ANALISIS PENINGKATAN KEAMANAN SERVER MENGGUNAKAN SNORT DAN PFSENSE PADA JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER DI POLITEKNIK NEGERI JAKARTA

LAPORAN SKRIPSI

SUCI RAHMADHANI **4817050415**

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2021

RANCANG BANGUN KEAMANAN SISTEM SERVER

ANALISIS PENINGKATAN KEAMANAN SERVER MENGGUNAKAN SNORT DAN PFSENSE PADA JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER DI POLITEKNIK NEGERI JAKARTA

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

SUCI RAHMADHANI
4817050415

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2021

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	**: Suci Rahmadhani**
NIM	**: 4817050415**
Tanggal	**: 23 juni 2021**
Tanda Tangan	**:**

HALAMAN PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Suci Rahmadhani
NIM	:	4817050415
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Peningkatan Keamanan Server Menggunakan Snort dan Pfsense pada Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri jakarta

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 30, Bulan Juni Tahun 2021 Dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I : Defiana Arnaldy, S.Tp., M.Si. ( )

Penguji I : Maria Agustin, S.Kom., M.Kom. ( )

Penguji II : Muhammad Yusuf Bagus Rasyiidin, S.Kom., M.TI. ( )

Penguji III : Ariawan Andi Suhandana, S.Kom., M.T.I. ( )

Mengetahui:

Ketua Jurusan Teknik Informatika dan Komputer

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini. Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan skripsi, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. Bapak Defiana Arnaldy, S.Tp., M.Si. selaku kepala program studi serta dosen pembimbing yang menyediakan waktu serta tenaga dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini.
b. Bapak Fachroni Arbi Murad, S.Kom., M.Kom. Selaku dosen yang juga telah ikut membantu untuk mengarahkan penulis dalam penyusunan skripsi ini.
c. Orang tua dan keluarga penulis yang sudah memberikan bantuan dukungan penuh secara moral dan material. Dalam mendukung penulis pembuatan skripsi.
d. Febby Rahmi A. kakak saya tercinta yang memberikan dukungan moral serta mendengarkan segala keluh kesah penulis dan membantu penulis dalam penyelesaian skripsi.
e. Dita Nurhayati, selaku teman satu tim, satu perjuangan dalam penyusunan laporan skripsi ini yang telah memberikan bantuan dukungan secara moral
f. Sabrina Annisa A., Trisya Talia D. dan Laily Rachmi atas waktunya mendengarkan segala keluh kesah penulis dan menemani penulis begadang untuk mengerjakan skripsi hingga larut setiap harinya.
g. Sahabat-sahabat saya, teman-teman Cahya Mulyadi, David Matius, Kevin K., Aji Trinio, Marta Surya dan teman “Bismillah” lainnya, teman kelas satu perjuangan dari awal hingga akhir masa perkuliahan yang tidak pernah putus memberi semangat.

Yolanda Wahyu R, Vina Rachmawaty dan Reni Afriyanti sahabat saya memberikan semangat serta mendengarkan segala dukungan dalam segi moral.

Egi Dita A. dan Norma Asyifa sahabat saya memberikan dukungan moral serta mendengarkan segala keluh kesah penulis. Serta membantu penulis dalam segala yang dibutuhkan penulis dalam pembuatan skripsi.

Akhir kata, penulis berharap Allah SWT. Membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini dapat bermanfaat bagi semua masyarakat.

Depok, 23 Juni 2021

Suci Rahmadhani

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan dibawah ini:

Nama	: Suci Rahmadhani
NIM	: 4817050415
Program Studi	: Teknik Multimedia dan Jaringan
Jurusan	: Teknik Informatika dan Komputer
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

Analisis Peningkatan Keamanan Server Menggunakan Snort dan Pfsense Pada Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri Jakarta.

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database)*, merawat, dan mempublikasikan skripsi saya selama tetap mencamtumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok Pada tanggal : 30 juni 2021

Yang Menyatakan

(Suci Rahmadhani)

Analisis Peningkatan Keamanan Server Menggunakan Snort dan Pfsense pada Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri Jakarta.

