BAB II

TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Tinjauan Jurnal ini menjadi satu acuan penulis dalam membuat laporan akhir sehingga dapat memperkaya teori yang digunakan dalam mengkaji penelitian yang dilakukan. Berikut merupakan tinjauan jurnal dengan judul akhir penulis.

Tinjauan Jurnal sebelumnya dilakukan oleh Dyakso Anindito Nugroho, Adian Fatchur Rochim, Eko Didik Widianto dalam jurnal yang berjudul "**PERANCANGAN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM DI JARINGAN UNIVERSITAS DIPONEGORO" .** Tujuan dari penelitian tugas akhir ini adalah untuk mengimplementasikan intrusion detection system untuk mereprentasikan dan menampilkan log informasi akses ilegal pada jaringan yang dihasilkan sensor dalam tabel dan grafik agar lebih mudah dipahami**.**

Tinjauan jurnal sebelumnya dilakukan oleh Alamsyah dalam jurnal yang berjudul **"IMPLEMENTASI KEAMANAN INTRUSION DETECTION SYSTEM (IDS) DAN INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN CLEAROS".** Tujuan penelitian ini yaitu mengawasi jika terjadi penetrasi kedalam sistem, mengawasi traffic yang terjadi pada jaringan, mendeteksi anomali terjadinya penyimpangan dari sistem yang normal atau tingkah laku user, mendeteksi signature dan membedakan pola antara signature user dengan attacker.

Tinjauan jurnal sebelumnya dilakukan oleh Achmad Hambali dan Siti Nurmiati dengan jurnal yang berjudul "**IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) PADA KEAMANAN PC SERVER TERHADAP SERANGAN FLOODING DATA"** Tujuan dari penelitian tugas akhir ini yaitu digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas

inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) .

Tinjauan jurnal sebelumnya dilakukan oleh Maria Ulfa yang berjudul "**IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) DI JARINGAN UNIVERSITAS BINA DARMA"** tujuan dari penelitian tugas akhir ini yaitu untuk mencegah adanya penyusup yang memasuki system tanpa otorisasi (missal:cracker) atau seorang user yang sah tetapi menyalahgunakan *privilege* sumber daya system.

Dari uraian jurnal diatas ada kesamaan dengan latar belakang masalah penulisan laporan tugas akhir ini yaitu tentang Implementasi *Intrusion Detection System* untuk membantu administrator dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya. Perbedaan nya yaitu pada penelitian yang lainnya tentang *IDS* menerapkan fitur pemblokiran atau pencegahan pada penyerang yang mana fitur tersebut akan memblokir seluruh permintaan yang dapat membahayakan jaringan yang ada namun pada penelitian kali ini hanya memberikan peringatan kepada administrator sistem jaringan dalam mengetahui adanya suatu kekeliruan dalam jaringan.

2.2 Jaringan Komputer

Jaringan ialah sebuah sistem yang didalamnya perangkat lunak, perangkat keras, media berkomunikasi yang dimana dibutuhkan untuk menyatukan beberapa sistem komputer dan perangkat lainnya menurut (Sharon dan Supardi, 2014) Jaringan mempunyai peran yang penting karena memiliki beberapa alasan dan kegunaan. Pertama, jaringan komputer memudahkan dalam melakukan sebuah bisnis sehingga tidak memakan waktu serta lebih fleksibel. Kedua jaringan mempermudah sebuah kegiatan dalam memberikan data, membagi data, meminta data dari komputer lain ke komputer lain. Ketiga jaringan komputer memudahkan beberapa orang dalam berbagi data *real-time* yang sedang dikerjakan. Dan yang terakhir, jaringan komputer memudahkan beberapa pekerjaan yang seharusnya

diadakan pertemuan menjadi tidak harus karena bisa melakukan pertemuan *online*.

2.3 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan (Akhmad, 2013: 2).

