PERANCANGAN INTRUSION DETECTION SYSTEM UNTUK MENDETEKSI SERANGAN MENGGUNAKAN APLIKASI TELEGRAM

Friska Yudhistira [1)], Dahliyusmanto [2)], Linna Oktaviana Sari[3)]
[1)]Mahasiswa Program Studi Teknik Informatika, [2)]Dosen Teknik Informatika
Program Studi Teknik Informatika, Fakultas Teknik Universitas Riau
Kampus Bina Widya Jl. HR. Soebrantas Km. 12,5 Simpang Baru, Tampan, Pekanbaru 28293
Email: friska.yudhistira3767@student.unri.ac.id

ABSTRACT

Information technology is now much developed. With the ease of obtaining this information, it causes other obstacles, namely important information or data can be misused by other parties who are not responsible for their own benefit. So that a network security system becomes one of the important aspects to maintain the validity and integrity of data and ensure the availability of services for its users. The system should be equipped with security that allows it to be safe from all kinds of attacks and as well as intrusion attempts by irresponsible parties. With the IDS (Intrusion Detection System) administrator will detect the attack by an intruder so that notification of an attack can be identified quickly through a notification Telegram Sistem IDS (Intrusion Detection System)will provide notification or warning through application telegram if there are attacks on computer networks are detected in the system, so administrators networkable to find out the occurrence of the attack as soon as possible This system can detect attacks that occur on a computer network by scanning a number of sources and traffic that occurs within the network, so that all illegal events can be seen throughactivities monitoring using the application used to monitor the network, the IDS System. This will provide notifications or warnings via the Telegram application if an attack on the computer network is detected in the system, so that theadministrator networkcan find out the occurrence of the attack as quickly as possible.Of the 5 tests that have been carried out 80% successful 20% failed, it can be stated that the test was successfully carried out.

Keywords: IDS (Intrusion Detection System), Snort, Telegram , Computer network.

1. Pendahuluan

Pada masa sekarang ini, Teknologi Informasi (TI) sudah juah tumbuh berkembang, ini didukung keberadaan jaringan internet yang bisa mempermudah untuk melakukan komunikasi dengan pihak yang lain. Dengan kemudahan mendapatkan informasi tersebut menyebabkan timbulnya kendala lain yaitu informasi atau data-data penting bisa disalah gunakan oleh pihak lain yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri**.** Sehingga suatu sistem keamanan jaringan menjadi salah satu aspek yang penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Sistem seharusnya dilengkapi dengan keamanan yang memungkinkan aman dari segala macam serangan dan serta usaha penyusupan oleh pihak yang tidak bertangung jawab.

Sistem jaringan komputer bila tidak aman tentu akan berdampak tidak baik bagi penguna sistem tersebut dan akan mengakibatkan kerusakan *(crash*) pada komputer Maka penerapan IDS (*Intrusion Detection System*) disarankan sebagai solusi yang dapat digunakan untuk membantu pengaturan jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket

berbahaya yang terdapat dalam jaringan tersebut, hal ini bertujuan agar mencegah adanya penyusupan yang memasuki sistem tanpa otorisasi atau seorang *user* yang sah tetapi menyalahgunakan *privilege* sumber daya sistem. Dengan adanya IDS *administrator* akan mendeteksi serangan yang dilakukan oleh penyusup sehingga pemberitahuan akan adanya serangan dapat diketahui dengan cepat melalui notifikasi Telegram.

Sebuah server yang terhubung dalam jaringan komputer memiliki masalah utama yaitu kemanan yang berupa *Ping Of Death, Nmap Port Scan, Denial of Service (DOS)*. Karena itu membuat dibutuhkanya alternatif untuk memiliki *Intrusion Detection System* (IDS) pada setiap jaringan. IDS yaitu perangkat lunak yang secara otomatis melakukan proses pemantauan (*monitoring*) terhadap insiden yang terjadi dalam server serta menganalisis keberadaan masalah dari keamanan sistem. IDS melakukan (*filtering)* pada lalu lintas data. didalam jaringan komputer dan melakukan analisis terhadap informasi yang didapatkan guna mendapatkan bukti adanya percobaan penyusupan atau percobaan intrusi terhadap sistem jaringan komputer salah satunya percobaan intrusi terhadap *server.*

