Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)

by Tri Widodo

Submission date: 18-Apr-2022 02:43PM (UTC+0700)
Submission ID: 1813344598
File name: 7-1-46-55-3045_-_Jiska_2022.pdf (457.23K)
Word count: 3593
Character count: 23089

JISKa, Vol. 7, No. 1, JANUARI, 2022, Pp. 46 – 55
ISSN: 2527 – 5836 (print) | 2528 – 0074 (online)

Pemanfaatan *Network Forensic Investigation Framework* untuk Mengidentifikasi Serangan Jaringan Melalui *Intrusion Detection System* (IDS)

Tri Widodo [(1)*], Adam Sekti Aji [(2)]
[1] Pendidikan Teknologi Informasi, Fakultas Bisnis dan Humaniora, Universitas Teknologi Yogyakarta, Yogyakarta
[2] Informatika, Fakultas Sains dan Teknologi, Universitas Teknologi Yogyakarta, Yogyakarta
e-mail : triwidodo@uty.ac.id, adamaji@staff.uty.ac.id.
* Penulis korespondensi.
Artikel ini diajukan 8 September 2021, direvisi 15 November 2021, diterima 15 November 2021, dan dipublikasikan 25 Januari 2022.

Abstract

Intrusion Detection System (IDS) is one of the technology to ensure the security of computers. IDS is an early detection system in the event of a computer network attack. The IDS will alert the computer network administrator in the event of a computer network attack. IDS also records all attempts and activities aimed at disrupting computer networks and other computer network attacks. The purpose of this study is to implement IDS on network systems and analyze IDS logs to determine the different types of computer network attacks. Logs on the IDS will be analyzed and will be used as leverage to improve computer network security. The research was carried out using the Network Forensic Investigation Framework proposed by Pilli, Joshi, and Niyogi. The stages of the Network Forensic Investigation Framework are used to perform network simulations, analysis, and investigations to determine the types of computer network attacks. The results show that the Network Forensic Investigation Framework facilitates the investigation process when a network attack occurs. The Network Forensic Investigation Framework is effectively used when the computer network has network security support applications such as IDS or others. IDS is effective in detecting network scanning activities and DOS attacks. IDS gives alerts to administrators because there are activities that violate the rules on the IDS.

Keywords: Network Forensic Investigation Framework, Intrusion Detection System (IDS), Network Attack, Network Scanning, DOS Attacks

Abstrak

Salah satu media untuk mengamankan komputer adalah menerapkan teknologi *Intrusion Detection System* (IDS). IDS merupakan sistem deteksi dini jika terjadi serangan jaringan komputer. IDS akan memberi peringatan kepada administrator jaringan komputer jika terjadi serangan jaringan komputer. IDS juga mencatat semua upaya dan kegiatan-kegiatan yang bertujuan mengganggu jaringan komputer maupun serangan jaringan komputer lainnya. Tujuan penelitian ini yaitu mengimplementasikan IDS pada sistem jaringan dan menganalisis catatan (*log*) IDS untuk mengetahui jenis-jenis dan tipe serangan jaringan komputer. *Log* pada IDS akan dianalisis secara mendalam untuk digunakan sebagai upaya meningkatkan keamanan jaringan komputer. Metode penelitian yang akan digunakan adalah penelitian terapan (*applied research*). Pelaksanaan penelitian menggunakan *Network Forensic Investigation Framework* yang dikemukakan oleh Pilli, Joshi dan Niyogi. Tahapan-tahapan *Network Forensic Investigation Framework* digunakan untuk melakukan simulasi jaringan, analisis dan investigasi untuk mengetahui jenis-jenis serangan jaringan komputer. Hasil penelitian menunjukkan *Network Forensic Investigation Framework* memudahkan proses investigasi ketika terjadi serangan jaringan. *Network Forensic Investigation Framework* efektif digunakan ketika jaringan komputer memiliki aplikasi pendukung keamanan jaringan seperti IDS atau yang lainnya. IDS efektif mendeteksi adanya aktivitas *network scanning* dan serangan DOS. IDS memberikan alert pada administrator karena ada aktivitas yang melanggar *rule* pada IDS.

