`

BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian tentang *Intrusion Detection* sudah bukan untuk yang pertama kalinya dilakukan. Pada penelitian yang sudah dilakukan sebelumnya menunjukkan bahwa *Intrusion Detection* dapat dilakukan dengan berbagai metode dan *Software* yang berbeda. Berikut merupakan beberapa penelitian terdahulu :

1. **Sistem deteksi intrusi menggunakan algoritma genetik pada serangan Dos di protokol TCP dan UDP, Muhammad Akmal Fauzi, Ir. Ahmad Tri Hanuranto, M.T , Casi Setianingsih, S.T., M.T., e-PoE 2019**[11]**.** Pada penelitian ini *Intrusion Detection System* diimplementasikan untuk mendeteksi *dos attack* pada *protocol TCP* dan *UDP* saja. penelitian ini berbeda dengan yang digunakan dengan penulis, penelitian yang akan digunakan yaitu melakukan *Intrusion Detection System* pada *web server*.
2. **Analisa kinerja *Fail2Ban* dan *DenyHost* dalam mengamankan *server* dari serangan *BruteForce,*Rudy Rinaldi, Agus Urip Wibowo, Yuli Fitrisia., Jurnal Teknik Informatika Vol 1 2012**[12]**.**

   Pada penelitian ini *Tools* yang digunakan yaitu *Fail2Ban*. dimana *Fail2Ban* juga mendeteksi serangan dari *log web server*, namun penelitian ini hanya mendeteksi serangan IP ini, tidak spesifik serangan apa saja yang sedang di jalankan oleh *attacker*
3. **Notifikasi *Network Intrusion Detection System* Menggunakan Media Aplikasi Telegram., Fitri Nuraeni, Indra Nurfajri., Kumpulan jurnal Ilmu Komputer (KLIK) 2019**[13]**.**

   Pada penelitian ini peneliti menggunakan *tools snort* dan *Mysql* sebagai tempat menyimpan *log* untuk pengimplementasian IDS yang mereka gunakan. sedangkan penulis menggunakan *tools* TELER berbasis *GoLang* dan tidak

memerlukan *Mysql* sebagai penyimpanan *log* , disini penulis langsung menganalisa pada *file log "/var/log/ngingx/access.log"*.

4. **Pengaruh penempatan snort terhadap keamanan jaringan., Yusuf abdulloh, Joko Triyono, Uning Lestari., Jurnal Jarkom Vol. 8 2020**[14]**.**
   Pada penelitian ini Intrusion Detection System diimplementasikan untuk menganalisa serangan data pada jaringan menggunakan tools snort. perbedaan penelitian ini dengan penulis adalah pengimplementasian sistem intrusion detection system ini untuk menganalisa web sever dan serangan terhadap web yang tersimpan didalam log web server.
5. **Analisis pengukuran penggunaan sumber daya komputer pada *Intrusion Detection System* dalam meminimalkan serangan jaringan., Sopian Alviana, Irfan Dwiguna Sumitra., Jurnal Ilmiah Komputer dan Informatika (KOMPUTA) 2018**[15]**.**
   Pada penelitian ini *Intrusion Detection System* diimplementasikan pada jaringan dan penelitian ini juga menganalisa sistem yang ada pada jaringan lokal serta lebih condong di pengukuran anomali pada sumber daya komputer. penelitian ini berbeda dengan yang digunakan dengan penulis, penelitian yang akan digunakan yaitu melakukan *Intrusion Detection System* pada *web server*.
6. **Simulasi Penggunaan *Intrusion Detection System* (IDS) Sebagai Keamanan Jaringan dan Komputer., Barani Fachri, Fadli Hamdi Harahap., Jurnal Media Informatika Budidarma 2020**[16]**.**
   Pada penelitian ini peneliti menggunakan *tools SNORT* sebagai IDS yang mereka gunakan. sedangkan penulis menggunakan tools TELER berbasis *GoLang*, disini perbedaan penelitian dan penulis adalah *SNORT* yang difokuskan hanya terbatas pada penganalisaan jaringan saja. Sedangkan penulis menganalisa sebuah serangan *web* pada *web sever*.
7. **Perancangan *Intrusion Detection System* untuk mendeteksi serangan menggunakan aplikasi TELEGRAM., Friska Yudhistira, Dahliyusmanto, Linna Oktaviana Sari., JOM FTEKNIK 2021**[17]**.**
   Pada penelitian ini peneliti menggunakan *tools SNORT* sebagai IDS yang mereka gunakan. sedangkan penulis menggunakan *tools* TELER berbasis

GoLang, disini perbedaan penelitian dan penulis adalah kurang nya informasi serangan yang terjadi pada server Sedangkan penulis hasil analisa serangan secara spesifik.