Sistem jaringan komputer bila tidak aman tentu akan berdampak tidak baik bagi pengguna system tersebut.seperti mengganggu sumber daya dari komputer akibatnya komputer berjalan lambat, menginfeksi sistem atau komputer, menyebarkan malware, virus, atau keylogger dll. Oleh karena itu, perlu diadakan *tools* untuk me*monitoring* keamanan jaringan dengan tujuan agar meminimalisir jika terjadinya percobaan penyusupan atau percobaan intrusi. Diantaranya yang digunakan *Intrusion Detection System* (IDS) yaitu *Snort* dan *PfSense*. Aplikasi *open source* tersebut mempunyai kemampuan dalam mendeteksi adanya penyusupan terhadap sistem keamanan di jaringan yang sesuai dengan aturan (*rule*) yang telah ditetapkan di dalam *Intrusion Detection System* (IDS).

Serta dapat dilakukan antisipasi penanganan awal dengan kontrol langsung terhadap *server* secara *real time*. Aplikasi *instant messaging* banyak yang dapat digunakan, diantaranya aplikasi tersebut yang memiliki berbagai fitur adalah Telegram. Telegram selain bisa untuk *chatting*, terdapat fitur *transfer* dokumen. Fitur tersebut bisa dimanfaatkan untuk mengirimkan laporan keamanan sistem jaringan komputer. Pemberitahuan adanya serangan terhadap jaringan dengan menggunakan IDS yaitu *Snort* dan *PfSense* dapat memberikan informasi secara *real time* melalui aplikasi Telegram. Berbeda dengan *instant messaging* lainnya seperti *WhatsApp* dan *LINE*. Pada *instant messaging WhatsApp* tidak menyediakan API bagi *public* sedangkan aplikasi *LINE* meyediakan API namun dengan versi *trial* atau terbatas. API yang disediakan oleh Telegram dapat digunakan oleh siapapun dan *unlimeted* . Telegram juga memiliki *bot* API yang memungkinkan untuk dengan mudah membuat program yang menggunakan pesan Telegram sebagai antar muka. API memungkinkan siapa saja untuk membuat bot yang akan membalas semua penggunanya jika mengirimkan pesan berupa instruksi/*command* yang dapat diterima oleh bot tersebut. Telegram *bot* merupakan cara khusus yang tidak memerlukan nomor telepon tambahan sebagai syarat khususnya. Akun *bot* tersebut berfungsi sebagai antarmuka untuk kode yang dapat dijalankan pada *server* pengembang (Santoso et al., 2019). Dengan adanya pemberitahuan melalui aplikasi Telegram *user* dengan cepat mengetahui bahwa serangan yang sedang terjadi pada jaringan sehingga keamanan dapat diatasi pada saat itu. Keunggulan menggunakan *snort* dibandingkan dengan *software* IDS lainnya kode sumber berukuran kecil dan dapat digunakan pada bnyak aplikasi, cepat mudah di konfigurasi dan juga snort besifat gratis.

