Live Forensics untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan pada Web Server

Isriade Putra[1], Yudi Prayudi[2], Ahmad Luthfi[3]
[1,2,3]Universitas Islam Indonesia
E-mail: 20917019@students.uii.ac.id, prayudi@uii.ac.id , ahmad.luthfi@uii.ac.id

Article Info
Article History
Received: 2023-03-27
Revised: 2023-05-22
Published: 2023-06-07

Keywords:
Forensika Langsung;
Web Server;
Router;
Keamanan Siber.

Abstract
File upload attacks on web servers cause someone to do Distributed denial-of-service which can kill the web server and web shell can make attackers execute commands remotely. This study uses the live forensics method, by collecting artifacts on network devices, namely routers, using winbox because a router is a network device that is directly connected to a web server when an attack occurs and the computer server uses wireshark visually and dynamically, so that the data obtained from the router and computer server can be a comparison. The results of the analysis of this study are to determine the characteristics of the Distributed denial-of-service attack artifacts, namely the number of Synchronization - Acknowledgment packets sent to the web server and web shell with the .php extension script upload artifact characteristic. Furthermore, the artifacts found in the distributed denial-of-service attack on routers using the Winbox application then provide recommendations for improvements to improve security on the web server.

Artikel Info
Sejarah Artikel
Diterima: 2023-03-27
Direvisi: 2023-05-22
Dipublikasi: 2023-06-07

Kata kunci:
Forensika Langsung;
Web Server;
Router;
Keamanan Siber.

Abstrak
Serangan file upload pada web server menyebabkan seseorang dapat melakukan *Distributed denial-of-*service yang bisa melumpuhkan web server dan web shell dapat membuat penyerang mengeksekusi perintah dari jarak jauh. Penelitian ini menggunakan metoide live forensics, dengan mengumpulkan artefak pada perangkat jaringan, yaitu router, menggunakan winbox karena router ialah perangkat jaringan yang terhubung langsung ke web server ketika terjadi serangan dan komputer server menggunakan wireshark secara visualisasi dan dynamic, sehingga data yang diperoleh dari router dan komputer server dapat menjadi perbandingan. Hasil dari analisis penelitian ini ialah mengetahui karakteristik artefak serangan distributed Denial-of-service yaitu banyaknya *paket Synchronization-Acknowledgment* yang dikirim ke web server dan web shell dengan ciri artefak unggahan script ekstensi .php. Selanjutnya artefak yang ditemukan pada serangan distributed denial-of-service pada router menggunakan aplikasi winbox kemudian memberikan rekomendasi perbaikan untuk meningkatkan keamanan pada web server.

I. PENDAHULUAN

BSSN (Badan Siber Sandi Negara) ialah pihak yang bertugas melaksanakan keamanan siber di Indonesia. Berdasarkan data BSSN, telah didapatkan 333 aduan serangan *web server* pada 2021 (BSSN, 2021a). Tren aduan siber ini menjadi acuan bahwa masih tingginya tindak kejahatan siber di Indonesia, sehingga menyebabkan kerugian, baik dari pemerintah maupun swasta. Penyebab terjadinya tindak kejahatan di ruang siber atau *cyber crime* (Teknologi.id, 2022) pada *web server* disebabkan oleh dua faktor. Faktor yang pertama, serangan dari *hacker* jahat (Cekerevac et al., 2018). Faktor kedua, karena masih lemahnya sistem keamanan pada *web server*. Dalam teknik *hacking web server,* ada banyak cara, salah satunya ialah dengan serangan *file upload* (Koprawi, 2020). Berdasarkan hasil laporan BSSN pada 2021, serangan *file upload* termasuk dalam 20 besar serangan yang sering dilaporkan pada aduan siber 2021(BSSN, 2021b).

File upload ialah serangan pengunggahan yang menyertakan file skrip yang dapat menyebabkan serangan DDos dan *Web Shell* (portswigger, 2021). Untuk dapat meminimalisasi terjadinya serangan *file upload* pada *web server,* perlu dilakukan peningkatkan kemanan pada *web server*. Saat ini ada beberapa cara meningkatkan keamanan pada aplikasi *website* (Arviana, 2021). *Pertama*, dengan cara *penetration testing* (Heiding et al., 2023). Penetration testing tidak kompleks dan hanya mengikuti daftar periksa, sehingga tidak cocok untuk jangka panjang. Saat melakukan pengujian serangan langsung pada web server, kinerja web server akan terpengaruh (Stefinko, Piskozub and Banakh, 2016). Cara kedua yaitu dengan pendekatan *live forensics*

yang merupakan cabang dari keilmuan forensika digital.

