SSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 19598-19608
Volume 8 Nomor 2 Tahun 2024

Pengembangan Aplikasi Monitoring Server dari Gangguan dan Serangan Dengan Metode Intrusion Detection System Berbasis Android

Ilhamdi Ramadhan[1], Ahmaddul Hadi[2], Hadi Kurnia Saputra[3], Khairi Budayawan[4]

[1234]Program Studi Pendidikan Teknik Informatika, Universitas Negeri Padang
e-mail: ilhamdir1412@gmail.com

Abstrak

Tugas Akhir ini menciptakan aplikasi monitoring server dari gangguan dan serangan dengan metode intrusion detection system berbasis android. Aplikasi ini memanfaatkan metode intrusion detection system sebagai metode untuk mendeteksi gangguan dan serangan. Aplikasi ini berbasis android yang dapat di install pada perangkat mobile sehingga membantu administrator dalam mengelola server. Server akan mendeteksi gangguan dan serangan yang telah dikonfigurasi berupa kondisi atau rules, jika kondisi atau rules terpenuhi maka server akan mendeteksi aksi tersebut menjadi gangguan dan serangan. Server akan menyimpan log atau history dari gangguan dan serangan tersebut dan server akan mengirim pesan gangguan dan serangan ke aplikasi dalam bentuk notifikasi berisi pesan dari gangguan dan serangan yang terjadi. Tugas akhir ini diharapkan dapat membantu administrator dalam mengelola server dari gangguan dan serangan yang terjadi.

Kata kunci: *Monitoring Server, Android, Intrusion Detection System.*

Abstract

This final project creates a server monitoring application for interference and attacks using an Android-based intrusion detection system method. This application utilizes the intrusion detection system method as a method for detecting intrusions and attacks. This application is based on Android which can be installed on mobile devices so that it helps administrators in managing servers. The server will detect disturbances and attacks that have been configured in the form of conditions or rules. If the conditions or rules are met then the server will detect these actions as disturbances and attacks. The server will store a log or history of these disturbances and attacks and the server will send disturbance and attack messages to the application in the form of notifications containing messages about the disturbances and attacks that occurred. This final

assignment is expected to help administrators in managing servers from disruptions and attacks that occur.

Keywords : *Server Monitoring, Intruison Detection System, Android.*

PENDAHULUAN

Masa inovasi data pada masa globalisasi saat ini dirasa berkembang semakin cepat, kemajuan teknologi ini disebabkan oleh munculnya pemikiran manusia yang semakin maju. Hal ini terlihat dari kemajuan ilmu komputer yang berkembang semakin pesat setiap harinya. Perbaikan mekanis secara progresif mendukung penyebaran data yang berharga bagi komunitas yang lebih luas dan dapat menjangkau semua tingkatan. Salah satu media penyebaran data yang dapat menjangkau berbagai lapisan dan tidak terbatas pada batas topografi adalah web. Namun di sisi lain, web bisa menjadi instrumen yang tidak aman, baik dengan mudahnya menyebarkan konten negatif seperti berita penipuan dan sebagainya, atau dengan efektif melakukan aktivitas kriminal berbasis dunia maya.(Kustyandi & Noor, 2021)

Seiring perkembangan zaman teknologi pada sistem komputer, semakin banyak jenis serangan cyber yang dialami oleh pengguna. Server yang terhubung ke internet menjadi sasaran yang empuk bagi seorang yang tidak bertanggung jawab untuk menyerang server. Serangan dapat berupa serangan malware, serangan denial-of-service (DoS), serangan brute-force, serangan phising, dan bentuk serangan lainnya. (Kustyandi & Noor, 2021)

Sistem Monitoring adalah sistem yang dirancang agar dapat memberikan respon saat menjalankan program. Respon yang ditujukan agar dapat memberikan informasi keadaan sistem. Sistem monitoring terdiri dari mekanisme serta program dengan menjalankan sistem informasi pada komputer yang dirancang untuk mendata serta mampu untuk mengirimkan data sesuai dengan data yang diperoleh. (Rahman et al., 2020)