Kata Kunci: *Network Forensic Investigation Framework*, *Intrusion Detection System* (IDS), *Network Attack*, *Network Scanning*, Serangan DOS

1. PENDAHULUAN

Internet merupakan kebutuhan yang sangat penting pada era digital seperti sekarang. Revolusi industri 4.0 mengharuskan setiap orang terhubung ke jaringan internet setiap saat untuk berkomunikasi. Institusi atau perusahaan menjadikan internet sebagai bagian dari infrastruktur untuk meningkatkan produktivitas karyawan dan perusahaan. Tingginya kebutuhan internet terkadang dimanfaatkan oleh pihak-pihak tertentu untuk serangan jaringan komputer. Serangan jaringan komputer meningkat secara signifikan pada era digital seperti ini. Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat ada 88.414.296 serangan siber di Indonesia yang terjadi sejak 1 Januari hingga 12 April 2020. Pada Januari terpantau ada 25.224.811 serangan dan kemudian pada Februari terekam 29.188.645 serangan. Lalu, pada Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 tercatat ada 7.576.851 serangan (Iskandar, 2020). Para *hacker* tidak hanya menargetkan serangan untuk melumpuhkan jaringan komputer suatu perusahaan. Mereka juga berusaha untuk mencuri berbagai data dari server.

Administrator jaringan komputer memiliki tugas dan tanggung jawab yang penting pada sebuah institusi atau perusahaan. Administrator jaringan bertanggung jawab atas desain, perencanaan, operasi, keamanan, dan manajemen sehari-hari dari jaringan, server, *switch*, jaringan internet organisasi dan semua komunikasi data. Salah satu tugas berat administrator jaringan komputer adalah mengamankan infrastruktur jaringan komputer dan data perusahaan dari serangan jaringan komputer. Serangan jaringan komputer atau *network attack* adalah upaya untuk mendapatkan akses tidak sah ke jaringan organisasi, dengan tujuan mencuri data atau melakukan aktivitas berbahaya lainnya. Intrusi adalah upaya tidak sah, upaya ilegal untuk mengakses, memanipulasi atau menguasai sistem/jaringan informasi untuk membuat mereka tidak dapat diandalkan atau tidak dapat digunakan (Kumar, 2017). Ada banyak bentuk implementasi keamanan jaringan mulai dari sistem AAA (*Authentication, Authorization & Accounting*), *Firewalls*, *Routing Filters*, *Access Control*, *Intrusion Prevention System*, *Intrusion Detection Systems*, *Honeypot*, dan lain-lain (Alsyaibani et al., 2021).

Administrator jaringan komputer dapat mengimplementasikan *Intrusion Detection System* (IDS) untuk mengetahui adanya serangan jaringan komputer (Lazzez, 2013). IDS akan memberikan *alert* (peringatan) kepada administrator jaringan jika terjadi serangan atau gangguan terhadap jaringan. Teknik pendeteksian pada IDS umum masih jauh dari sempurna jika dibandingkan dengan berbagai anomali dan alat modern yang digunakan oleh penyerang karena IDS masih menggunakan deteksi berbasis tanda tangan atau model deteksi berbasis anomali (Chowdhury et al., 2017).

Administrator jaringan dapat melakukan analisis terhadap catatan (*log*) yang direkam oleh IDS. Hasil analisis *log* IDS dapat digunakan untuk mengetahui jenis-jenis serangan jaringan komputer yang ditujukan ke jaringan komputer, sehingga administrator jaringan dapat melakukan perbaikan, pengaturan ulang jaringan, dan mengimplementasikan aplikasi-aplikasi tertentu untuk meningkatkan keamanan jaringan komputer yang dikelola.

Berbagai penelitian tentang *Intrusion Detection System* sudah pernah dilakukan. Penelitian yang dilakukan oleh Khaerani & Handoko (2015) dengan judul 'Implementasi dan Analisa *Data Mining* untuk Klasifikasi Serangan Pada *Intrusion Detection System* (IDS) dengan Algoritma C4.5' menggunakan data tahun 1999. Saat itu penggunaan internet belum semasif sekarang, jenis serangan jaringan komputer juga masih terbatas. Selanjutnya penelitian dilakukan Muhammad, (2016) yang secara khusus menganalisis *log* IDS berbasis *neural network* untuk mengetahui serangan DDOS. Sayangnya penelitian ini juga hanya mengkhususkan serangan jaringan DDOS, selain itu penelitian juga bersifat prediksi terhadap potensi serangan tersebut, sehingga penelitian sulit diimplementasikan dan tidak dapat mengetahui jenis-jenis serangan jaringan lainnya. Penelitian serupa juga dilakukan oleh Purba & Efendi (2021), penelitian ini juga berfokus pada serangan DDOS. Penelitian selanjutnya dilakukan oleh Suhartono & Patta (2017), para peneliti melakukan penelitian dengan membatasi lingkup serangan pada serangan melalui dua *port* jaringan yaitu, SSH dan FTP sehingga membuat penelitian tersebut lebih menarik.

