JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

STUDI KASUS IMPLEMENTASI METODE BLOCKING PORT DALAM PENCEGAHAN MALWARE

Cosmas Eko Suharyanto[1)], Pastima Simanjuntak[2)]
[12]Teknik Informatika, Universitas Putera Batam, Batam
email: costmust@gmail.com

ABSTRACT

Computer networks have become a staple in various fields. connected to the internet will increase the likelihood of threats or disruption to system security. Malicious Software (malware) is a program that is created with the aim of finding weaknesses or even damaging software and computer operating systems, they can enter through open ports that are not used in the network. After the author made observations at the XYZ School and conducted literature studies from various sources, the Router Mikrotik was needed to prevent this and the Dionaea Honeypot as a malware detection tool on the local network. This study aims to build a computer network security system with blocking port method at XYZ School by using observation, literature study and analysis methods. After the completion of this research, the security system of the XYZ School network can maximize system performance, prevent the entry of Malicious Software (malware).

Keywords: *malware, mikrotik, virus, blocking port*

PENDAHULUAN

Jaringan komputer dan internet sudah menjadi kebutuhan pokok di berbagai bidang saat ini. Di satu sisi berbagai kegiatan bisnis akan lebih efisien dari segi waktu dan biaya, tetapi juga tidak luput dari dampak negatif, yaitu akan memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem jaringan seperti *Malicious Software* (malware).

Malware merupakan singkatan dari *malicious software*, yaitu sebuah sebutan bagi *software* yang di desain sedemikian rupa agar dapat menyusup kedalam sebuah sistem komputer tanpa diketahui pemilik sistem, dimana di dalam *software* tersebut terdapat perintah-perintah khusus yang dibuat dengan tujuan khusus, seperti menyebarkan *virus*, *trojan*, *worm*, atau memasang *backdoor* (Mada R. Perdhana, 2011).

Malware dalam bentuk *virus*, *trojan*, *worm*, atau *backdoor* merupakan ancaman utama bagi keamanan sistem jaringan komputer. Kurangnya pengetahuan dari pengguna komputer terhadap masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah terhadap komputer. Sering dijumpai antivirus komputer tidak di update, atau bahkan komputer tidak dilengkapi dengan program *antivirus* sama sekali.

Sejak meningkatnya penggunaan teknologi internet, para pembuat malware mulai meningkatkan pola serangan dan penyebaran malware yang dibuat. Salah satu teknik yang digunakan adalah memanfaatkan komputer yang terinfeksi untuk mengirimkan pesan masal kepada pihak lain yang nantinya akan dijadikan host baru bagi malware. Pesan yang terkirim biasanya berupa pesan email iklan pesan IM melalui aplikasi IM yang popular seperti *Yahoo messenger*. Bahkan beberapa malware dirancang untuk menjadikan host yang terinfeksi sebagai tempat untuk melakukan serangan DOS massal terhadap sistem.

Di lingkungan Sekolah Swasta XYZ Batam telah menggunakan akses internet baik berbasis *wireless* (hotspot) maupun menggunakan kabel jaringan. Namun

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

jaringan di lingkungan Sekolah Swasta XYZ ini tidak memiliki sistem keamanan jaringan yang memadai, ini ditunjukkan dengan berdasarkan wawancara dengan pimpinan Sekolah XYZ serta beberapa pengguna jaringan yang mengeluhkan PC atau laptop yang digunakan sering mengalami kerusakan pada bagian software; adanya program asing yang berjalan sendiri, file-file yang tidak dapat diakses, dan tidak adanya management jaringan didalam Sekolah XYZ.

Dengan menggunakan Router mikrotik dibutuhkan konfigurasi sistem keamanan dan manajemen jaringan agar port-port yang tidak terpakai dapat segera dimatikan agar tidak menjadi pintu bagi malware.

PC Router Mikrotik dapat digunakan untuk memblokir port yang tidak terpakai pada jaringan komputer, sehingga meminimalkan risiko masuknya malware dan serangan dari luar yang dapat memicu terjadinya kelumpuhan jaringan lokal PC Router Mikrotik dapat digunakan untuk memblokir port yang tidak terpakai pada jaringan komputer, sehingga meminimalkan risiko masuknya malware dan serangan dari luar yang dapat memicu terjadinya kelumpuhan jaringan lokal (Sumardi, 2013). Bahkan, *Port Knocking* dengan *Fitur Limit per-IP connection Rate* dan *honeypot* sebagai keamanan jaringan pada Server Ubuntu Virtual mampu mengamankan server dengan cara mengalihkan penyusup dan seolah – olah penyusup sudah masuk ke server utama, selain itu dengan adanya honeypot bias memonitoring yang dilakukan penyusup selama berada di server banyangan dan bias dijadikan sebagai acuan untuk memperkuat system keamanan (Wilman, 2018).