8. **Analisis Kinerja *Intrusion Detection System* pada Deteksi Anomali dengan Metode *Decision Tree* Terhadap Serangan Siber., Muammar Fadhlurrohman, Anita Muliawati, Bayu Hananto., Jurnal Ilmu Komputer Agri-Informatika 2021**[18]**.**

   Pada penelitian ini difokuskan dalam pendeteksian penyerangan di jaringan saja menggunakan *tools wireshark* sebagai alat bantu menganalisa serangan jaringan, lalu IDS akan mendeteksi berapa banyak paket sebelum dan sesudah serangan terjadi jika terjadi anomali maka akan lanjut ke tahap seleksi apakah itu jaringan normal atau jaringan terkena serangan.

Dari penjelasan diatas, ringkasan penelitian yang relevan ditunjukan pada Tabel 2.1 dibawah ini :

Tabel 2. 1 Penelitian Terdahulu

No	Judul	Objek	Metode/Algoritme	Hasil	Pebedaan dengan penelitian yang dilakukan
1	Sistem deteksi intrusi menggunakan algoritma genetik pada serangan Dos di protokol TCP dan UDP 2019	*Server*	*Intrusion Detection System*, Algoritma K-NN	Hasil yang didapat dari seleksi fitur menggunakan algoritma genetik adalah dengan nilai fitness 84.171% dan fitur yang terseleksi berjumlah 18 dari 41 fitur yang ada.	penelitian ini berbeda dengan yang digunakan dengan penulis, penelitian yang akan digunakan yaitu melakukan *Intrusion Detection System* pada web server.
2	Analisa kinerja *Fail2Ban* dan *DenyHost* dalam mengamankan server dari serangan *BruteForce 2014*	*Server*	*Intrusion Detection System* dengan Fail2Ban & *DenyHost*	*Fail2ban* melakukan pemblokiran Internet Protocol (IP) dari *attacker* yang melakukan serangan *bruteforce* pada *IPTables*	penelitian ini berbeda dengan yang digunakan dengan penulis, penelitian yang akan digunakan yaitu melakukan *Intrusion Detection System* pada *web server*.
3	Notifikasi *Network Intrusion Detection System* Menggunakan Media Aplikasi Telegram (2019)	Web *server* Kantor Imigrasi TASIKMALAYA	*Intrusion Detection System* dengan SNORT	Digunakanya *Snort* sebagai IDS *administrator* dapat dengan mudah mendiagnosa serangan yang terjadi pada infrastruktur PC Server dan *system administrator* dapat menerima notifikasi adanya gangguan yang terdeteksi.	Perbedaan penelitian ini dengan milik penulis adalah penulis menggunakan tools TELER berbasis *GoLang* dan tidak memerlukan *Mysql* sebagai penyimpanan *log* , disini penulis langsung menganalisa pada *file log* "/var/log/ngingx/acess.log"
4.	Pengaruh penempatan *snort* terhadap keamanan jaringan (2020)	*Server laboratorium vi jaringan kampus 3 ist akprind yogyakarta*	*Intrusion Detection System* dengan *SNORT*	Hasil dari penelitian ini penggunaan Snort mempermudah *system administrator* untuk memonitoring data data yang ada, dan perlu aplikasi pendukung Snort seperti *base* dan *Snorby* alat untuk memonitoring *GUI Snort* dengan *web serve. Barnyard2* digunakan sebagai penerjemah *output file Snort* agar dapat mempermudah *system administrator* mengelola melalui *database MySQL*.	perbedaan penelitian ini dengan penulis adalah pengimplementasian sistem intrusion detection system peneliti adalah untuk menganalisa jaringan sedangkan penulis untuk menganalisa web sever dan serangan terhadap web yang tersimpan didalam log web server
5.	Analisis pengukuran penggunaan sumber daya komputer pada *Intrusion Detection System* dalam meminimalkan	*Server*	*Intrusion Detection System* , *anomaly based*	Metode anomaly based mempunyai waktu responsi yang lebih baik dibandingkan *signature based* dengan mencatat waktu responsi lebih cepat yaitu 7 detik dibandingkan dengan metode *signature based* yang mempunyai waktu responsi 9 detik dan Metode anomaly based	Perbedaan penelitian ini dengan milik penulis adalah penelitian ini berfokus pada jaringan dan penelitian ini juga menganalisa sistem yang ada pada jaringan lokal serta lebih condong di pengukuran anomali pada sumber daya

