Live Forensics Untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan Pada Web Server

Isriade putra

20197019

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2023

Lembar Pengesahan Pembimbing

Live Forensics Untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan Pada Web Server

Isriade putra
20197019

Yogyakarta, 06 September 2023

Pembimbing I	Pembimbing II
Dr. Yudi Prayudi, S.Si., M.Kom.	Dr. Ahmad Luthfi, S.Kom., M.Kom.

Lembar Pengesahan Penguji

Live Forensics Untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan Pada Web Server

Isriade putra

20197019

Yogyakarta, September, 2023

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom.
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Anggota I

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Live Forensics Untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan Pada *Web Server*

Serangan file upload pada web server menyebabkan seseorang dapat melakukan DDOS dan web shell pada web server. Serangan DDOS dapat melumpuhkan web server dan pada web shell penyerang dapat mengeksekusi kode jarak jauh, melihat isi database, meng-upload file berbahaya, menghapus file, dan mengedit file pada web server. Penelitian ini bertujuan untuk meningkatkan keamanan pada web server agar saat terjadi serangan, file upload kembali pada web server, sehingga serangan tersebut tidak begitu berdampak. 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 komparasi dan validasi. Hasil dari analisis penelitian ini ialah mengetahui karakteristik artefak serangan DDOS yaitu banyaknya paket SYN-ACK yang dicerium ke web server dan web shell dengan ciri artefak unggahan script ekstensi .php. kemudian setelah mengetahui artefak serangan diketahui selanjutnya memberikan rekomendasi perbaikan pada web server terkait serangan DDOS dengan melakukan pencegahan dengan pembatasan request selama beberapa waktu dan untuk serangan web shell memberikan pembatasan upload file dengan ekstensi dan ukuran yang di tentukan. Artefak yang ditemukan pada serangan DDOS pada router menggunakan aplikasi winbox Penelitian ini perlu dilakukan, karena melanjutkan dari penelitian sebelumnya yang menggunakan metode live forensic dalam menganalisis artefak serangan kemudian memberikan rekomendasi perbaikan akan lebih cepat dan spesifik untuk meningkatkan keamanan pada web server.

Kata Kunci:

Website; Router; Security; Artefak; Forensic;

Abstract

Live Forensics To Recognize the Characteristics of File Upload Attacks to Improve Security on Web Servers

Web servers are vulnerable to file upload attacks, which can lead to severe consequences such as DDoS attacks and web shell exploitation. DDoS attacks cripple web servers, while web shell exploitation grants attackers remote control, enabling them to execute malicious code, tamper with databases, upload dangerous files, delete important data, and modify server files. The purpose of this research is to fortify the security of web servers to mitigate the impact of such attacks by ensuring uploaded files can be recovered. The study employs the live forensics methodology, gathering evidence from network devices, specifically routers, utilizing Winbox. Routers play a crucial role as they directly connect to web servers during attacks. The server computer utilizes Wireshark for visual and dynamic analysis, facilitating data comparison and validation between the router and server. The research analysis reveals key characteristics of DDoS attack artifacts, such as a substantial influx of SYN-ACK packets directed at the web server. Additionally, web shell artifacts indicate the presence of uploaded scripts with .php extensions. Armed with this knowledge, recommendations for bolstering web server security are proposed. These include implementing preventive measures against DDoS attacks, such as temporary request rate limitations. Furthermore, restrictions on uploaded file types and sizes can be enforced to combat web shell attacks. The significance of the research is underscored by the artifacts uncovered in the router's Winbox application during DDoS attacks. By building upon previous studies that utilized live forensics methodology to analyze attack artifacts, this research aims to provide expedited and targeted recommendations for enhancing web server security.

Keywords:

Website; Router; Security; Artefak; Forensic

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Juni, 2023

Isriade putra

Daftar Publikasi

Publikasi berikut menjadi bagian dari Bab 3

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Isriade Putra	Mendesain eksperimen (60%) Menulis *paper* (70%)
Yudi Prayudi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)
Ahmad Luthfi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**".

Halaman Persembahan

Saya persembahkan tesis ini untuk:

“Kedua orang tuaku ”

“Kedua adikku ”

“Teman-temanku”

Dan

“calon pendamping hidupku”

yang selalu bertanya:

“kapan kelar kuliahnya?”

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur kami panjatkan ke hadirat Allah SWT, Tuhan yang Maha Esa, atas segala rahmat, hidayah, serta karunia-Nya yang melimpah. Shalawat dan salam tak henti-hentinya kami panjatkan kepada Nabi Muhammad SAW, sebagai suri tauladan bagi seluruh umat manusia.

Dalam kesempatan ini, kami dengan penuh rasa syukur dan bahagia dapat menyelesaikan tugas akhir berupa thesis dalam rangka meraih gelar Magister Informatika dari Universitas Islam Indonesia (UII). Thesis ini merupakan hasil jerih payah dan dedikasi kami dalam mengeksplorasi dan mendalami bidang ilmu informatika.

Tidak lupa, kami ingin mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, bimbingan, dan kontribusi dalam proses penyelesaian thesis ini.

Pertama-tama, kami mengucapkan terima kasih kepada Bapak/Ibu Dosen Pembimbing kami, Dr. Yudi Prayudi, M.Kom, dan Dr. Ahmad Luthfi, M.Kom atas bimbingan, arahan, serta dorongan yang luar biasa selama penulisan thesis ini. Bapak/Ibu adalah sosok yang tidak hanya memberikan pengetahuan dan wawasan, tetapi juga menjadi inspirasi dalam perjalanan kami di dunia akademik. Terima kasih atas kesabaran, motivasi, dan dedikasi yang Bapak/Ibu berikan.

Tak lupa, kami juga ingin menyampaikan rasa terima kasih kepada seluruh dosen dan tenaga pendidik di Program Studi Magister Informatika UII yang telah memberikan bekal ilmu dan pengalaman berharga kepada kami selama studi di UII. Terima kasih atas dedikasi dan komitmen Bapak/Ibu dalam memberikan pendidikan yang berkualitas.

Tidak ketinggalan, ucapan terima kasih kami sampaikan kepada keluarga kami yang selalu memberikan dukungan, doa, dan semangat dalam setiap langkah perjalanan kami. Keluarga adalah sumber kekuatan dan inspirasi bagi kami. Terima kasih atas cinta, pemahaman, dan dukungan tak terbatas yang Bapak/Ibu berikan.

Kami juga ingin berterima kasih kepada teman-teman seangkatan dan sejawat kami di Program Studi Magister Informatika UII. Terima kasih atas diskusi, kolaborasi, dan pengalaman berharga yang kami dapatkan dari Bapak/Ibu semua. Semua momen yang kami lewati bersama telah memberikan warna dan kenangan indah selama studi di UII.

Kami sadar bahwa penelitian ini tidak lepas dari keterbatasan dan kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat kami harapkan untuk perbaikan di masa depan.

Semoga hasil dari thesis ini dapat memberikan sumbangsih positif bagi pengembangan ilmu pengetahuan dan teknologi di bidang informatika.

Akhir kata, kami mengucapkan terima kasih yang sebesar-besarnya kepada Allah SWT, atas segala rahmat dan karunia-Nya yang telah melimpah dalam perjalanan penyelesaian thesis ini. Semoga segala usaha dan jerih payah yang kami lakukan dapat menjadi amal jariyah yang bermanfaat bagi umat dan bangsa.

Kami berharap bahwa thesis ini dapat menjadi kontribusi kecil dalam pengembangan ilmu pengetahuan dan teknologi, khususnya dalam bidang informatika. Semoga hasil penelitian yang kami sajikan dapat memberikan wawasan baru, pemahaman yang lebih mendalam, dan solusi yang relevan dalam menghadapi tantangan dan permasalahan yang ada.

Kami juga berharap bahwa thesis ini dapat menjadi inspirasi bagi peneliti dan akademisi lainnya untuk melakukan studi lebih lanjut dan mengembangkan konsep-konsep yang telah kami ajukan. Terbuka untuk kemungkinan adanya penelitian lebih mendalam dan pengembangan yang lebih luas di masa depan.

