Bit (Fakultas Teknologi Informasi Universitas Budi Luhur) p-ISSN: 1693-9166
Vol. 20, No. 1, April 2023, hlm. 50-57 e-ISSN: 2685-127X

PENGEMBANGAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN *NETWORK FORENSICS*

Ahmad Sakhowi Amin[1*], Pipit Dewi Arnesia[2]

[1,2]Magister Teknologi Informasi, Sekolah Tinggi Manajemen Informasi dan Komputer Jakarta STI&K, Jakarta, Indonesia
Email: [1]ahmadsa18@gmail.com, [2]pdarnesia@gmail.com

(Naskah masuk: 10 Februari 2023, diterima untuk diterbitkan: 22 Mei 2023)

Abstrak

Masalah utama dalam penelitian ini yaitu telah terjadi ancaman dan serangan pada jaringan komputer serta *Administrator* atau pengelola jaringan kesulitan dalam mendeteksi dan memonitoring jaringan selama 24 Jam penuh. Penelitian dilaksanakan untuk menguji dan menganalisis agar memperoleh data serangan dan ancaman sebagai bukti yang terjadi pada jaringan komputer serta mengatasinya; mengembangkan sistem keamanaan jaringan dengan menggunakan *network forensic* sehingga dapat membantu melindungi sistem dalam mempertahankan keamanan pada jaringan; serta pendeteksian dan penanggulangan kemungkinan serangan sejak dini sehingga dapat meminimalisir adanya serangan pada sistem keamanaan jaringan. Penelitian ini menujukkan bahwa: 1)melalui analisis bukti penyusupan *Firewall Filter* akan memblokir *IP Address* yang dicurigai mengirim paket data tidak wajar pada sistem jaringan; 2)metode yang diterapkan *network forensics* meliputi Pendeteksian, Pengecekan, Analisis, Notifikasi dan Tindakan; 3) *Network Forensics* yang dikembangkan mampu mendeteksi dan memblokir saat terjadinya penyerangan/ penyusupan sehingga setelah diterapkan notifikasi *email* secara *realtime*, maka diperlukan juga untuk tindakan/ aksi yakni monitoring jaringan yang dapat mempermudah administrator dalam memantau sistem jaringan atau mengetahui setiap perubahan yang terjadi di jaringan SD Muhammadiyah 1 Jakarta menggunakan Aplikasi Telegram.

Kata kunci: *network forensics, sistem keamanan jaringan*

NETWORK SECURITY SYSTEM DEVELOPMENT USING NETWORK FORENSICS

Abstract

The main problem in this research is that there have been threats and attacks on computer networks and network administrators or managers have difficulty detecting and monitoring the network for 24 hours straight. This study aims to conduct testing and analysis in order to obtain data on attacks and threats as evidence that occurs on computer networks and overcome them; develop a network security system usingnetwork forensic so that it can help protect the system in maintaining security on the network; as well as early detection and prevention of possible attacks so as to minimize attacks on network security systems. This study shows that: 1) through the analysis of evidence of infiltration Firewall Filter will block IP Address suspected of sending unnatural data packets on the network; 2)applied network forensics includes Detection, Checking, Analysis, Notifications and Actions; 3)Network Forensics developed is capable of detecting and blocking when intrusions occur so that after implementing email notifications in realtime, it is also necessary for actions, namely network monitoring which can make it easier for administrators to monitoring network systems or find out any changes that occur in the SD Muhammadiyah 1 Jakarta network using the Telegram.

Keywords*: network forensics, network security system*

1. PENDAHULUAN

Jaringan komputer secara istilah sistem yang menghubungkan komputer dengan perangkat-perangkat terkait agar menjadi satu kesatuan untuk saling berkomunikasi dengan bertukar data [1]. Mempunyai manfaat yang banyak dibandingkan dengan komputer yang berdiri sendiri. Hal ini tidak hanya terdiri dari perangkat keras atau perangkat lunak saja, melainkan perpaduan dari dua jenis perangkat tersebut yang dimana saat ini berkembang pesat sehingga menjadi layanan yang sangat dibutuhkan [2]. Tidak mengherankan kebutuhan penggunaannya semakin banyak, baik dalam *hardware* maupun *software* [3]. Sekarang ini sudah

menjadi kebutuhan kegiatan di instansi, baik yang berupa instansi komersial (perusahaan), universitas, departemen pemerintahan atau swasta, maupun milik pribadi untuk saling bertukar informasi data dan file [4]. Adanya kebutuhan tersebut, maka diperlukan kemampuan mumpuni dengan didukung infrastruktur dan perangkat yang sangat diperlukan saat ini.