Ada banyak kejadian penyerangan yang direncanakan dan berbagai kemungkinan cara penyerangan. Kegiatan harus dilakukan untuk mengantisipasi terjadinya penyerangan. Salah satu metode yang dapat digunakan untuk mendeteksi serangan adalah *intrusion detection system*. IDS merupakan salah satu cara untuk mengidentifikasi serangan yang terjadi pada komputer atau server pada jaringan komputer. IDS akan bekerja berdasarkan aturan untuk mengidentifikasi serangan atau upaya interupsi dari luar sistem, sebagian besar web, ke dalam sistem internal. IDS akan menyaring aktivitas organisasi, namun IDS memerlukan aktivitas dorongan untuk menginformasikan serangan dengan karakteristik klaim mereka. (Cinderatama et al., 2022)

Android adalah sebuah sistem operasi untuk perangkat mobile device berbasis linux yang mencakup sistem operasi, middleware dan merupakan platform terbuka opensource dan dapat digunakan dalam berbagai bidang. Pada saat ini sistem operasi

android sangat popular, banyak masyarakat yang menggunakannya. (Irvansyah et al., 2020)

Sering terjadinya gangguan dan serangan terhadap server maka dibutuhkan sistem yang dapat memantau server dari gangguan dan serangan. Sistem monitoring server biasanya hanya bisa memberikan informasi gangguan dan serangan ketika administrator sedang berada didepan komputer. Ketika administrator tidak berada didepan komputer, maka administrator terlambat mengetahui informasi ketika terjadi gangguan dan serangan sehingga penanganan masalah sedikit tertunda.

Intrusion detection system dapat membantu administrator dalam memberikan informasi gangguan dan serangan secara real-time. Metode intrusion detection system akan diberikan sebuah kondisi atau rules yang ketika kondisi atau rules terpenuhi maka server akan mengartikan aksi tersebut sebuah gangguan dan serangan. Metode ini hanya memberikan informasi gangguan dan serangan ketika administrator sedang berada didepan komputer.

Aplikasi monitoring server berbasis android dapat membantu administrator dalam menangani masalah yang terjadi karena administrator mendapatkan berupa pesan notifikasi dari aplikasi monitoring server yang dikembangkan. Aplikasi akan menerima pop-up notifikasi ketika terjadi gangguan dan serangan terhadap server sehinggan administrator dapat segera mengatasi masalah yang terjadi.

METODE

Metode yang digunakan untuk pengembangan aplikasi ini adalah dengan menggunakan metode prototype. Metode prototype merupakan pandangan dunia yang belum terpakai dalam strategi pengembangan perangkat lunak dimana metode ini tidak seolah-olah merupakan sebuah kemajuan dalam dunia pengembangan program komputer, namun juga merevolusi strategi pengembangan program komputer kuno. Dalam peragaan model tersebut, prototipe program komputer yang akan datang kemudian ditampilkan kepada klien, dan klien diberi kesempatan untuk memberikan masukan agar program komputer yang akan datang benar-benar memenuhi keinginan dan kebutuhan pelanggan. (Supandi et al., 2019)

1. Pengumpulan Kebutuhan dan Analisis Sistem

   Pada tahap utama yang digunakan dalam pembuatan aplikasi ini adalah mengumpulkan kebutuhan dan analisis sistem dari aplikasi yang akan dibuat. Pada tahap ini dilakukan anlisis dari kebutuhan dari sistem yang akan dikembangkan
2. Perancangan model object oriented

   Langkah selanjutnya yaitu membuat perancangan dari aplikasi yang akan dikembangkan yang digunakan untuk menjadi acuan dalam pengembangan aplikasi.

3. Pembentukan Prototype

   Pada tahap ini dilakukan pembuatan aplikasi berdasarkan rancangan pada langkah sebelumnya. Pembuatan aplikasi dilakukan berdasarkan dari rancangan yang telah dibuat.

