p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PENINGKATAN KEAMANAN PADA *SIMPLE NETWORK TIME PROTOCOL(SNTP)* UNTUK MENDITEKSI *CYBER CRIME* DI DALAM AKTIFITAS JARINGAN

Kotim Subandi[1]*, Victor Ilyas Sugara[2] , Adriana Sari Aryani[3]
Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Pakuan ,Jl. Pakuan, RT.02/RW.06, Tegallega, Kecamatan Bogor Tengah, Kota Bogor, Jawa Barat 16129
**Corresponding Author* : kotim.subandi@unpak.ac.id

Abstrak.

Di era sekarang ini teknologi informasi dan komputasi telah berkembang pesat sehingga kejahatan dunia maya meningkat secara drastis karena pandemi, penjahat dunia maya kini juga menargetkan orang, bukan hanya sistem. Modus kejahatan di dunia maya saat ini sangat beragam. Cara yang digunakan oleh penyerang semakin beragam dan kompleks. Dengan mengimplementasi antivirus *client server* bertujuan melakukan scan di setiap client yang sudah terhubung jaringan *local* secara *real time* maupun terpusat juga mengupdate secara terpusat pula, serta mendeteksi jenis serangan yang sering terdapat system jaringan serta medeteksi jenis serangan yang sering terdapat system jaringan dan meberikan proteksi seluruh komputer client dari segala serangan (*malware, virus, worm, Trojan*) yang terdapat pada jaringan.Sebagai upaya meningkatan keamanan dijaringan perusahaan dan mermerikan kenyaman disaat melaukan aktivitas komunikasi di jaringan *Internet*, peneliti melakukan *migrasi software sophos* ke *trend Micro.* Hasil log dari scanning antivirus dengan menggunakan *Trend Micro, Risk Level High, action* yang harus dilakukan segera *Blocked*

Kata kunci: keamanan, network,protocol,cyber crime

Abstract

. In today's era of information and computing technology has developed rapidly so that cyber crime has increased drastically due to the pandemic, cybercriminals are now also targeting people, not just systems. The mode of crime in cyberspace today is very diverse. The methods used by attackers are increasingly diverse and complex. By implementing an antivirus client server, it aims to scan every client that is connected to the local network in real time or centrally and also update it centrally, as well as detecting types of attacks that often occur in network systems and detecting types of attacks that are often found in network systems and provide protection for all computers. client from all attacks (malware, viruses, worms, Trojans) found on the network. As an effort to improve security in the company's network and provide comfort when carrying out communication activities on the Internet network, researchers migrated Sophos software to Trend Micro. Log results from antivirus scanning using Trend Micro, Risk Level High, actions that must be taken immediately Blocked

Keywords : security , network,protokol , cyber crime

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PENDAHULUAN

Di era sekarang ini teknologi informasi dan komputasi telah berkembang pesat sehingga kejahatan dunia maya meningkat secara drastis karena pandemi, penjahat dunia maya kini juga menargetkan orang, bukan hanya sistem yang ada di dalam perusahaan saja, dengan terintegrasi dengan teknologi informasi serta layanan sentris komunikasi di jaringan (Adnan, 2018). Arsitektur komputasi dan sifat akses dengan jaringan ini mengubah secara drastis *format model* penyampaian informasi .

Modus kejahatan di dunia *cyber* saat ini sangat beragam. Cara yang digunakan oleh penyerang semakin beragam dan kompleks. Berbagai serangan tersebut melibatkan *malicious software* atau yang biasa disebut *malware* yang merupakan suatu program jahat (Hidayatulloh, 2020). Ancaman *malware* dan penyebarannya bisa melalui berbagai cara. Salah satu cara yang sering dilakukan untuk menyebarkan *malware* dengan cara menyisip-kannya di sebuah aplikasi ataupun file tertentu. (Cakrawala, 2022)

Dengan Migrasi kita dapat melakukan pencegahan dengan terkelola sehingga dapat membantu tim keamanan dan IT Infrastruktur Jaringan. Dengan memperbaharui *Simple Network Time Protocol* dapat memberikan dukungan dan pemantauan multiregional se-panjang waktu, serta merespon ancaman secara langsung bila diperlukan (Sitompul, 2022)