Beberapa penelitian diantaranya membahas sistem keamanan jaringan menggunakan metode *Firewall* untuk mengontrol lalu lintas antara beberapa area yang terhubung dalam dua atau lebih keamanan jaringan [5]. Hasil dari penelitian ini mewujudkan sistem perlindungan keamanan dan sarana manajemen keamanan untuk melengkapi perangkat lunak anti-virus dan *firewall* dalam jaringan untuk meningkatkan keamanan jaringan. Adapun metode *penetration testing* ditujukan sebagai pengujian terhadap keamanan jaringan pada perusahaan *Pay2home* dengan cara melakukan identifikasi dan eksploitasi celah-celah yang terdapat pada jaringan [6]. Namun *port service* terdapat *open service* sehingga dapat mengakibatkan terjadi penyerangan, sistem keamanan jaringan yang baru dapat dicapai dengan mematikan *sevice port* serta menggunakan *Deny* dan *Sameorigin*. Penelitian lain dengan menggunakan *network forensics*, menunjukkan analisis yang dilakukan terhadap semua lalu lintas jaringan menggunakan *tools Instrution Detection System Snort*[7]. Namun IDS *Snort* tidak menampilkan informasi data serangan, hanya membuat *log* dan menganalisis paket data ditemukan pada jaringan. *Network forensics* digunakan sebagai analisis, simulasi serta peninvestigasian untuk mendapatkan informasi macam-macam serangan pada jaringan komputer. Adapun hasil penelitiannya memudahkan proses investigasi ketika terjadi serangan pada jaringan [8].

Masalah-masalah yang ditemukan pada penelitian di SD Muhammadiyah 1 Jakarta. Pertama, akses pada router yang sangat berat, tidak bisa diakses dan terkadang tidak dapat masuk ke sistem router karena adanya ancaman dan penyerangan terjadi pada jaringan. Kemudian adanya peristiwa-peristiwa yang mengganggu pada jaringan. Oleh karena itu perlu diterapkan sistem keamanan jaringan dari orang yang tidak bertanggung jawab. Agar router terlindungi diperlukan sebuah konfigurasi yakni menggunakan network forensics. Kedua, masih kurangnya pemahaman administrator mengenai sistem keamanan jaringan sehingga kesulitan dalam mendeteksi dan memonitoring jaringan selama 24 Jam penuh. Berdasarkan pembahasan di atas, diharapkan adanya solusi berupa kajian pengembangan *network forensics* untuk memberikan gambaran sebuah sistem keamanan jaringan, dengan melakukan pendeteksian serangan dan penanggulangan kemungkinan serangan sedini mungkin sebelum *intruder*/ penyusup masuk ke dalam jaringan, dan pada penelitian ini akan ditambahkan proses pengujian dan analisis sistem keamanan pada jaringan.

2. METODE PENELITIAN

BAB ini memaparkan tahap-tahap dalam pengembangan sistem keamanan jaringan menggunakan *network forensics*, serta pada bagian akhir disajikan rencana penelitian yang dilakukan.

2.1 Pengumpulan Data

Mengumpulkan informasi di SD Muhammadiyah 1 Jakarta sebagai bahan referensi dan sebagai penunjang dalam mengembangkan sistem keamanan jaringan. Ada beberapa tahapan dalam melakukan penyelesaian studi kasus:

1. Studi Pustaka yakni mengumpulkan teori-teori yang berkaitan dengan penelitian sebagai pedoman dari beberapa buku dan jurnal, meliputi dasar-dasar *references* bagi peneliti untuk perancangan dan pembangunan sistem kemanan jaringan. Hal ini bertujuan sebagai rujukan dalam penelitian.
2. Observasi yaitu mengamati objek untuk mengetahui informasi yang relevan dengan penelitian, dengan tujuan merancang dan mengembangkan sistem untuk disempurnakan.
3. Wawancara dilakukan dengan cara bertanya langsung kepada pihak yang berkepentingan yaitu pimpinan dan manajemen SD Muhammadiyah 1 Jakarta untuk mengumpulkan informasi yang relevan dengan pokok bahasan penelitian.

2.2 Tahapan Penelitian

Tahapan penelitian ini menjelaskan bagaimana cara penelitian ini dilakukan, sehingga dapat memberikan rincian tentang alur atau langkah-langkah yang dibuat secara sistematis serta dapat digunakan dijadikan pedoman dengan jelas dalam menyelesaikan masalah dan membuat analisis terhadap hasil penelitian. Secara garis besar tahapan dalam sistem keamanan jaringan terbagi dalam empat proses besar yaitu:

1. Proses pada perancangan dan implementasi sistem keamanan jaringan.
2. Proses pada analisis dan pengujian terhadap sistem keamanan jaringan.
3. Proses di dalam menampilkan data serangan dan peningkatan keamanan jaringan.
4. Proses di dalam mengembangkan sistem keamanan jaringan dengan menggunakan *network forensics*.

Beberapa proses yang harus dilakukan di dalam penelitian ini agar mendapat hasil yang diharapkan. Dari identifikasi masalah sampai dengan tahap kesimpulan dan saran untuk penelitian lebih lanjut. Adapun proses penelitian tertuang dalam diagram alur pada gambar 1 berikut ini:

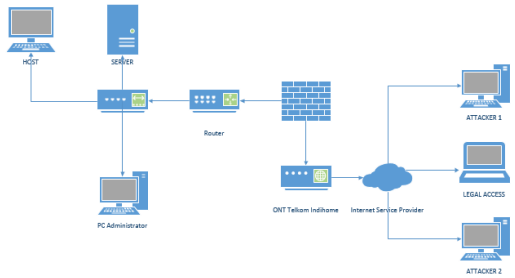
Gambar 1. Tahapan Penelitian

Berikut penjelasan dari bagan tahapan penelitian yang meliputi lima tahap yaitu Identifikasi Sistem, Perancangan Topologi Jaringan, Konfigurasi Sistem Keamanan Jaringan, Pengujian Sistem Keamanan Jaringan dan Implementasi Sistem yang Berjalan:

1. Identifikasi Sistem

   Sebelum sistem keamanan jaringan digunakan, adapun kebutuhan sistem yang harus diperhatikan terlebih dahulu. Kebutuhan sistem tersebut, yang dibutuhkan agar sistem dapat berjalan baik yaitu kebutuhan perangkat keras dan kebutuhan perangkat lunak.
2. Perancangan Topologi Jaringan

   Perancangan topologi yang dimaksud adalah untuk membuat topologi jaringan yang kiranya sesuai dengan sistem yang dikembangkan, sehingga gambaran topologi berikut dapat memberikan gambaran secara jelas tentang sistem yang akan diterapkan. Adapun dalam mengembangkan sistem keamanan jaringan ini, skenario pengiriman paket serangan dan menunjukkan bahaya yang dapat ditimbulkan oleh serangan. Gambar 2 menunjukkan gambaran umum dari skenario kasus deteksi serangan.



Gambar 2. Studi Kasus

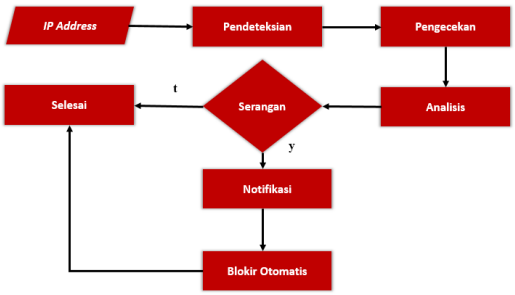
Perancangan topologi yang akan digunakan dapat dilihat pada gambar atas yaitu menggunakan topologi star, yang terdiri dari PC Server, PC Client dan *Attackers*, Router dan kabel UTP jenis *straight*. Skema serangan menunjukkan dimana komputer administrator dan host DHCP dihubungkan model topologi *star* dengan *switch* kemudian berturut-turut dihubungkan dengan router kemudian dibuat firewall sebagai sistem pengamanan jaringan dan yang terakhir dihubungkan dengan ONT ISP/ sumber internet. Kondisi jaringan tersebut dapat diakses baik dari dalam maupun dari luar jaringan komputer.

3. Konfigurasi Keamanan Jaringan

   Tahap ini melakukan konfigurasi dasar keamanan jaringan seperti melakukan pemberian *IP Address, Interfaces, DHCP Client, DHCP Server, DNS Server, Firewall, Gateway* dan konfigurasi pengembangan dari sistem keamanan jaringan menggunakan *network forensics.*
4. Pengujian Sistem Keamanan Jaringan

   Tahap ini perlu dilakukan pengujian network forensics dalam mendeteksi adanya penyusupan atau serangan. Tujuan utamanya untuk melakukan uji dan simulasi terhadap sistem keamanan jaringan dalam mendeteksi penyusup atau serangan yang melakukan tindak kejahatan pada router target. Studi kasus kali ini terdapat skenario pengujian sistem dilakukan dalam tiga tahapan antara lain: 1) Jaringan normal tanpa ada penerapan *network forensics*; 2) *mode Disable Port*; dan 3) sudah menerapkan *network forensics* namun mode yang digunakan adalah mode *Enable Port*, sehingga layanan pada router tidak dapat diakses oleh siapapun. Ketika seseorang mencoba mengakses layanan jaringan yang terdapat pada router harus melakukan autentikasi terlebih dahulu, bertujuan untuk membuka port yang tertutup.
5. Implementasi *Network Forensics*

   Pada tahap implementasi ini mengembangkan sistem keamanan jaringan menggunakan *network forensics* yang ditunjukkan pada gambar berikut ini:



Gambar 3. Tahapan Network Forensics

Adapun tahapan yang diterapkan pada pengembangan *network forensics*, dimana IP Address yang mengakses router akan masuk ke dalam sistem keamanan jaringan meliputi Pendeteksian, Pengecekan, Analisis, Notifikasi dan Tindakan. Penjelasan masing-masing tahapan sebagai berikut:

a. Pendeteksian

   Pada tahap ini merupakan langkah awal untuk mendeteksi dan mencari bukti-bukti. Proses ini membantu *administrator* untuk menemukan bagaimana, kemana, dan

berapa besar kapasitas internet yang lewat pada jaringan.

b. Pengecekan

Administrator mencari informasi yang tersembunyi *IP Address* penyusup pada router seperti memeriksa urutan paket, jumlah paket data, dan lain-lain yang dikirimkan oleh intruder/ penyusup.

c. Analisis

Tahap ini bertujuan untuk menganalisis sistem keamanan jaringan. *Administrator* dapat mengetahui adanya serangan dari intuder/ penyusup dapat dilakukan secara otomatis yaitu menggunakan *Log Activity* dan *IP Address List*. Adapun tahapan analisis yang akan menjawab pertanyaan forensik sehingga mengidentifikasi peristiwa yang terjadi:

1) Apakah penyerangan yang dilakukan?
2) Siapa yang melakukan serangan IP Address?
3) Kapan penyerangan dilakukan?
4) Dimana penyerangan dilakukan?
5) Mengapa penyerangan dilakukan?
6) Bagaimana penyerangan tersebut dapat terjadi?

d. Notifikasi

Tahap ini router memberikan notifikasi kepada administrator atau bagian yang berwenang untuk menangani permasalahan jaringan berupa *report*/ laporan adanya serangan melalui *email* secara otomatis.

e. Tindakan

Tahap ini merupakan pengembangan Network forensics dimana router dapat melakukan pencegahan hak akses yaitu memblokir IP Intruder/ penyusup secara otomatis. Selain itu administrator dapat memonitoring jaringan selama 24 jam penuh melalui aplikasi telegram.