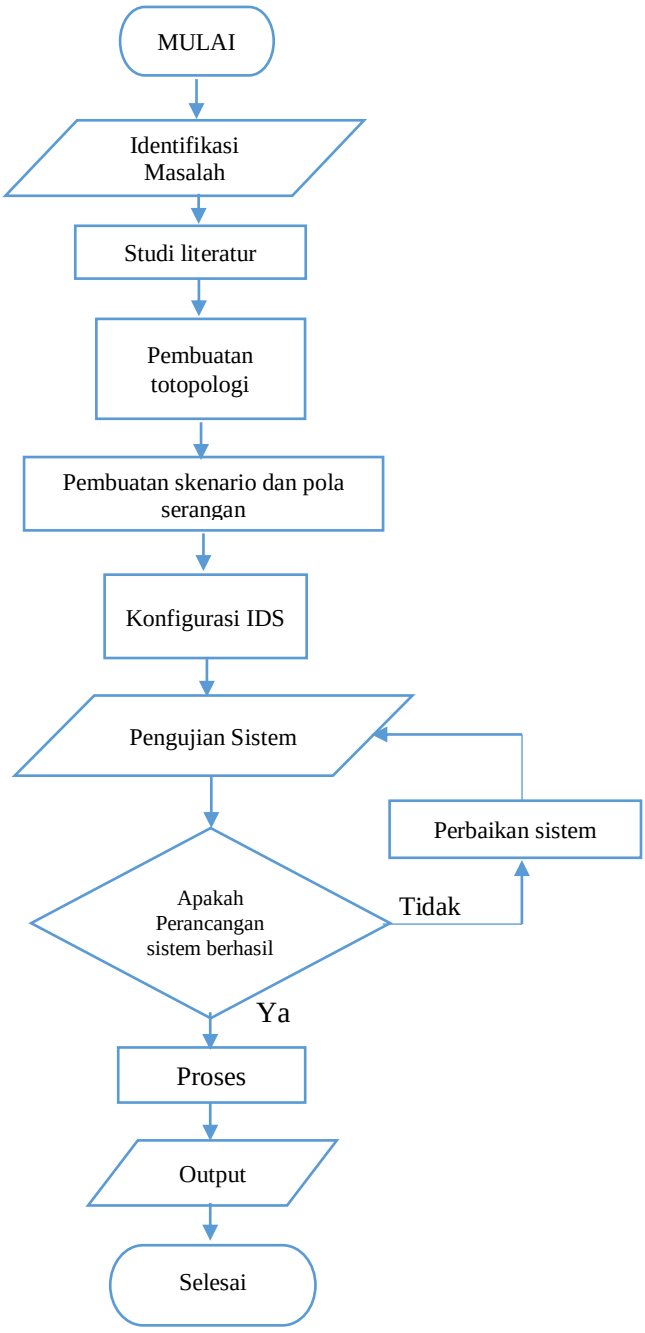
Berdasarkan latar belakang tersebut, maka pada skripsi ini akan dibuat Perancangan IDS (*Intrusion Detection System*) Untuk

Mendeteksi Serangan Menggunakan Aplikasi Telegram.

2. Metodologi

2.1 Metode Penelitian

Tahapan yang dilakukan dalam penelitian ini dimulai dengan studi pustaka, lokasi penelitian, alat dan bahan, prosedur penelitian, teknik pengumpulan data, serta analisis dan permodelan sistem.



Gambar 1. Diagram alir penelitian

2.2 Perancangan Sistem Secara Umum

Metode perancangan sistem pendeteksian notifikasi serangan berbasis telegram yang dibuat dalam penelitian ini adalah sebagai berikut :

a. Perancangan ip address

IP Address merupakan pengalamatan yang berfungsi untuk komputer dapat berkomunikasi satu sama lain, *ip address* ini akan di konfigurasi pada *server suricata* dan juga komputer *attacker* . Ada pun *ip address* untuk *router Pfsense* adalah sebagai berikut:

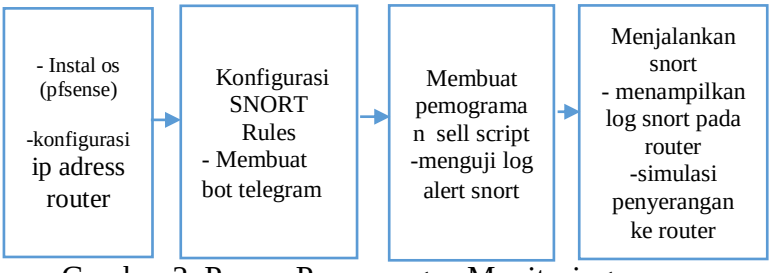
IP Address : *Router Pfsense*
Ethernet1 : DHCP
Ethernet2 : 192.168.10.100/24

Pada perancangan *ip address router* diatas *user* menggunakan 2 buah *Network Adapter* pada *Ethernet* satu digunakan untuk menghubungkan *server* dengan internet dan ini diperlukan untuk mengirim *log* melalui *bot* telegram dan *Ethernet* dua digunakan untuk menghubungkan dengan komputer (*attacker/tester*). Sedangkan *ip address* yang digunakan pada komputer *attacker* adalah:

IP Address : 192.168.10.200/24
SubnetMask : 255.255.255.0
Gateway : -

2.3 Alur Proses Perancangan Monitoring Berbasis *SNORT*

Perancangan secara global dari sistem sangat diperlukan, mulai dari tahapan awal hingga akhir, hal ini agar lebih terarah,seperti pada Gambar 2.



