Monitoring Keamanan Jaringan Dengan Snort IDS Menggunakan Metode Forensic Jaringan (Studi Kasus: CV.Triem Gunung Mas Sejahtera)

Idrus Ramadhan
Komputerisasi Akuntansi AMIK AL MUSLIM, idrusramadhan73@gmail.com

Abstract

A network and internet server manager (system administrator) has responsibility for system security from time to time, ensuring that the system and network being managed are protected from various threats. The company is one of the places where the use of the internet network is open to its users. CV. Triem Gunung Mas Sejahtera uses a Wireless Local Area Network (WLAN) network as a local network and internet. These uses can be used properly and are not misused. Therefore, a system is needed to deal with network abuse or threats that will occur. The system that only detects this will be implemented using the Intrusion Detection System (IDS) application, namely Snort and Mikrotik, Netcut as a follow-up to the resulting snort alert. Based on attack experiments with computers installed, Snort can find out what is going on which is generated by alerts such as Ping Of Death attacks. After that the ip address can be seen and to follow up can block the ip address and mac address using Mikrotik and Netcut so that it cannot attack again.

Kata Kunci: *Alert, IDS, MikroTik, Snort, Netcut*

Abstrak

Seorang pengelola server jaringan dan internet (system administrator) memiliki tanggung jawab terhadap keamanan sistem dari waktu ke waktu, memastikan bahwa sistem dan jaringan yang dikelola terjaga dari berbagai peluang ancaman. Perusahaan merupakan salah satu tempat dimana penggunaan jaringan internet terbuka terhadap pemakai-pemakainya. CV. Triem Gunung Mas Sejahtera menggunakan jaringan Wireless Local Area Network (WLAN) sebagai jaringan local dan internet. Penggunaan tersebut bisa dipergunakan dengan benar dan tidak pula disalahgunakan pemakaiannya. Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi. Sistem yang hanya mendeteksi ini akan diimplementasikan dengan menggunakan aplikasi Intrusion Detection System (IDS) yaitu Snort dan Mikrotik, Netcut sebagai penindak lanjutnya terhadap alert snort yang dihasilkan. Berdasarkan percobaan serangan dengan komputer yang terpasang snort dapat mengetahui apa yang sedang terjadi yang di hasilkan pada alert seperti serangan Ping Of Death. Setelah itu ip address dapat terlihat dan untuk menindak lanjuti dapat mem-block ip address dan mac address menggunakan Mikrotik dan Netcut sehingga tidak dapat menyerang lagi.

Kata Kunci: *Alert, IDS, Mikrotik, Snort, Netcut*

I. PENDAHULUAN

CV Triem Gunung Mas Sejahtera adalah salah satu produsen solid surface material yang memenuhi kebutuhan solid surface untuk berbagai proyek seperti rumah, kantor, villa, hotel, dll. Penelitian ini dilakukan pada perusahaan CV Triem Gunung Mas Sejahtera dan menemukan permasalahan yang terjadi pada perusahaan tersebut yaitu tidak adanya keamanan jaringan diperusahaan tersebut. Salah satunya adalah serangan terhadap komputer target ini bisa mengakibatkan kerusakan pada komputer seperti server mengalami hang atau melakukan reboot dan ini bisa menghambat pekerjaan pada perusahaan.

Keamanan jaringan merupakan faktor penting untuk menjamin data dari pencurian atau pengrusakan data. Dengan meningkatnya pengetahuan tentang hacking dan cracking serta di dukung banyaknya tool yang bisa digunakan secara mudah untuk melakukan serangan atau penyusupan. Ketika serangan terjadi, maka perlu dilakukan investigasi. Salah satu metode forensic jaringan untuk memonitoring serangan terhadap jaringan menggunakan Snort IDS.

Untuk itu diperlukan monitoring keamanan jaringan untuk mengantisipasi serangan tersebut supaya tidak terjadi pada perusahaan CV Triem

Gunung Mas Sejahtera untuk itu di butuhkan metode forensic jaringan salah satunya adalah snort IDS. Untuk keamanannya menggunakan Netcut dan mikrotik sebagai firewallnya. Perangkat lunak ini memudahkan admin jaringan dalam memanajemen sebuah keamanan jaringan komputer. Berdasarkan uraian diatas, maka penulis melakukan penelitian dengan judul "Monitoring Keamanaan Jaringan Dengan Snort IDS Menggunakan Metode Forensic jaringan".