Sistem preventif yang dapat diimplementasikan adalah IDS/IPS (*Intrusion Detection System/Intrusion prevention system*). IDS mampu memberikan informasi serangan melalui web untuk dapat dianalisa oleh administrator, perpaduan antara sistem deteksi dengan *firewall* merupakan suatu metode yang dinamakan *Intrusion Detection and Prevention System* (IDPS) (Prihasmoro, 2014).

Adanya celah kelemahan dari keamanan jaringan yang paling umum yaitu tidak adanya sistem untuk mendeteksi adanya serangan. Upaya meningkatkan keamanan jaringan dibutuhkan sistem yang dapat mendeteksi serta mengindentifikasi ancaman atau serangan, khususnya serangan malware. Rancangan sistem yang baru menggunakan *Honeypot Dionaea* untuk melakukan deteksi terhadap ancaman atau serangan dari malware, yang merupakan ancaman utama bagi keamanan sistem jaringan komputer (Harjono, 2013). Implementasi *Honeypot* pada jaringan *nirkabel hotspot* yang sangat berkembang akan memberikan tambahan kesulitan kepada penyerang yang mencoba melakukan penyerangan, kombinasi *Honeypot* dan *IDS* dengan *Honeyd* dan *Snort* memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang ditujukan ke jaringan *hotspot* (Muhammad Masuri Mustofa, 2013).

Dengan demikian, implementasi *honeypot* dapat digunakan sebagai alat bantu administrator untuk melihat laporan aktivitas yang dihasilkan Honeyd agar dapat membantu dalam menentukan kebijakan keamanan jaringan (Nugroho, 2013).

METODE PENELITIAN

Dalam penelitian ini penulis menggunakan metode *Action Research* (penelitian tindakan). Menurut (Widi, 2010), Penelitian tindakan adalah suatu penyelidikan atau penelitian dalam konteks usaha yang berfokus pada peningkatan kualitas organisasi atau

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

kinerjanya. Penelitian dilakukan pada Sekolah XYZ Batam dengan tahapan sebagai berikut:

1. Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan, untuk pengembangan keamanan jaringan Sekolah XYZ pada tahap ini peneliti mengidentifikasi masalah akan keamanan pada jaringan komputer Sekolah XYZ.
2. Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada, pada tahap ini pengembangan keamanan jaringan memasuki tahapan desain dengan melihat topologi jaringan Sekolah XYZ. Dengan memperhatikan kebutuhan terhadap penggunanan jaringan dan keamanan jaringan penelitian memulai melakukan beberapa persiapan seperti daftar alat- alat yang akan dipakai, *Operating System* yang digunakan dan Aplikasi-aplikasi pendukung seperti aplikasi *honeypot dionaea* dan lain-lain.
3. Peneliti mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah. Selanjutnya setelah rencana dibuat, dilanjutkan dengan tahapan tindakan berdasarkan rencana yang ada kemudian peneliti melakukan pemasangan alat-alat yang dibutuhkan seperti penggantian *router* menjadi router mikrotik dengan menyesuaikan settingan jaringan yang sudah ada, kemudian melakukan penginstalan *operating system Ubuntu* pada Pc yang nantinya akan dijadikan server, kemudian penginstalan aplikasi *dionaea* dan beberapa aplikasi pendukung pada *OS* Ubuntu, kemudian menjalankan *dionaea* pada *linux ubuntu*, lalu melihat hasil dari menjalankan aplikasi *dionaea* tersebut, kemudian setelah mendapatkan hasil dari aplikasi *dionaea*, selanjutnya melakukan *blocking port* pada jaringan Sekolah XYZ dengan menggunakan router mikrotik.
4. Setelah melakukan implementasi (*action taking*) dianggap cukup kemudian peneliti melaksanakan evaluasi hasil dari implementasi yang telah dilakukan, dalam tahap ini dilihat bagaimana aplikasi *dionaea* dapat menelusuri *port* mana saja yang sering dilalui oleh *malware* dan dengan menggunakan *router* mikrotik dapat melakukan *blocking port* yang dilalui oleh *malware*.
5. Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan review tahap-pertahap yang telah berakhir kemudian penelitian ini dapat berakhir. Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi atau keadaan dievaluasi oleh peneliti dan dikomunikasikan kepada klien, peneliti dan klien merefleksikan terhadap hasil penelitian ini, yang nampak akan dilaporkan secara lengkap dan hasilnya secara eksplisit dipertimbangkan dalam hal implikasinya terhadap penerapan *Canonical Action Reaserch* (*CAR*). Untuk hal tertentu, hasilnya dipertimbangkan dalam hal implikasinya untuk tindakan berikutnya dalam situasi organisasi lebih-lebih kesulitan yang dapat dikaitkan dengan pengimplementasian perubahan proses. Jika ditemukan kegagalan maka akan dilakukan kembali dari Diagnosa dan seterusnya menurut dengan langkah penelitian yang digunakan sampai mendapatkan hasil dari penelitian ini.