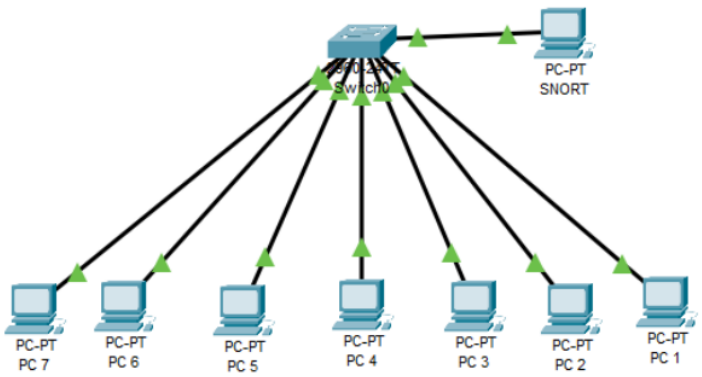
Penelitian yang dilakukan ini berfokus dalam mengimplementasikan konsep *Network Forensic Investigation Framework* dan Snort IDS dalam mendeteksi berbagai jenis serangan jaringan. Penelitian ini juga menggabungkan aspek keamanan jaringan komputer dengan aspek forensik digital. Penelitian ini tidak ditujukan untuk menguji IDS dengan serangan tertentu, tetapi difokuskan pada contoh pemanfaatan IDS dan juga bagaimana melakukan investigasi serangan jaringan secara efektif dan mudah menggunakan *Network Forensic Investigation Framework*.

2. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah penelitian terapan. Menurut Irina (2017) penelitian terapan atau *applied research* dilakukan berkenaan dengan kenyataan-kenyataan praktis penerapan dan pengembangan ilmu pengetahuan yang dihasilkan oleh penelitian dasar dalam kehidupan nyata. Penelitian terapan berfungsi untuk mencari solusi tentang masalah-masalah tertentu. Tujuan utamanya adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau kelompok maupun untuk keperluan industri atau politik dan bukan untuk wawasan keilmuan semata. Penelitian ini akan menggunakan *Network Forensic Investigation Framework* yang dikemukakan Pilli et al. (2010) dengan menggunakan 9 (sembilan) tahapan.

2.1. *Preparation and Authorization* (Persiapan dan Otorisasi)

Pada tahap ini akan buat sistem jaringan yang terdiri dari 7 PC *client*, 1 buah *switch*, dan 1 PC yang ter-*install* Snort IDS seperti terlihat pada Gambar 1. *Framework* ini juga mengharuskan otorisasi dan akses penuh terhadap sistem jaringan dan Snort IDS.



Gambar 1. Desain Topologi Jaringan Simulasi.

Spesifikasi perangkat pada topologi jaringan dapat dilihat pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Jaringan.

No	Perangkat	Alamat IP	Perangkat Lunak
1	Komputer Server	192.168.56.1	1. Sistem Operasi Ubuntu 2. Snort IDS
2	Komputer *Client* 1	192.168.56.100	Windows 10
3	Komputer *Client* 2	192.168.56.101	Linux
4	Komputer *Client* 3	192.168.56.102	Windows 10
5	Komputer *Client* 4	192.168.56.103	Windows 10
6	Komputer *Client* 5	192.168.56.104	Windows 10
7	Komputer *Client* 6	192.168.56.105	Linux
8	Komputer *Client* 7	192.168.56.106	Windows 10
9	*Switch*	-	-

2.2. *Detection and Incident/Crime* (Deteksi Insiden/Kejahatan)

Setelah jaringan dan Snort IDS ter-*install* dan terkonfigurasi, akan dilakukan berbagai simulasi serangan jaringan. Uji coba akan menggunakan teknik serangan jaringan sederhana yaitu *network scanning* dan serangan DOS. IDS akan ditambahkan dengan *rule* untuk mendeteksi adanya *network scanning* dan serangan DOS. IDS akan menganalisis aktivitas jaringan berdasarkan *rule* yang diberikan dan memberikan *alert* (peringatan) kepada administrator jika ada aktivitas yang melanggar *rule*.

2.3. *Incident Response* (Penanganan Insiden)

Insiden respon dini yang dilakukan adalah adanya *alert* (peringatan) dari Snort IDS. Respon selanjutnya yang akan dilakukan adalah mengubah dan memodifikasi *rule* (aturan) pada Snort IDS. Perubahan beberapa *rule* digunakan untuk mengetahui kemampuan dan fungsi Snort IDS.

2.4. *Collection of Network Traces* (Koleksi Jejak Jaringan)

Setelah serangan jaringan komputer, dilakukan pelacakan dan verifikasi kesesuaian sumber serangan, jenis serangan, dan peringatan yang diberikan Snort IDS.