ABSTRAK

Kendala luar yang menggangu keamanan pada sistem server jurusan Teknik Informatika dan Komuter di Politeknik Negeri Jakarta seperti serangan pada sistem server serangan DoS Attack. Dalam meningkatkan segi keamanan sistem server Jurusan Teknik Informatika dan Komputer Di Politeknik Negeri Jakarta. Oleh sebab itu dibutuhkan penanggulangan dari ancaman berupa penggunaan Intrusion Detection System (IDS) mengetahui adanya serangan yang masuk berupa peringatan pada sistem jaringan komputer. Serta penerapan Intrusion Prevention System (IPS) sebagai proteksi keamanan sistem server berupa penggunaan pfsense. Metode yang digunakan berupa alert atau monitoring server apabila adanya serangan yang masuk, Log snort membantu system administrator mencatat segala jenis aktivitas yang mencurigakan pada server dan penggunaan firewall sebagai hardening apabila terjadi serangan yang masuk dari jaringan local, serta dapat melakukan deny akses apabila serangan mencoba akses sistem server Jurusan TIK-PNJ. Firewall pada pfsense menghalau dan memproteksi serangan yang mencoba masuk menuju server. Dari hasil pengujian, snort mampu melakukan monitoring dan menyimpan log dan pfsense dapat melakukan blocking akses pada saat jaringan mencoba masuk pada sistem server serta pada serangan ping of death dan smurf attack berlangsung.

Kata Kunci: *Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Pfsense, Snort.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABLE

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era global saat ini, pengelola server jaringan serta internet (*system administrator*) mempunyai kendala serta tanggung jawab terhadap keamanan sistem dari waktu ke waktu. *Administrator* yang bertugas dalam pengaksesan jaringan sebagai *monitoring* apabila terjadi adanya serangan dan penyalahgunaan jaringan. Berbagai macam kendala seperti serangan yang terjadi dari luar mengganggu keamanan jaringan sistem server serta koneksi internet. penyalahgunaan atau penyusupan data maupun jaringan sistem menyebabkan administrator harus memastikan sistem dan pengelolaan jaringan berjalan dengan baik dari adanya ancaman penyalahgunaan jaringan tersebut.

Pemecahan masalah tersebut diperlukan keamanan sistem pada server dari ancaman luar seperti serangan *Ping of Death* dan *Smurf Attack* menggunakan *Intrution Detection System* (IDS) dan *Intrution Prevention System* (IPS) berupa metode kemananan jaringan sistem dapat melindungi server pada sebuah jaringan. IDS sebagai *alert* atau mendeteksi ketika terjadi adanya serangan. Serta IPS yang dapat *rules* menindaklanjuti dalam serangan dengan cara menindaklanjuti serangan yang terjadi dengan cara mem*block* akses server atau sistem jaringan pada komputer penyerang.

Pekerjaan utama sistem deteksi intrusi adalah mengumpulkan paket dari jaringan, memprosesnya dan jika serangan mengidentifikasi maka Ini akan menghasilkan peringatan untuk kemungkinan serangan. Keamanan jaringan, sistem deteksi intrusi memiliki dua rasa untuk jaringan dan host berdasarkan kategori dan ragam itu yang dikenal sebagai tanda tangan atau basis aturan deteksi intrusi dan deteksi intrusi berbasis anomali. (Patel, S. K. & Sonker, A., 2016.).

Suatu serangan dapat dideteksi atau tidak oleh Snort dikonfigurasi pada pengaturan jaringan dan *rule* Snort yang ada. Pengujian Snort IDS dilakukan dengan beberapa pola serangan untuk menguji kehandalan Snort dalam mendeteksi sebuah serangan terhadap sistem keamanan. Berdasarkan hasil pengujian sistem Snort IDS dengan ping, nmap, eksploitasi, dan *Ping of Death*, Snort dapat memberikan peringatan adanya serangan keamanan terhadap sistem jaringan. Hasil peringatan tersebut dapat digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan.(Pratama, I. P. A. E. & Handayani, N. K. M., 2019.)

Intrusion Detection and Prevention System (IDPS) merupakan salah satu pilihan untuk meningkatkan keamanan jaringan dalam sebuah jaringan baik intranet maupun internet. Penerapan *Intrusion Detection* and *Prevention System* (IDPS) digunakan sebagai salah satu solusi yang dapat digunakan untuk membantu *administrator* dalam memantau dan menganalisa paket-paket berbahaya yang terdapat dalam sebuah jaringan. IDPS diterapkan karena mampu mendeteksi penyusup atau paket-paket berbahaya dalam jaringan dan memberikan laporan berupa *log* kepada *administrator* tentang aktivitas dan kondisi jaringan secara real-time sekaligus melakukan drop packet terhadap penyusup. Sehingga segera dapat diambil tindakan terhadap gangguan atau serangan yang terjadi. (Arsin, F., Yamin, M. & Surimi, L., 2017.)

