang dapat diberikan dari Implementasi *Intrusion Prevention System* menggunakan Snort di Lab *Development* BPPT adalah:

1. Mampu memberikan fungsi proteksi pada jaringan yang berada di Lab *Development* BPPT
2. Mampu meningkatkan keamanan jaringan khususnya di Lab *Development* BPPT
3. Membantu administrator jaringan dalam melakukan pemantauan keamanan jaringan dari serangan peretas.

### 1.4 Ruang Lingkup

Ruang lingkup Implementasi *Intrusion Prevention System* menggunakan Snort di Lab *Development* BPPT adalah sebagai berikut:

1. Sistem ini bersifat simulasi yang dibangun menggunakan jaringan BPPT yang dihubungkan dengan *Virtual Private Network* yang dibuat oleh tim PKL Sekolah Vokasi IPB sehingga dapat diakses jarak jauh
2. Snort IPS menggunakan sistem operasi Linux Ubuntu 16.04
3. Pengujian Snort IPS menggunakan *rules* yang dibuat sederhana untuk mendeteksi SQL Injection dan XSS
4. Snort IPS menggunakan DAQ NFQ
5. DVWA dan Wordpress digunakan sebagai target percobaan peretasan
6. Rules dan serangan yang digunakan bersifat sederhana

## 2 METODE KAJIAN

### 2.1 Tempat dan Waktu PKL

Praktik Kerja Lapangaan (PKL) dilaksanakan di lantai 3 gedung Teknolgi 3 Kawasan Puspiptek, Serpong, Tangerang Selatan. PKL berlangsung selama 45 hari kerja terhitung mulai tanggal 06 Januari 2020 hingga 13 Februari 2020. Waktu pelaksanaan dimulai pada pukul 07.30 WIB sampai dengan 16.00 WIB.

### 2.2 Metode Bidang Kajian

Metode yang digunakan dalam Implementasi *Instrusion Prevention System* (IPS) Menggunakan Snort di Lab *Development* BPPT terdiri atas 4 tahap, yaitu :