Gambar 2. Proses Perancangan Monitoring SNORT

-O – mencoba menebak sistem operasi yang digunakan oleh mesin target.

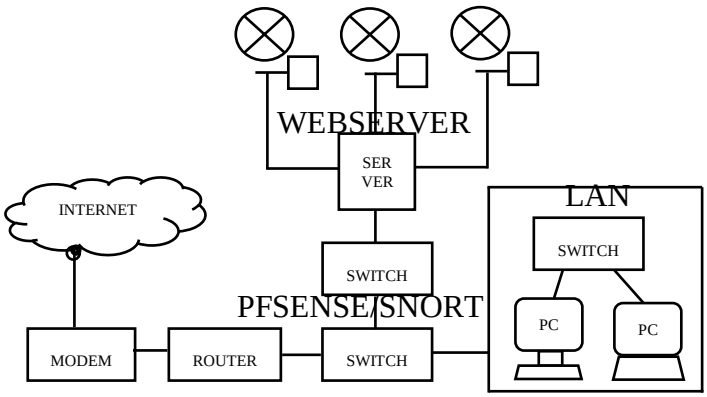
contoh penggunaan nmap ke domain unri.ac.id
localhost:~ # nmap -v -sS -O unri.ac.id
Starting Nmap 7.70 (https://nmap.org) at 2020-12-29 20:31 WIB
Initiating Ping Scan at 20:31
Scanning unri.ac.id (103.158.167.212) [4 ports]
Completed Ping Scan at 20:31, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:31
Completed Parallel DNS resolution of 1 host. at 20:32, 7.06s elapsed
Initiating SYN Stealth Scan at 20:32
Scanning unri.ac.id (103.158.167.212) [1000 ports]
Discovered open port 22/tcp on 103.158.167.212
Discovered open port 443/tcp on 103.158.167.212
Increasing send delay for 103.158.167.212 from 0 to 5 due to 11 out of 13 dropped probes since last increase.

Terlihat dari hasil scan melalui nmap di atas domain unri.ac.id hanya membuka port 20/SSH dan port 443/HTTPS, dari hasil scan tersebut dapat disimpulkan domain unri.ac.id memiliki pertahanan baik.

b. Analisis Kebutuhan

Ada beberapa analisis kebutuhan dalam perancangan sistem monitoring serangan jaringan ini diantaranya :

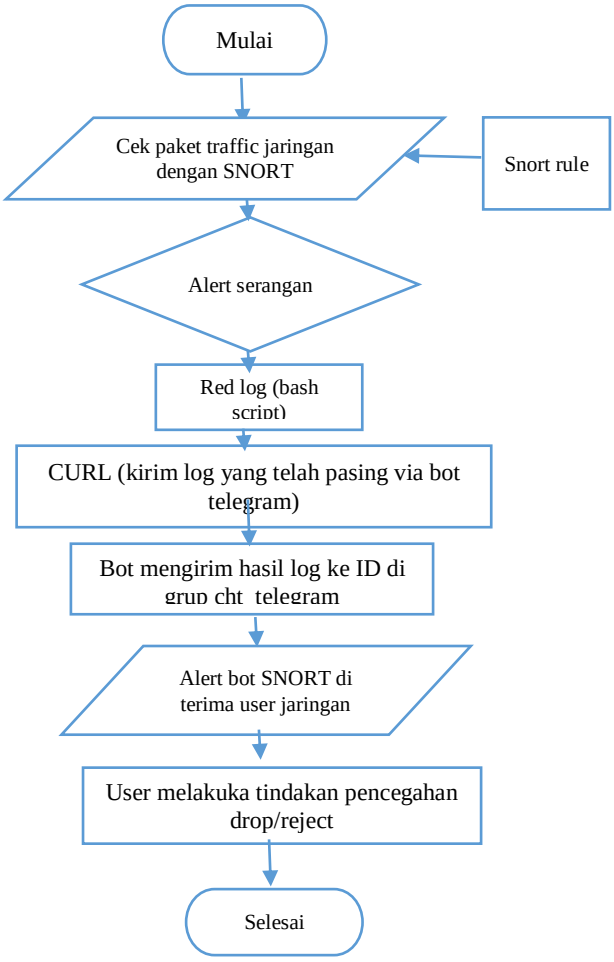
Topologi yang diusulkan pada Universitas Riau dapat dilihat pada Gambar 3.