Tujuan yang akan dicapai dalam penelitian ini adalah: menerapkan snort IDS untuk monitoring keamanan jaringan yang ada di CV Triem Gunung Mas Sejahtera.

II.METODE PENELITIAN

Metode Pengumpulan Data

Adapun teknik pengumpulan data yang penulis gunakan adalah kepustakaan, wawancara, dan observasi.

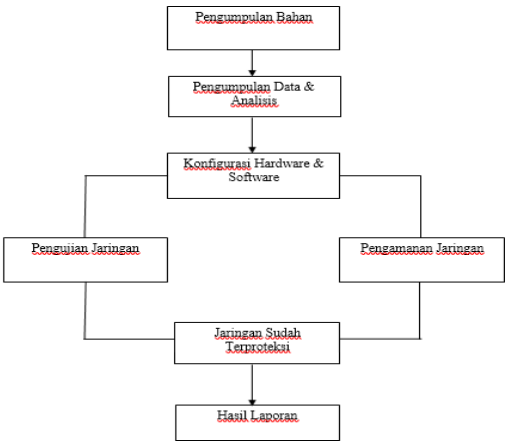
Pada studi literatur ini dilakukan proses pemilihan suatu masalah yang akan digunakan sebagai tugas akhir. Selanjutnya diteruskan dengan pencarian referensi sebagai landasan dan penunjang terhadap pengerjaan sekaligus sebagai pemecahan masalah yang dihadapi. Tahapan terakhir dari studi pustaka ini adalah perumusan dan batasan masalah yang dihadapi menjadi lebih jelas.

Metode ini dilakukan dengan melakukan komunikasi antar dua orang atau lebih untuk memperoleh informasi yang menyangkut perancangan jaringan area local pada CV. Triem Gunung Mas Sejahtera.

Metode ini dilakukan dengan cara mengamati dan mencatat secara sistematik gejala-gejala yang diselidiki di CV. Triem Gunung Mas Sejahtera.

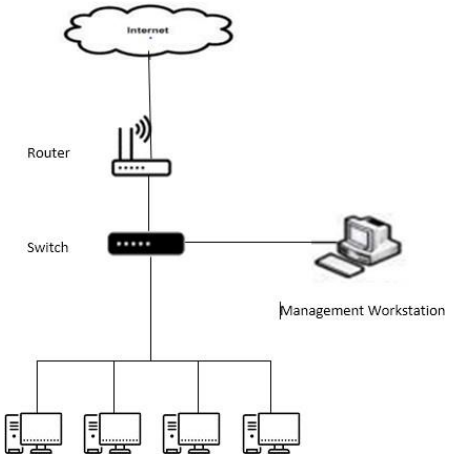
Kerangka Berfikir

Merupakan suatu gambaran akan pembahasan yang akan dipecahkan sehingga mendapatkan suatu solusi. Dimana setiap alur dan tahapan nya dibuat untuk membantu penulis memusatkan pada permasalahan yang diteliti. Adapun kerangka berfikir dalam penulisan ini adalah sebagai berikut:



Gambar 1. Kerangka Berfikir Penelitian

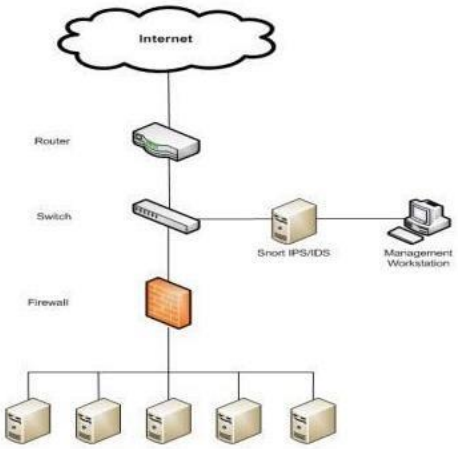
Infrastruktur Jaringan Saat Ini



Gambar 2. Infrastruktur Jaringan CV.Triem Gunung Mas Sejahtera

Keamanan Jaringan Yang Diusulkan

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.



Gambar 3. Arsitektur Jaringan Usulan

III. HASIL DAN PEMBAHASAN

Konfigurasi Rule Snort

Snort menyediakan paket instalasi yang cocok untuk versi Windows.