Hal ini juga bermanfaat dalam meng-atasi kendala yang terkait dengan kinerja di lingkungan jaringan, menjamin ketersediaan sumber daya, menjamin keamanan, men-yediakan layanan-layanan yang mendukung pekerjaan selama *Work From Home (WFH)*. Pengguna layanan dalam system jaringan serta applikasi-applikasi yang terkait dengan komputasi ini sangat membutuhkan kinerja tinggi, (Yuliandoko, 2018) karena hal inilah yang paling diinginkan untuk membantu kiner-ja, mereka membutuhkan teknologi layanan jaringan yang aman disaat melakukan *transfers* data dan pertukaran informasi melalui media jaringan. Kita sebagai peneliti sangat berharap dapat berkontribusi dalam membantu perma-salah yang ada.

Pandemi Covid yang sudah terjadi beberapa tahun belakangan ini mengharuskan beberapa karyawan bekerja dari rumah *Work From Home* (WFH). Hal ini mengakibatkan serangan *ransomware attack* meningkat di ikuti juga dengan penjahat dunia maya yang memanfaatkan perubahan cara bekerja pada saat pandemi ini, sehingga keamanan jaringan dari tindak kejahatan *(cyber security*) sangat penting aktifitas bekerja jarak jauh. (Nasional, 2020)

Cara yang paling mudah untuk mem-batasi akses adalah dengan mengharuskan pengguna untuk mengotentikasi dirinya sebelum memberikannya akses, tetapi tetap saja banyak kasus serangan yang dilaporkan. Pada umumnya langkah pertama yang dilakukan penyerang adalah mencari infor-masi lengkap tentang korbannya, seperti layanan yang berjalan, *port* yang terbuka dan versi dari *software* untuk menemukan kele-mahan yang belum di *Patch* bahkan *Zero-Day*. (Humaira Aliya, 2021)

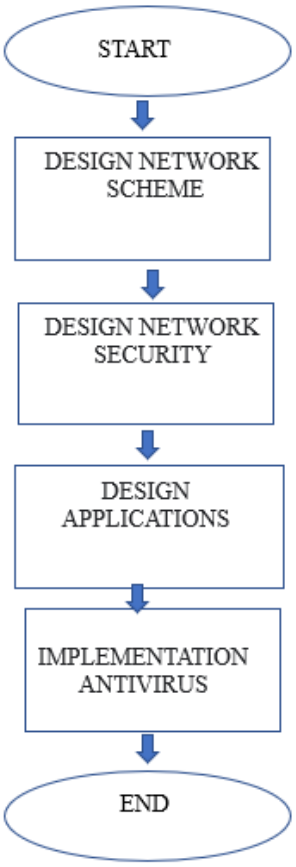
Berdasarkan latar belakang yang sudah disampaikan pada paragraf diatas, masalah yang akan diangkat oleh peneliti dapat diru-muskan sebagai berikut. Bagaimana cara kon-figurasi dan mengimplementasikan *trendmicro Antivirus client*, baik untuk PC, *notebook* ataupun *server* pada infrastruktur jaringan, bagaimana melindungi jaringan dari gangguan *cybercrime* termasuk *virus worm, Trojan, malware, spyware, phishing* dan lain sebagai-nya, dan bagaimana menscan *system* jaringan dari *server* pusat (Retno Adenansi, 2017).

Pada akhir penilitian bertujuan mengim-plementasi antivirus *client server* yang dapat melakukan scan di setiap client yang sudah ter-hubung jaringan *local* secara *real time* maupun terpusat juga mengupdate secara terpusat pula, serta mendeteksi jenis serangan yang sering terdapat system jaringan.

METODE

Penelitian ini meliputi 4 tahap rancangan skema jaringan, rancangan keamanan jaringan, rancangan aplikasi dan pengujian jaringan seperti dalam Gambar 1.

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar 1. Tahap Penelitian

***Design Network Scheme* (Rancangan Skema Jaringan)**

Dalam tahap ini dilakukan perancangan skema jaringan pada PT Retail Group Indonesia. Hasil rancangan untuk memperoleh topologi jaringan yang akan digunakan sehingga dapat dilakukan analisa kebutuhan yang diperlukan.