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

HASIL DAN PEMBAHASAN

1. Implementasi Deteksi Malware Menggunakan Honeypot Dionaea.
   Sistem kerja Dionaea menggunakan python sebagai bahasa cripting, menggunakan libemu untuk mendeteksi shellcodes. Honeypot Dionaea bertujuan mendapatkan dan mencari informasi dari malware. Setelah dionaea mendapat salinan dari malware, dionaea akan menyimpan file lokal untuk dianalisa lebih lanjut, kemudian dengan menggunakan virus total diketahui jenis malware yang menyerang jaringan local Sekolah XYZ.
2. Hasil Analisis Deteksi Malware Dengan Menggunakan Honeypot Dionaea Sebelum Dilakukan Blocking Port.
   Analisis file binner dilakukan agar dapat diketahui jenis malware yang didapat setelah dijalankan honeypot dionaea sebagai alat pendeteksi serta menjadikan server ini sebagai korban dari serangan malware. Analisis file binner dilakukan dengan bantuan antivirus offline atau online seperti pada penelitian ini menggunakan antivirus total sebagai alat untuk mengetahui jenis-jenis malware yang ada di dalam file binner. Berikut tabel dari hasil analisis file binner:

Tabel 1. Analisis Pada Pengujian Sebelum Blocking Port

No	File Binary	Jenis Malware	Jumlah
1	1b191a667e792270d9bf5dd6994e7f9e	Trojan.UKP.Generic.4!c	19
		Trojan.Generic.D4F2C70	
		W32/Virut.AX	
		Trojan.Generic.5188720	
		Win.Trojan.Joanap-6574508-0	
		Malware@#ocf7ugdu11tf	
		W32/Virut.7116	
		Trojan.DownLoader9.29243	
		Trojan.Generic.5188720 (B)	
		W32/Virut.7116	
		Trojan.Generic.5188720	
		Trojan.Generic.5188720	
		Trojan.Generic	
		malware (ai score=86)	
		Trojan.Generic.5188720	
		Virus.Win32.Virut.ljfw	
		Win32/Virus.da3	
		Mal/HckPk-A	
		W32.Virut.CF	
2	1d53fb866c27a421f7557e3cda0592ac	Trojan.UKP.Swdld.4!c	17
		Generic.Malware.SWdld.1EF69FB6	

		Generic.Malware.SWdld.1EF69FB6	
		Win.Downloader.73594-1	
		Malware@#fk9e8ok5zreb	
		W32/HLL-SysDlrSharer!Eldorado	
		Trojan.Swizzor.17843	
		Generic.Malware.SWdld.1EF69FB6 (B)	
		W32/HLL-SysDlrSharer!Eldorado	
		Generic.Malware.SWdld.1EF69FB6	
		Generic.Malware.SWdld.1EF69FB6	
		Virtob.Win32	
		Generic.Malware.SWdld.1EF69FB6	
		Trojan.Win32.Agent.bivrap	
		Win32/Trojan.Downloader.a8e	
		Troj/DLoad-IK	
		Trojan.Gen.2	
3	2c8f62d7325ef1bce2k26H9eea7a1d79	Worm.Generic.230976	19
		TR/Agent.grpm	
		Worm.Generic.230976	
		Win.Spyware.78857-1	
		Malware@#pq0d290k1654	
		W32/Agent.IX.gen!Eldorado	
		Win32.HLLW.Brambul.1	
		Worm.Generic.230976 (B)	
		W32/Agent.IX.gen!Eldorado	
		Worm.Generic.230976	
		Worm.Generic.230976	
		Trojan.Spy.ZBot	
		Worm.Generic.230976	
		Trojan.Win32.Agent.bmgds	
		Win32/Trojan.a3a	
		Mal/Spy-Y	
		Trojan Horse	
		Win32.Trojan.Agent.Ecbe	
		Downloader.OpenConnection.JS.97665	
4	3jcc5ag99d1bjd7c03578152di78b387	Trojan.UKP.Generic.4!c	19
		Worm.Generic.D38640	
		TR/Agent.grpm	
		Worm.Generic.230976	
		Win.Spyware.78857-1	
		Malware@#f0ld0886ylp7	
		W32/Agent.IX.gen!Eldorado	

