Journal of SAKIRA (*Secure And Knowledge-Intelligent Research in Cybersecurity And Multimedia*) e-ISSN 3046-773X

Vol.1, No.2, December 2023, pp. 52~56

Data Security Analysis Using Virtual Ridgeback in Network Forensics

Firmansyah[1], Yusuf Hendra Pratama[2], Bayu Wibisana[3], Hendri Purnomo[4]
Ilmu Komputer, Universitas Islam Al-Azhar

f.firman@unizar.ac.id

Article Info

Article history:

Received November 6, 2023
Revised November 10, 2023
Accepted November 17, 2023

Keyword:

security, defense, ridgeback, virtual, network forensics.

ABSTRACT

Recorded two hospitals in Jakarta were hit by cyberattacks which caused patient data in hospital computer networks to be inaccessible. Symantec is an American company that manufactures data security software, according to Symantec's report entitled Internet Security Threat Report Volume 24 which was released in February 2019 then, in 2018, as much as 2.23%, cyberattacks in the global arena occur in Indonesia, increasing from the previous year, namely 1.67%. Meanwhile, the figure also places Indonesia in fifth place as the country that has the most cyber threats in 2018. It can operate on physical networks or on virtual networks. The only requirement is that the Ridgeback installation has access to the layer 2 network layer. Ridgeback Network Defence makes resistance to intruders using interactive defences and causes intruders to spend unnecessary resources. Interactive Defence is an advanced disguise and fraud capability designed to ensnare intruders in several ways, namely by managing billions of feeds in the network that can trigger intruder responses, affect intruder behavior so that they are easier to detect, and block access to protected network services without revealing that service has been blocked. This research is expected to create a control center by adopting a Software Defined Network (SDN) so that it can capture intruders and get data about the attack, which can be used as evidence in the process of investigating network forensics quickly and precisely.

I. PENDAHULUAN

Pada taggal 7 November 2016, Indonesia telah menetapkan aturan mengenai perlindungan data pribadi, dituangkan dalam bentuk Peraturan Menteri (Permen) No 20, diundangkan dan berlaku sejak 1 desember 2016. Data pribadi wajib diberikan apabila adanya keperluan, atas permintaan dari aparat penegak hukum. Pada tahun 2017, tercatat dua rumah sakit di Jakarta terkena serangan cyber yang menyebabkan data pasien dalam jaringan komputer rumah sakit tidak bisa diakses. Symantec adalah perusahaan asal Amerika yang memproduksi perangkat lunak pengamanan data, menurut laporan Symantec berjudul Internet Security Threat Report Volume 24 yang dirilis pada Februari 2019 lalu, pada tahun 2018, sebanyak 2,23%, serangan siber di ranah global terjadi di Indonesia, meningkat dari tahun sebelumnya, yakni 1,67%. Adapun, angka tersebut juga menempatkan Indonesia diposisi kelima sebagai negara yang paling banyak mendapatkan ancaman siber pada tahun 2018 untuk kawasan Asia Pasifik. Ilmu pengetahuan tentang keamanan komputer yang terkait dengan penyelidikan untuk menentukan sumber serangan jaringan berdasarkan data log bukti, identifikasi, analisis, dan rekonstruksi kejadian adalah Forensik Jaringan yang merupakan cabang dari Forensik Digital (A, Fadlil, dkk, 2017). Metode paling mudah untuk mengatasi serangan jaringan adalah dengan cara memutuskan jaringan untuk sementara waktu atau dengan cara menggunakan 2 atau lebih IP address untuk digunakan bergantian ketika jaringan yang kita akses mendapat serangan. (A, Fadlil, dkk, 2018). Saat ini sudah banyak sekali perusahaan yang mempunyai banyak

e-ISSN 3046-773X

cabang menggunakan jasa internet dengan teknologi yang ditawarkan oleh provider internet dengan jenis dan harga yang bervariasi untuk memenuhi kebutuhan komunikasi perusahaan. Namun, masih banyak yang menggunakan dial-up privat dari cabang ke pusat. Sistem ini lebih mengeluarkan biaya yang besar setiap koneksinya (Albert, S, 2015).