***Design Network Security* (Rancangan Keamanan Jaringan)**

Dalam tahapan ini dilakukan rancangan keamanan jaringan PT Retail Group Indo-nesia. sesuai yang dibutuhkan oleh didalam perusahaan. (EdyHaryanto, 2016)

***Design Application* (Rancangan Aplikasi)**

Pada tahap ini dilakukan perancangan aplikasi menggunakan *software* Tren Micro dengan melakukan Migrasi software lama. Untuk system keamanan beraktifitas didalam jari-ngan. (Infantono, 2020)

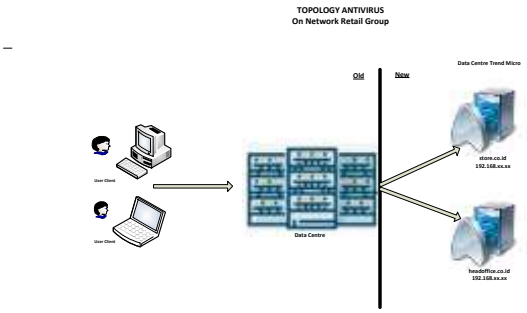
***Netwok Testing* /Pengujian Jaringan**

Dalam melakukan pengujian dilakukan untuk beberapa *client* yang terhubung didalam baik yang menggunalkan system operasi yang beragam mulai dari windows 8, windows 10, SQL server 2008. Pengujian dila-kukan untuk mengetahui apakah perancangan yang telah dilakukan sudah meme-nuhi kebutuhan yang diharapkan (Wijaya, 2020).

HASIL DAN PEMBAHASAN

Usulan Topologi Jaringan

Dalam penerapan jaringan , untuk dapat menghubungkan antara kantor pusat (*head office*) dengan kantor cabang (*store*), pada masing masing kantor membutuhkan sebuah *router* yang digunakan sebagai lalulintas jaringan luar menuju *data center* jaringan *virtual privat network* (VPN), dimana kantor pusat sebagai *server* dan kantor cabang dan jaringan luar yang dikases ketika karyawan /*user* tidak bekerja diruang lingkup kantor *Work From Fome* (WFH) sebagai *client*. Sebagai salah satu peningkatan keamanan maka perlu penerapan migrasi *anti virus* ter-barukan sebagai salah satu bagian infrastruktur *Simple Network Time Protocol (SNTP)*. Adapun topology yang diusulan seperti pada Gambar 2.



Gambar 2. *New Topology Antivirus*

Penerapan Keamanan Jaringan Jaringan

Perangkat yang dipasang dan dikon-fugurasi sebagai *gateway* lalu lintas keluar masuk data didalam infrastruktur adalah *router mikrotik* yang memiliki dua fitur yang ada di

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

firewall yaitu *Network Address Translation* (NAT) dan *filtering*.

1. *Network Address Translation*

NAT menjadi protokol dalam suatu sistem jaringan yang menghubungkan antara jaringan *internal* dengan jaringan *eksterna*l melalui perngakat keras bernama *router mikrotik*. *Network Address Translation* juga berfungsi sebagai *firewall* yang memiliki peranan melakukan perubahan IP address pengirim dari sebuah paket data. NAT ini berkerja pada *router-router* yang menjadi batas antara jaringan lokal dan jaringan internet. Secara teknis NAT mampu mengubah paket data yang berasal dari PC/laptop *client* seperti berasal dari router.

Router mikrotik nantinya akan menjalankan NAT tugas dengan cara menyamar, sehingga mengubah semua paket data yang berasal PC/laptop *client* seperti berasal dari *router*. Penyamaran ini wajib dijalankan oleh *router-router* pintu gerbang yang berfungsi menyembunyikan *IP Address Private* yang akan gunakan pada jaringan lokal, sehingga tidak terlihat dari internet. Aksi Penyaman ini tadi akan menyembunyikan PC/laptop *client* yang ada dijaringan lokal sekaligus membuat PC/laptop *client* tersebut terlindungi ke IP Address router.

2. Filtering

Keamanan jaringan yang menjadi salah satu aktivitas berbahaya harus diting-katkan dengan cara memfungsikan PPTP (*Point-to-Point Tunneling Protocol*.) sebagai *filtering* di *server*. Jika PPTP *filtering* difungsikan dengan baik, maka PPTP server di jaringan pribadi hanya akan menerima dan mengirim paket PPTP dari semua *client* yang tervalidasi atau sah. Hal ini sangat membantu, mencegah semua paket yang tidak sah untuk masuk ke dalam server PPTP dan jaringan pribadi. Begitu juga untuk pemakaian enkripsi PPTP, PPTP *filtering* melindugi agar data yang terenkripsi dan terverifikasi bisa keluar masuk LAN privat perusahaan melalui *gateway*.