Jika terindikasi adanya aktifitas yang mencurigakan terhadap aliran (*traffic*) paket-paket yang keluar dan masuk pada sistem, maka IDS akan merekam aktifitas tersebut. IDS merupakan software atau hardware yang melakukan otomatisasi proses *monitoring* kejadian yang muncul di sistem komputer atau jaringan, menganalisanya untuk menemukan permasalahan keamanan (Wijaya, B. & Pratama, A., 2020)

Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi yaitu dengan menggunakan aplikasi *Intrusion Detection System* (IDS) yaitu Snort dan PfSense (Router OS) sebagai penindak lanjut terhadap *alert* snort yang dihasilkan. (Sutarti, pancaro, A. P. &

Saputra, F. I., 2018.). Meningkatkan keamanan server dengan Snort IDS melalui beberapa pengujian, sehingga, manfaat yang didapat dari hasil penelitian ini adalah meningkatnya keamanan dalam jaringan, dapat digunakan pada banyak sistem operasi, cepat dan mampu mendeteksi serangan pada jaringan, mudah dikonfigurasi dan open source. (Pratama, I. P. A. E. & Handayani, N. K. M., 2019.)

1.2 Perumusan Masalah

Perumusan masalah yang terdapat pada analisis keamanan jaringan IDS/IPS Snort dan Pfsense pada jurusan Teknik Informatika dan Komputer adalah:

a. Bagaimana menguji serangan pada *Ping of Death* dan *Smurf Attack* pada sistem server ?
b. Bagaimana cara penanggulangan sistem keamanan *Ping Of Death* dan *Smurf Attack* pada server menggunakan IDS/IPS ?
c. Bagaimana penggunaan Snort dan Pfsense pada server?
d. Bagaimana kelebihan dan kekurangan dari metode penggunaan *Snort* dan *Pfsense* pada server (untuk keamanan server)?
e. Bagaimana implementasi efeketivitas penggunaan Pfsense pada keamanan sisttem server?
f. Bagaimana meningkatkan keamanan server?

1.3 Batasan Masalah

Batasan masalah yang ditentukan dalam Analisis keamanan jaringan menggunakan IDS/IPS adalah sebagai berikut :

a) Sistem keamanan pada server *dummy* jurusan TIK PNJ menggunakan sistem operasi Ubuntu 16.04 CLI yang dijalankan dengan *Virtual machine* (VirtualBox).
b) Pengujian uji coba serangan *Denial of Service* (DoS) berupa serangan *Ping of Death* dan *Smurf Attack* dilakukan berupa *Intrusion Detection System* (IDS) *monitoring* server mengggunakan snort dan *Intrusion Prevention System* (IPS) berupa *blocking* akses menggunakan pfsense

c) Serangan disimulasikan secara *Local Area Network* (LAN), penyerang berada dalam satu jaringan internet dengan server.
d) Serangan *Ping of Death* dan *Smurf Attack* menggunakan LOIC dan HPING3.
e) Pengujian penelitian berupa prosedur waktu penyerangan *(Real Time)*, prosedur Efektifitas dan prosedur kualifikasi.
f) Hasil berupa *traffic* dan jumlah paket yang dihasilkan berupa dilakukan sebelum dan sesudah penyerangan dengan durasi waktu secara *real time* 5 dan 10 menit.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah Diantaranya adalah sebagai berikut :

a. Meningkatkan penanggulangan sistem keamanan pada serangan *Ping of Death* dan *Smurf Attack* pada sistem server.
b. Meningkatkan dalam pengamanan data penting seperti data jurusan Teknik Informatika dan Komputer.

1.4.2 Manfaat

Manfaat dari Implementasi *Intrusion Prevention System* menggunakan Snort dan Pfsense pada sistem server Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta adalah sebagai berikut :

1) Dihasilkan sistem server yang aman dari dari serangan *Ping of Death* dan *Smurf Attack* pada server jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.
2) Dihasilkan sistem keamanan server yang aman bagi Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

1.5 Metode Pelaksanaan

Penelitian menggunakan pendekatan metedologi penelitian berupa PPDIOO *(Prepare, Plan, Design, Implement, Operate* dan *Optimize)* sebagai berikut:

1.5.1 Fase Persiapan *(Prepare)*

Pada langkah ini, penulis melakukan persiapan berupa jurnal, studi literatur dan referensi jurnal yang berhungan dengan topik penelitian. Serta mempersiapkan perangkat lunak dan perangkat keras yang akan digunakan dalam realisasi sistem.