Gambar 3. Usulan topologi dengan penerapan sistem IDS

c. *Flowchart* Sistem

Perancangan diagram alir sistem IDS *(Intruticction Detection System*) pendeteksian serangan pada layanan *cloud computing* berbasis notifikasi telegram dapat dilihat pada Gambar 4.



Gambar 4. *Flowchart* Sistem IDS pendektesian serangan

2.3 Teknik Pengujian Sistem

Pengujian sistem merupakan proses pengeksekusian sistem perangkat lunak untuk menentukan apakah sistem perangkat lunak tersebut cocok dengan spesifikasi sistem dan berjalan sesuai dengan yang diinginkan. Pengujian sistem sering disamakan dengan pencarian *bug*, ketidaksempurnaan program, kesalahan pada baris program yang menyebabkan kegagalan pada eksekusi sistem perangkat lunak.

Adapun pengujian sistem yang akan dilakukan pada penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Tabel Pengujian Sistem

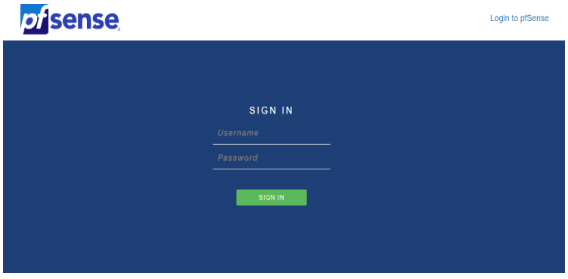
No	Jenis Pengujian	Tools Yang Digunakan	Hasil Yang Di harapkan
1	*Scanning port*	NMAP	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot
2	*Bruteforce*	HYDRA	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot
3	*Scanning WebServer*	NIKTO	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot
4	*Scanning WebServer*	NIKTO	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot
5	*Scanning port*	NMAP	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot

3. Hasil dan Pembahasan

Hasil dari implementasi dari "perancangan sistem *intrusion detection system* (ids) untuk mendeteksi serangan menggunakan aplikasi telegram" akan ditampilkan pada setiap halaman serta penjelasannya**.**

a. Tampilan Halaman *Login pfsense*

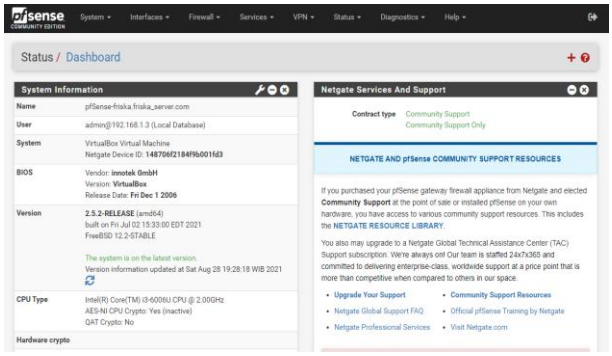
Menampilkan halaman login *pfsense* menggunakan *username* dan *password*. Setelah *user* mengisikan *username* dan *password* pada *field* yang telah disediakan, maka *user* akan menekan tombol enter atau klik tombol *sign in*. Tampilan dapat dilihat pada Gambar 5.



Gambar 5. Tampilan Halaman *Login pfsense*

b. Halaman *Control Snort* di *Pfsense*

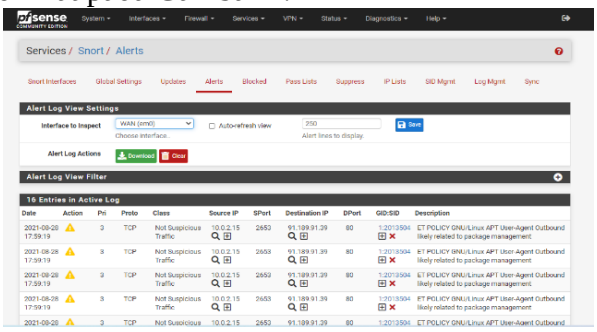
Halaman *dashboard pfsense* menampilan informasi-informasi pada sistem jaringan yang terkoneksi pada pfsense. Informasi sistem yang ditampilkan yaitu *Name, User, System, BIOS, Version, CPU Type dan Hardware Crypto*. Tampilan halaman *dashboard* dapat dilihat pada Gambar 6.