***Design Application* (Rancangan Aplikasi)**

Sebagai upaya meningkatan keamanan dijaringan perusahaan dan mermerikan kenyaman disaat melaukan aktivitas komu-nikasi di jaringan *Internet*, peneliti melakukan *migrasi software sophos* ke *trend Micro* seperti pada Gambar 3.

Gambar 3. Antivirus Trend Micro

Ketika akan mengimplementasikan anti virus sebagai langkah menerapkan kea-manan dari tindak kejahatan yang akan menyusupi *system*, dimana antivirus yang digunakan sebelum sudah tidak mampu lagi mendukung kinerja keamanan jaringan dalam menditeksi penyerang atau tindak kejahatan yang terjadi didalam aktifitas jaringan, hal yang penting untuk diketahui adalah adanya suatu keseimbangan antara mengamankan data dari user untuk diverifikasi oleh antivirus dari seluruh aktifitas yang ter-hubung ke jaringan luar agar dapat masuk ke dalam jaringan *internal*. Maka dari itu, hal yang perlu dilakukan adalah dengan melakukan analisis resiko pada jaringan, menen-tukan *level* keamanan yang diperlukan pada suatu organisasi, serta melakukan identifikasi terhadap informasi-informasi yang perlu untuk dilindungi dari berbagai tindakan serangan pada jaringan.

Hal ini sangat penting untuk menentukan cara terbaik implementasi kebijakan kea-manan pada suatu organisasi atau perusahaan yang sudah ada dan memastikan tidak terjadi masalah baik dari sisi manajemenl maupun teknis. Cara yang terbaik adalah dengan mengimplementasi antivirus yang mendukung dengan kondisi sistem operasi yang digunakan user dalam berinteraksi dengan jaringan luar dan di verifikasi kepentingannya serta memas-tikan bahwa user yang melakukan akses terhadap suatu sumber daya secara aman dan efisien. Untuk implementasi kebijakan keama-nan dengan migrasi antivirus yang mampu mendukung peningkatan keamanan jaringan.

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Untuk melakukan migrasi antivirus lama menjadi antivirus terbaru dalam hal ini pe-neliti menerpakana antivirus *trend micro*. yang harus di lakukan adalah persiapkan applikasi *seperti CCsetup563.exe Revo-Uninstaller Portable.* Setelah itu *harus Instal CCleaner V5.63 Setup* sebagai upaya menerapkan sistem keamanan yang lebih handal dalam mendektsi serangan yang datang dari jaringan luar. Berikut adalah tahapan untuk migrasi sebelum implementasi *software* antivirus baru.

Gambar 4.Setup CCleaner V5.63

Setup CCleaner ini berfungsi untuk membersihkan *cache* pada PC atau laptop agar dapat bekerja secara optimal. *CCleaner* mampu untuk membersihkan *internet cache, internet history, download history yang merupakan celah yang disusupi penyerang*

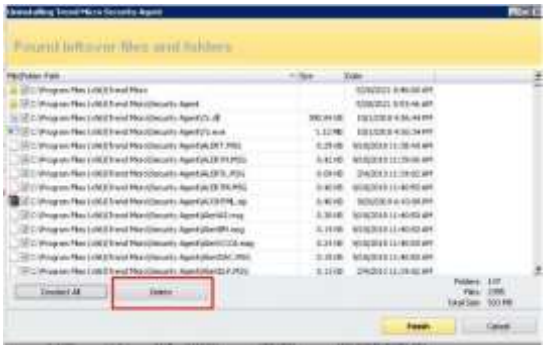
Gambar 5.*Finisehd Setup CCleaner V5.63*

Setelah semua langkah-langkah seperti *Custom Clean, Custom Clean, Custom Clean, Registry, Scan For Isuse*, dijalankan maka akan muncul tahap finish seperti pada gambar 4. Jika prosedur konfigurasi *CCleaner V5.63* selesai hal yang harus dilakukan adalah dengan menjalakan *Revo Uninstale*

Gambar 6. *Revo Uninstaler*

Ini dilakukan untuk menghidari masalah memori perangkat penuh. Hal ini dikare-nakan banyaknya aplikasi yang terpasang. Untuk meringankan memori perangkat, sebaiknya hapus beberapa aplikasi yang tidak terpakai. Maka pilihan peneliti adalah *Revo Uninstaller* untuk melakukan pelepasan aplikasi yang terpasang.