No	Judul	Objek	Metode/Algoritme	Hasil	Pebedaan dengan penelitian yang dilakukan
	serangan jaringan(2018)			mengkonsumsi jumlah memori yang lebih sedikit dan cenderung lebih stabil dibandingkan dengan metode *signature based* yang mengkonsumsi jumlah memori lebih besar. Anomaly based mencapai 60% penggunaan memori, sedangkan *signature based* mencapai 62%.	komputer. penelitian ini berbeda dengan yang digunakan dengan penulis, penelitian yang akan digunakan yaitu melakukan *Intrusion Detection System* pada *web server*.
6.	Simulasi Penggunaan *Intrusion Detection System* (IDS) Sebagai Keamanan Jaringan dan Komputer (2020)	*Server*	*Intrusion Detection System* dengan *SNORT*	Hasil analisis penelitian ini. Snort menganalisa *file log* yang ada pada jaringan. dan *system administrator* melakukan analisa *forensic* pada *file log* yang teridentifikasi terjadi sebuah serangan pada *web server*	Perbedaan penelitian ini dengan milik penulis adalah penelitian ini menggunakan *Intrusion Detection System* dengan SNORT sedangkan penulis melakukan hasil unjuk kerja *Intrusion Detection System* dengan *TELER*.
7.	Perancangan *Intrusion Detection System* untuk mendeteksi serangan menggunakan aplikasi *TELEGRAM*(2021)	*Web Server*	*Intrusion Detection System* dengan *SNORT*	Hasil keseluruhan pengujian yang telah dilakukan, diketahui seluruh fungsionalitas sistem berjalan sesuai yang diharapkan dan dapat disimpulkan Dari 5 pengujian yang telah dilakukan, 80% berhasil dan 20% gagal, maka dapat dinyatakan pengujian berhasil dilakukan	Perbedaan penelitian ini dengan milik penulis adalah penelitian ini menggunakan *Intrusion Detection System* dengan SNORT sedangkan penulis melakukan hasil unjuk kerja *Intrusion Detection System* dengan *TELER*.
8.	Analisis Kinerja *Intrusion Detection System* pada Deteksi Anomali dengan Metode *Decision Tree* Terhadap Serangan Siber(2021)	Server	*Intrusion Detection System , Decision Tree*	Hasil dari penelitian ini adalah IDS akan mendeteksi adanya paket serangan jika paket_perdetik_serangan yang didapat dikategorikanm menjadi keadaan normal, dan keadaan terjadi penyerangan.	Perbedaan penelitian ini dengan milik penulis adalah penelitian ini menggunakan *Intrusion Detection System* dengan metode decision tree sedangkan penulis melakukan hasil unjuk kerja *Intrusion Detection System* dengan *TELER*.

2.2 Landasan Teori

2.2.1 *Cyber Attack*

Cyber attack atau serangan siber adalah setiap kegiatan atau upaya yang dilakukan oleh seorang *attacker* menggunakan *software*, jaringan komputer atau kode tertentu yang bertujuan untuk merusak,menghancurkan, mengubah suatu sistem informasi suatu instansi maupun perangkat pribadi dan secara sengaja melawan hukum bisa disebut *cyber attack*. Dalam melakukan serangan siber, *attacker* dapat menggunakan beberapa cara seperti injeksi *malware* , *phising* , *ddos* dan lain-lain[19].

2.2.2 *Teler*

TELER adalah *package* keamanan yang dibuat untuk mendeteksi serangan pada sebuah *website* yang berbasis *GoLang*. Aplikasi ini juga bekerja dengan melakukan *monitoring* jumlah serangan *website* (*CVE, Bad IP Address , Directory Bruteforce, Web Crawler, Bad Referer* , beberapa serangan *website* pada umumnya) dan selanjutnya ditindak lanjuti dengan mengirim peringatan kepada *administrator website*.TELER melakukan *scanning* terhadap *file log* (pada /var/log/apache2/access.log) dan mendeteksi jika ada tanda tanda *request* yang berbahaya. Kondisi bahaya yang dimaksud adalah seperti *request* dengan *payload*, mencari eksploitasi, dan lain-lain[20].

2.2.3 *Directory Bruteforce attack*

Directory Bruteforce adalah metode untuk menemukan direktori tersembunyi yang ada dalam sebuah *website*,dengan metode ini *attacker* dengan mudah mencari *file-file* penting yang tersembunyi didalam direktori sebuah website yang tidak sengaja atau secara default berada di sebuah direktori namun admin server lupa menyembunyikan direktori tersebut sehingga masih dapat diakses jika *attacker* mengetahui dimana letak direktori tersebut [21].