		Win32.HLLW.Brambul.1	
		Worm.Generic.230976 (B)	
		W32/Agent.IX.gen!Eldorado	
		Worm.Generic.230976	
		Worm.Generic.230976	
		Trojan.Spy.ZBot	
		Worm.Generic.230976	
		Trojan.Win32.Agent.bmgds	
		Win32/Trojan.a3a	
		Mal/Spy-Y	
		Trojan.Gen.NPE	
		Win32.Trojan.Agent.Eclf	
5	04d689941b2db3j02f2g413e5g613fa3	Win32.Sality.E	17
		W32/Sality.L	
		Win32.Sality.E	
		Win.Trojan.Sality-1014	
		Malware@#36zbruqsdz5cv	
		W32/Sality.K	
		Trojan.Swizzor.17843	
		Win32.Sality.E (B)	
		W32/Sality.K	
		Win32.Sality.E	
		Win32.Sality.E	
		Win32.Sality.E	
		Virus.Win32.Sality.cdbf	
		Win32/Virus.5d3	
		W32/Sality-I	
		W32.Sality	
		Downloader.OpenConnection.JS.96749	
6	3f12e802befe2e392cf0132e146f1f98	Trojan.UKP.Generic.4!c	17
		W32/Virut.AX	
		Trojan.Generic.5188720	
		Win.Trojan.Joanap-6574508-0	
		Malware@#25c19isw7k2s2	
		W32/Dropper.gen8!Maximus	
		Trojan.DownLoader9.29243	
		Trojan.Generic.5188720 (B)	
		W32/Dropper.gen8!Maximus	
		Trojan.Generic.5188720	
		Trojan.Generic.5188720	
		malware (ai score=97)	

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

		Trojan.Generic.5188720	
		Virus.Win32.Virut.ljfw	
		Win32/Virus.da3	
		Mal/HckPk-A	
		Trojan Horse	
7	4bb31ab74c23d05540d47d732f63df38	Trojan.UKP.Generic.4!c	17
		Trojan.Generic.D1BE4F4	
		Trojan.GenericKD.1828084	
		Win.Downloader.99276-1	
		W32/HLL-SysDlrSharer!Eldorado	
		Trojan.Swizzor.18641	
		Trojan.GenericKD.1828084 (B)	
		W32/HLL-SysDlrSharer!Eldorado	
		Trojan.GenericKD.1828084	
		Trojan.GenericKD.1828084	
		Virtob.Win32	
		malware (ai score=89)	
		Trojan.GenericKD.1828084	
		Trojan.Win32.Agent.deisvl	
		Win32/Trojan.Downloader.a6c	
		Troj/DLoad-IK	
		Trojan.Gen.2	

Dari hasil tabel di atas terdapat 7 file biner yang telah dianalisis sehingga mendapatkan berbagai jenis *Malware* dan mengindikasikan jaringan Sekolah XYZ Batam telah diserang oleh *malware.*

3. Implementasi Blocking Port

Blocking port dilakukan dengan tujuan agar dapat menghambat atau mempersulit masuknya *malware* pada sistem. *Blocking port* dilakukan setelah implementasi deteksi *malware* dengan menggunakan *honeypot dionaea*. Sebelum melakukan *blocking port* pada sistem jaringan Sekolah XYZ Batam, terlebih dahulu merancang *port* yang akan diblock. Rancangan *port* yang akan diblock disesuaikan dengan pengambilan port menggunakan bantuan software port scanner dan serangan malware yang terjadi. Berikut adalah daftar *port* yang akan dilakukan block sebagai berikut:

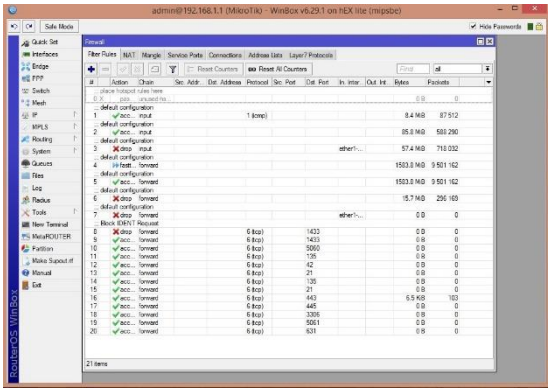
Tabel 2. Daftar Port Dilakukan Blocking

NO	PORT	JENIS PROTOCOL	SERVICE
1	1433	TCP	mssqld
2	5060	TCP	SipSession
3	135	UDP	epmapper
4	42	TCP	mirrord
5	21	TCP	ftpd
6	80	TCP	http
7	135	TCP	msrpc
8	443	TCP	https
9	445	TCP	microsoft-ds
10	631	TCP	ipp
11	3306	TCP	mysql
12	5061	TCP	sip-tls

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

13	554	TCP	-
14	2869	TCP	-
15	2968	TCP	-
16	5040	TCP	-

Setelah dilakukan perancangan daftar port yang akan diblock, kemudian dilakukan blocking port dengan menggunakan mikrotik RB750. Berikut adalah hasil tampilan block port pada mikrotik RB750:



Gambar 1. Hasil Blocking Port Pada Winbox Mikrotik RB750

4. Hasil Analisis Deteksi Malware Menggunakan Honeypot Dionaea Setelah Dilakukan Blocking Port

Setelah dilakukan *blocking port* dengan menggunakan Mikrotik RB750, kemudian dilanjutkan dengan menganalisa kembali dengan tujuan melihat keberhasilan dari *blocking port* tersebut. Analisa kembali dilakukan selama 1 minggu. Dari analisa setelah 1 minggu dijalankannya blocking port masih didapatkan serangan malware yang tertangkap oleh Honeypot Dionaea tetapi dalam jumlah yang sedikit dibandingkan sebelum menggunakan metode *blocking port*, berikut adalah hasil *report* selama 1 minggu setelah berjalannya metode *blocking port*:

Tabel 3. Analisis Pada Pengujian Setelah Blocking Port

No	File Binary	Jenis Malware	Jumlah
1	5d2932dffe1b62d81df3dcd47f7799bc	Worm.UKP.Generic.o!c	13
		Worm.Generic.D69B04	
		Worm.Generic.432900	
		Win.Trojan.Agent-6316606-0	
		W32/Trojan.ABWT-1072	
		Win32.HLLW.Autoruner1.15292	
		Worm.Generic.432900 (B)	
		Worm.Generic.432900	
		Worm.Generic.432900	
		Worm.SuspectCRC	
		malware (ai score=89)	
		Trojan.Win32.Swisyn.cugzap	
		Mal/Generic-S	
2	31dd69df12d981e77a0b7c535edd4580	Trojan.UKP.Generic.4!c	16
		TR/Agent.grpm	
		Gen:Win32.SMTP-Mailer.dqW@aqb@WXmG	
		Win.Spyware.78857-1	
		Malware@#2cfheiba8qh5k	

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

		W32/Agent.IX.gen!Eldorado	
		Gen:Win32.SMTP-Mailer.dqW@aqb@WXmG (B)	
		W32/Agent.IX.gen!Eldorado	
		Gen:Win32.SMTP-Mailer.dqW@aqb@WXmG	
		Gen:Win32.SMTP-Mailer.dqW@aqb@WXmG	
		Gen:Win32.SMTP-Mailer.dqW@aqb@WXmG	
		Trojan.Win32.Agent.bmgds	
		Win32/Trojan.a3a	
		Mal/Spy-Y	
		Trojan.Gen	
		Win32.Trojan.Agent.Lkef	
3	65bc5c80b91192d0738c5d2f47af06d9	Worm.UKP.Generic.o!c	18
		Worm.Generic.D38640	
		Worm.Generic.230976	
		Win.Spyware.78857-1	
		Malware@#39c5nhg34lj4	
		W32/Agent.IX.gen!Eldorado	
		Win32.HLLW.Brambul.1	
		Worm.Generic.230976 (B)	
		W32/Agent.IX.gen!Eldorado	
		Worm.Generic.230976	
		Worm.Generic.230976	
		Trojan.Spy.ZBot	
		malware (ai score=81)	
		Worm.Generic.230976	
		Trojan.Win32.Agent.bmgds	
		Win32/Trojan.20b	
		Mal/Spy-Y	
		Trojan.Gen.NPE	