2.3 Tinjauan Pustaka

2.3.1 Keamanan Jaringan

Gambaran umum keamanan jaringan merupakan suatu metode atau teknik yang digunakan untuk memberikan perlindungan pada sebuah jaringan dengan maksud terhindar dari berbagai ancaman luar atu dalam yang dapat merusak jaringan. Oleh karena itu dalam implementasi jaringan komputer merupakan bagian yang terpenting. Masalah yang sering terjadi dikarenakan kelalaian administrator jaringan dalam membangun sebuah jaringan komputer. Akibat kelalaian tersebut, dapat memberikan peluang bagi *hacker* untuk meretas dan merusak jaringan yang telah dibangun. Untuk mengurangi timbulnya penyalahgunaan jaringan oleh hacker, maka perlu dilakukan peningkatan keamanan jaringan yang akan dibangun.

2.3.2 *Network Forensics*

Network forensics merupakan fase lanjutan dari keamanan jaringan. Keamanan jaringan melindungi sistem dari serangan, sementara *network forensics* berfokus pada perekamanan bukti serangan yang berkaitan dengan menangkap, memantau, dan menganalisis lalu lintas jaringan untuk menemukan serangan keamanan. Menangkap lalu lintas jaringan melalui jaringan secara teori sederhana, tetapi relatif rumit dalam praktiknya.

Penjahat seringkali lebih paham mendahului dari penegakan hukum untuk melindungi mereka sendiri dan meleburkan *evidence*. Pembuktian di dunia maya memiliki ciri khas tersendiri. Ini karena sifat teknologi komputer memungkinkan jejak penjahat disembunyikan. Demikian usaha dalam membuka kejahatan komputer yaitu dengan menguji kemanan sistem dalam peran pendeteksian daripada pengguna. Beberapa klasifikasi kebutuhan digital forensik secara umum meliputi:

a. Kebutuhan investigasi tindak kejahatan dan tindakan pelanggaran hukum.
b. Pemahaman sistem yang baik dengan perangkat digital.
c. Reka ulang peristiwa keamanan dari komputer.
d. Usaha dalam memperbaiki kegagalan sistem.
e. Troubleshooting meliputi perangkat keras dan perangkat lunak.

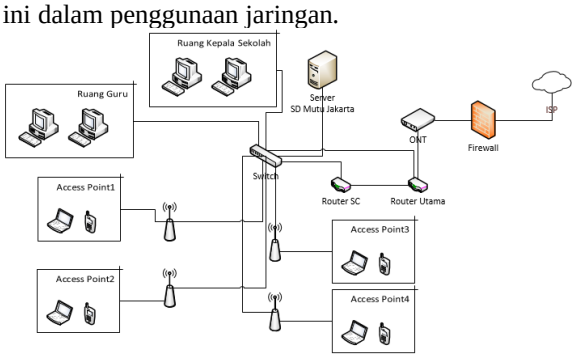
3. HASIL DAN PEMBAHASAN

3.1 Hasil Identifikasi Sistem

Pada tahap ini dilakukan identifikasi sistem jaringan yang berada di SD Muhammadiyah 1 Jakarta sebagai objek penelitian. Terdiri dari komponen berupa kebutuhan perangkat keras dan perangkat lunak.

3.2 Hasil Perancangan Topologi

Tahap ini akan melakukan perancangan topologi sistem keamanan jaringan. Penelitian ini menggunakan Router yang bertindak sebagai target serangan. Saat proses autentikasi dapat menyebabkan hal-hal yang tidak diinginkan, misalnya ada *client* yang mengetahui kata sandi dalam proses otentikasi ini dalam penggunaan jaringan.



Gambar 4. Hasil Topologi Jaringan Baru

Topologi jaringan di atas menjelaskan mengenai topologi serta gambaran mengenai sitem jaringan yangdiamankan. Pada sistem ini menggunakan *Router* untuk membuat konfigurasi sistem keamanan

jaringan serta mengirimkan notifikasi ke email (bukti adanya serangan) dan Aplikasi Telegram untuk monitoring jaringan yang sedang berjalan. Sistem keamanan jaringan *network forensics* ini dikembangkan, dimana Router ditempatkan pada titik yang sesuai pada jaringan agar adminstrator dalam melakukan pemantauan lalu lintas dan dari semua perangkat di jaringan. Idealnya, semua lalu lintas dari luar atau dalam jaringan akan dipindai.