2.5. *Preservation and Protection* (Pengamanan dan Perlindungan Data)

Tahap ini berisi pengamanan data yang menjadi bukti serangan jaringan. Bukti ini berupa *log* (catatan) dan peringatan yang diberikan oleh Snort IDS. Pengamanan ini perlu dilakukan karena beberapa serangan dapat memungkinkan penyerang untuk menghapus jejak dan bukti.

2.6. *Examination* (Pemeriksaan)

Pemeriksaan data digunakan untuk memisahkan data aktivitas normal dan data serangan jaringan komputer. Pemeriksaan ini juga digunakan untuk mengetahui adanya sumber data lain selain *log* (catatan) IDS yang dapat digunakan untuk membantu proses analisis.

2.7. *Analysis* (Analisis)

Bukti-bukti yang sudah terkumpul, kemudian dianalisis menggunakan berbagai Teknik dan perangkat bantu (*tool*). Analisis ini menggunakan berbagai parameter seperti jenis koneksi jaringan, sistem operasi, dan protokol jaringan yang digunakan.

2.8. *Investigation and Attribution* (Investigasi dan Atribusi)

Hasil analisis kemudian diinvestigasi untuk mengetahui komputer mana yang melakukan serangan, siapa pemilik komputer tersebut, serangan jenis apa yang digunakan, dampak serangan tersebut bagi sistem, dan bagaimana cara mengatasi serangan tersebut selanjutnya.

2.9. *Presentation* (Presentasi)

Hasil analisis akan dibuat laporan dan penjelasan yang lebih mudah dipahami oleh berbagai pihak terkait. Presentasi juga memuat saran dan tindakan perbaikan yang berguna untuk meningkatkan tingkat keamanan jaringan.

3. HASIL DAN PEMBAHASAN

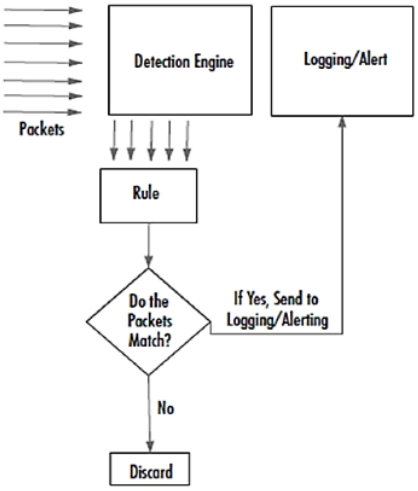
Intrusion Detection System (IDS) adalah perangkat atau aplikasi perangkat lunak yang memantau lalu lintas data pada jaringan komputer untuk mengetahui aktivitas berbahaya atau pelanggaran kebijakan (Barracuda Networks, 2021). Ada beberapa jenis IDS, yaitu:

1) *Network Intrusion Detection Systems* (NIDS), yaitu IDS yang menganalisis lalu lintas data jaringan komputer.
2) *Host-Based Intrusion Detection Systems* (HIDS), yaitu IDS yang memantau file sistem operasi.

Intrusion Detection System (IDS) dalam mendeteksi menggunakan metode *signature based* dan *anomaly based* (Alviana & Sumitra, 2018). Menurut Alviana & Sumitra (2018) metode *anomaly based* merupakan metode dalam mendeteksi serangan melalui pola lalu lintas jaringan di luar kebiasaan, sedangkan metode *signature based* merupakan metode dalam mendeteksi serangan melalui pola atau paket data yang dibaca kemudian dibandingkan dengan data atau paket yang sudah tersimpan dalam *database* yang ada atau *rule* yang sudah ada.

Snort merupakan salah satu sistem deteksi intrusi (IDS) *open source* yang banyak digunakan untuk mendeteksi intrusi atau aktivitas mencurigakan pada lalu lintas jaringan (Paramitha et al., 2020). Snort merupakan salah contoh program dari *Network-based Intrusion Detection System* (Sandi & Arrofiq, 2018). Cara kerja Snort mirip dengan TcpDump, tetapi fokus sebagai *security packet sniffing*. Fitur utama Snort yang membedakan dengan TcpDump adalah *payload inspection*, di mana Snort melakukan analisis *payload rule set* yang disediakan (Dewi, 2017).

Menurut Singh & Tomar (2015), Snort bekerja sebagai *detection engine* dengan IDS *mode*, Ketika terdapat *packet* datang melalui *switch* maka akan terdeteksi oleh *detection engine* pada Snort, kemudian Snort sebagai IDS akan mencocokkan *packet* tadi dengan dengan *rules* yang sudah diatur. Ketika *packet* tersebut tidak sesuai *rule* (*packet* mengandung konten serangan) maka akan tersimpan di *log* Snort dan akan membangkitkan *alarm*, namun jika *packet* tersebut sesuai *rule* (tidak mengandung konten serangan) maka *packet* tersebut di-*discard* (diabaikan) dan langsung diteruskan.