Akhir kata, kami mengucapkan terima kasih kepada semua pihak yang telah turut serta mendukung dan membantu kami dalam perjalanan penyelesaian thesis ini. Semoga segala upaya yang telah kami lakukan dapat bermanfaat bagi perkembangan ilmu pengetahuan dan teknologi, serta membawa manfaat yang nyata bagi masyarakat dan bangsa.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

ISRIADE PUTRA
Magister Informatika
Universitas Islam Indonesia (UII)

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

BSSN	- Business Process Management
DDOS	- Business Process Management System
IP	- Control Flow Complexity
HTTP	- Experience Driven Learning
MITM	- Multi-Criteria Decision-Making
ARP	- List Address Resource Protocol
MAC	- Media Access Control
DVWA	- Damn Vulnerable Web Application
TCP	- Transmission Control Protocol
DHCP	- Dynamic Host Configuration Protocol
DNS	- Domain Name System
SQL	- Structured Query Language
XSS	- Cross-Site Scripting
OWASP	- Open Web Application Security Project
SYN	- Synchronize
ACK	- Acknowledge
HTML	- HyperText Markup Language
ISP	- Internet Service Provider
NAT	- Network Address Translation
DOS	- Denial Of Services
IDS	- Intruction Detection System
FIM	- File Integrity Monitoring
HTTP	- Hypertext Transfer Protocol
GWS	- Google Web Server
DFRWS	- Digital Forensics Research Workshop
NIST	- National Institute of Standards and Technology

BAB 1
Pendahuluan

1.1 Latar Belakang

Berdasarkan data Badan Siber Sandi Negara (BSSN), terdapat 333 aduan serangan *web server* pada tahun 2021 yang tersebar di beberapa sektor, antara lain sektor infrastruktur informasi vital nasional 12%, ekonomi digital 51%, pemerintah pusat 23%, pemerintah daerah 25%, dan lainnya 25% (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 yang mencoba untuk mendapatkan keuntungan sepihak yang menyebabkan kerugian pihak lain (shilvirichiyanti, 2020). Faktor kedua, karena masih lemahnya sistem keamanan pada *website* yang memberikan peluang pada tindakan kejahatan. 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 adalah serangan yang terjadi ketika pengguna diizinkan untuk mengunggah file ke sistem server tanpa adanya validasi yang memadai terhadap aspek-aspek seperti nama file script, jenis file, konten, atau ukuran file. Kelemahan dalam menerapkan pembatasan yang tepat pada fungsi unggah file, seperti gambar, dokumen, dan lainnya, dapat dimanfaatkan untuk mengunggah file dengan cara yang sewenang-wenang dan berpotensi berbahaya. Bahkan, serangan semacam ini dapat menyertakan file skrip sisi server yang memungkinkan eksekusi kode dari jarak jauh. Dalam beberapa kasus, tindakan mengunggah file itu sendiri dapat menyebabkan serangan berbahaya seperti membuat server down yang dapat merusak fungsi web server. Serangan lainnya mungkin melibatkan permintaan HTTP terhadap file yang diunggah tersebut, biasanya untuk memicu eksekusi file tersebut oleh server (portswigger, 2021).

Untuk meminimalisasi terjadinya serangan *file upload* pada *web server,* perlu dilakukan pencegahan terhadap faktor-faktor penyebabnya. Salah satunya ialah dengan meningkatkan kemanan pada *web server* agar menjadi lebih aman ketika terjadi serangan

kembali. Saat ini ada beberapa cara meningkatkan keamanan pada aplikasi *website* (Arviana, 2021). *Pertama*, dengan cara *penetration testing*. *Penetration testing* ialah pengujian kerentanan yang dilakukan pada aplikasi *web server* untuk mencari celah pada sistem *web server*, sehingga dari celah yang didapatkan bisa dilakukan perbaikan (Bacudio et al., 2011). Metode *penetration testing* memiliki kekurangan yaitu tidak terlalu kompleks dalam mendeteksi sumber daya yang terdampak, karena hanya mengikuti *cek list,* sehingga tidak cocok untuk jangka panjang, kemudian saat pengujian serangan secara langsung dilakukan pada *web server* untuk mencari *bug* yang ada, maka akan memengaruhi kinerja *web server* secara langsung (scalefocus, 2022).

Kedua, yaitu dengan pendekatan *live forensics* yang merupakan cabang dari keilmuan forensik digital. Forensik digital ialah cabang dari ilmu forensik yang menggunakan ilmu pengetahuan untuk mengumpulkan, menganalisis, mendokumentasikan, dan menyajikan bukti digital yang berhubungan dengan kejahatan siber di persidangan (Hassan, 2019). Teknik forensik digital digunakan oleh penyidik untuk mengumpulkan bukti dari berbagai macam perangkat digital. Ada banyak *tool* dan teknik yang bisa digunakan untuk mencari bukti-bukti digital yang relatif sulit ditemukan, seperti bukti yang telah dihapus, dikunci, atau disamarkan (Oleg Afonin, 2015). Ilmu forensik digital juga dapat digunakan untuk merekonstruksi ulang aktivitas dari pelaku kejahatan dan untuk mendapatkan informasi mengenai si pemilik komputer (Garfinkel, 2007). 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) .

Metode *live forensics* dapat melakukan analisis serangan yang sedang terjadi secara lebih kompleks dan memberikan rekomendasi perbaikan pada sisi *security*, sehingga memiliki keunggulan daripada metode *penetration testing,* karena dapat dilakukan pada saat sistem sedang berjalan namun tidak memengaruhi sistem *web server* sehingga akan lebih cepat dan tepat sasaran dalam melakukan mitigasi serangan yang terjadi, seperti yang dilakukan pada penelitian sebelumnya tentang analisis serangan MITM *(Man In The Middle Attack).* (Ahmad et al., 2017)

Sebelumnya, telah banyak dilakukan penelitian berkaitan dengan *cyber security* dan *live forensics,* yaitu pada 2017 penelitian tentang *live forensics* pada Router OS menggunakan API Services untuk investigasi serangan jaringan. Penelitian ini menggunakan metode *live forensics* serangan *brute force*. Hasil penelitian ini mendapatkan pemberitahuan serangan melalui API *(Application Programming Interface)* tersebut yaitu "*Log Activity*, IP

Address List, ARP, DHCP Leases, DNS Cache, dan Router Board Info" selanjutnya untuk mengetahui aktivitas tidak sah pada router dilakukan analisis (Riadi et al., 2017). Penelitian lain pada forensik jaringan (Aji et al., 2017) memfokuskan pada pengembangan sistem untuk pengaman jaringan komputer menggunakan analisis forensik jaringan. Metode yang digunakan ialah *live forensics* dan jenis serangan yang digunakan pada HTTP Flooding selanjutnya deteksi serangan pada router dilakukan menggunakan aplikasi *winbox* dengan login ke dalam *router* kemudian melakukan pemantauan jaringan sehingga mendapatkan *resource*, IP Address penyerang, IP Address korban, jumlah paket data, dan *timestamp*.

Penelitian pada penggunaan *live forensics* untuk menganalisis artefak serangan bertujuan pada peningkatan keamanan yang pernah dilakukan oleh Kurniawan (Kurniawan, 2019), berfokus pada pencegahan serangan SQL Injection dan XSS dengan menggunakan *framework* OWASP dan metode *network forensic* untuk melakukan deteksi, analisis, dan pencegahan pada serangan dari sisi pengguna yang pada penelitian ini melakukan uji coba pencegahan serangan melalui *browser* yang digunakan. Tahun 2021 dilakukan forensik *router* untuk penanganan forensik kasus pada serangan *denial of service* (DOS) dengan bentuk serangan *flooding attack* menggunakan metode *live forensics* (Pradhana et al., 2021). Namun, pada penelitian ini hanya fokus pada penanganan kasus forensik untuk mencari bukti digital, tidak memberikan rekomendasi perbaikan pada sistem *web server*. Sehingga, penelitian tentang *live forensis*, terutama pada serangan *file upload* yang memiliki resiko tinggi, menjadi alasan penting untuk dilakukan pada penelitian saat ini.

Skenario serangan *file upload* ialah melakukan *upload file* ke *web server* dengan 2 pengujian serangan, yaitu *file upload* untuk serangan DDOS dan *file upload* untuk serangan *web shell*. Setelah serangan dilakukan, selanjutnya akuisisi data *log* serangan dari *router* menggunakan *tool winbox* untuk meilihat data dari perangkat jaringan *router* (Kompas.com, 2022) dan dari *web server* (Ditanaya et al., 2016) menggunakan *tool wireshark* (Wireshark, 2022), kemudian dilakukan analisis artefak serangan yang didapatkan guna mengenali karakteristik serangan yang dilakukan oleh penyerang. Tujuan dilakukan penelitian ini ialah untuk mendapatkan karakteristik artefak serangan, kemudian memberikan rekomendasi perbaikan yang tepat untuk menutup kerentanan yang ada pada web server.

Tujuan utama dari penelitian ini adalah *"Untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan Pada Web Server menggunakan metode live forensics".*

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang maka dapat dirumuskan suatu permasalahan yaitu : Bagaiamana karakteristik serangan file upload yang dapat terdeteksi menggunakan metode live forensik?

1.3 Batasan Penelitian

a) Lingkup Web Server: Penelitian ini akan difokuskan pada penggunaan live forensics untuk mengenali karakteristik serangan file upload pada satu jenis web server tertentu atau beberapa web server yang serupa. Hal ini bertujuan untuk memfokuskan penelitian pada implementasi dan analisis yang spesifik terhadap web server yang dipilih.
b) Jenis Serangan File Upload: Penelitian ini akan membatasi pada serangan file upload tertentu, seperti serangan yang bertujuan untuk mengunggah dan menjalankan file berbahaya, atau serangan yang mencoba mengunggah file dengan ekstensi yang tidak diizinkan. Jenis serangan lainnya, seperti serangan SQL injection atau cross-site scripting (XSS), tidak akan menjadi fokus penelitian ini.
c) Metode Live Forensics: Penelitian ini akan menggunakan metode live forensics untuk mengenali karakteristik serangan file upload. Metode lain, seperti analisis pasca kejadian (post-mortem forensics) atau analisis forensik offline, tidak akan menjadi fokus utama penelitian ini.
d) Keamanan Web Server: Penelitian ini akan menekankan pada bagaimana penggunaan metode live forensics dapat meningkatkan keamanan pada web server terkait serangan file upload. Aspek keamanan lainnya, seperti serangan XSS atau SQL Injetion attacks, tidak akan menjadi fokus penelitian ini.