Selanjutnya sebelum menjalan snort tersebut, maka membutuhkan beberapa langkah lagi yaitu dengan mengkonfigurasikan rules snort agar snort dapat bekerja dengan baik. Rules snort tersebut dapat diperoleh http://www.snort.org/snort

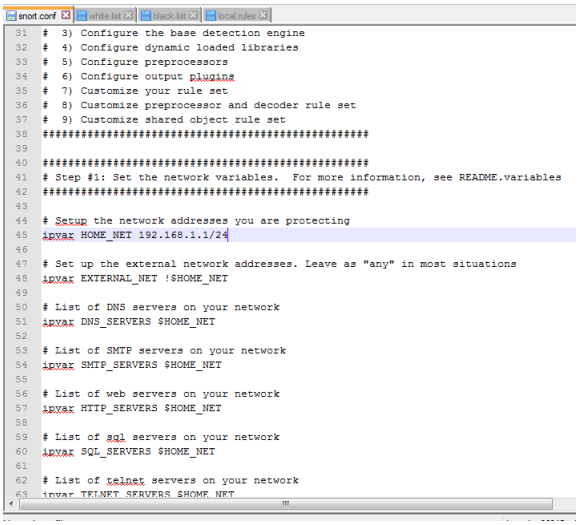
Setelah berhasil men-download rules snort tersebut, langkah selanjutnya meng-ekstrak snort rules ke direktori C:\snort. Proses akan berhasil ditandai dengan adanya beberapa rules berformat .rules pada direktori C:\snort\rules.

Konfigurasi snort

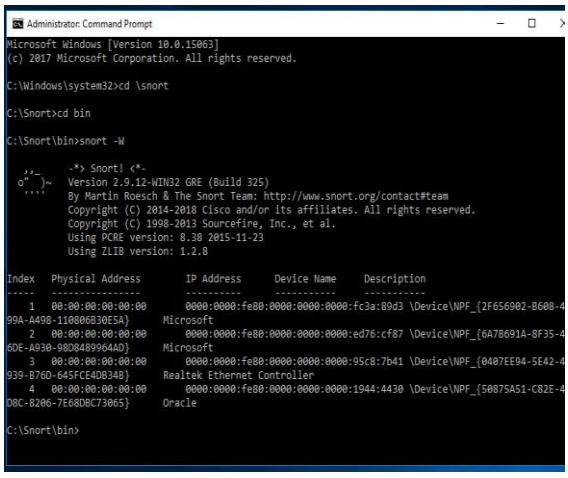
Untuk mengkonfigurasi dengan membuka file snort.conf yang terdapat pada Folder C:\Snort\etc kemudian edit dengan menggunakan text editor, akan tetapi lebih disarankan menggunakan Notepad++.

Menjalankan Snort

Menjalankan snort yaitu dengan menggunakan Command Prompt dalam modus Administrator. Caranya adalah dengan memilih icon Command Prompt, meng- klik kanan dan memilih menu "Run As Administrator". Sebelum itu perhatikan options yang diberikan oleh snort. IDS Snort adalah perangkat lunak IDS yang berbasis open source dan banyak digunakan untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Snort dapat digunakan sebagai alternative untuk mendeteksi paket yang berorientasi serangan dalam keamanan jaringan. Snort secara kerja mirip dengan tcpdump, tetapi lebih fokus sebagai aplikasi sekuriti packet sniffing. Fitur utama snort yang membedakan degan tcpdump adalah payload inspection, dimana memungkinkan snort melakukan analisa payload berdasarkan rule set yang disediakan. Gambar 9 merupakan implementasi Snort yang digunakan pada penelitian ini yaitu menggunakan versi 2.9.12. Sedangkan spesifikasi sistem operasi yang digunakan adalah Windows 7, Win 32.



Gambar 4. konfigurasi snort.conf pada Notepad++



Gambar 5. Versi Snort

Rule snort

Rule yang di set memberikan knowledge pada saat proteksi, sehingga proses investigasi sangat bergantung dari knowledge rule. Terdapat 5 rule yang digunakan pada penelitian ini yaitu: Rule yang di set memberikan knowledge pada saat proteksi, sehingga proses investigasi sangat bergantung dari knowledge rule. Terdapat 3 rule yang digunakan pada penelitian ini yaitu:

```
alert icmp any any -> any any (msg:"Seseorang sedang melakukan ping of death!"; sid:1000001;)
```