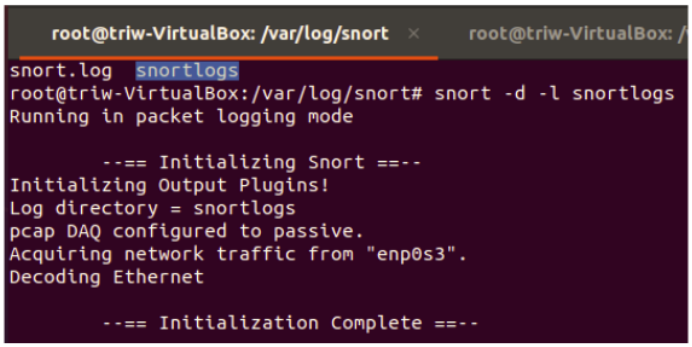
Gambar 2. Cara Kerja Mesin Deteksi Snort (Singh & Tomar, 2015).

Data *log* IDS Snort ini dapat dimanfaatkan oleh administrator jaringan untuk menganalisis performa sistem keamanan jaringan (Paramitha et al., 2020).

Network Forensic Investigation Framework yang dikemukakan Pilli et al. (2010) yang menggunakan 9 (sembilan) tahapan, implementasinya dijelaskan sebagai berikut.

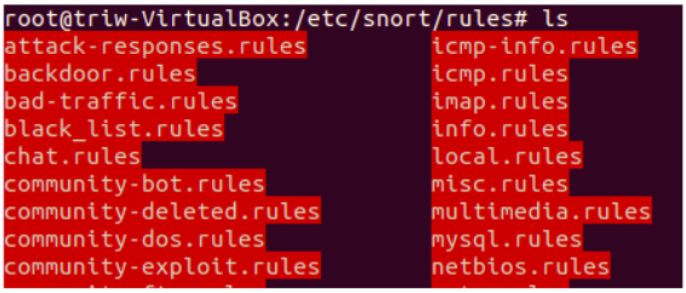
3.1. *Preparation and Authorization* (Persiapan dan Otorisasi)

Jaringan komputer secara umum dilengkapi dengan berbagai aplikasi pengaman, seperti *firewall*, *anti-virus*, *proxy* atau IDS. Seorang administrator jaringan harus memiliki akses dan kendali penuh terhadap jaringan komputer yang dikelola. Administrator juga memastikan berbagai aplikasi pengaman tersebut aktif. Pada Gambar 3 terlihat IDS Snort dalam posisi aktif dan merekam segala aktivitas jaringan komputer.



Gambar 3. Mengaktifkan *logging mode* pada Snort.

IDS Snort bekerja berdasarkan *rule* atau aturan yang ditentukan oleh administrator. *Rule* tersebut yang akan menjadi patokan kerja IDS, seperti menolak paket, meneruskan paket atau memberikan *alert*. *Rule* tersebut dapat dipisah menjadi beberapa aturan seperti terlihat pada Gambar 4.



Gambar 4. Konfigurasi *rule* pada Snort.

3.2. *Detection and Incident/Crime* (Deteksi insiden / kejahatan)

IDS Snort akan mendeteksi berbagai serangan berdasarkan pada *rule* yang telah ditentukan. Snort akan memberikan *alert* atau peringatan pada administrator terkait serangan atau akses tertentu pada jaringan seperti terlihat pada Gambar 5. Pada penelitian ini PC 4 mencoba melakukan enumerasi pada komputer server dengan melakukan *scanning*. Proses *scanning* tersebut dapat dengan baik dideteksi oleh Snort IDS. Selanjutnya PC 4 juga melakukan pengiriman *ping* secara terus menerus yang dapat diindikasikan sebagai serangan DOS.

Gambar 5. Alert yang muncul pada *console* yang mendeteksi adanya serangan.

3.3. *Incident Response* (Penanganan Insiden)

Ketika administrator menerima *alert* atau *alarm* dari IDS. Administrator dapat menindaklanjuti dengan beberapa Tindakan, seperti *blocking port* seperti pada Gambar 6, *blocking* IP, atau menonaktifkan beberapa *protocol*.

```
root@triw-VirtualBox:/home/triw# ufw deny 23/tcp
Rule updated
Rule updated (v6)
```

Gambar 6. Respon berupa penutupan *port* tertentu.