1.4 Tujuan Penelitian

Tujuan dari penelitia ini adalah :

a) Mengidentifikasi karakteristik serangan file upload: Tujuan utama penelitian ini adalah untuk mengidentifikasi karakteristik serangan file upload yang dapat membahayakan keamanan web server. Dengan menganalisis pola dan tanda-tanda serangan file upload, penelitian ini bertujuan untuk mengembangkan pemahaman yang lebih baik tentang jenis serangan yang mungkin terjadi dan cara mereka dapat mempengaruhi keamanan web server.

b) Menerapkan metode live forensics: Penelitian ini bertujuan untuk menerapkan metode live forensics dalam mengenali serangan file upload. Dengan menggunakan pendekatan live forensics, penelitian ini akan menggabungkan teknik dan alat yang relevan untuk melakukan analisis secara real-time terhadap data dan aktivitas pada web server. Hal ini akan memungkinkan deteksi dini dan respons cepat terhadap serangan file upload yang terjadi.

c) Meningkatkan keamanan pada web server: Tujuan akhir penelitian ini adalah untuk meningkatkan keamanan pada web server melalui penggunaan metode live forensics dalam mengenali serangan file upload. Dengan mengidentifikasi dan mengklasifikasikan serangan file upload secara efektif, langkah-langkah keamanan yang tepat dapat diambil untuk mencegah atau memitigasi dampak serangan tersebut. Hal ini diharapkan dapat meningkatkan keandalan dan keamanan web server secara keseluruhan.

1.5 Manfaat Penelitian

Manfaat penelitian dari judul tersebut adalah sebagai berikut:

a) Deteksi dini serangan: Dengan menerapkan metode live forensics, penelitian ini dapat membantu dalam mendeteksi serangan file upload secara lebih dini. Dengan adanya pemahaman yang lebih baik tentang karakteristik, pola dan tanda-tanda serangan, tindakan respons yang cepat dapat diambil untuk memitigasi serangan tersebut sebelum menyebabkan kerusakan yang lebih parah atau pencurian data.
b) Meningkatkan keamanan web server: Penelitian ini dapat memberikan manfaat signifikan dalam meningkatkan keamanan pada web server. Dengan mengenali karakteristik serangan file upload melalui metode live forensics, langkah-langkah keamanan yang lebih efektif dapat diimplementasikan. Hal ini akan membantu mengurangi risiko serangan yang berhasil dan melindungi data sensitif yang disimpan di web server.
c) Pengembangan strategi keamanan yang lebih efektif: Penelitian ini dapat memberikan wawasan baru tentang karakteristik serangan file upload yang sering terjadi pada web server. Hal ini dapat digunakan sebagai dasar untuk mengembangkan strategi keamanan yang lebih efektif dan adaptif. Dengan pemahaman yang lebih baik tentang serangan

file upload, kebijakan keamanan dan sistem deteksi yang lebih kuat dapat diterapkan untuk menghadapi ancaman yang muncul.

Dengan manfaat-manfaat ini, penelitian tersebut diharapkan dapat memberikan kontribusi yang berarti dalam meningkatkan keamanan pada web server dan melindungi data pengguna dari serangan file upload yang berbahaya.

1.6 Luaran Penelitian

Luaran penelitian ini adalah publikasi di jurnal lokal yang terakreditasi Sinta. Dengan menerbitkan penelitian ini dalam jurnal terakreditasi Sinta, peneliti dapat berbagi temuan dan kontribusi mereka dengan komunitas ilmiah dan praktisi di bidang keamanan informasi. Publikasi ini dapat menjadi sumber referensi bagi para akademisi, peneliti, dan profesional keamanan untuk memperoleh wawasan dan pemahaman yang lebih dalam tentang penggunaan metode live forensics dalam mengenali serangan file upload pada web server. Selain itu, publikasi ini juga dapat meningkatkan visibilitas dan reputasi peneliti serta institusi di mana penelitian tersebut dilakukan.

BAB 2
Tinjauan Pustaka

2.1 Penelitian Terdahulu

Forensik digital adalah cabang dari ilmu forensik yang menggunakan ilmu pengetahuan untuk mengumpulkan, menganalisa, mendokumentasikan, dan menyajikan bukti digital yang berhubungan dengan kejahatan siber di persidangan (Hassan 2019). Teknik forensik digital digunakan oleh penyidik untuk mengumpulkan bukti dari berbagai macam perangkat digital. Ada banyak tool dan teknik yang bisa digunakan untuk mencari bukti-bukti digital yang relatif sulit ditemukan, seperti bukti yang telah dihapus, dikunci, atau disamarkan (Oleg Afonin 2015). Ilmu forensik digital juga dapat digunakan untuk merekonstruksi ulang aktivitas dari pelaku kejahatan dan untuk mendapatkan informasi mengenai si pemilik komputer (Garfinkel 2007)

Sebelumnya telah banyak dilakukan penelitian berkaitan dengan cyber security dan live forensics yaitu pada tahun 2017 penelitian tentang live forensics pada Router OS menggunakan API Services untuk investigasi serangan jaringan, metode pada penelitian ini menggunakan live forensics serangan brute force dengan hasil penelitian ini mendapatkan pemberitahuan serangan melalui API (Application Programming Interface) berupa Log Activity, IP Address List, ARP, DHCP Leases, DNS Cache, dan Router Board Info yang kemudian dianalisis untuk mengungkapkan aktivitas illegal pada router (Riadi, Luthfi, and Mazdadi 2017)

Penelitian lain pada forensik jaringan (Aji, Fadlil, and Riadi 2017), yang fokus pada pengembangan sistem pengaman jaringan komputer berdasarkan analisis forensik jaringan, untuk metode yang digunakan adalah live forensics dan jenis serangan yang digunakan pada HTTP Flooding kemudian proses mendeteksi terjadinya serangan pada jaringan dilakukan dengan menggunakan aplikasi WinBox yang aplikasi tersebut dapat menunjukkan resource, IP Address penyerang, jumlah paket data serta waktu serangan terjadi.

Selain itu penelitian lain terkait forensik jaringan yang dilakukan oleh Caesarano (Caesarano and Riadi 2018), melakukan penelitian tentang forensik jaringan yang bertujuan untuk melakukan pendeteksian serangan SQL Injetion menggunakan metode NIST. Panelitian ini menggunakan tools snort yang mendeteksi intrusion pada web server yang bisa digunakan untuk membantu melakukan pendeteksian serangan dengan log informasi yang dihasilkan. Metode yang digunakan aalah NIST 800-30 yaitu terdapat 9 tahapan yang harus

dilakukan untuk meminimalisir risiko. Kemudian untuk simulasi kasus dilakukan terdapat 5 tahapan yaitu pengujian kerentanan, scenario serangan, konfigurasi snort, pengumpulan data dan tahapan analisis. Hasil dari penelitian ini yaitu pengembangan system web server menggunakan Snort untuk system deteksi serangan SQL Injection dan notifikasi serangan real time menggunakan email.

Kemudian penelitian monitoring log aplikasi dengan tujuan Agar akuisisi data pada proses investigasi keamanan dapat dilakukan secara komprehensif, responden perlu mengambil informasi umum yang mencakup log, layanan terkonfigurasi, tugas cron, status patch, dan akun pengguna. Informasi-informasi ini dikenal sebagai artefak forensik. Lokasi dan formatnya bervariasi di setiap sistem. Salah satu manifestasi dari artefak forensik yang sering diinvestigasi oleh para praktisi adalah file. Framework Grr Rapid Response telah membangun kerangka kerja untuk mendeskripsikan artefak forensik yang memungkinkan data yang diperlukan dapat dikumpulkan dan dikondisikan dengan cepat menggunakan live forensics pada log aplikasi mobile native menggunakan laravel. Pengambilan barang bukti forensik menggunakan metode NIST memiliki langkah-langkah seperti akuisisi, eksaminasi, analisis, dan pelaporan. Penelitian ini menghasilkan log file dari framework laravel dan informasi aktifitas detail dari user saat mengakses server. Hasil log yang diperoleh akan menjadi barang bukti untuk untuk menjadi bahan laporan. (Yogi et al., 2019)

Selanjutnya ada penelitian tentang forensik jaringan untuk mendeteksi serangan flooding dengan melakukan eksplorasi pada router untuk menemukan data-data kemudian dilakukan analisis seingga mendapatkan bukti digital bukti digital yang bisa digunakan dalam proses invenstigasi. Untuk simulasi memanfaatkan tools metasploit yang digunakan sebagai penyerangan dan aplikasi wireshark, winbox sebagai media yang digunakan dalam mendeteksi serangan flooding secara live forensics. Dari hasil penelitian berhasil dilakukan akuisisi informasi serangan melalui metode live forensics meggunakan aplikasi wireshark sehingga informasi yang didapatkan dapat dilakukan analisis dan mendapatkan bukti yang diinginkan dan juga karakteristik serangan yang dilakukan pada router (Pradhana, Riadi, and Prayudi 2021).