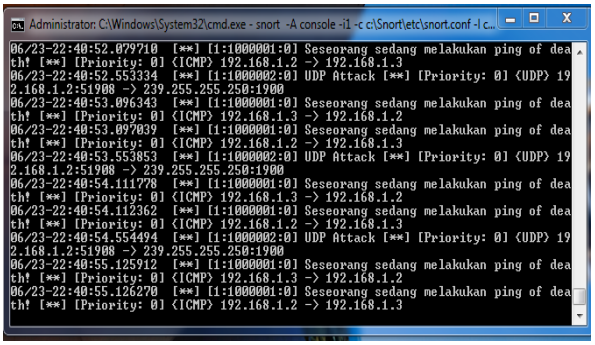
Rule diatas akan membuat Snort melakukan pencatatan untuk semua paket ICMP yang masuk kejaringan. Ketika ada paket yang dicurigai maka akan muncul pesan "Seseorang sedang melakukan ping of death, dengan sid 1000001. Ping of death merupakan jenis serangan pada komputer yang melibatkan pengiriman Ping yang salah atau berbaya ke komputer target. sebuah Ping biasanya berukuran 56 byte (atau 84 bytes ketika header IP dianggap)

```
alert udp any any -> any any (msg:" Testing UDP alert "; sid:1000002;)
```

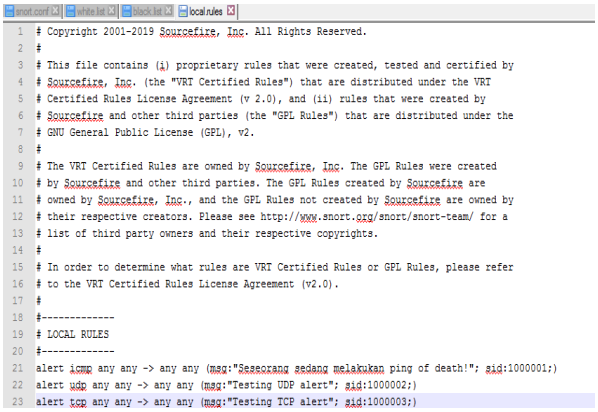
Rule diatas akan membuat Snort melakukan pencatatan untuk semua paket UDP yang masuk kejaringan. Ketika ada paket yang di curigai maka akan muncul pesan "Testing UDP alert", dengan sid 1000002. UDP merupakan kependekan dari User Datagram Protocol merupakan bagian dari internet protocol. Dengan UDP, aplikasi komputer dapat mengirimkan pesan kepada komputer lain dalam jaringan lain tanpa melakukan komunikasi awal.

```
alert tcp any any -> any any (msg:" Testing sid:1000003;)
```

Rule diatas akan membuat Snort melakukan pencatatan untuk semua paket TCP yang masuk ke jaringan. Ketika ada paket yang di curigai maka akan muncul pesan "Testing TCP alert", dengan sid 1000003. TCP merupakan salah satu jenis protokol yang memungkinkan kumpulan komputer untuk berkomunikasi dan bertukar data didalam suatu network (jaringan).

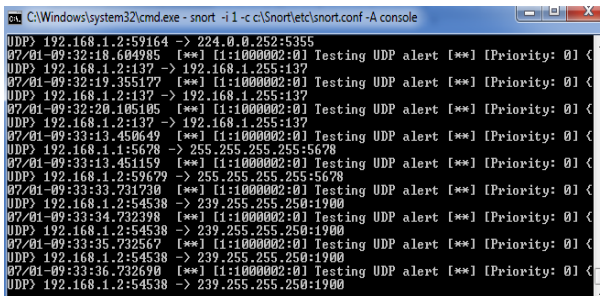


Gambar 8. Serangan Ping of Death



Gambar 6. Rule Snort

Tahapan Pengujian



Gambar 7. Standby Snort

Pada gambar diatas snort sedang melakukan standby dengan perintah:

snort -i 1 -c c:\Snort\etc\snort.conf –A console

Disini snort sedang monitoring jaringan untuk menangkap dan mencatat bila ada serangan.

Komputer yang terpasang Snort akan dicoba dengan metode penyerangan ping of death dari

komputer penyerang. Hasil yang terjadi pada saat komputer diserang adalah sebagai berikut:

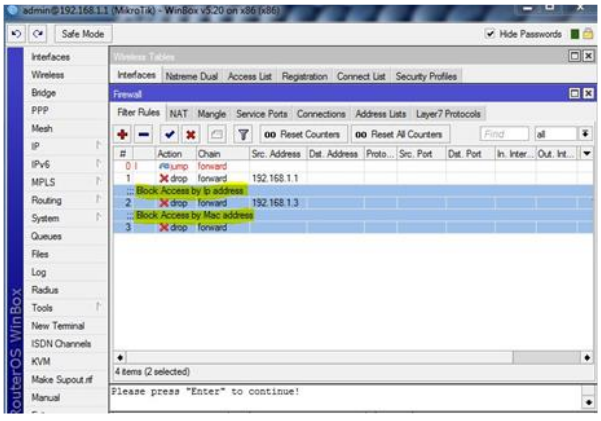
Gambar menunjukkan IP 192.168.1.3 (komputer penyerang) melakukan ping of death terhadap IP 192.168.1.2 (komputer yang terpasang snort) dengan peringatan "Seseorang sedang melakukan ping of death".