Admisntrator juga dapat menindaklanjuti dengan merubah beberapa *rule* agar keamanan jaringan lebih optimal seperti Gambar 7.

```
root@triw-VirtualBo...   root@triw-VirtualBo...   root@triw-VirtualBo...
  GNU nano 4.8                        local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
#percobaan rule baru
log tcp any any -> 192.168.56.0/24 !6000:6010
alert tcp any any -> 192.168.56.103 23 (msg: "Ada yang telnet ke mesin!"; sid:>
alert icmp any any <> 192.168.56.103 any (msg:"Ada yang ECHO PING"; icode:0; i>
alert icmp any any <> 192.168.56.103 any (msg:"Ada yang ECHO REPLY PING"; icod>
```

Gambar 7. Penyesuaian dan perubahan *rule* Snort untuk mengantisipasi serangan jaringan.

3.4. *Collection of Network Traces* (Koleksi Jejak Jaringan)

Semua aktivitas jaringan akan direkam IDS Snort pada *log* atau catatan seperti terlihat pada Gambar 8.

```
root@triw-VirtualBox:/var/log/snort/snortlogs# ls -l
total 308184
-rw-r--r-- 1 root snort         0 Sep  4 01:21 alert
-rwsrwxr-t 1 root snort       787 Sep  1 17:16 snort.log.1630491357
-rw------- 1 root snort      1899 Sep  1 17:43 snort.log.1630492975
-rw------- 1 root snort  50641079 Sep  2 17:07 snort.log.1630566064
-rw------- 1 root snort 129963719 Sep  4 01:23 snort.log.1630689641
-rw------- 1 root snort 134216566 Sep  4 01:52 snort.log.1630694117
-rw------- 1 root snort    730999 Sep  4 02:55 snort.log.1630695145
```

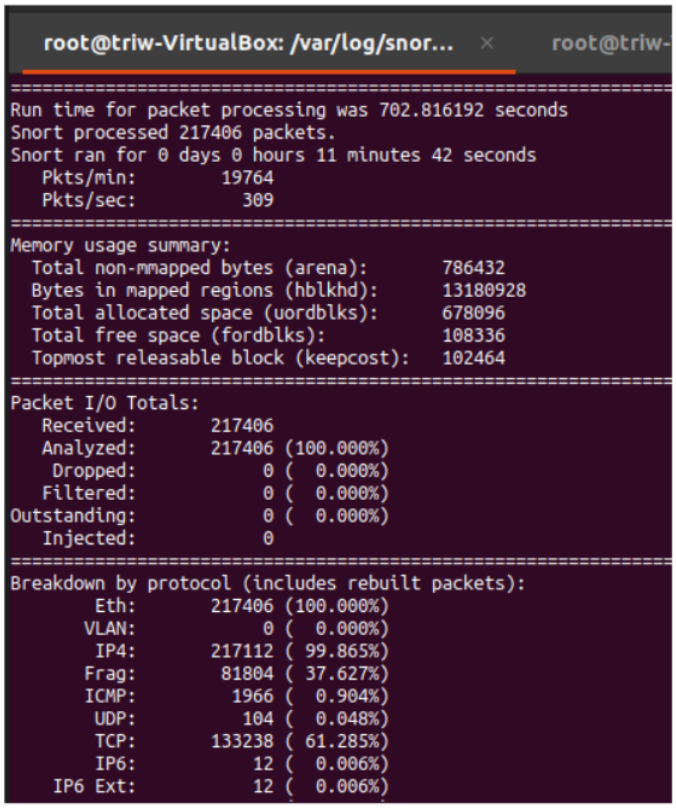
Gambar 8. *Log* (catatan) aktivitas *log* yang didapat dari Snort.

3.5. *Preservation and Protection* (Pengamanan dan Perlindungan Data)

Tugas selanjutnya administrator ketika mengidentifikasi adanya serangan atau gangguan jaringan adalah mengamankan *log* atau catatan yang direkam oleh IDS Snort, karena catatan tersebut akan menjadi data penting bagi administrator untuk mengetahui jenis serangan, sumber serangan dan *protocol* yang menjadi sasaran.

3.6. *Examination* (Pemeriksaan)

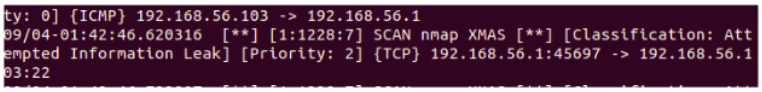
Administrator jaringan setelah mendapatkan catatan atau *log* IDS Snort selanjutnya melakukan pemeriksaan dan identifikasi aktivitas jaringan komputer. *Log* IDS Snort akan memberikan informasi aktivitas jaringan seperti besar paket maupun *protocol* yang digunakan seperti pada Gambar 9.