Pada penelitian sebelumya ada yang membahas terkait forensik jaringan terhadap serangan Cross-Site Scripting atau XSS yaitu Ade kurniawan 2019 tentang penerapan framework OWASP dan network forensics untuk analisis, deteksi, dan pencegahan serangan injeksi di sisi host-based, pada penelitian tersebut metode yang digunakan adalah live forensics yaitu melakukan akuisisi bukti digital saat sistem sedang berlajalan secar langsung,

kemudian dilakukan sebuah simulasi serangan, analisis, dan pencegahan serangan di sisi pengguna. Host based attack dalam penelitian ini akan meluncurkan beberapa serangan, antara lain yang sering atau mungkin terjadi di sisi pengguna, seperti: pengumpulan informasi, webcam screenshot, keylogger, dan spoofer. Simulasi ini mengasumsikan korban memakai firefox mozzilla dengan metode serangan awal menggunakan social engineering attack dengan mengirim sebuah phishing email. Alat yang digunakan adalah OWASP Xenotix XSS Exploit Framework v6.2. untuk menangkap, mengekstraksi, dan menganalisis lalu lintas paket menggunakan teknik network forensics dengan pendekatan akuisisi barang-barang bukti mengggunakan teknik live forensics. Network forensics (forensik jaringan), umumnya mengacu pada studi ilmiah dengan bukti berbasis jaringan. Network forensics adalah bidang studi untuk menemukan petunjuk kejahatan di internet alat yang digunakan untuk analisis paket data menggunakan wireshark dan live HTTP Header. Selanjutnya, pada tahap prevent solution, pendekatan dilakukan dengan membuat patching stages. prevent solution dilakukan dengan membuat browser patching pada mozilla firefox dalam bentuk add-on extension dengan nama XSS Filter Ade yang mampu menyediakan fungsi sebagai peringatan dini, mematikan plugin, dan membatasi payload/script kepada korban ketika akan membuka alamat situs web (Kurniawan 2019).

Salah satu penelitian sebelumnya yang berjudul “Analisis Web Server Log Dalam Pencarian Pola Pengunjung Dengan Teknik Association Rules” dengan fokus pembahasan pada teknik assosiation rules bertujuan untuk menentukan pola kunjungan website. Access log merupakan daftar semua aktifitas pengunjung selama mengakses suatu website. Informasi tersebut akan sangat berguna apabila website mengalami serangan sehingga akan dapat dicari penyebabnya berdasarkan log file yang terdapat pada web server. Namun, untuk mencari informasi yang relevan dari data yang terkait dengan serangan pada log file itu menjadi tugas yang sulit bagi seorang administrator website. Banyaknya permintaan yang dilakukan oleh pengunjung website, akan meningkatkan ukuran rekaman data log yang tersimpan dalam sebuah website. Pada penelitian ini, dibuat sebuah sistem yang berfungsi sebagai alat untuk mengetahui informasi aktivitas pengunjung pada sebuah website menggunakan data access log dengan teknik regular expression. Regular Expression merupakan sebuah bahasa mini untuk mendeskripsikan string atau teks. Regular Expression dapat dipakai untuk mencocokkan sebuah string dengan sebuah pola. Pengujian dilakukan dengan data access log dari tiga website yaitu katakutu.net, berkahbarang.id dan screen6.id. Berdasarkan hasil penelitian, sistem mampu memberikan informasi mengenai pola

kunjungan seperti jumlah kunjungan halaman terbanyak, informasi data pengguna dan aktifitas berbahaya pada website. Hasil pengujian pada sistem, mendeteksi 46 serangan Cross Site Scripting, dan 983 serangan Path Traversal dengan total serangan sebanyak 1029 serangan yang merupakan aktifitas berbahaya pada website (Yogi et al., 2019)

Selanjutnya Monitoring server merupakan proses pemantauan sumber daya sistem server seperti memantau kinerja server juga membantu mengidentifikasi masalah terkait kinerja lainnya seperti pemanfaatan sumber daya, waktu henti aplikasi, dan waktu respon terhadap suatu service. File Integrity Monitoring (FIM) merupakan aktifitas memonitor integritas sebuah file untuk menjaga keutuhan suatu file dari perubahan yang tidak terotorisasi, dengan memanfaatkan Wazuh sebagai salah satu aplikasi open source untuk melakukan monitoring memiliki berbagai macam fitur untuk melakukan monitoring. Keamanan jaringan komputer menjadi hal yang perlu diperhatikan seiring berkembangnya teknologi yang pesat. Menjadi tanggung jawab bagi seorang administrator jaringan untuk memonitor keamanan sistem sewaktu-waktu. Mengingat adanya berbagai ancaman yang bisa masuk kedalam sistem kapan saja, dibutuhkan aplikasi yang dapat mendeteksi dan mencegah adanya ancaman tersebut secara realtime. Permasalahan tersebut menimbulkan gagasan untuk memanfaatkan salah satu aplikasi, yaitu Suricata yang di dalamnya terdapat metode IDS (Intruction Detection System) yang akan berfungsi sebagai pendeteksi attacker. Suricata akan menampilkan alert ketika ada paket yang mencurigakan. Alert yang dihasilkan akan disimpan didalam log file. Kemudian log tersebut akan ditampilkan pada web interface Wazuh. Alert yang tampil pada Wazuh nantinya akan dikirimkan kepada administrator jaringan melalui e-mail. (Fitri Nova et al., 2022)

Serangan File Upload yang sangat berbahaya karena memiliki posisi 10 besar pada tingkat aduan BSSN aduan pada tahun 2020 (BSSN 2021a), namun penelitian dan analisis untuk forensik terhadap serangan ini masih sedikit dan belum terlalu fokus pada live forensik terutama pada bidang cyber security terhadap serangan file upload.

Penelitian ini diharapkan dapat menambah referensi penyidik untuk mendapatkan atau mengidentifikasi serangan file upload yang selama ini semakin tinggi. Metode yang dipakai untuk mengidentifikasi tindakan serangan file upload mengunakan metode Live forensics untuk mencari artefak digital dalam log serangan yang terjadi secara real-time . Biasa dilihat tabel 2.1 Ulasan Kritis Tema.

Tabel 2.1 Ulasan Kristis Tema.

No	Peneliti	Tujuan	Pendekatan/ Metode Penelitian	Hasil Penelitian	Aspek Kritis Penelitian
1.	(Riadi et al., 2017)	Mendeteksi serangan pada router secara langsung melalui API asd	Metode yang digunakan adalah live forensics	hasilnya adalah mendapatkan pemberitahuan serangan melalui API yang dianalisis untuk mengungkapkan aktivitas illegal pada router	Penelitia ini memang menggunakan live forensik tapi hanya terbatas Serangan Brute Force.
2.	(Aji et al., 2017)	Mengembangkan sistem pengamanan jaringan berdasarkan analisis forensik jaringan	Metode menggunakan live forensics.	mengembangkan sistem pengamanan jaringan berdasarkan analisis forensik jaringan dengan fokus pada serangan HTTP Flooding menggunakan live forensics.	Hanya terbatas serangan HTTP Flooding Attack dan Tool Winbox.
3.	(Caesarano & Riadi, 2018)	Penelitian ini bertujuan untuk mengembangkan sistem web server	Mengadopsi metode NIST 800-30	Hasilnya adalah sistem web server yang menggunakan Snort untuk mendeteksi	Penelitian ini dilakukan dalam domain

No	Peneliti	Tujuan	Pendekatan/ Metode Penelitian	Hasil Penelitian	Aspek Kritis Penelitian
		yang menggunakan Snort untuk deteksi serangan SQL Injection.		serangan SQL Injection dan mengirim notifikasi serangan secara real-time melalui email.	forensik jaringan.
4.	(Riadi et al., 2019)	Tujuan penelitian ini adalah mengumpulkan log file dari framework Laravel dan mendapatkan informasi aktivitas detail dari pengguna saat mengakses server sebagai barang bukti yang dapat digunakan dalam pembuatan laporan.	Metode penelitian yang digunakan melibatkan penggunaan Framework Grr Rapid Response untuk mendeskripsikan artefak forensik dan melakukan pengambilan barang bukti forensik dengan menerapkan metode NIST.	Hasil dari penelitian ini mencakup log file dari framework Laravel yang dapat digunakan sebagai bukti dalam analisis forensik keamanan. Selain itu, penelitian ini juga berhasil mengumpulkan informasi aktivitas detail dari pengguna saat mengakses server, yang dapat menjadi bukti tambahan dalam	Penelitian ini dilakukan dalam domain forensik keamanan, khususnya dalam investigasi keamanan melalui analisis log dan artefak forensik pada aplikasi, tapi belum menggunakan metode live forensik.