Forensika digital adalah ilmu untuk dapat kumpulkan, analisis, & sajikan bukti digital di persidangan dan bisa digunakan untuk rekonstruksi aktivitas pelaku kejahatan & dapatkan info tentang pemilik komputer. (Marjie T. Britz, 2013). Metode *live forensics* merupakan pendekatan mencari artefak secara *real time* pada barang bukti digital yang penyimpanan data yang bersifat *volatile* atau mudah hilang (Faiz et al., 2016). Keuntungan dibanding penetration testing karena tidak memengaruhi sistem web server dan lebih cepat serta tepat sasaran dalam mitigasi serangan, seperti yang dilakukan pada penelitian sebelumnya tentang analisis serangan MITM *(Man In The Middle Attack).* (Ahmad, Riadi and Prayudi, 2017)

Penelitian pada penggunaan *live forensics* untuk menganalisis artefak serangan bertujuan pada peningkatan keamanan yang pernah dilakukan oleh Kurniawan (Kurniawan, 2019), Fokus pada pencegahan serangan SQL Injection dan XSS dengan menggunakan framework OWASP dan metode network forensic. Melakukan deteksi, analisis, dan juga pencegahan pada serangan pengguna melalui browser pada penelitian ini. Pada 2021, forensik router digunakan untuk menangani kasus serangan DOS menggunakan metode live forensics. (Pradhana, Riadi and Prayudi, 2021). Namun, Penelitian ini hanya fokus pada penanganan kasus forensik untuk mencari bukti digital, tanpa memberikan rekomendasi perbaikan pada sistem web server. Penelitian tentang *live forensics* penting dilakukan terutama pada serangan *file upload* berisiko tinggi. Penelitian ini berfokus pada skenario serangan file upload dengan dua tujuan serangan, yaitu *DDoS* dan *web shell*. Data log serangan diakuisisi dari router menggunakan winbox dan dari web server menggunakan wireshark, kemudian dianalisis artefak serangan untuk mengenali karakteristik serangan.

Tujuan yang ingin dicapai ialah dapat memberikan kontribusi penelitian, khususnya pada peningkatan keamanan pada *web server* dari serangan *file upload* dengan menggunakan metode *live forensics* dari perangkat jaringan *router* (Kompas.com, 2022), aplikasi *wireshark* (Wireshark, 2022) , dan *log server* (Ditanaya, Ijtihadie and Husni, 2016) untuk mengenali karakteristik artefak serangan, dari artefak serangan yang didapatkan akan dilakukan analisis dan memberikan rekomendasi perbaikan pada *web server*.

II. METODE PENELITIAN

Merujuk pada metode *Digital Forensics Research Workshop* (DFRWS) yang dibuat tahun 2002 mengusulkan 6 tahapan, yaitu identifikasi, persiapan, *collection*, *examination*, *analysis*, dan *presentation* (Riadi, Herman and Rafiq, 2022). Gambar 1 berikut merupakan langkah-langkah yang dilakukan pada penelitian ini.

Gambar 1. Tahapan Metodologi yang Diusulkan

1. Studi Pustaka

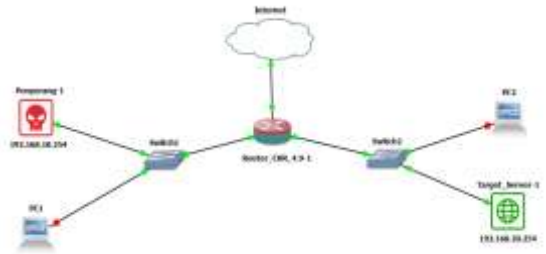
Studi pustaka dilakukan dengan menyiapkan beberapa referensi dari buku, buku, jurnal, dan artikel ilmiah lainnya.

2. Alat dan Persiapan

Untuk simulasi serangan, dibutuhkan satu komputer penyerang dengan OS Kali linux, satu router Mikrotik CHR, satu komputer investigator, dan satu komputer server sebagai target serangan. Tool yang digunakan adalah Winbox, Wireshark, dan Burpsuite.

3. Simulasi Serangan

Simulasi serangan dilakukan dengan target web server melalui jaringan router yang sama. Penyerang kemudian melakukan file upload pada website DVWA milik server target untuk meninggalkan jejak digital pada perangkat router. Selanjutnya, dilakukan investigasi forensik terhadap serangan tersebut, termasuk serangan DDoS melalui web server dan serangan web shell dengan mengupload script malicous. Untuk topologi yang digunakan dapat dilihat pada Gambar 2.