4. Evaluasi Prototype

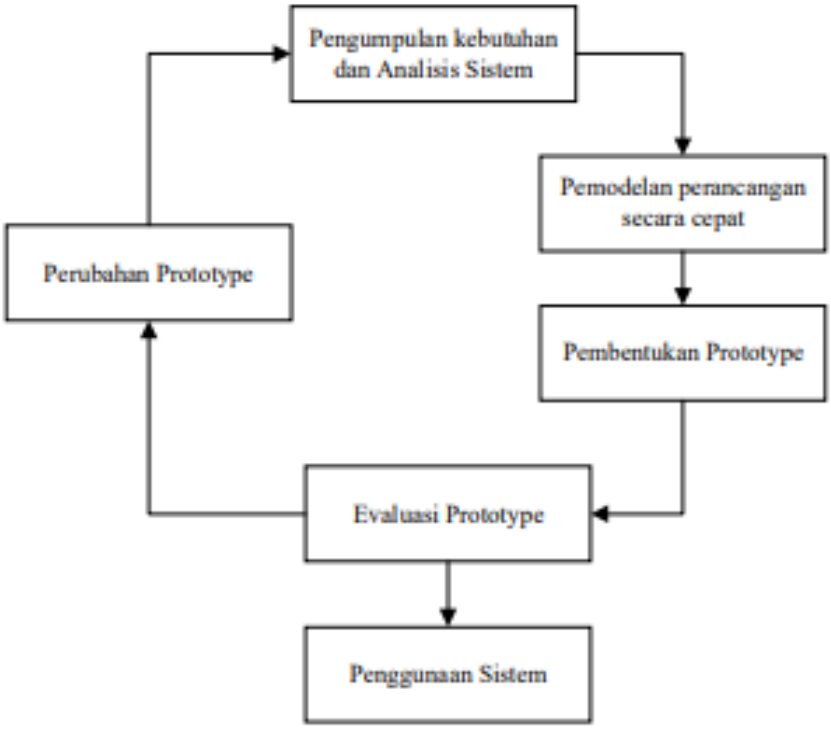
   Langkah selanjutnya yaitu penilaian terhadap aplikasi yang telah dibuat sudah sesuai dengan racangan. Jika aplikasi yang dibuat belum sesuai dengan maka dilakukan perubahan pada aplikasi.

5. Perubahan Prototype

   Pada tahap ini dilakukan penyempurnaan dari pembuatan aplikasi. Pada langkah sebelumnya di lakukan evaluasi maka pada tahap ini dilakukan perubahan aplikasi berdasarkan evaluasi pada tahap sebelumnya.

6. Penggunaan Sistem

   Tahap terakhir dari pengembangan aplikasi yaitu penggunaan sistem yang telah di kembangkan.



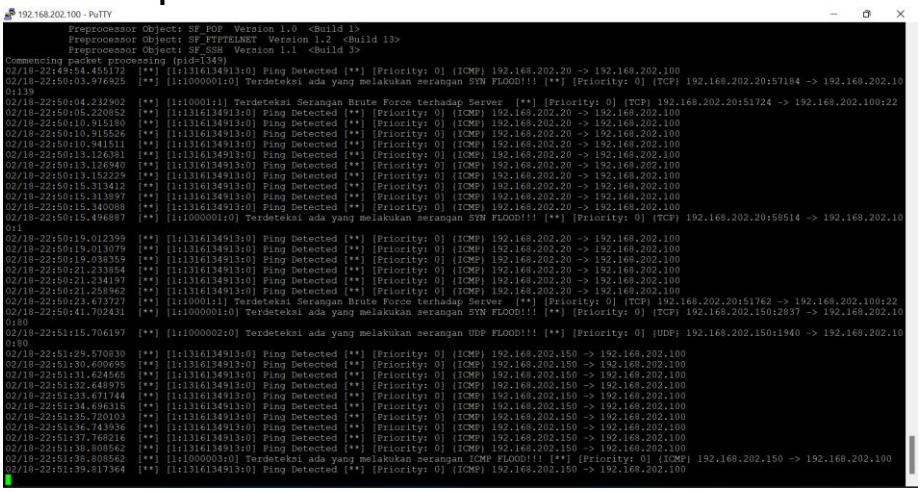
Gambar 1. Metode Prototype

SSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 19598-19608
Volume 8 Nomor 2 Tahun 2024

HASIL DAN PEMBAHASAN

Hasil Pembuatan Aplikasi



Gambar 2. Server Deteksi Serangan

Server mendeteksi serangan yang telah di konfigurasi sesuai dengan rules yang telah di kondisikan, jika kondisi rules terpenuhi maka server akan mendeteksi sebagai serangan dan gangguan. Terdapat beberapa rules yang telah di konfigurasi di file local.rules pada server dan ketika kondisi rules tercapai maka akan muncul pesan seperti pada gambar. Data history atau log dari gangguan dan serangan dapat dilihat pada server.

```
05/07-14:36:29.637809  [**] [1:1000001:0] Terdeteksi ada yang melakukan seran
gan SYN FLOOD!!! [**] [Priority: 0] {TCP} 192.168.202.150:1785 -> 192.168.202
.100:80
05/07-14:36:39.002963  [**] [1:1000001:0] Terdeteksi ada yang melakukan seran
gan SYN FLOOD!!! [**] [Priority: 0] {TCP} 192.168.202.150:12753 -> 192.168.20
2.100:80
05/07-14:36:49.000856  [**] [1:1000001:0] Terdeteksi ada yang melakukan seran
gan SYN FLOOD!!! [**] [Priority: 0] {TCP} 192.168.202.150:60917 -> 192.168.20
2.100:80
```