No	Peneliti	Tujuan	Pendekatan/ Metode Penelitian	Hasil Penelitian	Aspek Kritis Penelitian
				investigasi keamanan. Hasil ini akan berguna dalam penyelidikan keamanan, identifikasi serangan, dan pembuatan laporan forensik.	
5.	(Pradhana et al., 2021)	Penelitian ini bertujuan untuk menerapkan forensik jaringan dalam mendeteksi serangan flooding pada router dengan menggunakan metode live forensics dan alat-alat seperti Wireshark dan Winbox.	Metode penelitian ini melibatkan penerapan framework OWASP dan network forensics untuk menganalisis, mendeteksi, dan mencegah serangan injeksi pada sisi host-based. Analisis paket data dilakukan menggunakan Wireshark dan	Hasil dari penelitian ini mencakup simulasi serangan dan solusi pencegahan. Penelitian ini menyajikan solusi pencegahan dengan melakukan browser patching pada Mozilla Firefox menggunakan add-on extension yang	Penelitian ini hanya terbatas dilakukan dalam domain forensik jaringan, khususnya dalam mendeteksi serangan flooding pada router dan menganalisis serangan injeksi di sisi host-

No	Peneliti	Tujuan	Pendekatan/ Metode Penelitian	Hasil Penelitian	Aspek Kritis Penelitian
			Live HTTP Header.	disebut XSS Filter Ade. Selain itu, penelitian ini juga memberikan pemahaman yang lebih baik tentang serangan flooding pada router dan teknik analisis forensik jaringan yang dapat digunakan untuk mendeteksi dan mencegah serangan injeksi di sisi host-based.	based, belum ada pada serangan file upload.
6.	(Yogi et al., 2019)	Penelitian ini bertujuan untuk menganalisis log server web untuk mencari pola kunjungan pengunjung	Metode penelitian yang digunakan adalah dengan mengimpleme ntasikan sistem yang menggunakan teknik regular	Hasil dari penelitian ini menunjukkan bahwa sistem yang dikembangkan berhasil mengidentifikasi 46 serangan	Penelitian ini dilakukan hanya dalam domain analisis log server web dan

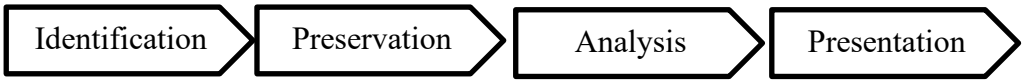
No	Peneliti	Tujuan	Pendekatan/ Metode Penelitian	Hasil Penelitian	Aspek Kritis Penelitian
		menggunakan teknik association rules	expression untuk menganalisis access log dan mengidentifikasi pola kunjungan, informasi data pengguna, serta aktivitas berbahaya pada website. Sistem ini berfungsi sebagai alat untuk memperoleh informasi tentang aktivitas pengunjung pada sebuah website.	Cross Site Scripting dan 983 serangan Path Traversal.	tujuannya adalah untuk mengidentifikasi pola kunjungan pengunjung serta aktivitas berbahaya pada website.
7.	(Fitri Nova et al., 2022)	Tujuan utamanya adalah untuk menyediakan solusi yang efektif dalam memantau	Metode penelitian yang digunakan melibatkan penerapan File Integrity Monitoring	Hasil dari penelitian ini mencakup implementasi monitoring server yang efektif dengan	Penelitian ini hanya dilakukan pada domain monitoring server dan

No	Peneliti	Tujuan	Pendekatan/ Metode Penelitian	Hasil Penelitian	Aspek Kritis Penelitian
		kinerja server, memastikan integritas file terjaga, serta mendeteksi dan mencegah ancaman keamanan secara real-time.	(FIM) untuk memantau perubahan file, serta penggunaan aplikasi Suricata sebagai Intrusion Detection System (IDS) untuk mendeteksi ancaman keamanan. Log hasil deteksi akan disimpan dalam log file dan diakses melalui antarmuka web Wazuh. Notifikasi tentang alert yang muncul akan dikirimkan kepada administrator melalui email.	menggunakan File Integrity Monitoring (FIM) dan aplikasi Suricata sebagai IDS. Dengan adanya solusi ini, administrator dapat memantau kinerja server secara aktif, memastikan integritas file terjaga, dan mendeteksi serta mencegah ancaman keamanan secara real-time.	keamanan jaringan, tapi belum menggunakan metode live forensik.

2.2 Konsep Pengetahuan

2.2.1 Digital Forensik

Digital forensik merupakan sebuah keahlian, seni dan keterampilan dalam menganalisa dan memulihkan data dari perangkat digital seperti computer, smartphone, leptop, dan lainnya (Prasad & Pandey, 2016). Tujuannya untuk mendapatkan temuan-temuan dari penyelidikan yang nantinya berguna untuk menjawab dipersidangan (Quick & Choo, 2016). Pada umumnya, proses digital forensic dibagi menjadi 4 (empat) tahap (Freiling et al., 2018) bisa dilihat pada gambar 2.1, antara lain:



Gambar 2.1 Proses Digital Forensik

a) Proses ini adalah tahapan awal (Identifikasi bukti digital). Perlu diketahui apa saja jenis bukti digitalnya, dimana disimpan, dan bagaimana penyimpanannya. Proses ini sangatlah penting dimana bukti digital yang ditemukan akan mendukung proses penyelidikan selanjutnya.
b) Proses ini adalah tahapan kedua (Preservasi bukti digital). Proses ini meliputi penyimpanan dan penyiapan bukti digital. Bukti digital memiliki sifat mudah rusak, terjadi perubahan dan bisa saja terhapus (volatile), sedikit saja terjadinya perubahan pada bukti digital maka tidak dapat di ajukan ke pengadilan.
c) Proses ini adalah tahapan ketiga (Analysis bukti digital). Setelah proses kedua ditemukan maka perlu dilakukan proses extraksi dan dilakukan proses selanjutnya yaitu analisis bukti digital. Pemeriksaan ini untuk mendapatkan suatu informasi yang digunakan untuk menjawab yang berhubungan dengan investigasi seperti siapa pelaku, apa yang terjadi, apa saja aplikasi yang digunakan, siapa pelakunya dan kapan waktunya.
d) Proses ini adalah proses terakhir (Presentation). Temuan yang didapatkan dalam proses pemeriksaan sampai analisis perlu dipresentasikan ke pihak terkait seperti penyidik ataupun pengadilan.

2.2.2 Live Forensics

Investigasi Live Forensic (Forensik Langsung) dalam konteks penelitian mengacu pada proses pengumpulan dan analisis bukti digital yang terjadi secara real-time pada sistem atau perangkat yang masih aktif. Metode ini melibatkan intervensi dan investigasi langsung pada sistem yang sedang berjalan, tanpa mengganggu operasional perangkat atau menghentikan aktivitasnya. (Umar et al., 2021)

Investigasi live forensik melibatkan pengumpulan dan analisis bukti digital dari sistem atau perangkat yang sedang berjalan. Pendekatan ini terutama menargetkan data volatil komputer, yang hanya dapat diperoleh dari sistem yang sedang berjalan (Davies et al., 2020). Beberapa teknik umum yang digunakan dalam investigasi live forensik meliputi analisis memori, pencitraan langsung, analisis garis waktu, analisis jaringan, analisis proses, dan analisis file. Teknik-teknik ini sering digunakan dalam kombinasi satu sama lain untuk memberikan pandangan menyeluruh tentang sistem dan mengidentifikasi potensi ancaman atau pelanggaran keamanan (Triawan Adi Cahyanto et al., 2022). Investigasi live forensik digunakan di berbagai bidang seperti keamanan dunia maya, investigasi kriminal, dan pemeriksaan dokter hewan forensik (Yatsenko, 2022).

1. Teknik Umum Investigasi Live Forensik

Investigasi forensik live melibatkan pengumpulan dan analisis bukti digital dari sistem atau perangkat yang sedang berjalan. Beberapa teknik umum yang digunakan dalam investigasi live forensik meliputi:

a) Analisis memori: Ini melibatkan analisis memori yang mudah menguap dari sistem yang sedang berjalan untuk mengidentifikasi proses yang sedang berjalan, koneksi jaringan, dan informasi sistem lainnya yang mungkin tidak tersedia melalui cara lain.
b) Pencitraan langsung: Ini melibatkan pembuatan gambar forensik dari sistem atau perangkat yang sedang berjalan, yang dapat digunakan untuk analisis dan penyelidikan lebih lanjut.
c) Analisis garis waktu: Ini melibatkan analisis log sistem dan data stempel waktu lainnya untuk merekonstruksi urutan peristiwa yang mengarah ke suatu insiden.
d) Analisis jaringan: Ini melibatkan analisis lalu lintas jaringan untuk mengidentifikasi aktivitas yang mencurigakan, seperti akses tidak sah atau eksfiltrasi data.
e) Analisis proses: Ini melibatkan analisis proses yang berjalan pada sistem untuk mengidentifikasi aktivitas berbahaya atau mencurigakan.

f) Analisis file: Ini melibatkan analisis file pada sistem yang sedang berjalan untuk mengidentifikasi malware, data tersembunyi, atau indikator penyusupan lainnya.