Software ini menjadi *uninstaller* yang cukup efektif untuk menghapus aplikasi berserta file-file yang terdapat di dalam PC atau Laptop. Sehingga seluruh bagian aplikasi yang dihapus pun tidak ada yang tertinggal dalam perangkat. Revo ini dibuat khusus untuk windows.



Gambar 7. *Finished Revo Uninstaler*

Berikut tahapan dalam menjalankan Revo Unistaller. Pilih *Trend Micro Security Agent*, pilih *Uninstal*, kemudian pilih yes, pilih Trend *Micro Security Agent* pilih *Uninstal, Select All* kemudian *delete, Select All*, lalu klik *Delete*, terakhir *finish* seperti terlihat pada gambar 6.

Berikut ini *antivirus Trend Micro* yang di implementasikan untuk mendeteksi serangan sebagai peningkatakan keamanan jaringan ketika user melakukan aktifitas dengan jaringan

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

luar. Pastikan *instalasi* antivirus ini sudah dijalankan dengan benar hingga *finish*

Gambar 8. *Instal Trend Micro*

Setelah semua tahapan dalam imple-mentasi antivirus sudah dilakukan, maka perlu dilakukan pengamatan untuk memas-tikan bahwa antivirus *(Trend Micro*) mampu bekerja dengan baik. Cara termudah yang dapat dilakukan adalah dengan menggunakan *command ping* untuk melakukan verifikasi terhadap komunikasi.

Gambar 9. Koneksi Jaringan

Jika percobaan koneksi jaringan dengan menggunakan perintah ping tidak berhasil atau time out, maka dapat dilakukan dengan cara menghentikan antivirus untuk kemudian dijalankan kembali. Hal ini harus dilakukan pada semua PC atau laptop yang terhubung dalam jaringan. Pengujian serangan jaringan dilakukan dengan menscan atau *running* antivirus. Pastikan jaringan sudah terhubung, dalam *log* akan terlihat serangan yang me-nyusupi seperti gambar 10.

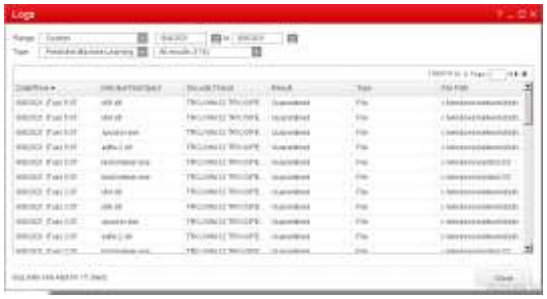
Gambar 10. Scan Antivirus

Dari pengujian *scanning* yang dilakukan dengan menggunakan antivirus Trend micro ini didapat ada penyerang berupa *malware Trojan* sperti pada gambar 11 masuk kedalam ruang lingkup jaringan LAN, hal yang harus dilakukan untuk menghetikan *malware* ini *cleaned*

Gambar 11. Hasil Scan Antivirus

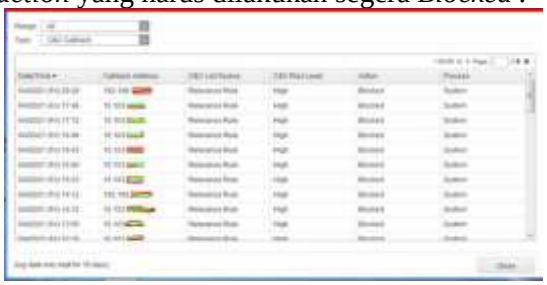
Pengujian terhadap serangan Malware dilakukan peneliti selama periode 6/4/2021 sampai dengan 6/8/2021 dari hasil *log* ini menjadi acuan untuk menganalisa langkah yang harus dilakukan untuk mencengah terjadi dampak yang merugikan, seperti pada gambar 11. Bahwa malware *trojan* ini sudah harus di *quarantined* karena sudah menyusup ke dalam *file*

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar12. Log Scan Antivirus

Pengujian terhadap serangan *Malware* juga dilakukan peneliti diberberpa IP Addres di ruang lingkup jaringan LAN terhubung dengan jaringan luar atau Internet, seperti pada gambar 13. Hasil log dari scanning antivirus dengan menggunakan *Trend Micro, Risk Level High, action* yang harus dilakukan segera *Blocked* .