Beberapa alasan untuk memperoleh dan menggunakan IDS *(Intrusion Detection System)* (Ariyus, 2007: 31), diantaranya adalah:

1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab dan hukuman yang diberikan atas kegiatan tersebut.
2. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem umum pakai seperti *firewall*, sehingga banyak menyebabkan adanya begitu banyak lubang keamanan, seperti:
    a. Banyak dari *legacy sistem*, sistem operasi tidak patch maupun update.
    b. Patch tidak diperhatikan dengan baik, sehingga menimbulkan masalah baru dalam hal keamanan.
    c. User yang tidak memahami sistem, sehingga jaringan dan protokol yang mereka gunakan memiliki lubang keamanan.
    d. User dan administrator membuat kesalahan dalam konfigurasi dan dalam menggunakan sistem.
3. Mendeteksi serangan awal, penyerang akan menyerang suatu sistem yang biasanya melakukan langkah-langkah awal yang mudah diketahui yaitu dengan melakukan penyelidikan atau menguji sistem jaringan yang akan menjadi target, untuk mendapatkan titik-titik dimana mereka akan masuk.
4. Mengamankan *file* yang keluar dari jaringan.
5. Sebagai pengendali untuk rancangan keamanan dan administrator, terutama bagi perusahaan yang pesat.

6. Menyediakan informasi yang akurat terhadap gangguan secara langsung, meningkatkan diagnosis, *recovery*, dan mengoreksi faktor-faktor penyebab serangan.

Adapun Terdapat Kelebihan dan Kekurangan IDS tersebut yaitu :

Kelebihan dari *IDS* :

1. Dapat Mendeteksi "*External Hackers"* dan serangan Jaringan Internal
2. Dapat Disesuaikan dengan mudah dalam menyediakan perlindungan untuk keseluruhan jaringan
3. Dapat dikelola secara terpusat dalam menangani serangan yang tersebar dan bersama-sama
4. Menyediakan pertahanan dalam bahian dalam
5. Menyediakan layar tambahan untuk perlindungan
6. *IDS* memonitor Internet untuk mendeteksi serangan
7. *IDS* membantu organisasi untuk mengembangkan dan menerapkan kebijakan yang efektif
8. IDS meelacak aktivitas dari pengguna saat masuk hingga saat keluar

Kekurangan dari *IDS* :

1. Lebih beraksi pada serangan daripada mencegahnya
2. Menghasilkan data yang besar untuk dianalisis
3. Rentan terhadap serangan yang *"rendah dan lambat"*
4. Tidak dapat menangani *traffic* jaringan yang terenkripsi
5. *IDS* hanya melindungi dari karakteristik yang dikenal
6. *IDS* tidak mengidentifikasi asal serangan
7. *IDS* hanya seakurat informasi yang menjadi dasarnya

2.4 Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara *real time* traffic dan logging ke dalam *database* serta mampu mengidentifikasi berbagai serangan yang

berasal dari luar jaringan (Ariyus, 2007:145). (Program *snort* dapat dioperasikan dengan tiga mode:

1. Paket *sniffer* Membaca paket-paket dari jaringan dan memperlihatkan bentuk aliran tak terputus pada konsol (layar). Jika hanya ingin melihat paketpaket header dari TCP/IP pada layar cobalah gunakan perintah: ./snort -v.
2. Paket logger Mencatat log dari paket-paket ke dalam disk. Jika ingin menyimpan catatan paket-paket ke dalam disk, maka perlu mencantumkan direktori logging, yaitu dimana data log disimpan padanya. Melalui perintah berikut Snort akan secara otomatis berjalan pada mode pencatatan paket: ./snort –dev –l ./log.
3. NIDS (Network Intrusion Detection System) Pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

Untuk mengaktifkan mode sistem deteksi penyusup jaringan NIDS (Network Intrusion Detection System) gunakan perintah berikut: ./snort –dev –l ./log –h 192.168.1.0/24 –c snort.conf Snort memiliki komponen yang bekerja saling berhubungan satu dengan yang lainnya seperti berikut ini (Ariyus, 2007:146) :

1. *Decoder:* sesuai dengan paket yang di-capture dalam bentuk struktur data dan melakukan identifikasi protokol, *decode* IP dan kemudian TCP atau UDP tergantung informasi yang dibutuhkan, seperti *port number*, dan IP address. Snort akan memberikan peringatan jika menemukan paket yang cacat.
2. *Preprocessors*: suatu saringan yang mengidentifikasi berbagai hal yang harus diperiksa seperti *Detection Engine*. *Preprocessors* berfungsi mengambil paket yang berpotensi membahayakan, kemudian dikirim ke detection engine untuk dikenali polanya.
3. *Rules File*: merupakan suatu *file* teks yang berisi daftar aturan yang sintaksnya sudah diketahui. Sintaks ini meliputi protokol, address, *output plug-ins* dah hal-hal yang berhubungan dengan berbagai hal.
4. *Detection Engine*: menggunakan *detection* plugins, jika ditemukan paket yang cocok maka *snort* akan menginisialisasi paket tersebut sebagai suatu serangan.