3.3 Hasil Konfigurasi Sistem Keamanan Jaringan

Pada tahap ini dilakukan bagaimana implementasi dan konfigurasi pada routerboard mikrotik RB750G menggunakan perangkat lunak WinBox, yang diterapkan di SD Muhammadiyah 1 Jakarta. Langkah ini melakukan beberapa instalasi dan konfigurasi pada router agar dapat melakukan akses internet.

```
[sdmutujakarta@MIKROTIK SC] > ip address pr
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   ;;; R . KEPSEK
     10.10.0.1/29       10.10.0.0       ether2
 1   ;;; SW R . GURU
     100.100.10.1/28    100.100.10.0    ether3
 2   192.168.100.1/24   192.168.100.0   ether4
 3 D 192.168.1.11/24    192.168.1.0     ether1
```

Gambar 5. Hasil Konfigurasi IP Address

Pengembangan sistem keamanan jaringan difokuskan kepada port yang digunakan sebagai remote access seperti *SSH, telnet, winbox,* ataupun *web config (webfig)*. Pembuatan rules tersebut bertujuan untuk menutup semua akses pada port yang digunakan sebagai *remote access* dan hanya akan dapat dibuka jika host mampu melakukan akses port dengan memasukkan *Username* dan *Password* yang benar. Adapun hasil konfigurasi *Firewall Rule* pada *Router* sebagai berikut:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Pelaku											
0	add src to address list	input			1 (ic...					1648.1 KiB	26 351
;;; Pelaku + Security Accept											
1	add src to address list	input			6 (tcp)		23			48.3 KiB	790
;;; Drop											
2	drop	input			6 (tcp)		8291,22,...			111.6 KiB	1 087
3	drop	input			6 (tcp)		21			308 B	7
4	drop	input			6 (tcp)		22			88 B	2
5	drop	input			6 (tcp)		23			140 B	3
6	drop	input			6 (tcp)		53			5.6 KiB	112
7	drop	input			6 (tcp)		80			3936 B	76
8	drop	input			6 (tcp)		2000			308 B	7
9	drop	input			6 (tcp)		8291			760 B	17
;;; Log Security Alert											
10	log	input			1 (ic...					1555.6 KiB	24 802
;;; Drop_invalid_connections											
11	drop	input								2323.6 KiB	56 396
;;; UDP											
12	accept	input			17 (u...					61.1 MiB	849 986
;;; Allow_limited_pings											
13	accept	input			1 (ic...					1166.2 KiB	19 584
;;; Drop_excess_pings											
14	drop	input			1 (ic...					6.9 KiB	71

Gambar 6. Hasil Konfigurasi Firewall Rule

3.4 Pengujian Sistem Kemanan Jaringan

Tahapan berikutnya melakukan simulasi desain jaringan yang telah dibangun menggunakan Microsoft Visio 2013 dan melakukan konfigurasi pada Router, kemudian diuji dalam sistem keamanan jaringan menggunakan *ssh, telnet* dan *webfig* untuk mengetahui port jaringan terbuka.

Gambar 7. Skenario Pengujian Sistem Keamanan Jaringan

Adapun skenario pengujian sistem yang ditunjukkan pada gambar di atas meliputi tiga tahapan antara lain Pengujian pertama dilakukan pada saat jaringan normal tanpa ada penerapan *network forensics*; Pengujian kedua dilakaukan pada saat jaringan sudah menerapkan *network forensics* dengan mode *Disable Port*; dan Pengujian ketiga dilakukan pada saat jaringan sudah menerapkan *network forensics* namun mode yang digunakan adalah *mode Enable Port*.

3.5 Hasil Perbandingan Analisis Pengujian Jaringan

Berdasarkan hasil analisis dan pengujian jaringan dengan menargetkan *IP Addres Router* 10.10.X.X, mendapatkan hasil bahwa dalam pengujian dan implementasi keamanan jaringan menggunakan tanpa buka atau tutup *port* pada *router* dapat berfungsi dengan optimal. Hasil pengujian perbandingan dapat dilihat pada tabel dibawah ini:

Tabel 1. Hasil Pengujian

Pengujian	Kondisi Akses	Jenis Pengujian	Software Pengujian	Hasil Pengujian
1	Kondisi Normal	*Scanning*	Zenmap	*Discovered open port*
2	Kondisi Normal	*Sniffing*	Wireshark	Tidak Terenskripsi
3	Kondisi Normal	*Authetication*	PuTTy	Berhasil Login
4	Kondisi Normal	*Authetication*	Webfig	Berhasil Login
5	Kondisi *Disable Access*	*Scanning*	Zenmap	*Port Disable*
6	Kondisi *Disable Access*	*Sniffing*	Wireshark	Terenskripsi
7	Kondisi *Disable Access*	*Authetication*	PuTTy	Berhasil Login
8	Kondisi *Disable Access*	*Authetication*	Webfig	Berhasil Login
9	Kondisi *Enable Access*	*Scanning*	Zenmap	*Discovered open port*
10	Kondisi *Enable Access*	*Sniffing*	Wireshark	Tidak Terenskripsi
11	Kondisi *Enable Access*	*Authetication*	PuTTy	Berhasil Login
12	Kondisi *Enable Access*	*Authetication*	Webfig	Berhasil Login

Adanya pengujian ini dan diterapkannya sistem keamanan jaringan menggunakan *network forensics*, sehingga dapat meminimalisir terjadinya serangan/ pemindaian oleh intruder/ penyusup karena dengan menutup celah port router yang berada di jaringan.