2.2.4 *RealTime System*

Realtime system adalah merupakan waktu ketika menjalankan program sistem yang berjalan memiliki tenggat waktu untuk menyelesaikan tugas yang berjalan. *Realtime system* sendiri dibagi menjadi dua sistem yaitu *Hard Realtime* yaitu dimana kondisi sistem harus mencapai tenggat waktu yang ditentukan jika tidak mencapai tenggat waktu maka akan menimbulkan masalah serius ketika

sistem ini diterapkan. Sedangkan *Soft Realtime* yaitu dimana kondisi sistem dapat melewatkan tenggat waktu yang ditentukan, dan jika terlalu banyak yang terlewat maka kinerja nya akan menurun[22].

2.2.3 Apache2

APACHE2 adalah *software web server* yang bersifat *open source*. Saat pertama kali APACHE2 dirilis, APACHE2 hanya berfungsi sebagai *HTTP web serving* saja. Namun seiring perkembangan zaman dan permintaan *user* banyak sekali, software ini melakukan perkembangan juga, dan berperan sebagai *reverse proxy,SMTP*, *email proxy* untuk *IMAP*, *HTTP load balancer*, dan, *POP3*[23].

2.2.4 Damn Vulnerable Web Application

DVWA adalah singkatan dari *Damn Vulnerable Web Application*, DVWA sendiri merupakan sebuah *website* yang sudah dirancang memiliki banyak celah keamanan. beberapa di antara nya adalah : *SQL Injection, BruteForce, CSRF, XSS* dan lain nya. untuk bisa menggunakan DVWA dibutuhkan sebuah *web server* yang akan menjadi tempat DVWA ini di *install*[24].

2.2.5 DirSearch

Dirsearch sebuah *tool* yang dirancang untuk melakukan *bruteforce* direktori file pada sebuah website. *dirsearch* ini dapat melihat isi direktori atau *file* di dalam sebuah website walaupun tidak semua direktori atau *file* dapat terlihat , namun sangat berguna jika *web administrator* melakukan sebuah kesalahan yaitu tidak memberi *permission file* atau direktori, dari kesalahan itu bisa dijadikan sebuah celah keamanan jika *file* atau direktori tersebut memiliki *credential* tertentu[25].

2.2.6 Go Language

Bahasa Go atau biasa disebut golang dirancang oleh Robert Griesemer, Rob Pike , dan Ken Tompson. Pada tahun 2012 golang resmi dirilis untuk public dan dibuat secara *opensource* Ketika versi 1.0 dirilis. Golang sangat cepat diterima oleh masyarakat karena memiliki beberapa keunggulan karena sederhana dari segi penulisan program, efisiensi , dan memiliki *cocurrent* yang berarti dapat menjalankan tugas secara bersamaan dalam satu waktu. Golang juga dapat digunakan untuk pembuatan *backend server*, pembuatan *game*, bahkan *data*

science. Tidak heran golang sangat disukai masyarakat karena dirancang memiliki banyak fungsi[26].

2.2.7 Mysql

Mysql adalah sebuah program berbasis *database* yang mampu mengirimkan data dengan cepat. Mysql juga merupakan sebuah *database server* yang *free* dengan begitu masyarakat dapat mengguanakan mysql untuk keperluan usaha maupun pribadi tanpa harus membeli lisensi. *Database* mysql merupakan *database* yang berbentuk *relational database management system* (RDBMS)[27].

2.2.8 Telegram

Telegram adalah aplikasi *social media* yang memungkinkan *user* yang menggunakanya dapat mengirim pesan rahasia yang dienkripsi *end-to-end* sebagai keamanannya. Selain sebagai *social media* telegram juga sangat berguna khususnya para *programmer* untuk membuat *BOT* dalam memudahakan pekerjaan mereka[28].

2.2.9 Discord

Discord adalah aplikasi yang mempunyai banyak fitur.discord dirancang untuk menciptakan sebuah komunitas sosial dengan aplikasi discord pengguna dapat saling mengirim *chat*, gambar, *video*, *share screen*, dan bahkan mengembangkan sebuah komunitas forum didalam aplikasi tersebut. Discord sangat digemari oleh masyarakat karna memiliki banyak fitur yang sangat berguna[29].

2.2.10 Slack

Slack adalah aplikasi yang dirancang khusus untuk *Project Management*. Slack digunakan para pekerja untuk melakukan konferensi *video* , pengiriman *file*, maupun pesan. Slack ini memiliki fitur unggulan yaitu dapat mengumpulkan orang dalam satu *channel* yang sama dan mengelompokan sesuai divisi/*jobdesk* mereka dengan begitu slack dapat mempermudah pekerja dalam mengelompokan pekerjaan mereka[30].