Gambar 2. Simulasi Serangan

4. Tahapan Monitoring Traffic

Tahapan monitoring traffic bertujuan untuk memantau aktivitas pada router meng-

gunakan winbox dan pada komputer server menggunakan wireshark.

5. Tahap Akuisisi Data

Metodologi yang diusulkan merujuk pada penelitian sebelumnya (Pradhana, Riadi and Prayudi, 2021), sehingga pada metode pada penelitian ini cara akuisisi data log terdapat pada Gambar 3.

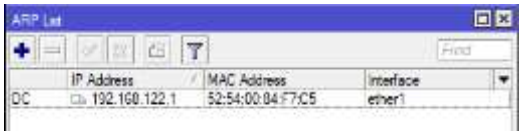
Gambar 3. Tahapan Akuisisi Data Secara *Live Forensics*

III. HASIL DAN PEMBAHASAN

Mengikuti skenario simulasi pada Gambar 2, serangan DDoS dan *web shell* akan dilakukan melalui *file upload* di *web server*.

1. Analisis dan Observasi

Pertama, dilihat router dalam keadaan normal atau diserang dengan analisis pada Interface dan Traffic di Winbox. Kemudian, jika grafik traffic pada router masih normal, berarti web server belum diserang. Gambar 4 menunjukkan traffic router masih normal. Informasi IP yang terhubung dengan router hanya ada satu yaitu ip router itu sendiri karena tidak ada aktivitas jaringan IP yang terhubung ke router.



Gambar 4. ARP List Pada Router

2. Penerapan Simulasi Serangan

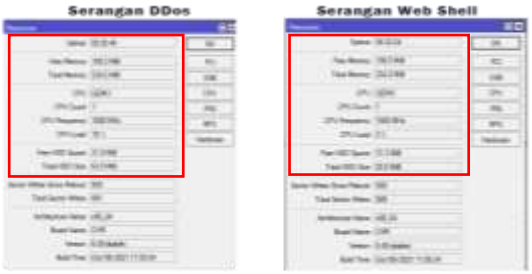
Serangan pertama yaitu DDoS menggunakan tool burpusite dan serangan kedua web shell menggunakan script php yang dapat mengeksekusi perintah dari jarak jauh dapat dilihat pada Gambar 5 simulasi serangan Ddos dan Web Shell.

Gambar 5. Simulasi Serangan DDoS dan Web Shell

Pada Gambar 5 tersebut tampak bahwa IP 192.168.20.254 merupakan target serangan dan juga sumber serangan berasal dari 192.168.10.254 mengirimkan *web shell*.php. Setelah serangan *web shell* berhasil dilaksanakan.

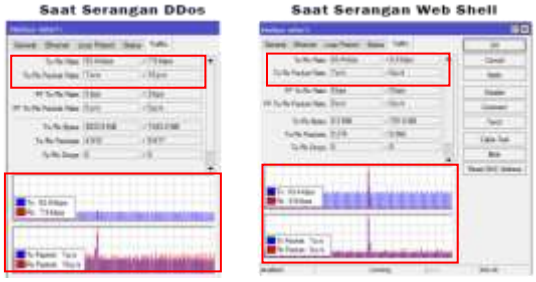
3. Monitoring Trafik dan Akuisisi

Kemudian melakukan *monitoring* serangan pada *router*. Pada proses ini, trafik lalu lintas *router* akan ditangkap menggunakan aplikasi WinBox melaui komputer investigator dan *wireshark* menggunakan komputer *server*.



Gambar 6. Pemantauan *Resource Router* saat serangan DDoS dan Web Shell

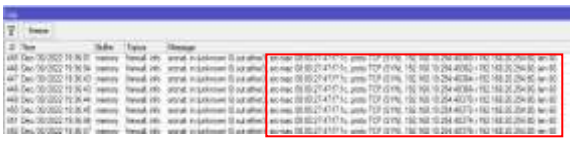
Gambar 6 saat pemantauan resource router serangan DDoS meperlihatkan terjadinya peningkatan pada penggunakan CPU Load yang normalnya 1% atau 2% meningkat menjadi 10%. Dan saat serangan web shell terjadi peningkatan CPU dan juga memori Peningkatan ini disebabkan oleh meningkatnya aktivitas *traffic* pada *router* yang jika diteruskan dapat mengakibatkan kelebihan beban pada *router* dan *web server*. Sehingga, *router* dapat mengalami *restart* dan *web server* tidak dapat diakses oleh pengguna lain.