Perkembangan teknologi digital saat ini sangat pesat, diantaranya adalah mengenai teknologi virtualisasi. Teknologi virtual memungkinkan kita untuk membuat suatu model perangkat lunak yang sesuai dengan perangkat keras yang diinginkan. Ridgeback dapat beroperasi di jaringan fisik atau di jaringan virtual. Satu-satunya persyaratan adalah bahwa instalasi Ridgeback memiliki akses ke lapisan jaringan layer 2. Produk keamanan jaringan, pada saat ini berupaya untuk mengklasifikasikan aktivitas pada jaringan sebagai penyusup atau bukan penyusup, tetapi pendekatannya kurang optimal karena penyusup mahir dalam menghindari skema ini. Alat keamanan dan professional, menghabiskan sumber daya yang besar untuk mencoba memantau dan mengevaluasi status keamanan setiap sumber daya terakhir pada jaringan, sementara itu tidak melakukan apapun untuk mempengaruhi perilaku penyusup. Dengan produk keamanan yang lama, pertahanan jauh lebih mudah dari pada untuk menyerang. Ridgeback adalah plarform keamanan untuk menyuntik, memodifikasi, dan menjatuhkan frame Ethernet, sesuai kebutuhan, dengan tujuan memengaruhi perilaku penyusup. Ridgeback dapat beroperasi di jaringan fisik atau di jaringan virtual. Satu-satunya persyaratan adalah bahwa instalasi Ridgeback memiliki akses ke lapisan jaringan layer 2. Ridgeback Network Defense melakukan perlawanan ke penyusup menggunakan pertahanan interaktif dan menyebabkan penyusup menghabiskan sumber daya yang tidak perlu. Pertahanan Interaktif adalah kemampuan penyamaran dan penipuan canggih yang dirancang untuk menjerat penyusup dalam beberapa cara yaitu dengan mengelola miliaran umpan dalam jaringan yang dapat memicu respon penyusup, mempengaruhi perilaku penyusup sehingga mereka lebih mudah untuk dideteksi, serta memblokir akses ke layanan jaringan yang dilindungi tanpa mengungkapkan bahwa layanan telah diblokir. Pertahanan Interaktif secara dinamis mengubah apa yang diamati oleh para penyusup, menyamarkan postur keamanan jaringan dan menciptakan keadaan untuk menangkap penyusup.

Penelitian ini diharapkan dapat terciptannya pusat kendali dengan mengadopsi sistem Software Defined Network (SDN). Membangun Sistem otomatis gangguan pada jaringan yang secara langsung menolak aktifitas pencurian data melalui pendekatan pertahanan interaktif, apabila terjadi serangan dari pihak yang tidak bertanggung jawab sehingga dapat menangkap penyusup dan mendapatkan data mengenai serangan tersebut, yang bisa dijadikan bukti dalam proses investigasi pada forensik jaringan secara cepat dan tepat. Virtualisasi dan cloud computing telah menjadi tren teknologi informasi khususnya untuk perusahaan skala enterprise. MetaROUTER merupakan implementasi virtualisasi pada RouterOS v3.21 keatas yang berjalan pada RouterBoard dengan platform MIPS-BE. Penelitian sebelumnya telah membuktikan bahwa antar virtual router tidak saling berhubungan dan memiliki fungsi yang berbeda (Asmunin, dkk, 2016). Forensik jaringan memforkuskan pada data yang diperoleh. Tools yang bisa dimanfaatkan untuk Forensik Jaringan adalah Snort. Snort bekerja dengan beberapa bagian yang bertugas melakukan proses tertentu, antari lain paket capture block, decoder block, dan preprosesor block. Rule snort di buat terlebih dahulu sehingga ketika terjadi serangan yang sama dengan rule, maka akan muncul alert, dan serangan tersimpan di log database. Log yang tersimpan di database berfungsi sebagai alat bukti pelaporan (E, K, Dewi, dkk, 2017). Alert adalah User Interface yang bertujuan untuk menyampaikan pemberitahuan kepada user dalam selang waktu tertentu sebelum diproses tampilan berikutnya. Alert dapat terdiri dari text string (untaian kata) dan image (gambar). Visualisasi dari alert dapat diatur berdasarkan tipe dari pemberitahuannya. Kecenderungan penggunaan. Alert adalah pemberitahuan user tentang suatu kesalahan (errors) dan kondisi lain yang tidak biasa (Fadhila, dkk, 2012). Target utama attacker sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja router. Hal ini dapat merugikan perusahaan jasa jaringan yang bekerja sama dengan perusahaan seperti perusahaan jasa keuangan, bank, sekolah, universitas, warung internet, ataupun perusahaan e–commerce yang mengakibatkan transaksi berhenti. Bagi intruder, router sangat berperan penting untuk melancarkan aksi serangannya agar dapat masuk kedalam sistem utama atau pusat data yang diinginkan untuk melakukan tindak kejahatan. Pengendalian penuh pada router menyebabkan jaringan lain yang terhubung pada router juga dapat dikendalikan Penelitian sebelumnya memanfaatkan Intrusion Detection System sebagai sistem monitoring untuk mendeteksi serangan distributed denial of service (DDoS) secara real time (Faizin, dkk, 2016). Penelitian mengenai Virtualisasi sebelumnya dilakukan oleh (Galang, dkk, 2017) yang mengimplementasikan teknik virtualisasi router menggunakan MetaRouter. Virtualisasi router dibangun menggunakan metode Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle. Virtualisasi router menggunakan MetaRouter dapat menghemat biaya pembuatan jaringan komputer, pemakaian energi listrik dan penggunaan tempat dibandingkan router non-virtualisasi. Metarouter Memungkinkan terjadinya kemanan data dan pengambilan log data yang dilakukan dalam satu panel Routerboard walaupun terdapat beberapa client. Untuk menanggulangi terjadinya kerusakan data dan serangan yang tidak diinginkam maka melakukan proteksi terhadap serangan atau alur data yang tidak wajar salah satunya dengan melakukan pembatasan akses (Kristono, dkk, 2018). Penelitian terhadap bukti tindak kriminal, telah dilakukan oleh (Mandowen, dkk, 2016), yang menganalisis dan melaporkan konten file yang diambil pada jaringan (nitroba.pcap.zip), yang merupakan arsip yang berisi kegiatan