Keamanan

Setelah melakukan proses monitoring di komputer yang sudah terpasang snort maka ip penyerang dapat terlihat dan serangan jenis apa yang menyerang komputer tersebut. Terlihat pada gambar 13 ip si penyerang yaitu 192.168.1.3 dengan jenis serangan ping of death.

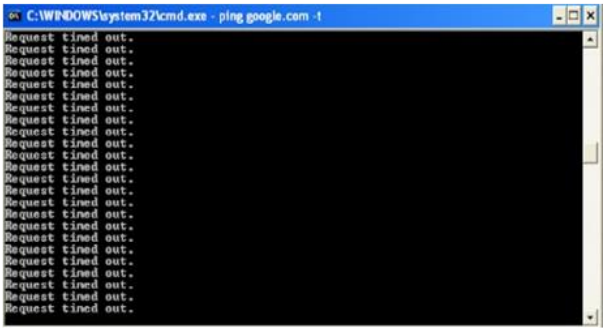
Untuk mengatasi hal tersebut mengamankannya menggunakan Mikrotik untuk manajemen firewallnya. Mikrotik merupakan sistem operasi jaringan komputer yang memungkinkan untuk dapat digunakan sebagai router dalam jaringan. Mikrotik memiliki beberapa fitur yang sangat memudahkan admin jaringan dalam memanajemen sebuah jaringan komputer seperti Firewall dan NAT, Routing, Hospot, Web Proxy, DHCP dan masih banyak lagi.

Disini penulis kali ini menggunakan mikrotik untuk block ip address dan Mac address. jadi nantinya client atau peyerang komputer server yang di blok ip address dan mac address akan tidak bisa mengakses jaringan local dan internet.



Gambar 9. drop IP address dan MAC address

Pada gambar diastas, Setelah melakukan proses monitoring menggunakan snort penulis bisa mengisi ip dan mac address yang akan di block, ip yang akan diblock yaitu 192.168.1.3 ip penyerang, dan terlihat pada gambar diatas ip address dan mac address sudah terblock.

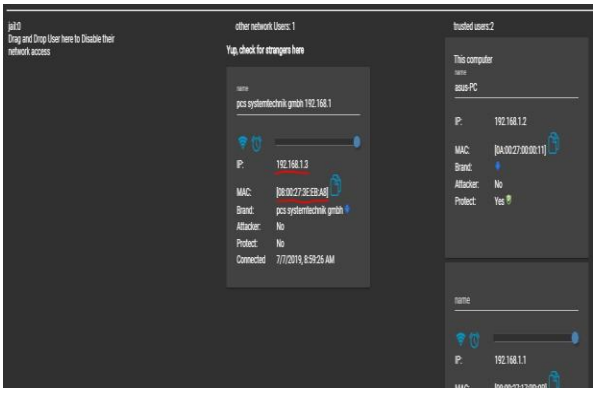


Gambar 9. Hasil Output

Pada gambar diatas merupakan hasil ouput dari block ip dan macc address. Terlihat pada gambar tersebut komputer si penyerang tidak bisa melakukan akses internet lagi karena sudah terblock menggunakan mikrotik.

Netcut merupakan perangkat lunak manajemen jaringan. Menggunakan program ini seorang administrator jaringan dapat memanfaatkan daftar tabel IP-MAC untuk mengelola jaringan dan memproteksinya dari kejahilan ARP (Address Resolution Protocol) dan bentuk lain dari serangan dan pengacauan. kemudian administrator untuk menghidupkan dan mematikan jaringan pada perangkat apa saja yang tersambung dengannya, termasuk pemindah/switcher, router, desktop, laptop.