Gambar 9. Hasil rekap aktivitas jaringan yang dicatat Snort.

3.7. *Analysis* (Analisis)

Administrator melalui *log* mengetahui sumber IP penyerang yaitu 192.168.56.103, aktivitas yang dilakukan adalah scanning port pada server 192.168.56.1 seperti pada Gambar 10.



Gambar 10. Gambar 10. Identifikasi sumber serangan jaringan.

3.8. *Investigation and Attribution* (Investigasi dan Atribusi)

Administrator mengidentifikasi bahwa PC 4 192.168.56.103 telah melakukan pengiriman paket sebanyak 217406 kali dengan durasi 11 menit 42 detik. Administrator mengidentifikasi *host* dengan IP 192.168.56.103 juga telah mengirimkan paket sebesar 13180928 bytes atau sekkitar 206 MB yang dapat diindikasikan merupakan *packet flooding* atau jenis serangan DOS. PC 4 juga terindikasi melakukan enumerasi dengan melakukan *scanning.* Hal itu patut dicurigai bahwa PC 4 berusaha mencari celah keamanan dari komputer server.

3.9. *Presentation* (Presentasi)

Langkah *digital forensic* terakhir administrator adalah membuat laporan hasil investigasi agar dapat dilaporkan pada pimpinan dan ditindaklanjuti dengan pembaharuan keamanan jaringan.

4. KESIMPULAN

Penelitian ini menunjukkan *Network Forensic Investigation Framework* memudahkan proses investigasi ketika terjadi serangan jaringan. *Network Forensic Investigation Framework* efektif digunakan ketika jaringan komputer memiliki aplikasi pendukung keamanan jaringan seperti IDS atau yang lainnya. IDS efektif mendeteksi adanya aktivitas *network scanning* dan serangan DOS. IDS memberikan *alert* pada administrator karena ada aktivitas yang melanggar *rule* pada IDS. Catatan atau *log* IDS mempermudah proses investigasi sehingga serangan jaringan dapat terlacak sampai pada sumber serangan dan media serangan. Penelitian selanjutnya diharapkan dapat mengkolaborasikan perangkat keamanan jaringan dengan perangkat kecerdasan buatan atau *machine learning*. Penelitian-penelitian yang menggabungkan aplikasi keamanan jaringan komputer dan kecerdasan buatan atau *machine learning* sangat penting terutama untuk mendeteksi pornografi maupun serangan *malware*.

UCAPAN TERIMA KASIH

Terima kasih kami sampaikan kepada Direktorat Sumber Daya Direktorat Jenderal Pendidikan Tinggi yang telah memberikan dukungan penelitian melalui skema Penelitian Dosen Pemula tahun 2021 sesuai dengan Kontrak Penelitian Tahun Tunggal Penelitian Dasar dan Pemberdayaan/Kapasitas Tahun Anggaran 2021 dengan LLDIKTI Wilayah V Nomor 006/E4.1/AK.04.PT/2021, tanggal 12 Juli 2021 dan segenap pihak yang telah membantu penelitian ini.

DAFTAR PUSTAKA

Alsyaibani, O. M. A., Utami, E., & Hartanto, A. D. (2021). Survey on Deep Learning Based Intrusion Detection System. *Telematika*, *14*(2), 86–100. https://doi.org/10.35671/telematika.v14i2.1317

Alviana, S., & Sumitra, I. D. (2018). ANALISIS PENGUKURAN PENGGUNAAN SUMBER DAYA KOMPUTER PADA INTRUSION DETECTION SYSTEM DALAM MEMINIMALKAN SERANGAN JARINGAN. *Komputa : Jurnal Ilmiah Komputer Dan Informatika*, *7*(1), 27–34. https://doi.org/10.34010/komputa.v7i1.2533

Barracuda Networks. (2021). *What is an Intrusion Detection System?* Barracuda Networks, Inc. https://www.barracuda.com/glossary/intrusion-detection-system

Chowdhury, F. Z., Kiah, L. B. M., Ahsan, M. A. M., & Bin Idris, M. Y. I. (2017). Economic denial of sustainability (EDoS) mitigation approaches in cloud: Analysis and open challenges. *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, 206–211. https://doi.org/10.1109/ICECOS.2017.8167135

Dewi, E. K. (2017). ANALISIS LOG SNORT MENGGUNAKAN NETWORK FORENSIC. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *2*(2). https://doi.org/10.29100/jipi.v2i2.370

Irina, F. (2017). *Metode Penelitian Terapan.* (1st ed.). Parama Ilmu.