e-ISSN 3046-773X

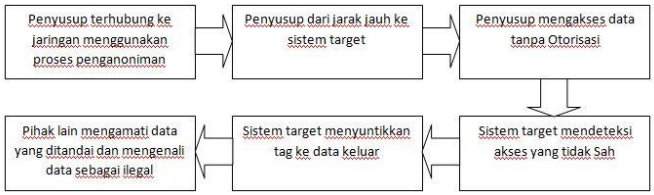
berbasis jaringan yang dipantau dan dicatat dalam jaringan Universitas Nitroba menggunakan alat forensik jaringan yang disebut Wireshark. File tangkapan jaringan yang diunduh berisi aktivitas yang dapat melanggar hukum cyber. Penelitian selanjutnya dilakukan oleh (I. Riadi. 2011), yang menganalisis proses untuk menentukan alur lalu lintas yang melewati proses pemfilteran menggunakan firewall, desain untuk mendapatkan cara yang paling efektif dan efisien mengimplementasikan router, implementasi serta pengujian yang dilakukan dengan metode stress test. Berdasarkan penelitian yang telah dilakukan aplikasi router menggunakan MikroTik yang di hasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna.

II. METODE

Metodologi yang digunakan dalam penelitian ini telah diungkapkan pada pendahuluan yaitu menggunakan metode pertahanan interaktif. Ridgeback dapat beroperasi di jaringan fisik atau di jaringan virtual. Satu-satunya persyaratan adalah bahwa instalasi Ridgeback memiliki akses ke lapisan jaringan layer 2. *Pertahanan Interaktif* adalah kemampuan penyamaran dan penipuan canggih yang dirancang untuk menjerat penyusup dalam beberapa cara yaitu dengan mengelola miliaran umpan dalam jaringan yang dapat memicu respon penyusup, mempengaruhi perilaku penyusup sehingga mereka lebih mudah untuk dideteksi, serta memblokir akses ke layanan jaringan yang dilindungi tanpa mengungkapkan bahwa layanan telah diblokir. Pertahanan Interaktif secara dinamis mengubah apa yang diamati oleh para penyusup, menyamarkan postur keamanan jaringan dan menciptakan keadaan untuk menangkap penyusup. Dalam melakukan penelitian ini diperlukan 3 tahapan yaitu:

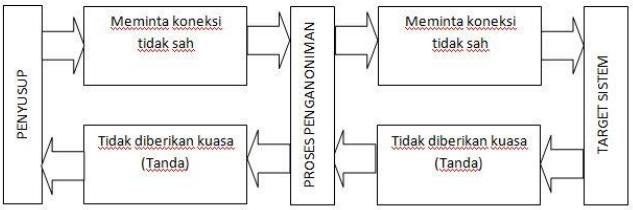
1. Deceive (Meperdaya).
   Mengelola miliaran umpan di jaringan yang akan segera dapat memicu respons Ridgeback terhadap keberadaan penyusup.
2. Influence (Pengaruh).
   Mempengaruhi perilaku penyusup sehingga mereka lebih mudah untuk dideteksi.
3. Eliminate (Menolak).
   Memblokir akses ke layanan jaringan yang dilindungi tanpa mengungkapkan bahwa layanan telah diblokir.

Gambar 1 menunjukkan contoh diagram jaringan yang digunakan untuk menggambarkan berbagai perwujudan yang diungkapkan. Penyusup dapat terhubung ke jaringan menggunakan proses penganoniman, misalnya, Tor, Freenet, atau sistem proxy lainnya. Proses penganoniman dapat memberikan serangkaian sistem informasi komputer antara kriminal dan sistem target potensial, dan dapat beroperasi untuk menyembunyikan lokasi atau identitas penyusup dari sistem target. Penyusup kemudian dapat terhubung, tanpa otorisasi, dari jarak jauh ke sistem target, Misalnya, server, PC, Tablet, atau sistem lain yang terhubung ke jaringan kabel atau nirkabel, melalui proses penganoniman. Sebagai hasil dari koneksi yang tidak sah itu, penyusup kemudian dapat secara tidak sah mengakses data pada sistem jarak jauh. Untuk melacak penyusup agar bisa ditangkap, sistem target memiliki perangkat lunak atau sistem yang diinstal untuk mendeteksi akses penyusup dari sistem jarak jauh. Pengaturan instruksi ini dapat dilakukan dengan berbagai metode, termasuk, misalnya klasifikasi jaringan, atau perangkat lunak pendeteksi intrusi lainnya. Menggunakan deteksi intrusi sistem, target yang terafiliasi dengan sistem jarak jauh mendeteksi akses data yang tidak sah. Setelah mendeteksi akses tidak sah, sistem target dapat memasukkan tanda atau tanda tangan ke semua lalu lintas jaringan yang dimaksudkan untuk kembali ke penyusup, seperti yang dijelaskan secara lebih rinci di bawah ini. Tanda atau tanda tangan dapat ditempatkan di satu atau lebih bagian dari paket jaringan, misalnya, segmen tcp, paket IPv4, atau paket IPv6. Lalu lintas jaringan yang ditandai dapat diperiksa oleh pembawa jaringan swasta atau publik, atau penegakan hukum di setiap titik di sepanjang jaringan, termasuk pada titik di luar perlindungan proses anonim penyusup atau layanan proxy, untuk mendeteksi lokasi dan identitas jaringan kriminal yang sebenarnya. Inspeksi data yang ditandai memungkinkan pihak swasta atau publik untuk mengamati data yang ditandai, mengenali data sebagai ilegal, dan kemudian mengambil tindakan yang sesuai. Selain penggunaan yang dijelaskan ini, sistem dan metode ini dapat digunakan untuk tujuan lain, misalnya, untuk mengaktifkan sistem perantara agar dapat mengidentifikasi setiap pengguna yang mengakses sistem informasi komputer untuk tujuan apa pun.



Gambar 1. Model Proses Penyusup

Gambar 2 adalah diagram alir contoh yang menggambarkan suatu proses untuk menghasilkan informasi. Penyusup akan melalui jalur yang sama dari tahapan meminta koneksi, namun penyusup tidak menyadari bahwa jalur yang digunakan akan kembali pada tahapan meminta koneksi kembali.



Gambar 2. Proses Sumber Daya Penyusup

.