5. *Output Plug-ins*: suatu modul yang mengatur format dari keluaran untuk alert dan file logs yang bisa diakses dengan berbagai cara, seperti *console, extern files, database*, dan sebagainya.

2.5 WinPcap

WinPcap adalah driver untuk penangkap paketpaket yang hilir-mudik dalam jaringan. Secara fungsional artinya *WinPcap* menangkap paket-paket dari kabel jaringan dan melemparnya ke program *Snort*. *WinPcap* mungkin dapat diserupakan dengan *libpcap* versi Windows, yang digunakan untuk menjalankan *Snort* dalam *Linux* atau *UNIX* (Rafiudin, 2010: 6). *Driver WinPcap* melakukan fungsi-fungsi berikut untuk *snort:*

1. Menangkap daftar adapter jaringan yang beroperasi dan sekaligus mengambil informasi tentang adapter tersebut.
2. Mengawasi paket-paket menggunakan salah satu adapter yang dipilih.
3. Menyimpan paket-paket ke dalam hard-drive (atau lebih penting lagi, meneruskannya ke program *snort).*

2.6 PfSense

PfSense adalah open source *firewall* atau router software distribusi komputer berbasis FreeBSD ini dipasang pada komputer fisik atau mesin virtual untuk membuat *firewall* atau router khusus untuk jaringan ini dapat dikonfigurasi dan ditingkatkan melalui antarmuka berbasis *web*, dan tidak memerlukan pengetahuan tentang sistem FreeBSD yang mendasari untuk dikelola. *PfSense* biasanya digunakan sebagai *firewall* perimeter, router, titik akses nirkabel, server *DHCP*, server *DNS* dan sebagai *VPN* titik akhir *PfSense* mendukung pemasangan paket pihak ketiga seperti Snort atau Squid melalui Package Manager-nya.

2.7 VirtualBox

Oracle VM VirtualBox atau sering disebut dengan VirtualBox merupakan salah satu produk perangkat lunak yang sekarang dikembangkan oleh Oracle. Aplikasi ini pertama kali dikembangkan oleh perusahaan Jerman, Innotek GmbH.

Februari 2008, Innotek GmbH diakusisi oleh Sun Microsystems. Sun Microsystem kemudian juga diakuisisi oleh Oracle.

VirtualBox berfungsi untuk melakukan virtualisasi sistem operasi. VirtualBox juga dapat digunakan untuk membuat virtualisasi jaringan komputer sederhana. Penggunaan VirtualBox ditargetkan untuk Server, desktop dan penggunaan embedded. Berdasarkan jenis VMM yang ada, Virtualbox merupakan jenis hypervisor type 2. Oracle VM VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama. Sebagai contoh, jika seseorang mempunyai sistem operasi Microsoft Windows yang terpasang di komputernya, maka yang bersangkutan dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi Microsoft Windows tersebut. Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada. Fungsi-fungsi Virtualbox 1. Mencoba Operation System apapun. Virtualbox dapat memainkan semua sistem operasi baik itu menggunakan Windows, Linux atau turunan Linux lainnya. Virtualbox juga dapat dipergunakan untuk menguji coba OS baru. 2. Sebagai media untuk membuat simulasi jaringan. Di dalam Virtualbox dapat membuat banyak mesin virtual dan memainkannya sekaligus. Dapat menggabungkan semua mesin yang aktif tadi dalam satu jaringan. Seolah-olah mempunyai banyak komputer yang terkoneksi. 3. Sebagai komputer yang fleksibel dan dapat dipindah-pindahkan. Misalnya saat membuat sebuah server antivirus dan server absensi sekaligus untuk keperluan kantor dalam bentuk virtual di satu komputer. Server antivirus dan absensi dapat dipindahkan ke komputer lain dengan memindahkan mesin virtual ke komputer lain jika sewaktu waktu komputer utamanya rusak. Biasanya format file virtualbox berekstensi .VDI. maka tinggal copy paste format .VDInya saja ke komputer lain

2.8 Jenis Serangan

Jenis Serangan Beberapa jenis serangan pada jaringan komputer yaitu sebagai berikut:

1. Ping of Death Jenis serangan pada komputer yang melibatkan pengiriman ping yang salah atau berbahaya ke komputer target. Sebuah ping biasanya berukuran 56 byte (atau 84 bytes ketika header IP dianggap). Dalam sejarahnya, banyak sistem komputer tidak bisa menangani paket ping lebih besar daripada ukuran maksimum paket IP, yaitu 65.535 byte. Mengirim ping dalam ukuran ini (65.535 byte) bisa mengakibatkan kerusakan (crash) pada komputer target. Secara tradisional, sangat mudah untuk mengeksploitasi bug ini. Secara umum, mengirimkan paket 65.536 byte ping adalah illegal menurut protokol jaringan, tetapi sebuah paket semacam ini dapat dikirim jika paket tersebut sudah terpecah-pecah. Ketika komputer target menyusun paket yang sudah terpecah-pecah tersebut, sebuah buffer overflow mungkin dapat terjadi seperti crash.
2. Nmap (Port Scan) Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan tool ini, dapat melihat host yang aktif, port yang terbuka, sistem operasi yang digunakan, dan fitur-fitur scanning lainnya.
3. Denial of Service (DOS) Merupakan sebuah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet. DOS ini bekerja dengan cara menghabiskan resource yang dimiliki oleh komputer tersebut sampai akhirnya komputer tersebut tidak dapat menjalankan fungsinya dengan benar. DOS ini akan menyerang dengan cara mencegah seorang pengguna untuk melakukan akses terhadap sistem atau jaringan yang dituju. Ada beberapa cara yang dilakukan oleh DOS untuk melakukan serangan tersebut, yaitu:
    a. Membanjiri traffic atau lalu lintas jaringan dengan banyaknya data-data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Biasanya teknik ini disebut sebagai traffic flooding.

b. Membanjiri jaringan dengan cara me-request sebanyak-banyaknya terhadap sebuah layanan jaringan yang disediakan oleh sebuah client sehingga request yang datang dari para pengguna terdaftar tidak dapat dilayani aleh layanan tersebut. Biasanya teknik ini disebut sebagai request flooding.

4. Trojan Horse Merupakan salah satu jenis Malicious software atau malware yang dapat merusak sebuah sistem. Trojan ini dapat digunakan untuk memperoleh informasi dari target seperti password, system log dan lain-lain, dan dapat memperoleh hak akses dari target. Trojan merupakan software yang berbeda dengan virus atau worm karena trojan ini bersifat stealth dalam beroperasi dan seolah-olah seperti program biasa yang tidak mencurigakan dan trojan juga bisa dikendalikan dari komputer lain (attacker). Berikut jenis-jenis Trojan, yaitu:
   a. Pencuri Password: jenis trojan ini dapat mencuri password yang disimpan didalam sistem dengan cara membuat tampilan seolaholah tampilan login dengan menunggu host memasukan password-nya pada saat login kemudian password tersebut akan dikirimkan ke attacker.
   b. Keylogger: jenis Trojan akan merekam semua yang diketikan oleh host dan mengirimkanya ke attacker.

      RAT (Remote Administration Tools): jenis trojan ini mampu mengambil alih kontrol secara penuh terhadap sistem dan dapat melakukan apapun yang attacker mau dari jarak jauh seperti mem-format harddisk, meng-edit dan menghapus data.

2.9 Manajemen Jaringan Usulan

Manajemen Jaringan Usulan Jaringan Usulan IDS merupakan suatu sistem yang memiliki kemampuan untuk menganalisis data secara realtime dalam mendeteksi, mencatat (log) dan menghentikan penyalahgunaan dan penyerangan. IDS merupakan security tools yang dapat digunakan untuk menghadapi aktivitas hackers. IDS ini mampu memberikan peringatan kepada administrator apabila

terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.

2.10 Firewall

Firewall atau dinding api adalah sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk dapat melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Pada dasarnya sebuah *firewall* dipasang pada sebuah router yang berjalan pada *gateway* antara jaringan lokal dengan jaringan Internet (Wahana Komputer, 2014:72).