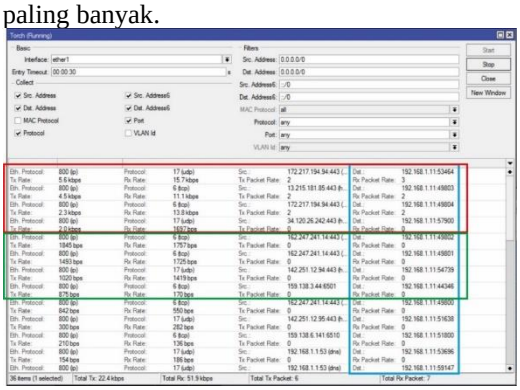
3.6 Hasil Implementasi *Network Forensics*

Implementasi sistem digunakan untuk menerapkan sistem yang telah dibuat sehingga dapat dioperasikan, berikut penjelesannya:

1. Pendeteksian

   Administrator mendeteksi adanya serangan dengan menganalisis aktifitas trafik pada jaringan dengan melihat aliran trafik yang lewat pada suatu interface, memonitoring IP Address yang dituju oleh pengguna, berapa besar *bandwidth* yang digunakan ke suatu IP tertentu,

besar pemakaian bandwidth internet secara keseluruhan pada suatu interface, serta IP Address mana yang yang menggunakan internet paling banyak.



Gambar 8. Akses Ilegal dan Legal

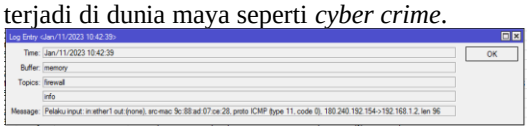
2. Pengecekan

Tahap ini Administrator mencari informasi yang tersembunyi berupa jumlah paket data, urutan paket serta lainnya yang dikirimkan oleh intruder/penyusup masuk ke dalam layanan jaringan komputer sebagai berikut:

Gambar 9. Pengecekan Jumlah Paket Data

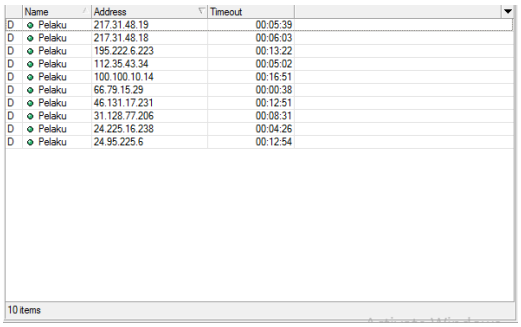
3. Analisis

Setelah melalukan pendeteksian dan pengecekan adanya akses ilegal pada pada router. *Administrator* melakukan perekaman berbagai aktivitas sistem dan informasi status *router*, proses yang terjadi di router dan menyimpan catatan (*Log*). Data *log* berperan penting dalam mengungkap kejahatan yang terjadi di dunia maya seperti *cyber crime*.



Gambar 10. Syslog pada router

Pada Gambar di atas menunjukkan adanya serangan lalu lintas traffic pada jaringan.. IP Gateway biasa dijadikan sebagai target dari suatu aktivitas serangan pada jaringan. Adanya serangan tersebut tentunya memberikan dampak dan pengaruh terhadap performansi jaringan. Berikut gambar di bawah ini menunjukkan hasil pengujian serangan ke router yang bertujuan menemukan informasi *port-port router.* Setelah dilakukan pengujian sebanyak 10 kali informasi yang didapat adalah port-port dalam keadaan tertutup. *Firewall Rule* ini digunakan sebgai pemblokiran IP Address yang dicurigai mengirim paket data tidak wajar pada jaringan *router*.



	Name	Address	Timeout
D	Pelaku	217.31.48.19	00:05:39
D	Pelaku	217.31.48.18	00:06:03
D	Pelaku	195.222.6.223	00:13:22
D	Pelaku	112.35.43.34	00:05:02
D	Pelaku	100.100.10.14	00:16:51
D	Pelaku	66.79.15.29	00:00:38
D	Pelaku	46.131.17.231	00:12:51
D	Pelaku	31.128.77.206	00:08:31
D	Pelaku	24.225.16.238	00:04:26
D	Pelaku	24.95.225.6	00:12:54

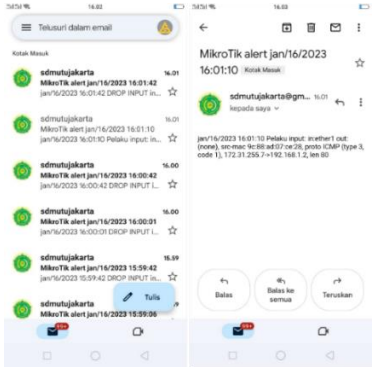
10 items

Gambar 11. Tampilan Serangan pada Router

Pada gambar di atas sudah dilakukan penerapan menggunakan *network forensics* dengan cara *blocking port* untuk jalan masuknya serangan. Dengan demikian *router* akan lebih aman, sebab *administrator* dapat melakukan blocking terhadap *port-port* yang rentan terhadap serangan.