Gambar 7. Pemantauan *Traffic Router* Saat Serangan DDoS dan Web Shell

Penggunaan CPU Load dan Memori pada *router* di menu *resource* Winbox, pada menu *interface* juga terjadi peningkatan *traffic* pada paket Rx Rate dan Rx Bytes yang lebih tinggi dari sebelumnya. Dari gambar 7 pemantauan traffic saat serangan DDos dan web shell. Memperkuat hasil analisis maka diperlukannya data, *investigator* menggunakan metode *live forensics,* kondisi perangkat harus dalam

keadaan hidup atau *running*, karena jika *router* dimatikan atau di-*restart* ada sebagian informasi di dalam *router* bersifat sementara/ mudah hilang. Oleh karena itu, investigator akan masuk ke dalam *router* sebagai *client* dan mengumpulkan informasi yang sudah tersimpan di *router*. Data yang didapatkan dari proses akusisi dan pemeriksaan forensik ini berupa *Log Resource*, *Traffic log,* dan *ARP list.*



Gambar 8. Monitoring Data *Log Activity Router* saat serangan DDoS

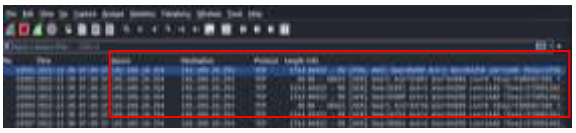
Router memiliki *log activity* yang dapat diakses melalui WinBox. Berikut ialah informasi yang didapatkan ketika terjadi serangan DDoS pada *log activty* pada *router* yaitu Time berisi bulan-tanggal-tahun, Buffer, Topics berisi info, Firewall, dan Message berisi interface, mac address, protocol, IP, dan Port seperti pada gambar berikut:

Gambar 9. Monitoring Data *Log Activity Router* saat serangan *Web Shell*

Log Activity pada *router* saat dilakukan serangan *Web Shell* sama seperti saat serangan sebelumnya, yaitu DDoS menampilkan informasi berupa Time (Bulan/tanggal/Tahun dan Waktu), Buffer, Topics (Firewall, info), *Message* (*interface*, *mac address*, *protocol*, IP Address, dan Port). Setelah dilakukan *Monitoring* pada data *log activity* saat terjadi serangan DDoS dan *Web Shel*, selanjutnya dilakukan penarikkan *data log* menggunakan *tool* WinBox seperti terlihat pada Gambar 10.

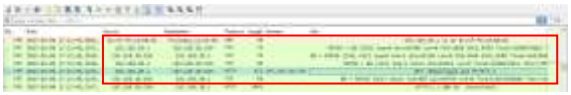
Gambar 10. Hasil Akuisisi Data *Log Activity Router* pada serangan DDoS dan Web Shell

Gambar 10 memperlihatkan proses akuisisi *log* Traffic pada *router* saat terjadi serangan DDoS dan web shell menggunakan menu terminal pada aplikasi WinBox. Tujuan dilakukannya akuisisi ini ialah untuk menyimpan data *log traffic* yang ada pada *router*, karena ketika *router* di-*restart* atau dimatikan data akan secara otomatis menghilang.



Gambar 11. Akuisisi Data *Log Traffic* Wireshark Serangan DDoS

Serangan pertama yang dilakukan ialah DDoS bersamaan juga dengan itu dilakukan *monitoring* dan akuisisi data *log traffic* pada Wireshark yang dilakukan melalui komputer *server* menampilkan data berupa Time (Tahun, Bulan, dan Tanggal, dan jam), Source (IP Address) pengakses, Destionation (IP Address) tujuan, Protocol (TCP), Lenght, dan Info yang dapat dilihat pada Gambar 11.



Gambar 12. Akuisisi Data *Log Traffic* Wireshark Serangan *Web Shell*

Pada Gambar 12 saat serangan *web shell* dilakukan *monitoring* dan akuisisi menunjukkan hasil berupa Time (Tahun, Bulan, dan Tanggal, dan jam), Source (IP Address) pengakses, Destionation (IP Address) tujuan, Protocol (TCP), Lenght, dan Info. Data ini didapatkan menggunakan Wireshark pada *router* melalui komputer *server,* kemudian akan dilakukan analisis untuk dapat mencari informasi yang diperlukan dalam proses penyelidikan.

4. Evaluasi

Evaluasi yang dilakukan bertujuan untuk melakukan validasi agar barang bukti yang didapatkan bisa dilakukan verifikasi.