Teknik-teknik ini sering digunakan dalam kombinasi satu sama lain untuk memberikan pandangan menyeluruh tentang sistem dan mengidentifikasi potensi ancaman atau pelanggaran keamanan (Maheswari & Shobana, 2021).

2. Live Forensik dan Investigasi Forensik Tradisional

Investigasi Live forensik dan investigasi forensik tradisional adalah dua pendekatan berbeda untuk mengumpulkan dan menganalisis bukti digital.

a) Investigasi Live Forensik.

Investigasi Live Forensik melibatkan pengumpulan dan analisis bukti digital dari sistem atau perangkat yang sedang berjalan. Pendekatan ini terutama menargetkan data volatil komputer, yang hanya dapat diperoleh dari sistem yang sedang berjalan (Savoldi et al., 2010). Beberapa teknik umum yang digunakan dalam investigasi live forensik meliputi analisis memori, pencitraan langsung, analisis garis waktu, analisis jaringan, analisis proses, dan analisis file. Teknik-teknik ini sering digunakan dalam kombinasi satu sama lain untuk memberikan pandangan menyeluruh tentang sistem dan mengidentifikasi potensi ancaman atau pelanggaran keamanan (Collie, 2015). Investigasi live forensik digunakan di berbagai bidang seperti keamanan dunia maya, investigasi kriminal, dan pemeriksaan forensik dalam bidang kedokteran hewan dan manusia (H. Guo et al., 2012).

b) Investigasi Forensik Tradisional

Investigasi forensik tradisional, di sisi lain, melibatkan pengumpulan dan analisis bukti digital dari sistem atau perangkat yang tidak berjalan (Savoldi et al., 2010). Pendekatan ini menargetkan data komputer yang tidak mudah menguap, yang dapat diperoleh dari sistem yang telah dimatikan atau disita. Beberapa teknik umum yang digunakan dalam penyelidikan forensik tradisional meliputi pencitraan disk, pengukiran file, pencarian kata kunci, dan analisis metadata. Teknik-teknik ini sering digunakan dalam kombinasi satu sama lain untuk memberikan pandangan menyeluruh tentang sistem dan mengidentifikasi bukti potensial (Eisenstein et al., 2012).

Perbedaan utama antara investigasi live forensik dan investigasi forensik tradisional adalah keadaan sistem yang sedang dianalisis. Investigasi live forensik mengumpulkan

data dari sistem yang berjalan, sedangkan investigasi forensik tradisional mengumpulkan data dari sistem yang tidak berjalan. Investigasi live forensik sering digunakan ketika waktu sangat mendesak, dan ada kebutuhan untuk mengumpulkan data dengan cepat untuk mencegah kerusakan lebih lanjut atau kehilangan bukti. Investigasi forensik tradisional sering digunakan ketika tidak ada kebutuhan mendesak untuk mengumpulkan data, dan ada kebutuhan untuk menyimpan data dalam keadaan aslinya untuk analisis selanjutnya (Savoldi et al., 2010).

Singkatnya, investigasi live forensik dan investigasi forensik tradisional adalah dua pendekatan berbeda untuk mengumpulkan dan menganalisis bukti digital. Investigasi live forensik mengumpulkan data dari sistem yang berjalan, sementara investigasi forensik tradisional mengumpulkan data dari sistem yang tidak berjalan. Kedua pendekatan tersebut memiliki keuntungan dan kerugiannya masing-masing, dan pilihan pendekatan tergantung pada keadaan khusus dari penyelidikan (Savoldi et al., 2010).

3. Data volatil investigasi live forensik

Selama investigasi live forensik, data volatil dikumpulkan dari sistem atau perangkat yang sedang berjalan (Carvajal et al., 2013). Beberapa sumber umum data volatil yang dapat dikumpulkan selama investigasi live forensik meliputi:

a) RAM (Memori Akses Acak): Ini termasuk data yang disimpan dalam memori volatil komputer, seperti proses yang berjalan, koneksi jaringan, dan informasi sistem lainnya yang mungkin tidak tersedia melalui cara lain.
b) Lalu lintas jaringan: Ini termasuk data yang dikirimkan melalui jaringan, seperti email, pesan obrolan, dan transfer file.
c) Menjalankan proses: Ini termasuk informasi tentang proses yang sedang berjalan di sistem, termasuk nama, lokasi, dan file terkait.
d) Data registri: Ini termasuk data yang disimpan di registri sistem, seperti pengaturan pengguna, perangkat lunak yang diinstal, dan informasi sistem lainnya.
e) File log: Ini termasuk data yang disimpan dalam log sistem, seperti log peristiwa, log aplikasi, dan log keamanan.
f) Koneksi jaringan aktif: Ini termasuk informasi tentang koneksi jaringan yang saat ini aktif di sistem, termasuk alamat sumber dan tujuan, port, dan protokolnya.

Sumber data volatil yang dapat dikumpulkan selama penyelidikan live forensik bergantung pada keadaan khusus penyelidikan dan alat serta teknik yang digunakan oleh pemeriksa

forensik. Mengumpulkan data volatil penting dalam investigasi digital karena dapat memberikan informasi berharga tentang keadaan sistem pada saat kejadian (Paligu & Varol, 2020; Rahman & Khan, 2015)

2.2.3 Router

Router adalah perangkat jaringan yang berfungsi menghubungkan beberapa jaringan komputer atau perangkat dalam sebuah jaringan lokal (LAN) atau jaringan yang lebih luas seperti Internet. Router bertindak sebagai titik penghubung antara berbagai perangkat atau jaringan, mengarahkan lalu lintas data dari satu jaringan ke jaringan lainnya (Lucas, 2009). Fungsi utama router adalah melakukan routing, yaitu mengambil paket data dari satu jaringan dan meneruskannya ke jaringan tujuan berdasarkan alamat tujuan dalam paket tersebut. Dalam konteks Internet, router berperan penting dalam mengarahkan lalu lintas data antara jaringan lokal dan jaringan luas seperti Internet Service Provider (ISP). Router juga dapat menerapkan berbagai kebijakan keamanan, seperti firewall, untuk melindungi jaringan dari serangan dan ancaman yang berpotensi (Wang et al., 2023).

Router biasanya memiliki beberapa port yang digunakan untuk menghubungkan perangkat seperti komputer, printer, atau perangkat jaringan lainnya melalui kabel Ethernet. Beberapa router juga mendukung koneksi nirkabel (Wi-Fi) untuk menghubungkan perangkat secara wireless. Router dapat memberikan alamat IP kepada perangkat yang terhubung ke jaringan, memfasilitasi komunikasi antara perangkat tersebut, dan memungkinkan akses ke Internet (Zhou et al., 2023).

Selain fungsi dasar routing, router juga dapat memiliki fitur tambahan seperti Network Address Translation (NAT), Quality of Service (QoS), Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), dan lainnya. Fitur-fitur ini membantu mengoptimalkan kinerja jaringan, mengelola lalu lintas data, dan meningkatkan keamanan jaringan (Rasool & Jalil, 2020).

Dalam lingkungan bisnis, router sering digunakan dalam jaringan yang lebih kompleks dan berukuran besar. Router-enterprise memiliki kapasitas yang lebih tinggi, fitur keamanan yang lebih canggih, dan kemampuan untuk mengelola lalu lintas data yang lebih kompleks. Di sisi lain, router rumahan atau konsumen dirancang untuk penggunaan pribadi dan rumah tangga yang lebih sederhana. Secara keseluruhan, router adalah perangkat kunci dalam infrastruktur jaringan yang memungkinkan penghubungan dan komunikasi antara berbagai perangkat dan jaringan dalam sebuah jaringan (Lucas, 2009).

2.2.4 Web Server

Text mining Sebuah web server adalah perangkat keras atau perangkat lunak yang menyediakan layanan hosting dan mengirimkan konten web kepada pengguna melalui protokol HTTP (Hypertext Transfer Protocol). Web server bertanggung jawab untuk menerima permintaan dari klien (seperti browser web) dan mengirimkan file HTML, gambar, dokumen, atau konten lainnya ke klien tersebut (Fachri et al., 2021).

Secara umum, web server berperan sebagai tempat penyimpanan dan pengiriman berkas-berkas yang membentuk situs web. Ketika pengguna mengakses URL situs web melalui browser, permintaan dikirim ke web server yang sesuai, kemudian web server menangani permintaan tersebut dan mengirimkan respons ke klien (Chen et al., 2022).