III. HASIL DAN PEMBAHASAN

Berdasarkan peneltian yang telah dilakukan pada pendahuluan maka dapat disimpulkan belum ada penelitian tentang analisis keamanan data dengan metode pertahanan interaktif menggunakan virtual ridgeback pada forensik jaringan. Pada gambar 3, peneliti merancang arsitektur alat keamanan ridgeback yang menyertakan fungsi-fungsi dari alat tambahan untuk menunjang keberhasilan

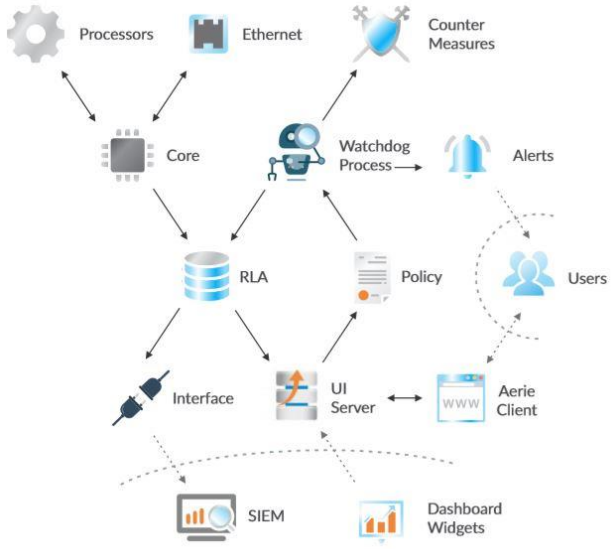
e-ISSN 3046-773X

sistem. Perbedaan yang sangat terlihat pada penelitian yang lain adalah sistem ini menggunakan platform pertahanan interaktif untuk keamanan jaringan dan manajemen jaringan yang disebut ridgeback hunter. Ridgeback Hunter dapat dikembangkan dengan plugins dan widget komersial, custom, atau open source.

Tabel 1. Database Ridgeback Hunter

Tabel	Deskripsi
Failure	Mencatat semua kegagalan upgrade sistem
History	Mencatat sejarah penggunaan sistem dengan basis data dan tanggal
Log	Mencakup informasi keamanan

Untuk dapat mengakses database dapat menggunakan perintah "sqlite3 /var/opt/ridgeback.db".



Gambar 3. Arsitektur Ridgeback (www.ridgebacknet.com/download-ridgeback-white-paper/)

- Core - Inti dari sistem Ridgeback, yang memproses data jaringan. Core dapat menyisipkan dan memodifikasi.
- RLA - Ridgeback Log Adapter, digunakan untuk mengadaptasi output Ridgeback ke sistem lain.
- DB - Ridgeback Hunter mempertahankan status yang mudah diakses dalam basis data Sqlite yang nyaman.
- Kebijakan - Kebijakan keamanan disimpan dalam file JSON standar.
- Watchdog - Memantau status sistem dan memulai peringatan atau tindakan balasan saat diperlukan.
- Peringatan - Dikirim ke pengguna.
- Penanggulangan - Akan diambil untuk menghilangkan ancaman dari jaringan.
- UI Server - Menyediakan antarmuka manajemen HTTPS ke instalasi Ridgeback.

Aerie Client - Antarmuka berbasis web untuk mengelola instalasi Ridgeback.

IV. KESIMPULAN

Berdasarkan penelitian terdahulu yang telah dipaparkan, maka penelitian akan dilaksanakan dengan metode pendekatan baru yaitu pertahanan interaktif dengan menggunakan alat keamanan ridgeback. Harapan dari penelitian ini yaitu merekomendasikan alat atau perangkat lunak keamanan yang lebih baik kepada pengelola jaringan. Memanfaatkan perangkat lunak ridgeback akan secara otomatis menolak kekuasaan penyusup, memadamkan ancaman secara real time dan keamanan data akan lebih mudah untuk dijaga. Penyusup akan dibuat kebingungan dengan memberikan jalur yang sama selama mereka terus mencoba masuk dalam pertahan, setelah penyusup mulai kehabisan daya, sistem akan secara langsung mendeteksi penyusup dengan mencatat alamat mac perangkat. Sama seperti dalam olahraga atau perang jika semua yang dilakukan adalah bermain pertahanan, pada akhirnya akan kalah dan pasti tidak akan menang. Ridgeback adalah pendekatan baru, berbeda dan efektif yang menggunakan strategi militer di dunia maya. Hanya terdiam ataukah melawan?