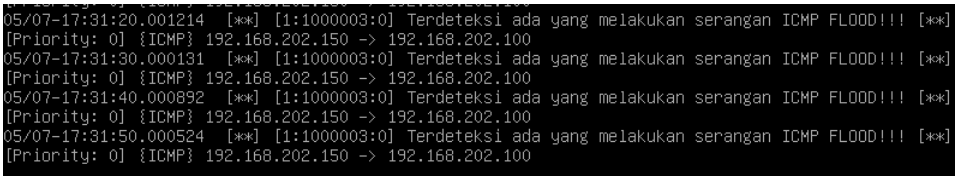
Gambar 3. Server Mendeteksi Serangan SYN Flood

Server mendeteksi serangan dan gangguan berupa serangan SYN Flood dari alamat yang mempunyai IP Address 192.168.202.100 dengan pesan terdeteksi serangan SYN Flood.

```
Commencing packet processing (pid=2195)
05/07-17:02:01.178398  [**] [1:1000002:0] Terdeteksi ada yang melakukan serangan UDP FLOOD!!! [**] [
Priority: 0] {UDP} 192.168.202.150:60413 -> 192.168.202.100:12345
05/07-17:02:11.000209  [**] [1:1000002:0] Terdeteksi ada yang melakukan serangan UDP FLOOD!!! [**] [
Priority: 0] {UDP} 192.168.202.150:1383 -> 192.168.202.100:12345
```

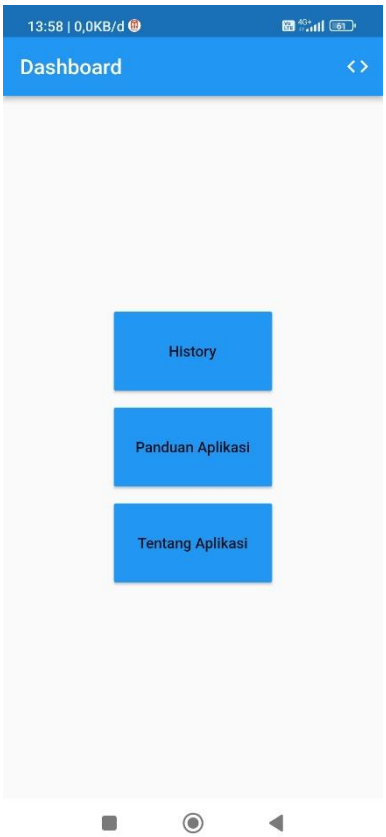
Gambar 4. Server Mendeteksi Serangan UDP Flood

Server dapat mendeteksi serangan dan gangguan berupa serangan UDP Flood dari alamat yang mempunyai IP Address 192.168.202.100 dengan pesan terdeteksi serangan UDP Flood.



Gambar 5. Server Mendeteksi Serangan ICMP Flood

Server dapat mendeteksi serangan dan gangguan berupa serangan ICMP Flood dari alamat yang mempunyai IP Address 192.168.202.100 dengan pesan terdeteksi serangan ICMP Flood.

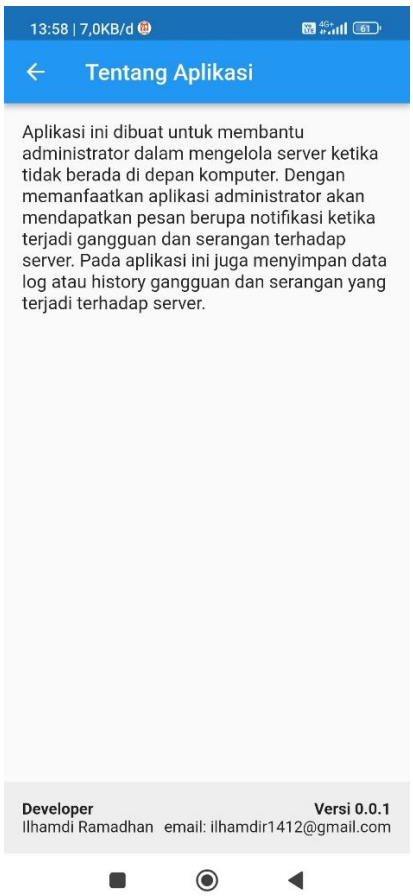


Gambar 6. Halaman Menu Utama

Tampilan ini merupakan halaman menu utama dari aplikasi yang buat. Pada halaman menu utama ini terdapat 3 menu yang terdiri dari menu History, menu Panduan Aplikasi, dan menu Tentang Aplikasi.