Tabel 1. Perbandingan Analisis *Log Router* dan *Log Wireshark*.

Evidence	Log Activity Winbox		Log Traffic Wireshark	
	DDoS	Web Shell	DDos	Web Shell
IP Penyerang	Ada	Ada	Ada	Ada
Mac Penyerang	Ada	Ada	Ada	Ada
IP korban	Ada	Ada	Ada	Ada
Mac korban	Ada	Ada	Ada	Ada
Timestamp	Ada	Ada	Ada	Ada
Port	Ada	Ada	Ada	Ada
File serangan	Tidak	Tidak	Ada	Ada

Tabel 1 menggambarkan perbandingan *log* serangan yang didapatkan dari *router* menggunakan aplikasi Winbox dan *log* yang didapatkan dari komputer *server* menggunakan aplikasi Wireshark. Hasil menunjukkan bahwa pada *router* saat dilakukan serangan DDoS dan *web shell* dapat mendeteksi IP penyerang, Mac penyerang, IP Korban, Mac korban, Timestamp, Port, tetapi tidak dapat mendeteksi file serangan karena *router* hanya dapat berjalan di layer 3 yang hanya dapat membaca *header* paket untuk menentukan tujuan paket (Microchip Technology, 2021). *Router* tidak dapat membaca isi file teks berupa *script*, gambar, video, audio, dll (Web Dev, 2020). Sehingga, pada simulasi serangan DDoS dan *web shell* yang di-*monitoring* menggunakan aplikasi Winbox, file serangan tidak dapat diketahui. Sedangkan pada *log* Wireshark yang dijalankan di komputer *server* dapat menemukan semua *list evidence.*

5. Analisis Forensika dan Rekomendasi Perbaikan

Setelah melakukan akuisisi pada router tahapan selanjutnya ialah analisis forensik, langkah penting dari penelitian ini karena tujuan dari analisis ialah untuk mencari informasi yang di inginkan. Analisis pada tahapan ini ialah pada data hasil akuisisi *router* sebelumnya yaitu *log* Activity dari aplikasi WinBox dan *log Traffic* dari Wireshark.

Log activity merupakan satu dari sekian bukti digital yang penting pada penelitian ini, karena di dalamnya terdapat informasi berupa Time (Bulan/tanggal/Tahun dan juga Waktu), Buffer, Topics (Firewall, info), Message (interface, mac address, protocol, IP Address, dan Port). Informasi tersebut merupakan komponen penting dalam penyelidikan yang akan dilakukan oleh investigator untuk mendapatkan pelaku penyerangan dan juga mengenali karakteristik artefak serangan sehingga dapat memberikan rekomendasi perbaikan. Setelah dilakukannya simulasi serangan, investigator melakukan penarikan aktivitas data *log* di *router* melalui aplikasi Winbox yang dapat dilihat hasil akuisisi log pada Gambar 8 dan 10. Pada Gambar 8 *Log Activity router* terlihat aktivitas yang tidak lazim pada waktu (Dec/30/2022), IP 192.168.10.254 menggunakan protokol TCP (SYN), melalui port 80 mengirimkan permintaan secara terus menerus kepada IP 192.168.20.254 yang merupakan IP dari komputer *server* sehingga mengindikasikan serangan yang terjadi ialah DDoS. Gambar 9 *Log Activity* pada *router* saat serangan kedua IP 192.168.10.254 mengirimkan paket SYN kepada IP 192.168.20.254. yang dicatat oleh *router* namun tidak sebanyak saat serangan pertama sehingga belum diketahui jenis serangan yang dilakukan penyerang.

Log Traffic sangat penting dalam penelitian ini karena *log traffic* akan menjadi komparasi sekaligus validasi data dari *log activity* pada *router*, sehingga analisis *forensic* dapat dilakukan lebih komprehensif. Informasi yang didapatkan pada *log* Traffic dari Wireshark ialah *Time* (Tahun, Bulan, dan Tanggal, dan jam), *Source* (IP Address) pengakses, *Destionation* (IP Address) tujuan, Protocol (TCP), Lenght, dan Info. Hasil *log traffic* tampak pada Gambar 11 dan 12.