UCAPAN TERIMA KASIH

Terima kasih atas dedikasi dan kerja keras teman-teman dalam menyelesaikan penelitian ini. Prestasi Anda sungguh luar biasa! Semoga hasil penelitian ini bermanfaat bagi banyak orang. Selamat dan sukses selalu!

DAFTAR PUSTAKA

[1] A, Fadlil., I, Riadi., & S, Aji. (2017). Pengembangan Sistem Pengamanan Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. Volume 3(1), 11-19.

[2] A, Fadlil, Imam Riadi, Sukma Aji. (2018). Pengaman Jaringan Menggunakan Sistem Berbasis Mikrokontroler Berdasarkan Analisis Forensik Jaringan, Palembang, 28-29 Mei 2016, ISBN: 978-602-19568-1-6.

[3] Albert, S., & Juni, E. (2015). Analisa Sistem Pengaman Data Jaringan Berbasis VPN. Stmik Ikmi, 10(18), 220. Retrieved from www.ikmi.ac.id

[4] Asmunin, Aditya Hermawan (2016). Penerapan dan Analisis Virtualisasi Router Menggunakan RouterOS, Jurnal MULTINETICS, Universitas Indonesia Jakarta, Vol.2 No.1 (2016) : 31-34.

[5] E, K, Dewi., Dwi, H., Nisa, M. (2017). Snort Ids Sebagai Tools Forensik Jaringan Universitas Nusantara Pgri Kediri, Kediri, 22 Februari 2017, e-ISSN : 2549-7952.

[6] Fadhila N.,T, Muhammad I.,P.,N, (2012). Implementasi Pemrograman Java Untuk Alert Intrusion Detection System, pematang siantar, 31 agustus – 2 september 2012, ISBN 978602-18749-0-5.

[7] Faizin Ridho, Anton Yudhana, Imam Riadi. (2016). Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time, Yogyakarta, 6 Desember 2016, Vol 2 No. 1, ISBN : 979-587-626-0.

[8] Galang, C. M., Eko, S., & Imam, A. (2017). Teknik Virtualisasi Router Menggunakan Metarouter Mikrotik (Studi Kasus: Laboratorium Jaringan Komputer Politeknik Negeri Lampung), 2641–2644. https://doi.org/10.1111/ijlh.12426

[9] I, Riadi. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori. JUSI, Universitas Ahmad Dahlan Yogyakarta, 1(1), 71–80.

[10] I,.Riadi. (2012). Log Analysis Techniques using Clustering in Network Forensics, International Journal of Computer Science and Information Security (IJCSIS) , Vol. 10, No.7.

[11] I Riadi, R Umar, FD Aini.,(2019)Analisis Perbandingan Detection Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector

e-ISSN 3046-773X

Machine (Svm). ILKOM, Universitas Ahmad Dahlan Yogyakarta, Vol 11(1), 17-24.

[12] Kristono., & Riadi, I. 2018. Simulation For Data Security Improvement In Exploited Metarouter. International Journal of Computer Science and Information Security. Vol 16(5): 6-15.

[13] Mandowen, S.A.,(2016). Wireshark dan NetworkMiner dalam investigasi mengekstrak dan menganalisa paket file yang direkam pada jaringan dan mendapatkan bukti. Universitas Cenderawasih, Jayapura, Vol 16(1), 14-20.

[14] R Umar, A Yudhana, MN Faiz. (2016). Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. ILKOM, Universitas Ahmad Dahlan Yogyakarta, Vol 8(3), 242-247.

[15] R Umar, A Yudhana, MN Faiz. (2017). Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. Jiska, Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, 1 (3), 108-114.

[16] Sahid Aris Budiman., Catur Iswahyudi., Muhammad Sholeh. (2014). Implementasi Intrusion Detection System (Ids) Menggunakan Jejaring Sosial Sebagai Media Notifikas. Yogyakarta, 15 November 2014. ISSN: 1979-911X.

[17] www.ridgebacknet.com/download-ridgeback-white-paper/

[18] Yudi Prayudi, Dedy Setyo Afrianto. (2007). Antisipasi Cybercrime Menggunakan Teknik Komputer Forensik, Yogyakarta, 16 Juni 2007, ISSN: 1907-5022..