1.5.2 Fase Perencanaan *(Plan)*

Langkah ini dilakukan perencanaan berdasarkan tujuan dan kebutuhan. Peneliti akan melakukan implementasi IDS *(Intrusion Detection System)* dan IPS *(Intrusion Detection Prevention)* berupa snort dan pfsense. Serta melakukan pengujian serangan *Ping of Death* dan *Smurf Attack* menggunakan *tools* LOIC dan HPING3.

1.5.3 Fase Desain *(Design)*

Pada langkah ini peneliti menggunakan langkah design penelitian dalam merancang topologi jaringan, alur pengerjaan, alur pengujian, serta skenario pengujian.

1.5.4 Fase Implementasi *(Implement)*

Peneliti melakukan pengimplementasian IDS dan IPS yaitu berupa *snort* serta aplikasi penunjang lainnya yang mendukung sistem keamanan seperti Pfsense yang akan menindaklanjuti serangan yang terjadi pada server untuk di*block*.

1.5.5 Fase Operasi *(Operate)*

Peneliti melakukan *monitoring* sistem yang bekerja pada snort dan pfsense. Berupa jumlah paket yang masuk, *traffic*, *States* dan *firewall* ketika terjadinya serangan.

1.5.6 Fase Optimasi *(Optimize)*

Setelah melakukan pengimplementasian selesai, apabila terjadi kesalahan yang ada pada sistem depat dilakukan *optimize* seperti penambahan source ,penambahan fitur atau lainnya yang menunjang penelitian lebih baik.

BAB V

PENUTUP

5.1 Simpulan

Berdasarkan penelitian ini bahwa yang dilakukan konfigurasi sistem keamanan berupa snort dan pfsense pada server *dummy* Jurusan TIK-PNJ, dapat disimpulkan bahwa:

- **Snort:**

a) Keamanan sistem *Intrution Detection System* (IDS) dapat menangani adanya serangan yang masuk denga penggunaan *Snort* yang mampu mengatasi adanya serangan atau jaringan yang masuk sebagai *alert* dan mencatat serangan yang masuk. Berupa jenis serangan *Ping of Death* dan *Smurf Attack* sukses.

b) Serta dalam rentang waktu yang telah dilakukan pengujian terbukti sistem dapat membaca jumlath paket data, waktu, dan protokol jaringan yang masuk pada sistem server.

- **Pfsense:**

a) Keamanan sistem sebagai *Intrution Prevention System* (IPS) pfsense dapat menangani adanya serangan berupa *Ping of Death* berupa keamanan *bloking* akses sukses. Serta Pfsese melakukan *blocking* akses dari serangan berupa *Smurf Attack* terjadi kegagalan dalam *blocking* akses dari serangan luar.

b) Pfsense mampu membaca *traffic* yang berjalan saat adanya serangan yang masuk dari pfsense menuju server *dummy* Jurusan TIK-PNJ.

5.2 Saran

Adapun beberapa saran diataranya dalam penelitian keamanan sistem yang telah dilaksanakan pada jurusan TIK-PNJ yaitu:

a) Penggunaan pfsense dapat melakukan percobaan serangan lainnya.

b) Menanambahkan fitur sistem keamanan lainnya pada sistem server Jurusan TIK-PNJ seperti Suricata atau *Honeypot*

DAFTAR PUSTAKA

A. Williams. (2018). The best Linux distros of 2018. *[Online]*, Available: https://www.techradar.com/news/best-linux-distro.

Abdulloh, Y., Triyono, J., & Lestari, U. (2020). Pengaruh Penempatan Snort Terhadap Kemanan Jaringan. *Jurnal JARKOM*, 2338-6304.

Ariyanto, Y., Firdaus, V. A., & Pramana, H. (2020). Klasifikasi Jenis serangan DOS dan Probing pada IDS menggunakan metode K-Nearest Neighbor.

Arman, M., & Inayatullah. (2019, Vol. 11 No. 1, April 2019, 49-58). Rancang Bangun Owncloud dan Melindunginya Terhadap Serangan DDOS. *Jurnal Integrasi*, 49-58.

Arman, M., & Rachmat, N. (2020). Implementasi Sistem KeamananWeb Server Menggunakan Pfsense. *Jurnal Sistem Komputer Musirawas, Vol. 05*, 13-23.