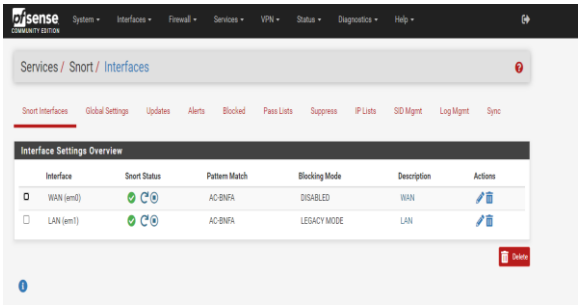
Gambar 6. Halaman *Dashboard*

c. Halaman *Alert Pfsense*

Halaman *Alert PfSense* menampilkan laporan detail dari *alert snort* jaringan yang memantau lalu lintas jaringan dan mendeteksi aktivitas yang tidak sah (serangan). Setiap aktivitas pada lalu lintas jaringan akan ditampilkan pada halaman ini dalam bentuk list. Tampilan halaman *Alert PfSense* dapa dilihat pada Gambar 7.



Gambar 7. Halaman *Alert Pfsense*

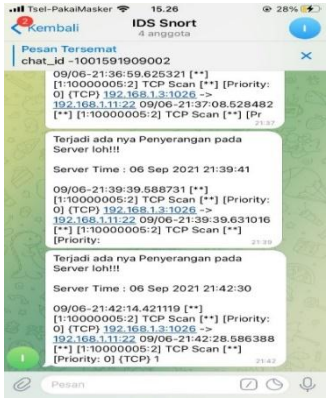


Gambar 8. Tampilan *control alert* di *pfsense*

Gambar 8. menunjukkan laporan detail dari *alert snort* jaringan. Jika serangan terdeteksi pada jaringan, maka informasi serangan berupa waktu dan alamat IP komputer yang diserang akan ditampilkan. Selanjutnya ada halaman *Control Pfsense*. Halaman ini digunakan untuk mengontrol *interface* dari dari *snort*. Halaman *control pfsense*

d. Tampilan notifikasi telegram

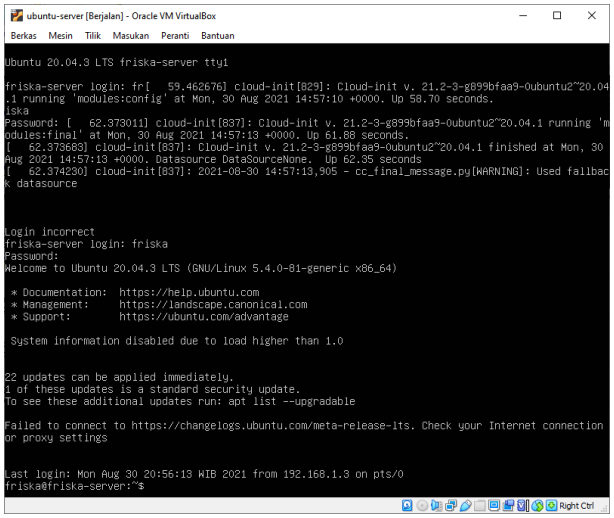
Halaman ini merupakan halaman tmpilan notifikasi telegram yang muncul apabila terdeteksi sebuah serangan dapat dilihat pada Gambar 9.



Gambar 9. Tampilan notifikasi telegram

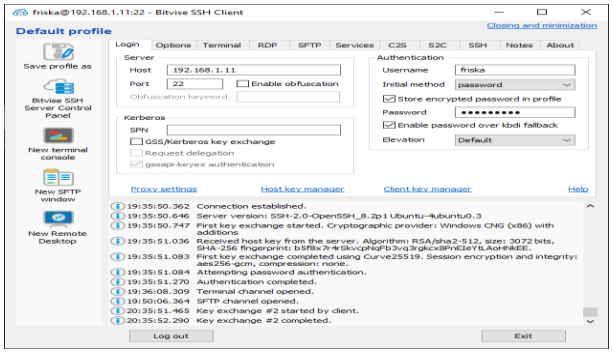
e. Pengujian Sistem IDS

Halaman ini merupakan halaman awal server *ubuntu*. Untuk masuk kedalam *server ubuntu* masukkan *user* name friska dan password friska123 dan selanjutny akan masuk pada perintah level admin dengan mengetikkan *command sudo su*. Dapat dilihat pada Gambar 10.