4. Notifikasi

Salah satu tanggung jawab *administrator* adalah mengantisipasi apabila ada gangguan pada jaringan/ server di SD Muhammadiyah 1 Jakarta. Agar administrator dapat melakukan perbaikan/ *maintenance* secepatnya, maka hal ini diperlukan notifikasi jika ada gangguan pada jaringan.



Gambar 12. Notifikasi Serangan ke Gmail

5. Tindakan

Selain itu untuk mendapatkan barang bukti, pengembangan *network forensics* ini dapat mengantisipasi sistem keamanan jaringan dengan cara memblokir *IP Address* dari penyerang agar tidak terjadi serangan yang sama di kemudian hari. Namun diperlukan juga untuk tindakan/ aksi yakni monitoring jaringan yang dapat mempermudah *administrator* dalam memantau sistem jaringan atau mengetahui setiap perubahan yang terjadi di jaringan. Selanjutnya dengan bot telegram dapat monitoring aktivitas router secara *realtime*, seperti pada gambar berikut ini:

Gambar 12. Tampilan Bot Telegram Pilihan Menu

Pada gambar diatas diharapkan *administrator* bisa mendapatkan informasi secepatnya dan bisa melakukan tindakan pencegahan yang juga se-responsif mungkin. Disana administrator dapat memilih pilihan menu antara lain: 1) Menu Info Mikrotik berisikan spesifikasi umum router yang digunakan seperti *type, paltform* dan versi yang digunakan; 2) Menu *Interface* digunakan untuk memonitor kondisi jaringan up atau down; 3) Menu DHCP yang digunakan untuk mengetahui host yang sedag terhubung (aktif) dengan jaringan lokal; 4) Menu *Health* bertujuan untuk memonitoring temperatur pada routerboard seperti *voltage* dan *fan control*; 5) Menu *Run Script* digunakan untuk mengontrol routerboard dengan menggunakan telegram; 6) Menu *Resource Mikrotik* digunakan untuk mengetahui penggunaan *CPU (Central Processing Unit)* yang memberikan pengaruh performa dari perangkat *routerboard* itu sendiri; 7) Menu *Traffic* digunakan monitoring berapa pemakaian trafick setiap user ataupun total *traffic internet* pada suatu jaringan; 8) Menu IP Public yaitu mengetahui IP Publik *routerboard*; 9) Menu *Backup* digunakan untuk mengetahui melakukan *backup* konfigurasi *router* sekarang setiap minggu atau sebulan; 10) Menu *Restart* digunakan untuk melakukan *restart* ulang dari *routerboard*.

3.7 Hasil Analisis Serangan dan Peningkatan Sistem Keamanan Jaringan

Berdasarkan hasil pengujian analisis serangan serta peningkatan keamanan jaringan di SD Muhammadiyah 1 Jakarta, adapun hasil penelitian studi kasus ini berupa laporan *Network Forensics*, yang mengacu pada proses sedang dan sudah dilaksanakan. Hasil analisis ditampilkan pada tabel 2:

Tabel 2. Hasil Analisis

No	Analisis	Keterangan
1	Penyerangan terhadap router menggunakan Zenmap, Wireshark, PuTTy dan Webfig	Berhasil melakukan serangan pada jaringan menjadi *down* karena penyerangan terhadap *router* dilakukan secara bertubi-tubi.
2	Administrator berhasil menangkap aktivitas lalu-lintas yang mencurigakan melalui *network forensics*	Diperoleh informasi adanya serangan pada *router* mulai dari proses penyerangan mengirim paket data serta jumlah paket data untuk me-request akses masuk pada *router*
3	*Protocol* yang diserang	Protocol ICMP dan TCP
4	*Port* yang diserang	Port 443 dan Port 53
5	*Port Destination* target	53464, 49803, 57900
6	*Log Activity*	Ditemukan kegagalan login yang sangat banyak. Kegiatan ini dicurigai sebagai tindakan yang tidak wajar, dimana melakukan komunikasi data pada Protocol DNS 180.240.192.154 terhadap router dengan IP Address Jaringan Local 192.168.1.2
7	a. *IP Address Router*	192.168.1.11/24 10.10.0.1/29 100.100.10.1/28 192.168.100.1/24
	b. *IP Address List* Penyerang	217.31.48.19 217.31.48.18 195.222.6.223 112.35.43.34 100.100.10.14 66.79.15.29 46.131.17.231 31.128.77.206 24.225.16.238 24.95.225.6
	c. *IP Gateway Internet to ISP*	192.168.1.2
	d. *IP Router to ISP (Internet Services Provider)*	100.100.10.1 (Utama) 10.10.0.1 (Cadangan)
	e. *IP Network Administrator*	100.100.10.11
8	Pengembangan sistem keamanan jaringan	Menggunakan *Firewall Rule* dan *Address List*, dengan melakukan notifikasi melalui email adanya penyerangan dan aplikasi telegran untuk memoniroting jaringan 24 jam.
9	Kondisi router setelah menerapkan network forensics	Koneksi terputus dengan IP Address penyerang yang diblokir dan akses diatur berdasarkan waktu timeout yaitu 20 menit.
10	Kondisi CPU dan Memory router MikroTik sebelum ada penyerangan	CPU Load 10% Memory 28/64M
11	Kondisi CPU dan Memory perangkat jaringan saat ada serangan	CPU Load 97% Memory 36/64M
12	Peningkatan sistem keamanan jaringan	Menggunakan *Network Forensics*