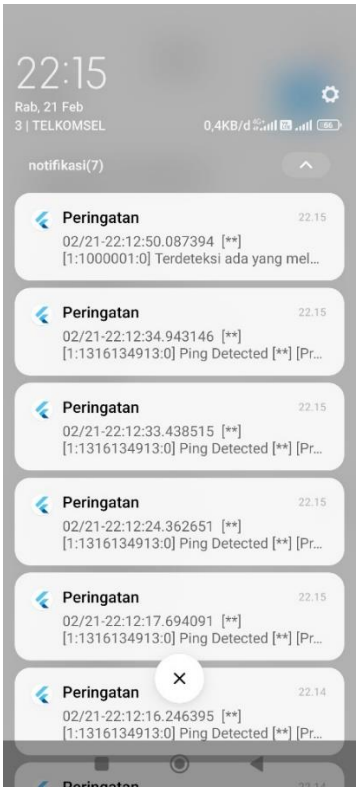
Gambar 7. History Gangguan dan Serangan

Tampilan ini merupakan halaman log atau history serangan yang terjadi terhadap server. Pada halaman ini di tampilkan jenis gangguan dan serangan yang terjadi terhadap server. Pada halaman log ini menampilkan data gangguan dan serangan berupa pesan dari kondisi rules gangguan dan serangan, sumber atau IP Address penyerang, dan waktu terjadi gangguan dan serangan. Data history atau log gangguan dan serangan ini berasal dari data log atau history serangan pada server.



Gambar 8. Tentang Aplikasi

Tampilan ini merupakan tampilan halaman dari menu tentang aplikasi yang menampilkan penjelasan tentang aplikasi yang di kembangkan.



Gambar 9. Notifikasi Serangan dan Gangguan

Tampilan ini merupakan notifikasi yang diberikan ke administrator ketika server mendeteksi gangguan dan serangan berdasarkan kondisi rules yang telah di konfigurasi. Ketika rules gangguan dan serangan terpenuhi server akan mengirimkan pesan gangguan dan serangan ke administrator berupa notifikasi sehingga administrator dapat dengan cepat untuk mengatasi masalah yang terjadi.

Pembahasan

Penitlitan ini menghasilkan aplikasi monitoring server dari gangguan dan serangan dengan metode intrusion detection system berbasis android. Dalam proses perancangan apliaksi, Figma menjadi aplikasi yang digunakan untuk merancangan tampilan menu dan tombol yang digunakan pada aplikasi ini. Dengan memanfaatkan metode intrusion detection system dapat membantu administrator dalam mengelola server. Metode ini dapat memberikan informasi tentang gangguan dan serangan secara real-time sehingga administrator cepat dalam mengetahui masalah yang terjadi. Dengan metode Ini server akan diberikan kondisi atau rules sehingga, ketika kondisi kondisi atau rules terpenuhi maka server akan mengartikan aksi tersebut sebagai gangguan dan serangan. Server akan menyimpan data log atau history serangan yang terjadi.

Aplikasi monitoring server ini akan memberikan administrator pesan ketika terjadi gangguan dan serangan. Server akan mengirim data pesan gangguan dan serangan yang terjadi ke aplikasi dalam bentuk pop-up notifikasi yang berisi pesan gangguan dan serangan yang terjadi. Aplikasi akan menyimpan data log atau history dari gangguan dan serangan yang terjadi pada menu history aplikasi.

Kekurangan dari pengembangan sistem monitoring server ini yaitu ketika terjadinya serangan dan gangguan terhadap server dan administrator sudah mendapatkan pesan dari notifikasi dari server, administrator harus berada didepan komputer untuk menangani masalah yang terjadi karena pada pengembangan sistem ini hanya membantu administrator dalam memantau server. Sistem yang dikembangkan belum bisa untuk mengelola server dari gangguan dan serangan yang terjadi terhadap server sehingga administrator harus segera untuk meremote server dalam penanganan masalah yang terjadi.

