BAB 1
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program, penggunanan bersama perangkat keras seperti printer, harddisk, dan sebagainya (Suyanto, 2004: 1). Sedangkan menurut Tri Wahyu W dan Aidil Sanjaya (2008:71), keamanan komputer adalah bagian dari ilmu komputer yang bertugas untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Berdasarkan pengertian jaringan komputer dan keamanan komputer diatas dapat disimpulkan bahwa keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Yang bertujuan untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

DPPKAD (Dinas Pendapatan Pengelolaan Keuangan dan Aset Daerah) mempunyai tugas pokok melaksanakan urusan pemerintahan daerah dan tugas pembantuan di bidang pendapatan, pengelolaan keuangan dan aset daerah. DPPKAD membangun jaringan intranet yang dipergunakan untuk mengakses aplikasi SIPKD (Sistem Informasi Pengelolaan Keuangan Daerah) yang terdiri dari *database server, web/application server* dan *file/comm* server, dan untuk mengakses aplikasi tersebut DPPKAD membuat dua buah akses yaitu melalui akses alamat ip statis yang terkoneksi dengan internet dan yang menggunakan jaringan lokal baik kabel dan nirkabel ke setiap kecamatan-kecamatan di kab.ciamis dan UPTD dinas Keuangan. Menurut hasil wawancara pada tanggal 28 januari dan 9 februari 2016 dengan bapak Arief Junaidi yang bertugas sebagai Staff IT yang menangani bagian server, pada server DPPKAD kab Ciamis sering kali terjadi gangguan seperti, akses pada aplikasi SIPKD yang sangat berat, aplikasi yang tidak dapat diakses, dan terkadang tidak dapat memasukan data ke

dalam *database* server , yang disebabkan komputer yang terkoneksi pada infrastruktur jaringan dan memiliki akses ke server tidak terjamin bebas dari virus, *spyware*, *malware*, dan semacamnya. Pada tahun 2015 terjadi kurang lebih 144 kali gangguan pada server DPPKAD, 57 kali diantaranya adalah serangan pada server yang menyebabkan akses pada server menjadi sangat berat. Dari indikasi-indikasi tersebut terdapat kemungkinan jika server tersebut terkena virus dari komputer-komputer yang terkoneksi pada server atau terjadi serangan pada server, baik seperti trojan, *DoS* attack ataupun *DDoS. Malware* atau yang biasa di sebut perangkat perusak adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, salah satunya adalah *worm* adalah sebuah program yang menyebarkan dirinya di dalam komputer dan menggandakan dirinya dalam memori setiap komputer, sehingga dapat menyebabkan sistem tersebut mengalami *crash* sehingga mengharuskan server harus di-*restart* dan ada pula jenis *worm* yang menghabiskan *bandwith* tersedia (Oktaviani, 2009 : 16-20). Apabila terjadi gangguan pada server maka penginputan data keuangan daerah akan terganggu dan berakibat keterlambatanya pelaporan dikarenakan pencetakan laporan pada aplikasi dikunci dengan tanggal penginputan dan sangat berbahaya apabila data yang terdapat pada server menjadi rusak atau *corrupt*.

Dalam buku hasil karya Srikanth Ramesh yang berjudul "Hacking Secrets Exposed" , terdapat banyak sekali jenis-jenis serangan yang dapat dilakukan melalui jaringan komputer seperti ARP Poisoning , DoS (*Denial of Service*), DDoS (*Direct Denial of Service*), *Sniffing*, *Malware*, Man In The Middle, Trojan, dan lainnya. Yang dimana semua infrastuktur jaringan komputer pasti memiliki celah untuk terkena serangan tersebut.

Honeypot merupakan teknologi keamanan yang bertujuan mengidentifikasi, mencari celah keamanan dam berkomprimasi aktif ketika terjadi aktifitas penyusupan keamanan. *Honey*pot itu sendiri bukanlah teknologi keamanan yang menanggulangi dan mencegah celah keamanan yang terjadi saat aktifitas penyusupan keamanan sedang berlangsung melainkan *honeypot* secara fungsional merekan setiap aktifitas penyusupan, termasuk identifikasi serta menunjukan celah keamanan yang sedang di eksploitasi oleh penyusup seperti

yang dijelaskan pada jurnal Perancangan Keamanan Cloud Computing Melalui Honeypot Sistem (Anggeriana, 2012 : 3-5).

IPS (*intrusion Prevention System*) adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer, IPS mengkombinasikan teknik *firewall* dan metode IDS (*Intrusion Detection System*) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan 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 (*log*) semua paket data yang teridentifikasi tersebut (Gondohanindijo, 2012 : 39).

Berdasarkan dari masalah dan penelitian tersebut, maka penulis merancang dan mengimplementasikan *honeypot* dan IPS agar dapat menangani suatu penyerangan berdasarkan *alert* yang telah ditampung pada *log* dan juga dapat memberikan *log* tentang serangan yang baru dan sebagai penunjang keamanan jaringan.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah di uraikan, maka yang menjadi pokok dalam penelitian ini adalah :

1. Bagaimana mengimplementasikan metode *Honeypot* dan IPS sebagai solusi dalam mengatasi masalah pada keamanan jaringan.
2. Bagaimana cara melakukan simulasi serangan pada jaringan komputer yang telah diimplementasikan.
3. Bagaimana meningkatkan keamanan jaringan di DPPKAD kab. Ciamis dengan menggunakan metode *Honeypot* dan IPS.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penelitian ini adalah melakukan perancangan dan pengimplementasian metode *Honeypot* dan IPS pada server DPPKAD. Sedangkan tujuan yang hendak dicapai dari penelitian ini adalah :