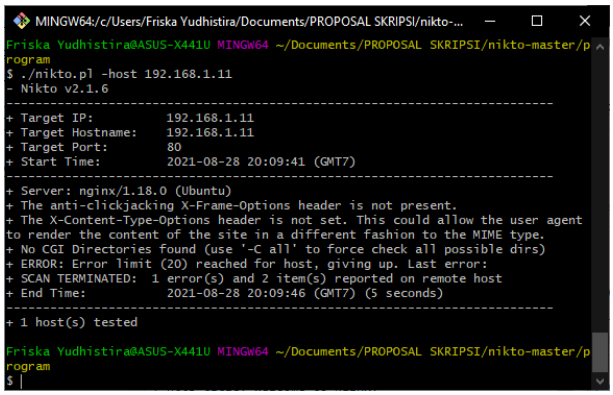
Gambar 10. Tampilan awal *login server ubuntu*

Untuk *login server* ubuntu secara *remote* gunakan aplikasi *SSH. SSH* berfungsi sebagai protocol administrasi *remote* yang memperbolehkan untuk mengontrol dan memodifikasi *server remote* melalui internet. Layanan *SSH* ini dibuat sebagai penganti yang aman untuk *telnet* yang tidak di *endkripsi*. Ssh juga dapat ,menjalankan tugas *monitoring log* file dan memulai atau menghentikan *service* (berlaku di layanan VPS/*Dedicated*). Pertama buka aplikasi SSH untuk login lalu ketikkn alamat ip dari *server ubuntu* yaitu 192.168.1.11. jika *login* berhasil maka akan menampilkan keterangan *connection eshtablised.* Dapat dilihat pada Gambar 11.



Gambar 11. *Betsive SSH* Untuk *Ubuntu Server*

Untuk melakukan pengujian *scanning web server*, digunakan aplikasi *Nikto*. *Nikto* adalah pemindai *web server Open Source* (GPL) yang melakukan pengujian menyeluruh terhadap server web untuk beberapa item, termasuk lebih dari 6700 file/program yang berpotensi berbahaya. Nikto juga memeriksa item konfigurasi server seperti adanya beberapa file indeks, pilihan server HTTP, dan akan mencoba untuk mengidentifikasi server web yang diinstal. Pengujian dengan Nikto dilakukan dengan cara klik kanan git bash lalu tekan ./nikto.pl. Selanjutnya aplikasi Nikto akan melakukan scanning terhadap *web server*. Proses scanning webserver menggunakan *Nikto* dapat dilihat pada gambar 12.



Gambar 12. *Scan Web Server* Menggunakan *Nikto*

3.1 Pengujian Sistem

Pengujian Sistem yaitu menguji kode program.Pengujian dimaksudkan untuk mengetahui masukan, dan keluaran dari perangkat lunak sesuai dengan spesifikasi yang dibutuhkan. Pengujian dilakukan dengan menguji setiap proses dan kemungkinan kesalahan yang terjadi untuk setiap proses. Hasil pengujian dikatakan valid apabila output sistem sesuai dengan yang diharapkan. Jika terdapat bug atau gangguan pada sistem, maka akan dikatakan invalid apabila terjadinya dilakukan perbaikan pada gangguan tersebut. Dari 5 pengujian yang telah dilakukan, 80% berhasil dan 20% gagal, maka dapat dinyatakan pengujian berhasil *nmap, hydra, nixto* dilihat pada Tabel 2.

Tabel 2. Hasil pengujian Sistem

Jenis Pengujian	Tools Yang Digunakan	Hasil Yang Diharapkan	Hasil Yang di peroleh	Kesimpulan

Scanning port	NMAP	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot	Menampilkan serangan yang terkirim va telegram	Valid
Bruteforce	HYDRA	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot	Menampilkan serangan yang terkirim via telegram grafik	Valid
Scanning WebServer	NIKTO	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot	Menampilkan serangan yang terkirim via telegram	Valid
Scanning WebServer	NIKTO	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot	Terjadi error dan tidak menampilkan notifikasi via tekegram	Invalid
Scanning port	NMAP	Log Serangan Pada SNORT Dashboard Pfsense, Log Pada CLI Pfsense dan Notifiksi Serangan Terkirim via Telegram Bot	Menampilkan serangan yang terkirim via telegram	Valid