Berikut adalah beberapa contoh web server populer:

a) Apache HTTP Server: Apache adalah web server yang paling banyak digunakan di seluruh dunia. Ini adalah perangkat lunak sumber terbuka yang stabil dan andal. Apache mendukung berbagai fitur dan dapat dijalankan di berbagai sistem operasi, seperti Linux, Windows, dan macOS (Piantadosi et al., 2019).
b) Nginx: Nginx juga merupakan web server yang populer dan sering digunakan dalam lingkungan produksi. Nginx dikenal karena performa tinggi dan kemampuannya dalam menangani lalu lintas tinggi dengan efisien. Nginx juga dapat digunakan sebagai server proxy, load balancer, dan cache (Ma & Chi, 2022).
c) Microsoft Internet Information Services (IIS): IIS adalah web server yang dikembangkan oleh Microsoft dan terintegrasi dengan sistem operasi Windows. IIS mendukung berbagai teknologi Microsoft, seperti ASP.NET dan Active Server Pages (ASP). Ini sering digunakan dalam pengembangan aplikasi web dengan menggunakan teknologi Microsoft.
d) Lighttpd: Lighttpd adalah web server open source yang dirancang untuk kinerja yang cepat dan penggunaan sumber daya yang efisien. Lighttpd sering digunakan dalam aplikasi yang membutuhkan kecepatan dan skalabilitas, seperti aplikasi web streaming media atau aplikasi permainan online.
e) Google Web Server (GWS): GWS adalah web server yang dikembangkan oleh Google untuk melayani lalu lintas pada produk dan layanan Google. GWS dikustomisasi dan dioptimalkan untuk kebutuhan Google yang sangat besar, dengan fokus pada kecepatan, keandalan, dan skalabilitas.

2.2.5 Serangan File Upload

Serangan file upload (NKD, 2019), mengacu pada upaya untuk memanfaatkan celah dalam mekanisme upload file pada suatu sistem untuk menyuntikkan atau mengunggah file yang tidak sah atau berbahaya. Serangan ini terjadi ketika pengguna dapat mengunggah file dengan ekstensi yang tidak seharusnya diizinkan oleh sistem. Contohnya, sistem hanya harus mengizinkan pengunggahan file gambar (seperti .jpg atau .png), tetapi pengguna dapat mengubah ekstensi file menjadi .php dan mengunggah file berbahaya yang dapat mengeksekusi kode di server sehingga penyerang dapat melakukan serangan web shell Serangan ini melibatkan pengunggahan file dengan ekstensi ganda, di mana file tampak seperti file yang aman (misalnya, gambar .jpg), tetapi sebenarnya file tersebut adalah file berbahaya (misalnya, shell.php.jpg). Jika sistem hanya memeriksa ekstensi pertama, file berbahaya dapat diunggah dan dijalankan.

Dalam serangan ini, penyerang mengunggah file yang berisi kode berbahaya, seperti JavaScript, yang dapat dieksekusi oleh sistem atau oleh pengguna lain yang melihat file tersebut. Tujuan serangan ini adalah untuk mencuri informasi atau mengendalikan sesi pengguna yang terhubung.Serangan ini terjadi ketika penyerang berhasil mengunggah file dengan nama yang sama dengan file yang sudah ada di server. Hal ini dapat menyebabkan file yang sah ditimpa dan mengganggu integritas data.Serangan ini melibatkan mengubah nama file atau memanipulasi ekstensi file untuk mengelabui sistem validasi. Penyerang dapat mengunggah file berbahaya dengan mengubah ekstensi file, misalnya dari .php menjadi .jpg, dan memanfaatkannya untuk menjalankan kode berbahaya.

2.2.6 Karakterisrik Serangan File Upload Secara Umum

Karakteristik serangan pada file upload secara umum penting diambil dari beberapa referensi (Huang et al., 2019; OWASP Foundation, 2023; Riadi & Aristianto, 2016; et al., 2016) adalah sebagai berikut:

a) Serangan file upload dapat memungkinkan penyerang untuk mengunggah file yang berisi kode jahat yang dapat dieksekusi pada server. Hal ini dapat memungkinkan penyerang untuk mengambil kendali atas sistem atau melakukan tindakan berbahaya sehingga menghasilkan serangan web shell atau Eksekusi Kode Jarak Jauh (Remote Code Execution)

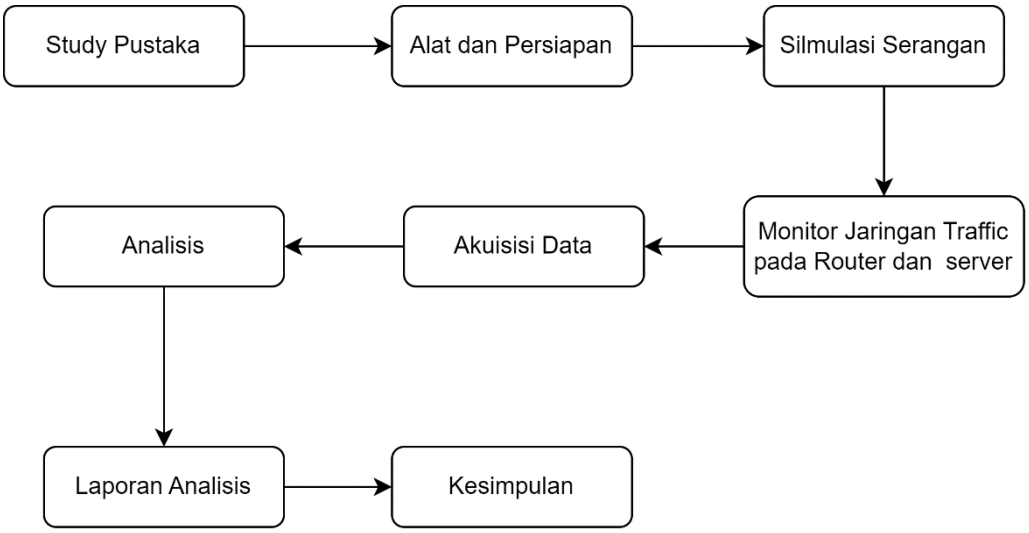
b) Penyerang dapat mencoba memanipulasi mekanisme validasi jenis file yang diunggah untuk mengunggah file yang tidak semestinya. Dengan melakukan ini, penyerang dapat memasukkan file yang berbahaya ke dalam sistem, seperti file eksekusi atau file dengan ekstensi yang tidak aman. Sehingga menjadi serangan Bypassing Tipe File.
c) Serangan file upload dapat memungkinkan penyerang untuk menyisipkan kode berbahaya ke dalam file yang diunggah. Kode ini dapat dieksekusi saat file tersebut diakses oleh pengguna lain atau sistem. Sehingga dapat melakukan Injeksi File.
d) Penyerang dapat menggunakan serangan file upload untuk mencoba mengunggah file yang berisi informasi sensitif, seperti file konfigurasi, basis data, atau file dengan data pengguna yang rahasia. Ini dapat mengarah pada pengungkapan informasi yang tidak diinginkan. Sehingga dapat melakukan Pengungkapan Informasi.
e) Penyerang dapat memanfaatkan serangan file upload untuk mengunggah file-file besar atau dalam jumlah yang sangat besar, yang dapat membebani kapasitas penyimpanan server dan mempengaruhi ketersediaan layanan misalnya serangan DDoS. Sehingga dapat menyebabkan Penyalahgunaan Kapasitas Penyimpanan
f) Penyerang dapat menggunakan serangan file upload sebagai metode untuk menyembunyikan serangan lainnya, seperti mengunggah file berbahaya dan memanfaatkannya dalam serangan XSS (Cross-Site Scripting) atau serangan lainnya terhadap pengguna atau sistem.

Mengetahui karakteristik serangan pada file upload penting untuk mengembangkan langkah-langkah pertahanan yang tepat dan menerapkan kebijakan keamanan yang kuat untuk mencegah serangan tersebut (Huang et al., 2019; OWASP Foundation, 2023; Riadi & Aristianto, 2016; et al., 2016)

BAB 3
Metodologi

3.1 Tahapan 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 et al., 2022). Metodologi penelitian ini akan menjelaskan alur kerja dari awal hingga selesai. Langkah-langkah penelitian dibuat secara sistematis dan dilengkapi dengan gambar, sehingga mudah dipahami dan kemudian bisa dijadikan panduan yang jelas untuk menyelesaikan permasalahan. Gambar 1 berikut merupakan langkah-langkah yang dilakukan pada penelitian ini.



Gambar 3.1 Tahapan Metodologi yang Diusulkan.

3.1.1 Studi Pustaka

Studi pustaka dilakukan dengan menyiapkan beberapa referensi dari buku, buku, jurnal, dan artikel ilmiah lainnya. Dalam penelitian ini, kami menggunakan pendekatan Systematic Literature Review (SLR) atau Tinjauan Literatur Sistematis untuk menyelidiki karakteristik serangan file upload pada web server dan bagaimana live forensics dapat digunakan untuk meningkatkan keamanan dalam konteks ini.

Pertama-tama, kami menentukan pertanyaan penelitian yang jelas dan terfokus, seperti "Apa saja karakteristik serangan file upload yang umum terjadi pada web server?" dan "Bagaimana live forensics dapat digunakan untuk mendeteksi dan mencegah serangan file upload pada web server?"

Kemudian, kami mengembangkan protokol penelitian yang mencakup kriteria inklusi dan eksklusi yang ketat untuk memilih artikel yang relevan dan berkualitas tinggi dalam tinjauan literatur kami. Kami melakukan pencarian literatur yang sistematis menggunakan basis data yang relevan seperti IEEE Xplore, ACM Digital Library, dan Google Scholar. Kata kunci yang relevan seperti "file upload attacks", "web server security", dan "live forensics" digunakan dalam pencarian kami.