Iskandar. (2020). *Indonesia Dibombardir 88,4 Juta Serangan Siber, Ini Detailnya*. Liputan6.Com. https://www.liputan6.com/tekno/read/4235211/indonesia-dibombardir-884-juta-serangan-siber-ini-detailnya

Khaerani, I., & Handoko, B. (2015). Implementasi dan Analisa Hasil Data Mining untuk Klasifikasi Serangan pada Intrusion Detection System (IDS) dengan Algoritma C4. 5. *Techno.COM*, *14*(3), 181–188. https://doi.org/10.33633/tc.v14i3.943

Kumar, D. A. (2017). INTRUSION DETECTION SYSTEMS: A REVIEW. *International Journal of Advanced Research in Computer Science*, *8*(8), 356–370. https://doi.org/10.26483/ijarcs.v8i8.4703

Lazzez, A. (2013). A Survey about Network Forensics Tools. *International Journal of Computer and Information Technology*, *2*(1), 2279–2764.

Muhammad, A. W. (2016). ANALISIS STATISTIK LOG JARINGAN UNTUK DETEKSI SERANGAN DDOS BERBASIS NEURAL NETWORK. *ILKOM Jurnal Ilmiah*, *8*(3), 220–225. https://doi.org/10.33096/ilkom.v8i3.76.220-225

Paramitha, I. A. S. D., Sasmita, G. M. A., & Raharja, I. M. S. (2020). Analisis Data Log IDS Snort dengan Algoritma Clustering Fuzzy C-Means. *Majalah Ilmiah Teknologi Elektro*, *19*(1), 95.

https://doi.org/10.24843/MITE.2020.v19i01.P14
Pilli, E. S., Joshi, R., & Niyogi, R. (2010). A Generic Framework for Network Forensics. *International Journal of Computer Applications*, *1*(11), 1–6. https://doi.org/10.5120/251-408
Purba, W. W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI*, *17*(2), 143–158. https://doi.org/10.24246/aiti.v17i2.143-158
Sandi, D. V., & Arrofiq, M. (2018). Implementasi Analisis NIDS Berbasis Snort Dengan Metode Fuzy Untuk Mengatasi Serangan LoRaWAN. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(3), 685–696. https://doi.org/10.29207/resti.v2i3.504
Singh, R. R., & Tomar, D. S. (2015). Network Forensics: Detection and Analysis of Stealth Port Scanning Attack. *International Journal of Computer Networks and Communications Security*, *3*(2), 33–42.
Suhartono, S., & Patta, A. R. (2017). SISTEM PENGAMANAN JARINGAN ADMIN SERVER DENGAN METODE INTRUSION DETECTION SYSTEM (IDS) SNORT MENGGUNAKAN SISTEM OPERASI CLEAROS. *Jurnal Teknologi Elekterika*, *14*(2), 145. https://doi.org/10.31963/elekterika.v14i2.1220

Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)

ORIGINALITY REPORT

15%	13%	3%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	akurat.co Internet Source	1%
2	Submitted to Universitas Negeri Padang Student Paper	1%
3	ojs.unud.ac.id Internet Source	1%
4	journal2.uad.ac.id Internet Source	1%
5	openjournal.unpam.ac.id Internet Source	1%
6	journal.ipb.ac.id Internet Source	1%
7	bksmpn2salam.blogspot.com Internet Source	1%
8	Submitted to Sriwijaya University Student Paper	<1%
	duniafintech.com	

9	Internet Source	<1%
10	ejournal.amikompurwokerto.ac.id Internet Source	<1%
11	researcher.life Internet Source	<1%
12	www.ojs.uma.ac.id Internet Source	<1%
13	text-id.123dok.com Internet Source	<1%
14	Submitted to RMIT University Student Paper	<1%
15	sikarsa.um.ac.id Internet Source	<1%
16	vzikx.wordpress.com Internet Source	<1%
17	jurnal.iaii.or.id Internet Source	<1%
18	www.springerprofessional.de Internet Source	<1%
19	eprints.uty.ac.id Internet Source	<1%
20	eric1878.wordpress.com Internet Source	<1%

21	lppm.unsri.ac.id Internet Source	<1 %
22	zombiedoc.com Internet Source	<1 %
23	core.ac.uk Internet Source	<1 %
24	123dok.com Internet Source	<1 %
25	ejournal.ust.ac.id Internet Source	<1 %
26	www.hariankita.com Internet Source	<1 %
27	eprints.undip.ac.id Internet Source	<1 %
28	"Computer Security – ESORICS 2021", Springer Science and Business Media LLC, 2021 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		