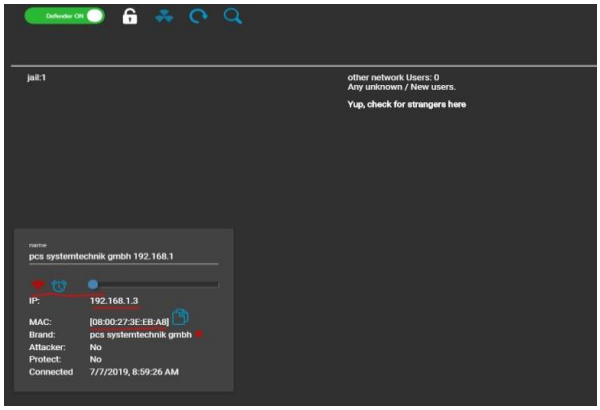
Aplikasi netcut digunakan untuk melihat pengguna yang terhubung pada jaringan Wireless Local Area Network (WLAN), selanjutnya.



Gambar 10. Scanning dengan Netcut

Setelah proses scanning dilakukan dengan menggunakan Netcut, maka penulis akan mengetahui

ip address dan mac address penyerang yaitu ip addres 192.168.1.3 dengan mac address [08:00:27:3E:EB:A8], dari hasil monitoting sebelumnya menggunakan snort yang terhubung dengan jaringan WLAN yang meyerang komputer server tersebut, setelah itu penulis bisa memutuskan koneksi jaringan dengan cara drag and drop data



Gambar 11. Proses off jaringan dengan Netcut

device tersebut ke kolom jail. Berikut ini adalah salah satu simulasi jaringan yang dibuat terputus koneksi WLAN.

Terlihat IP computer si penyerang yaitu 192.168.1.3 sudah di off jaringannya maka user terebut tidak dapat melakukan serangan lagi terhadap komputer server.

IV. KESIMPULAN

Berdasarkan dari hasil instalasi dan konfigurasi snort menunjukkan snort bisa berjalan dengan baik di Windows. Telah berhasil konfigurasi snort ids dalam jaringan wlan pada CV. Triem Gunung Mas Sejahtera dan untuk keamanannya menggunakan 2 keamanan yaitu mikrotik sebagai firewallnya dan menggunakan Netcut untuk memutuskan koneksi internetnya, sehingga jaringan keamanan komputer server aman, karena snort mampu mendeteksi jenis serangan berdasarkan bagian rule dari snort.

V.REFERENSI

Dewi Kusuma Ervi, Dwi Harini &Nisa Miftachurohmah., 2017. Snort IDS Sebagai Tools Forensik Jaringan Universitas Nusantara PGRI Keder.Kediri: Universitas Nusantara PGRI Kediri

Dewi Kusuma Ervin, Patmi Kasih., 2017. Analisis Log Snort Menggunakan *Network Forensic*

Gobel. Dkk. (2014). "Analisa dan Pengembangan Sistem Peringatan Keamanan JaringanKomputer Menggunakan SMS Gateway dan Paket Filter." Pengembangan Terhadap Sistem Keamanan. Vol.1. No.(2). 382-388

Gufron, R. (2013). Mengenal Aplikasi Virtualisasi Oracle VM VirtualBox. [Online]. Tersedia: http://dosen.gufron.com/artikel/mengenal-aplikasi-virtualisasi-oracle-vm-virtualbo/10/ [24 Februari 2018].

Hermawan, R. (2011). "Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denialof Service (DDOS)." Analisis Konsep dan Cara Kerja Serangan. Vol.5 No.(1). 1-14

Mentang Randi, Alicia A. E. Sinsuw, ST., MT., Xaverius B. N. Najoan, ST., MT.,2015.Perancangan Dan Analisis Jaringan Nirkabel Menggunakan *Wireless Intrusion Detection System*.Manado

Rafiudin Rahmat., 2010. Mengganyang Hacker Dengan SNORT

Riadi, I. (2011). "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik." Optimalisasi Keamanan Jaringan. Vol.1 No.(1). 1-5

Sutarti, Adi Putranto Pancaro, Fembi Isnanto Saputra., 2018. Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal: Universitas Serang Raya

Santoso. dkk. (2011). "Manajemen Keamanan Jaringan Informasi Menggunakan IDS/IPS Strataguard Studi Kasus STIMK Amikom Yogyakarta." Manajemen Keamanan Jaringan dengan Berbagai Metode. Vol.12 No.(1). 9-22

Sumardi. dan Triyono, R. A. (2012). "Rancang Bangun Sistem Keamanan Jaringan dengan Metode Blocking Port pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali."Meningkatkan Performance Jaringan Internet. Vol.2 No.(1). 16- 21

Yusuf, F. (2017). Mengenal Berbagai Jenis Serangan pada Jaringan Komputer.