No	Analisis	Keterangan
13	Kondisi CPU dan Memory perangkat jaringan setelah menerapkan *network forensics*	CPU turun menjadi 1% Memory 27/64M

Berdasarkan data hasil pengujian yang dilakukan dan peningkatan sistem keamanan jaringan menggunakan *network forensics* tercapai sesuai yang diinginkan. Semua sistem keamanan yang dibuat dapat berjalan dengan baik.

4. KESIMPULAN

Hasil penelitian studi kasus ini tentang pengembangan sistem keamanan jaringan menggunakan *Network Forensics*, dapat disimpulkan sebagai berikut: 1) Penerapan dan pengembangan sistem keamanan jaringan menggunakan *network forensics* bertujuan untuk menemukan intuder/ penyusup dan merekonstruksi tindakan serangan melalui analisis bukti penyusupan. Hal ini terbukti penyusup akan masuk ke dalam *Address List* Pelaku, karena *Firewall Filter* akan memblokir IP Address yang dicurigai mengirim paket data tidak wajar pada jaringan; 2) Metode yang diterapkan pada sistem keamanan jaringan menggunakan Network Forensics meliputi pendeteksian, pengecekan, analisis, notifikasi dan tindakan.; 3) Sistem jaringan yang sedang berjalan dilakukan pengujian dan analisis degan target beberapa port yang terbuka (*open*). *Network forensics* yang dikembangkan dalam penelitian ini mampu mendeteksi dan memblokir saat terjadinya penyerangan/ penyusupan sehingga setelah diterapkan notifikasi *email* secara *realtime*, monitoring jaringan yang dapat mempermudah dalam memantau sistem jaringan menggunakan aplikasi Telegram.

Saran dalam mengembangkan sistem keamanan jaringan lebih lanjut, yaitu: 1) Administrator jaringan hendaknya meningkatkan sistem keamanan jaringan menggunakan network forensics karena dapat menjadi salah satu alternatif dalam membantu keberlangsungan lalu lintas jaringan. Hal ini meminimalisir terjadinya penyalahgunaan akses router dari pihak yang tidak bertanggung jawab; 2) Diharapkan ada pengujian lagi dengan metode yang berbeda untuk mencari kekurangan dan kelemahan dalam sistem keamanan jaringan; 3) Sistem jaringan studi kasus penelitian ini masih menggunakan jaringan lingkup kecil, jadi hasil yang diperoleh masih belum maksimal. Diharapkan kepada peneliti selanjutnya untuk pengembangkan metode analisa dengan perbandingan metode logging yang lainnya menggunakan jaringan yang lebih besar.

UCAPAN TERIMA KASIH

Penulis menyampaikan terimakasih kepada Sekolah Tinggi Manajemen Informasi dan Komputer Jakarta STI&K dan SD Muhammadiyah 1 Jakarta yang memberikan ruang informasi untuk menyelesaikan pada studi kasus kali ini, penulis menyampaikan ucapan terimakasih kepada tim jurnal yang sudah bersedia memuat tulisan ini.

DAFTAR PUSTAKA

[1] S. Aji, A. Fadlil, and I. Riadi, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 11, 2017, doi: 10.26555/jiteki.v3i1.5665.

[2] B. Kurniawan and D. Herryanto, "Perancangan Dan Implementasi Data Center Menggunakan File Transfer Protocol (Ftp)," *J. Sist. Komput. Musirawas*, vol. 2, no. 2, pp. 91–97, 2017.

[3] J. Ekonomi *et al.*, "Sistem Informasi Perusahaan Pada E - Bussines," vol. 2, no. 1, pp. 27–30, 2023.

[4] G. H. A. Kusuma, "… Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19," *J. Informatics Adv. …*, vol. 2, no. 2, pp. 1–4, 2021, [Online]. Available: http://journal.univpancasila.ac.id/index.php/jiac/article/view/3259.

[5] J. Lu, "Research and Implementation of Security Technology in Campus Network Construction," *Proc. - 2nd Int. Conf. Comput. Network, Electron. Autom. ICCNEA 2019*, pp. 219–224, 2019, doi: 10.1109/ICCNEA.2019.00050.

[6] A. P. Surya, S. C. Relmasira, and A. T. A. Hardini, "Penerapan Model Pembelajaran Project Based Learning (PjBL) untuk Meningkatkan Hasil Belajar dan Kreatifitas Siswa Kelas III SD Negeri Sidorejo Lor 01 Salatiga," *J. Pesona Dasar*, vol. 6, no. 1, pp. 41–54, 2018, doi: 10.24815/pear.v6i1.10703.

[7] E. K. Dewi, "Kata kunci : Network Forensic, Instrution Detection System(IDS), Snort, Rancangan Keamanan.," vol. 2, pp. 34–41, 2016.

[8] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, 2022, doi: 10.14421/jiska.2022.7.1.46-55.