Gambar 11 menampilkan hasil akuisisi *log* Traffic, terlihat pada Time (2022-12-30), Pukul (07:36) banyak Info log paket data melalui protocol TCP SYN bersumber dari IP 192.168.10.254 melakukan pengiriman paket ACK ke IP 192.168.20.254 yang merupakan komputer *server*. Melihat dari artefak serangan yang terjadi ialah untuk melakukan serangan DDoS. Gambar 12 memperlihatkan adanya aktivitas SYN/ACK antara IP 192.168.10.254 dengan IP 192.168,20.254 pada info, namun tidak seperti sebelumnya paket SYN/ACK tidak terlalu banyak. Namun, melihat dari info penyerang berusaha mengakses url http://DVWA/File_upload dan juga setelah dilihat pada detail info IP 192.168.10.254 melakukan *upload* ke /DVWA/vunerabelities/upload/ script dengan ekstensi .PHP ke Web Sever, sehingga dapat di indikasikan serangan yang dilakukan ialah *Web Shell*.

Berdasarkan analisis, data *Log Activity* dan *Log Traffic* dilakukan komparasi. Dalam *Log Activity* dan juga *Log Traffic*, IP Address 192.168.122.1 merupakan IP Address pada Router. Namun, pada IP Address 192.168.10.254 memiliki src-mac yang sama 08:00:27:47:f7:1c saat terjadi serangan DDoS dan *Web Shell* merupakan IP penyerang, kemudian IP Addres 192.168.20.254 saat terjadi serangan DDoS ialah IP Korban yaitu *web server*, memiliki MAC Address yang sama dengan IP Address saat terjadinya serangan *web shell* yaitu 08:00:27:11:b9:8b. Berdasarkan hal tersebut, terindikasi bahwa pelaku penyerangan berupaya melakukan serangan DDoS untuk melumpuhkan jaringan dan

serangan *web shell* untuk melakukan eksekusi perintah dari jarak jauh.

Melihat dari sudut pandang keamanan, serangan ini disebabkan oleh kerentanan *file upload* yang tidak menerapkan pembatasan file (NKD, 2019). Dampak terburuk yang dapat terjadi ialah ketika situs *web* meng-izinkan mengunggah skrip sisi *server*, seperti file PHP, Java, atau Python, dan juga di-konfigurasi untuk dapat mengeksekusinya sebagai kode sehingga dapat melakukan *web shell* yang bisa menyebabkan *Remote Code Execution (RCE)* (Bugcrowd, 2022), yaitu melakukan eksekusi perintah pada sisi *server* dari jarak jauh seperti menghapus, mengedit, dan mengganti file yang ada dalam *database*.

IV. SIMPULAN DAN SARAN

A. Simpulan

Penulis menyimpulkan bahwa metode live forensics dapat digunakan untuk mengenali karakteristik artefak serangan. Penelitian ini fokus pada objek serangan file upload yang dapat menyebabkan serangan DDoS dan *Web Shell*. Pendekatan penelitian menggunakan data hasil eksperimen kualitatif, dari data router menggunakan *Winbox* dan komputer server menggunakan *Wireshark*. Hasilnya dapat mengidentifikasi IP pelaku penyerang. tanggal, waktu, protokol yang digunakan, jenis serangan, dan asal *script* yang digunakan penyerang. Hasil akhir dari penelitian ini memberikan rekomendasi perbaikan pada *web server* sehingga mencegah serangan selanjutnya terjadi. Pengalaman praktisi yang pernah dilakukan penulis tentang pencegahan serangan DDoS yaitu mengatur *firewall* pada *router* agar dapat memblokir serangan DDoS sebelum melumpuhkan jaringan. *Pertama*, rekomendasi perbaikan untuk serangan DDoS, mengatur *firewall* pada *router* agar dapat memblokir serangan DDoS sebelum melum-puhkan jaringan (Haris et al., 2022), kemudian menggunakan CND untuk dapat membantu memperluas jaringan dan mengurangi beban pada *server* ketika serangan terjadi (Yala, 2018).