5. Pembahasan

Setelah dilakukan Analisis dan Implementasi Mencegah Virus *Malware* Pada Jaringan Dengan Metode *Blocking Port* Menggunakan Mikrotik, selanjutnya membahas hipotesis yang telah menjadi bahan dalam penelitian ini :

1. Implementasi *blocking port* meningkatkan keamanan pada sistem jaringan. Berdasarkan analisis dan implementasi *blocking port* di Sekolah XYZ, kemanan jaringan cukup mampu dimaksimalkan dengan mencegah serangan *malware*, sehingga keamanan jaringan dapat ditingkatkan. Maka Hipotesis 1 diterima.
2. *Blocking Port* dapat menghambat serangan *malware* pada jaringan komputer. Berdasarkan hasil implementasi *blocking port* di Sekolah XYZ, metode ini mampu menghambat serangan *malware* dengan menutup akses port yang telah dianalisa. Maka Hipotesis 2 diterima.

3. Router mikrotik mampu mencegah masuknya serangan *malware* dari *port-port* yang kosong dan tidak terpakai dalam jaringan komputer. Berdasarkan implementasi blocking port dengan menggunakan mikrotik, yang dimana *port* tidak terpakai dalam jaringan diblock sehingga *malware* yang biasa memasuki jaringan dengan melewati *port* kosong atau tidak terpakai dapat dicegah dengan fasilitas yang ditawarkan oleh *mikrotik*. Maka hipotesis 3 diterima.

SIMPULAN

Berdasarkan hasil penelitian dan pengujian, maka dapat diambil kesimpulan dari implementasi yang telah diterapkan adalah sebagai berikut:

1. Berdasarkan analisis dan implementasi *blocking port* di Sekolah XYZ, kemanan jaringan cukup mampu dimaksimalkan dengan mencegah serangan *malware*, sehingga keamanan jaringan dapat ditingkatkan.
2. Berdasarkan hasil implementasi *blocking port* di Sekolah XYZ, metode ini mampu menghambat serangan *malware* dengan menutup akses port yang telah dianalisa.
3. Berdasarkan implementasi blocking port dengan menggunakan mikrotik, yang dimana port tidak terpakai dalam jaringan diblock sehingga *malware* yang biasa memasuki jaringan dengan melewati *port* kosong atau tidak terpakai dapat dicegah dengan fasilitas yang ditawarkan oleh *mikrotik*.

DAFTAR PUSTAKA

Mada R. Perdhana. (2011). *HARMLESS HACKING (Malware Analysis dan Vulnerability Development)*. Yogyakarta: Graha Ilmu.

Muhammad Masuri Mustofa. (2013). Penerapan Sistem Keamanan Honeypot Dan Ids Pada. *Sistem Keamanan Honeypot Dan IDS*, *1*(1), 111–118.

Nugroho, A. S. (2013). Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan. *Jurnal JARKOM*, *1*(1), 40–48.

Prihasmoro, S. A., Rachmawati, Y., Fatkhiyah, E., Informatika, J. T., & Industri, F. T. (2014). Jurnal JARKOM Vol . 2 No . 1 Desember 2014 ISSN : 2338-6313 Jurnal JARKOM Vol . 2 No . 1 Desember 2014 ISSN : 2338-6313, *2*(1), 59–68.

Studi, P., Informatika, T., & Teknik, F. (2013). MENGGUNAKAN DIONAEA (Malware Detection in the Network Using Dionaea) Harjono, *14*(2), 64–69.

Sumardi, R. A. T. (2013). Rancang Bangun Sistem Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali. *Indonesia Jurnal on Networking and Security*, *2*(Jaringan), 16–21.

Widi, R. K. (2010). *Asas Metodologi Penelitian (Sebuah Pengenalan dan Penuntun Langkah demi Langkah Pelaksanaan Penelitian*.

Wilman, W., Fitri, I., & Nathasia, N. D. (2018). Port Knocking Dan Honeypot Sebagai Keamanan Jaringan Pada Server Ubuntu Virtual. *J I M P - Jurnal Informatika Merdeka Pasuruan E-ISSN 2503-1945*, *3*(1), 27–33. Retrieved from http://ejurnal.unmerpas.ac.id/index.php/informatika/article/view/86/55