Kekurangan lain dari sistem ini yaitu pesan yang masuk berupa notifikasi akan tersimpan di history serangan ketika mengklik notifikasi serangan melalui handphone, jika tidak di klik atau di buka maka history serangan dan gangguan tidak tersimpan pada history gangguan dan serangan pada sistem.

Pengujian

Pada tahap ini akan dilakukan dengan menggunakan metode pengujian black box dengan cara menuliskan skenario pengujian yang di lakukan oleh pengguna sistem yaitu administrator server. Pengujian black box bertujuan untuk memastikan bahwa fungsional sistem yang dikembangkan telah berjalan dengan baik. Berikut hasil pengujian black box yang dilakukan oleh administration server terhadap sistem monitoring server yang dikembangkan:

Tabel 1. Pengujian System

No	Fungsi yang diuji	Cara yang dilakukan	Hasil yang diharapkan	Hasil Pengujian
1	Server Mendeteksi Serangan SYN Flood	Melakukan serangan Syn Flood terhadap server	Server dapat mendeteksi serangan SYN Flood berdasarkan rules yang telah dikonfigurasi	Berhasil dilakukan dapat dilihat pada Gambar 3
2	Server Mendeteksi Serangan UDP Flood	Melakukan Serangan UDP Flood terhadap Server	Server dapat mendeteksi serangan UDP Flood berdasarkan rules yang telah di konfigurasi	Berhasil dilakukan dapat dilihat pada Gambar 4
3	Server Mendeteksi Serangan ICMP Flood	Melakukan serangan ICMP Flood Terhadap Server	Server dapat mendeteksi serangan ICMP Flood berdasarkan rules yang telah di konfigurasi	Berhasil dilakukan dapat dilihat pada Gambar 5
5	Notifikasi aplikasi ketika terjadi	Melakukan serangan terhadap server	Server dapat menentukan serangan yang terjadi terhadap server dan	Berhasil dilkukan dapat dilihat pada

	serangan		memberikan notifikasi ke aplikasi monitoring server	Gambar 9
6	Halaman Log atau History Serangan	Menampilkan Log atau History Serangan	Pada sistem monitoring server dapat menampilkan log atau history serangan yang terjadi terhadap server berupa serangan atau gangguan yang terjadi	Berhasil dilakukan dapat dilihat pada Gambar 7

SIMPULAN

Terciptanya aplikasi monitoring server dari gangguan dan serangan dengan metode intrusion detection system berbasis android dapat digunakan kapanpun dan dimanapun. Aplikasi ini bertujuan untuk mambantu administrator dalam mengelola server dari gangguan dan serangan ketika administrator tidak sedang berada didepan komputer sehingga, administrator dapat dengan segera mengetahui gangguan dan serangan yang terjadi.

DAFTAR PUSTAKA

Cinderatama, T. A., Alhamri, R. Z., & Yunhasnawa, Y. (2022). Implementasi Metode K-Means, Dbscan, Dan Meanshift Untuk Analisis Jenis Ancaman Jaringan Pada Intrusion Detection System. *INOVTEK Polbeng - Seri Informatika*, *7*(1), 169. https://doi.org/10.35314/isi.v7i1.2336

Irvansyah, F., Setiawansyah, S., & Muhaqiqin, M. (2020). Aplikasi Pemesanan Jasa Cukur Rambut Berbasis Android. *Jurnal Ilmiah Infrastruktur Teknologi Informasi*, *1*(1), 26–32. https://doi.org/10.33365/jiiti.v1i1.253

Kustyandi, A., & Noor, S. (2021). *Sistem Informasi Monitoring Serangan Keamanan Mail Pendahuluan Kajian Teori*. *VIII*(2), 42–54.

Rahman, A. M., Seta, H. B., & Astriratma, R. (2020). Perancangan Bot Untuk Monitoring Server Dari Serangan Distributed Denial Of Service Dan Implementasi JSON Web Token Pada Sistem Notifikasi Serangan. *Informatik*, *16*(2), 116–127. https://ejournal.upnvj.ac.id/index.php/informatik/article/view/2008

Supandi, F., Desta P, W., Ambar S, Y., & Sudir, M. (2019). Analisis Resiko Pada Pengembangan Perangkat Lunak Yang Menggunakan Metode Waterfall Dan Prototyping. *Prosiding Seminar Nasional Dinamika Informatika 2018 (SENADI 2018)*, *2*(1), 83–86. http://prosiding.senadi.upy.ac.id/index.php/senadi/article/view/86