Menggunakan layanan mitigasi DDoS seperti Prolexic dapat membantu memblokir serangan DDoS sebelum mereka mencapai jaringan(Akamai, 2018). *Monitoring* jaringan secara terus-menerus dengan menginstall SIEM seperti Wazuh yang merupakan sebuah platform SIEM (*Security Information and Event Management*) menyediakan solusi yang terintegrasi untuk pemantauan keamanan jaringan, deteksi *intrusion*, dan analisis *log,* sehingga dapat membantu mengidentifikasi serangan DDoS lebih awal dan memastikan bahwa tindakan yang tepat diambil untuk memblokir serangan (Fitri Nova, Pratama and Prayama, 2022). Kemudian, untuk serangan *web shell* rekomendasi perbaikan yang dapat dilakukan ialah Terapkan Autentikasi dan Otentikasi Kuat yaitu memastikan hanya pengguna yang memiliki otoritas yang tepat yang dapat mengakses halaman dan aplikasi *web* (National Security Agency, 2020), Pastikan aplikasi dan sistem operasi yang digunakan selalu *up-to-date* dan memiliki *patch* keamanan terbaru (hss.gov, 2020), validasi semua input yang masuk ke aplikasi *web* dan *filter* semua input yang tidak valid atau berbahaya (Guo, Marco-Gisbert and Keir, 2020), Gunakan solusi keamanan *web* yang memiliki fitur deteksi dan mitigasi serangan, seperti WAF (*Web Application Firewall*) (Anggrahito Ibrahim, Fajri and Murniyanti, 2018), dan Terapkan pemantauan dan analisis *log* aktif untuk mendeteksi serangan *web shell* dan juga mengambil tindakan segera jika terdeteksi (Susanto, Nurcahyo and ..., 2022).

B. Saran

Penelitian ini masih terbatas pada objek seragan *File Upload*, saran untuk penelitian selanjutnya adalah meneliti objek serangan lain, atau melakukan komparasi metode pada penelitian ini dengan penelitian lain.

DAFTAR RUJUKAN

Ahmad, M.S., Riadi, I. and Prayudi, Y., 2017. Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin. *ILKOM Jurnal Ilmiah*, 9(1), pp.1–8. https://doi.org/10.33096/ilkom.v9i1.103.1-8.

Aji, S., Fadlil, A. and Riadi, I., 2017. Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, [online] 3(1), pp.11–19. https://doi.org/10.26555/jiteki.v3i1.5665.

Akamai, 2018. Mitigating DDoS Attacks in Zero Seconds with Proactive Mitigation Controls. p.11.

Anggrahito Ibrahim, R., Fajri, A. and Murniyanti, E., 2018. Implementasi Web Application Firewall Menggunakan Reverseproxy. 5(3), pp.1–7.

Arviana, G.N., 2021. *Kenali Apa Itu Aplikasi Web dan Kelebihannya Dibanding Aplikasi Mobile*. [online] Available at: <https://glints.com/id/lowongan/aplikasi-web-adalah/#.Y5z8vnbP3tQ> [Accessed 17 December 2022].

BSSN, 2021a. *Laporan Tahunan Monitoring Keamanan Siber 2021*. Jakarta.

BSSN, 2021b. *Laporan Tahunan Monitoring Keamanan Siber Terkait Serangan 2021*. Jakarta.

Bugcrowd, 2022. *Remote Code Execution (RCE)*. [online] Available at: <https://www.bugcrowd.com/glossary/remote-code-execution-rce/> [Accessed 16 December 2022].

Caesarano, A. and Riadi, I., 2018. Forensik Jaringan untuk Mendeteksi Serangan Injeksi SQL Menggunakan Metode NIST. *IJCSDF*, [online] 4(5), pp.436–443. https://doi.org/ISSN: 2305-001.

Cekerevac, Z., Dvorak, Z., Prigoda, L. and Cekerevac, P., 2018. Hacking, protection and the consequences of hacking. *Communications - Scientific Letters of the University of Žilina*, 20(2), pp.83–87. https://doi.org/10.26552/com.C.2018.2.83-87.

Ditanaya, T.H., Ijtihadie, R.M. and Husni, M., 2016. Rancang Bangun Sistem Log Server Berbasis Syslog dan Cassandra untuk Monitoring Pengelolaan Jaringan di ITS. *Jurnal Teknik ITS*, 5(2), pp.799–802. https://doi.org/10.12962/j23373539.v5i2.18815.

Faiz, M.N., Umar, R., Yudhana, A. and Dahlan, U.A., 2016. Analisis live forensics untuk perbandingan kemananan email pada sistem operasi proprietary. *Jurnal Ilmiah ILKOM*, [online] 8(3), pp.242–247. https://doi.org/https://doi.org/10.33096/ilkom.v8i3.79.242-247.

Fitri Nova, Pratama, M.D. and Prayama, D., 2022. Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1), pp.1–7. https://doi.org/10.30630/jitsi.3.1.59.

Guo, Y., Marco-Gisbert, H. and Keir, P., 2020. Mitigating webshell attacks through machine learning techniques. *Future Internet*, 12(1), pp.1–16. https://doi.org/10.3390/fi12010012.

Haris, A.I., Riyanto, B., Surachman, F. and Ramadhan, A.A., 2022. Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika : Jurnal Sistem Komputer*, 11(1), pp.67–76. https://doi.org/10.34010/komputika.v11i1.5227.