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan mengenai Perancangan Sistem *Intrusion Detection System* (IDS) Untuk Mendeteksi Serangan Menggunakan Aplikasi Telegram, maka diperoleh kesimpulan sebagai berikut :

1. Sistem ini dapat mendeteksi serangan yang terjadi pada suatu jaringan komputer dengan melakukan *scanning* terhadap sejumlah *source* dan lalu-lintas yang terjadi didalam jaringan, sehingga seluruh kejadian yang dianggap tidak sah dapat dilihat melalui kegiatan *monitoring* dengan menggunakan aplikasi yang digunakan untuk melakukan pemantauan jaringan.
2. Sistem IDS ini akan memberikan notifikasi atau peringatan melalui aplikasi telegram jika ada serangan pada jaringan komputer terdeteksi dalam sistem, sehingga *administrator* jaringan dapat mengetahui terjadinya serangan tersebut secepat mungkin.
3. Dari 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.

5. Saran

Sistem ini masih jauh dari kata sempurna , berikut beberapa saran bagi yang ingin mengembangkan sistem yang mungkin dapat menambah nilai dari sistem nantinya:

1. Sistem yang telah dibuat sudah cukup merespon terhadap lalu lintas dan serangan yang terjadi pada jaringan, akan tetapi lebih baik lagi jika menggunakan sistem yang memiliki

respon yang lebih sensitif terhadap berbagai jenis serangan, sehingga dapat diketahui jenis serangan yang sedang terjadi.

2. Dari sisi pencegahan masih harus dikembangkan lagi dalam melindungi aset yang terdapat pada komputer yang menjadi tujuan dari penyerangan.

DAFTAR PUSTAKA

Anif, M., Sindung, H.W.S., Huri, M, D. (2015). Penerapan *Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer*. Jurnal TELE. Vol.13 No.1 penerbit: Politeknik Negeri Semarang, Semarang pp.347-368.

Ariewijaya.(2015). *Optimalisasi Network Security Dengan Mengkombinasikan Instrusion Detection System dan Firewall pada Web Server.* Jurusan Teknik (KOMPUTA).Vol.1 No.1, Penerbit:STMIK Pangkal pinang , pp.97-101.

Awangga, D.N., Sajati, H., Astuti, Y. (2013). *Pemanfaatan Intrusion Detection System (Ids) Sebagai Otomatisasi Konfigurasi Firewall Berbasis Webservice Menggunakan Arsitektur Representationalstate Transfer* (Rest). Jurnal Media Neliti. Vol.2, No.2, penerbit:STTA Yogjakarta , pp.323-334.

Hariwan, Panca. (2012). *Pengembangan dan Analisa Kinerja Instrusion Detection Prevention System (IDPS).*Vol.12,penerbit:Universitas indonesia,Jakarta, pp.27-34.

Maria, Ulfa, (2015) dengan judul *Perancangan dan Implementasi Sistem Keamanan Berbasis IDS di Jaringan Internet Universitas Bina Darma*.. Vol 3, penerbit: Universitas Bina Darma Palembang, pp.239-242

Mohd siddik & Akmal Nasution, *(2018*) dengan judul *Perancangan Aplikasi Push Notification Berbasis Android* Vol.2 No.2, penerbit:STMIK royal Kisaran, Medan pp. 149-154.

Nugroho, D. A., Rochim, A. F., & Widianto, E. D. (2015). *Perancangan dan Implementasi Instrusion Detection System di Jaringan Universitas Diponegoro*. Jurnal Teknologi dan Sistem Komputer, Vol.2 No.2,penerbit Universitas Diponegoro,Semarang, pp. 171-178.

Sarifin, A. Astuti, B.R.T. (2012). *Penerapan Router Pfsense Berbasis Free BSD Di Warnet Emax Sragen.*.Vol.1 No.1,penerbit:Universitas Surakarta Solo ,pp.58-60.

Utami, A. S. P., Lidyawati, L., & Ramadhan, Z. (2013). *Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd*. Vol.1 No.1, penerbit:Institut Teknologi Nasional Bandung,Bandung pp.16-21.