1. Menunjukan metode *Honeypot* dan IPS dapat digunakan untuk mengamankan server DPPKAD dari serangan-serangan jaringan.
2. Mendapatkan informasi/laporan serangan jaringan kepada admin sehingga dapat dipelajari pola serangan yang terjadi dan mengantisipasinya

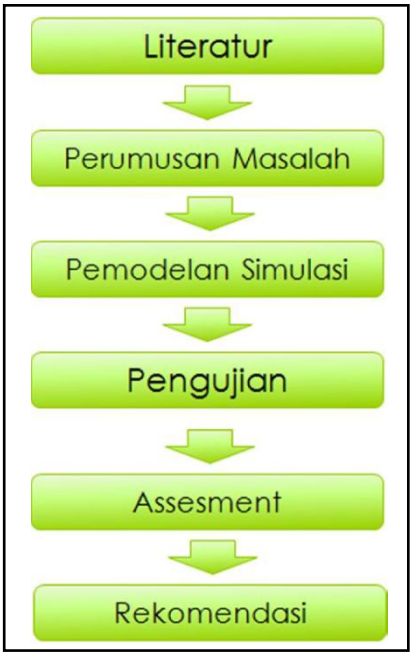
1.4 Batasan Masalah

Agar masalah yang ditinjau lebih terarah dan mencapai tujuan yang telah ditentukan, maka akan dibatasi masalah hanya kepada hal-hal berikut :

1. Pengimplementasian *Honeypot* dan IPS menggunakan Ubuntu Server.
2. Jenis *Honeypot* yang akan digunakan adalah *HoneyD.*
3. *Fwsnort* dan PSAD menjadi aplikasi yang digunakan dalam metode IPS.
4. Menggunakan *IP-Address* versi 4 dalam pengimplementasianya.
5. Menggunakan teknik pengamanan IPS dengan cara *Network-Based.*
6. Serangan pada jaringan akan dilakukan dalam pengujian berbentuk simulasi.
7. Serangan yang akan digunakan dalam pengujian ditentukan dan terbatas.
8. Menampilkan *log* serangan yang terjadi dalam bentuk txt

1.5 Metodologi Penelitian

Metodologi yang digunakan pada penelitian ini yaitu menggunakan metodologi deskriptif (prabowo, 2014 : 4). Tahapan-tahapannya adalah sebagai berikut yang dapat dilihat pada gambar 1.1 :



Gambar 1.1 Metodologi Penelitian

Berikut ini adalah penjelasan tahapan-tahapan metodologi penelitian berdasarkan gambar 1.1.

a. Literatur

   Mengumpulkan jurnal, literature, paper, dan bacaan-bacaan yang berkaitan dengan serangan-serangan pada jaringan, *Intrusion Prevention System, Fwsnort, Honeypot,* PSAD dan lain-lain.

b. Perumusan Masalah

   Melakukan analisa terhadap masalah-masalah yang biasanya muncul pada server atau infrastruktur, analisa dikakukan dengan menganalisa beberapa artikel, jurnal dan paper, serta hasil survey dan wawancara yang dilakukan oleh peneliti ke perusahaan yang terkait.

c. Pemodelan Simulasi

   Membuat model simulasi dalam hal ini adalah arsitektur jaringan yang digunakan untuk menganalisa jenis serangan dan menganalisa mengenai cara kerja dari *Honeypot* dan *Intrusion Prevention System.*

d. Pengujian

Pengujian dilakukan dengan menerapkan *Honeypot* dan *Intrusion Prevention System* dengan menggunakan aplikasi *honeyd, fwsnort*, PSAD dan aplikasi penunjang lainnya pada sebuah komputer yang akan di jadikan *web server*. Proses pengujian dilakukan dengan menyerang ke *server web* tersebut dengan beberapa metode yaitu *DoS, DDoS.*

e. *Assessment*

Pada tahap *assessment*, *attacker* yang terkoneksi dengan *server* akan mengakses layanan pada *web server* dan kemudian melakukan serangan.

f. Rekomendasi

Merekomendasikan pencegahan terhadap serangan-serangan yang mungkin terjadi pada *web server*.

1.6 Sistematika Penulisan

Sistematika penelitian ini disusun untuk memberikan gambaran umum tentang kasus yang akan dipecahkan. Sistematika penulisan tugas akhir ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini menguraikan tentang latar belakang permasalahan, merumuskan inti permasalahan yang akan dihadapi, menentukan maksud dan tujuan dari metode *Honeypot* dan IPS untuk menunjang keamanan sistem jaringan, yang kemudian diikuti dengan pembatasan masalah serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini membahas subyek permasalahan yang diangkat yaitu keamanan sistem jaringan server di DPPKAD, teori mengenai metode *Honeypot*, membahas mengenai IDS dan IPS, menjelaskan tentang *HoneyD, Fwsnort,* dan PSAD, yang kemudian di ikuti oleh pembahasan mengenai teknik pemodelan dan teknologi simulasi serangan yang akan digunakan.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan menjelaskan tentang proses analisis sistem dan rancangan umum dari konfigurasi yang akan dibangun serta metode-metode yang akan diterapkan pada topic masalah yang diambil.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini menyajikan penerapan metode-metode yang digunakan dalam membangun keamanan sistem jaringan. Serta pengujian simulasi keamanan tersebut.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir ini.