2.10.1 Fungsi Firewall

Menurut Wahana Komputer (2014:72), *Firewall* berperan dalam melindungi jaringan dari serangan yang berasal dari jaringan luar. *Firewall* mengimplementasikan paket *filtering*. Dengan demikian, *firewall* menyediakan fungsi kemanan yang digunakan untuk mengelola aliran data ke, dari, dan melalui router. Berikut fungsi – fungsi firewall secara umum:

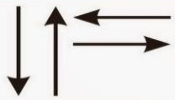
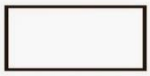
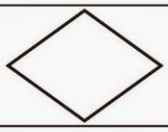
1. Mengontrol dan mengawasi paket data yang mengalir di jaringan.
   Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan *private* yang dilindungi *firewall*. *Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan melewati jaringan *private*. Beberapa kriteria yang dilakukan *firewall* apakah memperbolehkan paket data lewati atau tidak, antara lain:
   a. Alamat IP dari komputer sumber
   b. Port TCP/UDP sumber dari sumber
   c. Alamat IP dari komputer tujuan
   d. Port TCP/UDP tujuan data pada komputer tujuan
   e. Informasi dari *header* yang disimpan dalam paket data
2. Melakukan autentifikasi terhadap akses.
3. Aplikasi Proxy
   Firewall mampu memeriksa lebih dari sekedar *header* dari paket data, kemampuan ini menuntut *firewall* untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

4. Mencatat semua kejadian di jaringan.

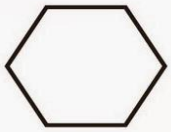
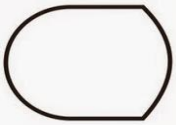
   Mencatat setiap transaksi kejadian yang terjadi di *firewall*. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

2.11 Flowchart

Flowchart adalah adalah suatu bagan dengan simbol-simbol tertentu yang menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses (instruksi) dengan proses lainnya dalam suatu program. Dalam perancangan *flowchart* sebenarnya tidak ada rumus atau patokan yang bersifat mutlak (pasti). Hal ini didasari oleh *flowchart* (bagan alir) adalah sebuah gambaran dari hasil pemikiran dalam menganalisa suatu permasalahan dalam komputer. Karena setiap analisa akan menghasilkan hasil yang bervariasi antara satu dan lainnya. Kendati begitu secara garis besar setiap perancangan *flowchart* selalu terdiri dari tiga bagian, yaitu input, proses dan output.

	**Flow Direction symbol** Yaitu simbol yang digunakan untuk menghubungkan antara simbol yang satu dengan simbol yang lain. Simbol ini disebut juga connecting line.
	**Terminator Symbol** Yaitu simbol untuk permulaan (start) atau akhir (stop) dari suatu kegiatan
	**Connector Symbol** Yaitu simbol untuk keluar - masuk atau penyambungan proses dalam lembar / halaman yang sama.
	**Connector Symbol** Yaitu simbol untuk keluar - masuk atau penyambungan proses pada lembar / halaman yang berbeda.
	**Processing Symbol** Simbol yang menunjukkan pengolahan yang dilakukan oleh komputer
	**Simbol Manual Operation** Simbol yang menunjukkan pengolahan yang tidak dilakukan oleh computer
	**Simbol Decision** Simbol pemilihan proses berdasarkan kondisi yang ada.
	**Simbol Input-Output** Simbol yang menyatakan proses input dan output tanpa tergantung dengan jenis peralatannya

Gambar 2.2 Simbol Flowchart

	**Simbol Manual Input** Simbol untuk pemasukan data secara manual on-line keyboard
	**Simbol Preparation** Simbol untuk mempersiapkan penyimpanan yang akan digunakan sebagai tempat pengolahan di dalam storage.
	**Simbol Predefine Proses** Simbol untuk pelaksanaan suatu bagian (sub-program)/prosedure
	**Simbol Display** Simbol yang menyatakan peralatan output yang digunakan yaitu layar, plotter, printer dan sebagainya.
	**Simbol disk and On-line Storage** Simbol yang menyatakan input yang berasal dari disk atau disimpan ke disk.
	**Simbol magnetik tape Unit** Simbol yang menyatakan input berasal dari pita magnetik atau output disimpan ke pita magnetik.
	**Simbol Punch Card** Simbol yang menyatakan bahwa input berasal dari kartu atau output ditulis ke kartu
	**Simbol Dokumen** Simbol yang menyatakan input berasal dari dokumen dalam bentuk kertas atau output dicetak ke kertas.

Gambar 2.3 Simbol Flowchart