Arsin, F., Yamin, M., & Surimi, L. (2017). IMPLEMENTASI SECURITY SYSTEM MENGGUNAKAN METODE IDPS (INTRUSION DETECTION AND PREVENTION SYSTEM) DENGAN LAYANAN REALTIME NOTIFICATION. *semanTIK, Vol.3*, pp. 39-48.

Bella, M. R., Data, M., & Yahya, W. (2019). Implementasi Load Balancing Server Web Berbasis Docker Swarm Berdasarkan Penggunaan Sumber Daya Memory Host. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*, 3478-3487 .

Cahyani, I. D. (2010). Sistem Keamanan Enkripsi SECURE SHELL (SSH) UNTUK Kemanan Data. *Majalah Ilmiah Universitas Pandanaran*, hal. 1-7.

Deepa, M., & P, S. (2020). Detection of DOS and probe attacks based on snort with density clustering. *ScienceDirect Journal*, 2-5.

Firdaus, B. P., & Suartana, I. M. (2020). Implementasi Keamanan Jaringan Intrution Detection System Menggunakan Pfsense. *Jurnal Manajemen Informatika , Vol. xx*, 40-47.

Gaddam, R., & Nandhini, D. M. (2017). An Analysis of Various Snort Based Techniques to Detect and Prevent Intrusions in Networks. *International Conference on Inventive Communication and Computational Technologies*, 10-15.

Hartawan, I. N., & Satwika, K. S. (t.thn.). Rancang Bangun Laboratorium Virtual Berbasis Cloud Computing di STMIK Stikom Indonesia. *Jurnal Ilmu Kompuer dan Sains Terapan*, 54=60.

Ihsana, A. N., & Maslan, A. (2020). Analisis Keamanan Jaringan Dari Serangan Paket Data Sniffing Di PT Raden Syaid Kantor POS PIAYU KOTA BATAM. *Jurnal Comasie, VOL.03 NO.05*.

Muhammad , A. R., Mochammad , F. R., & Tedi , G. (Vol.3, No.3 Desember 2017). IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN KALI NETHUNTER. *e-Proceeding of Applied Science , Vol.3*.

Patel, S. K., & Sonker, A. (2016). Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort. *International Journal of Future Generation Communication and Networking, Vol. 9*, 339-350.

Pratama, I. P., & Handayani, N. K. (2019). Implementasi IDS Menggunakan Snort Pada Sistem Operasi Ubuntu. *Jurnal Mantik Penusa, Vol. 3*, 176-181.

Pratiwi, D., Santoso, G. B., Mardianto, I., Sediyono, A., & Rochman, A. (2020). Pengelolaan Konten Web Menggunakan Wordpress, Canva dan Photoshop untuk Guru-Guru Wilayah Jakarta. *ABDIHAZ: Jurnal Ilmiah Pengabdian pada Masyarakat*, 11-15.

Putra, C. A., Munir, M. S., Via, Y. V., & Achmadipoetro, R. (2019). Deteksi Serangan Trojan Horse Dengan Memanfaatkan IDS Snort. *SEMINAR SANTIKA*, 203-206.

Saleh, K. (2020). Implementasi InstrutionDetection System (IDS) Pada Server Web PT.XYZ Menggunakan Snort.

Sharma, R., & Parekh, C. (2017). Firewalls: A Study and Its Classification. *International Journal of Advanced Research in Computer Science, Volume 8*, 1979-1983.

Sutarti, pancaro, A. P., & Saputra, F. I. (2018). IMPLEMENTASI IDS (INTRUSION DETECTION SYSTEM) PADA SISTEM KEAMANAN JARINGAN SMAN 1 CIKEUSAL. *Jurnal PROSISKO, Vol. 5*, 2406-7733.

Tohirin. (2020). Penerapan Keamanan Remote Server Melalui SSH Dengan Kombinasi Kriptografi Asimtris dan Autentikasi Dua Langkah. *Jurnal Teknologi Informasi*, 2580-7927.

Vasconcelos, G., G. C., Miani, R., Souza, J., & Guizilini, V. (2016). The impact of DoS attacks on the AR.Drone 2.0. *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium*, DOI 10.1109/LARS-SBR.2016.28.

Wijaya, B., & Pratama, A. (2020). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort. *Jurnal SISFOKOM (Sistem Informasi dan Komputer), Vol. 09*, 97-101.