Gambar 13. Log Pengujian IP

SIMPULAN DAN SARAN

Dari data yang didapatkan mengenai *protocol* jaringan hasil dari *scanning* antivirus menggu-nakan Trend Micro adalah antivirus untuk *scanning malware* mudah disbandingkan dengan aplikasi seperti *forensic tools snort* karena memerlukan penyetingan pada *snort.conf* sementara pada antivirus *trend micro* ini hanya cukup memilih menjalankan *scanning* hal ini bisa dilakukan oleh user ataupun *administrator* secara langsung. Sehingga *administrator* jaringan dapat meng-analisa paket jaringan yang sedang berlangsung.

Pengetahuan tentang *malware* juga diperlukan untuk antisipasi penyebaran *malware* yang semakin kompleks dengan berbagai macam cara. *Analysis malware* digunakan untuk mendeteksi *malware* terhadap suatu program yang terindikasi terkena *malware*. Pada *malware dynamic* terdapat beberapa *tools* yang dapat digunakan dan menambah pengetahuan penting bagi para pengguna jejaringan social atau internet. Diharapkan implementasi ini dapat melindungi seluruh komputer *client* dari segala serangan (*malware, virus, worm, Trojan*) yang terdapat pada jaringan.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada LPPM Universitas Pakuan yang telah mendanai penelitian ini,dan terima kasih kepada team editor jurnal yang bersedia memberikan masukan untuk kebaikan jurnal kami.

DAFTAR PUSTAKA

Adnan, M. I. S. d. R. Y., 2018. Implementasi Load Balancing Metode ECMP, NTH dan PCC dengan Empat Link Internet Menggunakan Mikrotik. *in Conference on Electrical Engineering, Telematics, Industrial technology, and Creative Media (CENTIVE,* Volume 2, pp. 308-314.

Cakrawala, A. I. C. s. C. s. K. M. P. 2022*https://infokomputer.grid.id/read/122710604/apa-itu-cyber security-mengapa-cyber-security-kini-makin-penting?page=all.* [Online]Availableat:https://infokomputer.grid.id[Accessed 2 Agustus 2022].

EdyHaryanto, 2016. *Meningkatka Keamanan Otorisasi Port Dengan Metode Simple Port knocking Tunneling.* Surakarta, Konferensi Nasional Penelitian Matematika dan Pembelajarannya (KNPMP I) ,Universitas Muhammdiyah Surakarta.

Hidayatulloh, 2020. Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSec. *Jurnal Informatika Fakultas Teknik dan Informatika Universitas Bina Sarana Informatika,,* Volume 1, pp. 93-104.

Humaira Aliya, K. T. C. d. S.-b., 2021. *https://glints.com/id/lowongan/cybersecurityadalah/#.YYYucmBBzIU.* [Online] Available at: https://glints.com [Accessed 31 Agustus 2022].

Infantono, C. B. a. A., 2020. Pengembangan Aplikasi Mobile Kamus Istilah Aeronautika pada Platform Android Sesuai Standar ISO 25010. *senastindo,* Volume 1, pp. 195-202.

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Nasional, P. O. K. S., 2020. *Monitoring Keamanan Siber,* Jakarta: Badan Siber Dan Sandi Negara.

Retno Adenansi, L. A. N., 2017. Malware Dynamic. *JOEICT (Jurnal of Education and Information Communication Technology),* Volume 1, pp. 37-43.

Sitompul, J., 2022. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana* [Interview] (05 Agustus 2022).

Wijaya, N. d. P. B., 2020. Analisis Litensi Metode PCC, NTH dan ECMP untuk Load Balance dan Failover. *Jurnal STRATEGI-Jurnal Maranatha,* Volume 1, pp. 177-189.

Yuliandoko, H., 2018. Jaringan Komputer Wire dan Wireless Beserta Penerapannya. *Jurnal Informatika dan Rekayasa Elektronik,* Volume 1, pp. 13-17.