Hassan, N.A., 2019. *Digital Forensics Basics - A Practical Guide Using Windows OS*. 1st ed. [online] *Digital Forensics Basics*. New York: Appress. https://doi.org/10.1007/978-1-4842-3838-7_1.

Heiding, F., Süren, E., Olegård, J. and Lagerström, R., 2023. Penetration testing of connected households. *Computers and Security*, 126(Computer & Security), pp.1–13. https://doi.org/10.1016/j.cose.2022.103067.

hss.gov, 2020. Web Shell Malware : Threats and Mitigations Slides Key : May, pp.1–21.

Kompas.com, 2022. *Apa Itu Router? Definisi, Fungsi, dan Jenis, dan Bedanya dengan Modem*. [online] Available at: <https://tekno.kompas.com/read/2022/08/29/14450017/apa-itu-router-definisi-fungsi-dan-jenis-dan-bedanya-dengan-modem> [Accessed 16 December 2022].

Koprawi, M., 2020. Dampak dan Pencegahan Serangan File Inclusion: Perspektif Developer. *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, [online] 5(1), pp.40–43. Available at: <https://doi.org/10.30743/infotekjar.v4i2.2332>.

Kurniawan, A., 2019. Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based. *Jurnal*

Telematika, 14(1), pp.9–18.

Marjie T. Britz, P.D., 2013. Computer Forensics and Cyber Crime. *Pearson*, 91(5), pp.291–296.

Microchip Technology, 2021. *TCP/IP Network Layer (Layer 3)*. [online] Available at: <https://microchipdeveloper.com> [Accessed 31 March 2023].

National Security Agency, 2020. Detect and Prevent Web Shell Malware. [online] (April), Apr., pp.1–17. Available at: <https://media.defense.gov>.

NKD, F., 2019. *Web security : Unrestricted File Upload Mengancam Keamanan Website*. [online] Available at: <https://www.logique.co.id> [Accessed 16 December 2022].

portswigger, 2021. *File upload vulnerabilities*. [online] Available at: <https://portswigger.net/web-security/file-upload> [Accessed 23 November 2022].

Pradhana, I., Riadi, I. and Prayudi, Y., 2021. Forensik Router untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic. *JRST (Jurnal Riset Sains dan Teknologi)*, 5(1), pp.31–38. https://doi.org/10.30595/jrst.v5i1.7662.

Riadi, I., Herman, H. and Rafiq, I.A., 2022. Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework. *International Journal of Artificial Intelligence Research*, 6(2), pp.1–9. https://doi.org/10.29099/ijair.v6i2.311.

Riadi, I., Luthfi, A. and Mazdadi, M.I., 2017. Live Forensics on RouterOS using API Services to Investigate Network Attacks. *Article in International Journal of Computer Science and Information Security*, [online] 15(2), pp.406–410. https://doi.org/https://sites.google.com/site/ijcsis/ ISSN 1947-5500.

Stefinko, Y., Piskozub, A. and Banakh, R., 2016. Manual and automated penetration testing. Benefits and drawbacks. Modern tendency. *Scienceelecommunications and Computer Science*, 1(Penetration testing), pp.488–491. https://doi.org/10.1109/TCSET.2016.7452095.

Susanto, M.F., Nurcahyo, A. and ..., 2022. Website Threat Monitoring Untuk Pemantauan dan Analisis Ancaman Pada Web Server. *IRWNS*, [online] 1(2), pp.13–14. Available at: <https://jurnal.polban.ac.id/>.

Teknologi.id, 2022. *Alasan Meningkatkan Keamanan Website*. [online] WSEAS Transactions on …. Available at: <https://teknologi.id> [Accessed 16 December 2022].

Web Dev, 2020. *7 Layar OSI*. [online] Available at: <https://newtonindonesia.co.id/7-layar-osi/> [Accessed 31 January 2023].

Wireshark, 2022. *Wireshark*. [online] Available at: <https://www.wireshark.org/> [Accessed 16 December 2022].

Yala, L., 2018. *Content Delivery Networks as a Service (CDNaaS) To cite this version : « Louiza Yala »*. Universite Rennes.

Yogi, Ruslianto, I. and Bahri, S., 2019. Analisa Log Web Server Untuk Mengetahui Pola Perilaku Pengunjung Website Menggunakan Teknik Regular Expressions. *Coding: Jurnal Komputer dan Aplikasi*, [online] 07(01), pp.120–130. https://doi.org/ISSN: 2338-493X.