Setelah mencari literatur, kami melakukan penilaian kualitas dan validitas artikel yang terpilih menggunakan pedoman penilaian yang telah ditetapkan sebelumnya. Kami mengevaluasi metodologi penelitian, relevansi, dan kontribusi ilmiah dari setiap artikel. Kami hanya memasukkan artikel yang memenuhi kriteria kualitas tinggi dalam tinjauan literatur kami.

Setelah mengumpulkan artikel yang relevan, kami melakukan analisis dan sintesis data dari artikel-artikel tersebut. Kami mengidentifikasi dan mencatat karakteristik umum dari serangan file upload pada web server, termasuk metode serangan, jenis file yang paling rentan, dan dampak yang mungkin timbul. Selanjutnya, kami menyelidiki bagaimana live forensics dapat diterapkan untuk mendeteksi serangan file upload secara real-time dan mencegahnya dengan mengidentifikasi pola dan perilaku yang mencurigakan.

Selama proses SLR, kami secara kritis mengevaluasi bukti yang dikemukakan dalam literatur, mengidentifikasi kelemahan, dan memberikan pemikiran kritis terhadap penggunaan live forensics untuk meningkatkan keamanan pada web server terkait serangan file upload.

Hasil dari penelitian kami disusun dan disajikan dalam laporan tinjauan literatur yang komprehensif. Kami memberikan gambaran yang jelas tentang karakteristik serangan file upload, menjelaskan konsep live forensics, dan mengidentifikasi gap penelitian yang ada serta arah penelitian masa depan yang mungkin dilakukan.

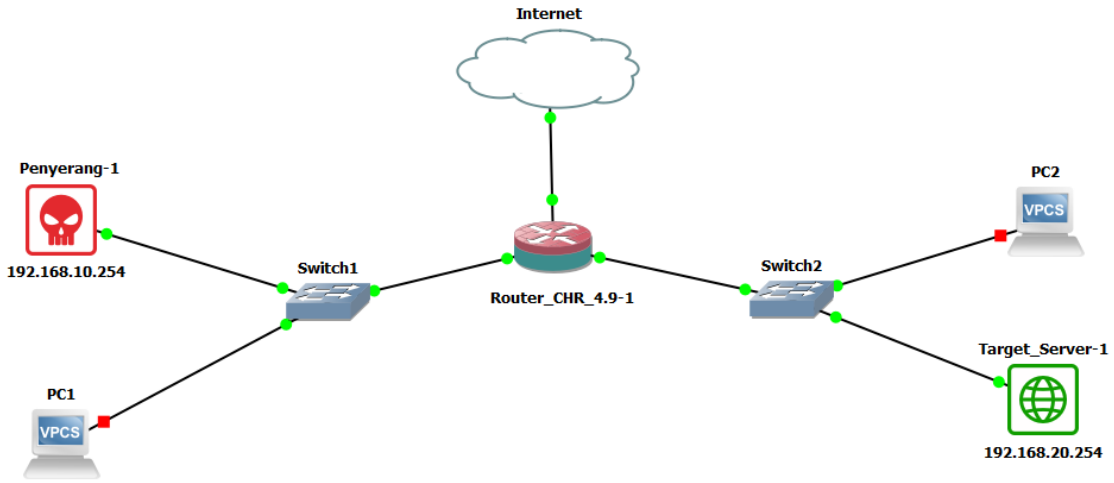
Melalui pendekatan SLR, penelitian ini diharapkan dapat memberikan kontribusi penting bagi pemahaman tentang karakteristik serangan file upload pada web server dan memberikan wawasan tentang penggunaan live forensics untuk meningkatkan keamanan.

3.1.2 Alat dan Persiapan

Alat dan persiapan yang dibutuhkan untuk melakukan simulasi serangan ini ialah satu komputer penyerang dengan OS Kali linux, satu *router* Mikrotik CHR, satu komputer *investigator*, dan satu komputer *server* sebagai targer serangan. Kemudian, *tool* yang digunakan ialah Winbox, Wireshark, dan Burpsuite.

3.1.3 Simulasi Serangan

Pada simulasi serangan, penyerang dan target *web server* terkoneksi pada jaringan *router* yang sama. Kemudian, skenario *file upload* dilakukan oleh penyerang pada sebuah *website* DVWA milik *server* yang menjadi target serangan. Serangan ke *web server* dilakukan untuk meninggalkan jejak digital pada perangkat *router*. Setelahnya, akan dilakukan proses investigasi forensik. Serangan Distributed Denial of Service (DDoS) melalui *web server* menggunakan *tools burpsuite* dan serangan *web shell* dengan meng-*upload script malicous* tersebut akan diterapkan pada simulasi ini.



Gambar 3.2 Simulasi Serangan.

Serangan DDos dan *web shell* akan disimulasikan menggunakan satu *router*, dua *switch*, satu komputer sebagai target serangan yang biasa, dan satu komputer sebagai penyerang. Dalam simulasi ini, penyerang harus melakukan dua tugas terpisah. Jenis pertama serangan DDoS dilakukan untuk meningkatkan lalu lintas di *server web* dengan mengunggah file, dengan tujuan membuat *server web* kelebihan permintaan dan mempersulit akses pengguna lain. Selama operasi normal, klien akan mengirim paket TCP SYN ke penerima untuk menyelesaikan penyesuaian paket. Penerima akan mendapatkan

respon atau pesan berupa paket *acknowledgment* TCP SYN-ACK. Setelah klien menerima paket TCP SYN-ACK, klien mengirim paket ACK yang merupakan bagian dari proses pengiriman atau pengambilan data. Serangan kedua ialah serangan *shell web*, yang melibatkan pengunggahan skrip berbahaya dengan tujuan menghancurkan *server web.* Saat *web shell* dipasang di direktori situs *web*, pengguna akan dapat mengubah direktori, memodifikasi skrip, membuat/memodifikasi *database*, dan melakukan tugas lainnya.

3.1.4 Tahapan Monitoring Traffic

Tahapan *monitoring traffic* bertujuan untuk memantau aktivitas pada *router* menggunakan *winbox* dan pada komputer *server* menggunakan *wireshark*.

Tahapan monitoring pada alat jaringan router dan web server melibatkan serangkaian langkah untuk mengamati dan menganalisis lalu lintas jaringan serta aktivitas pada server web. Berikut adalah penjelasan mengenai tahapan monitoring pada kedua alat tersebut:

a) Pengumpulan Data: Tahap pertama dalam monitoring adalah pengumpulan data terkait lalu lintas jaringan dan aktivitas pada web server. Pada router, data dapat dikumpulkan melalui log atau menggunakan tool winbox untuk memperoleh informasi tentang lalu lintas jaringan, pengguna, alamat IP, dan informasi lainnya. Pada web server, log server web dapat memberikan informasi tentang permintaan HTTP, status respons, dan aktivitas pengguna.

b) Analisis Lalu Lintas Jaringan: Data yang dikumpulkan dari router dapat dianalisis untuk mengidentifikasi pola lalu lintas yang tidak biasa atau mencurigakan. Analisis ini melibatkan pemeriksaan alamat IP asal dan tujuan, protokol yang digunakan, ukuran paket, dan pola komunikasi lainnya. Tujuannya adalah untuk mendeteksi potensi serangan atau aktivitas yang tidak diinginkan, seperti serangan DDoS, scanning port, atau anomali lalu lintas.

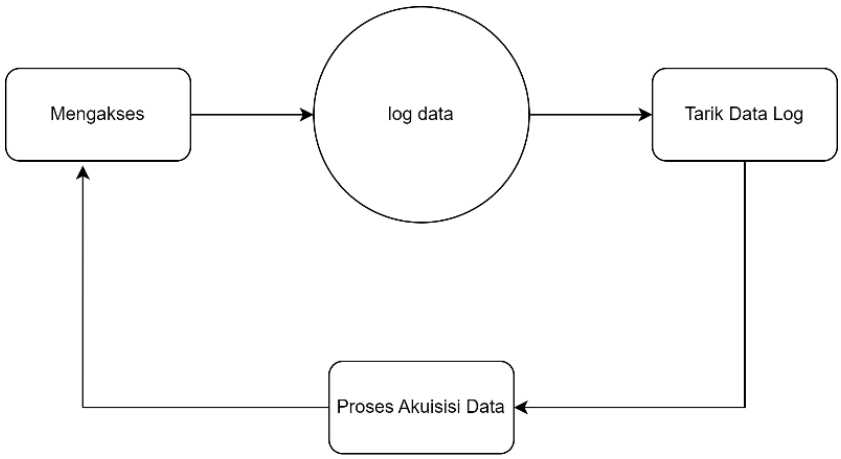
c) Analisis Log Server Web: Data dari log server web dapat dianalisis untuk memeriksa permintaan HTTP yang masuk, termasuk URL yang diakses, metode HTTP yang digunakan, status respons, dan header HTTP lainnya. Dengan menganalisis log ini, dapat terdeteksi upaya serangan, pencarian celah keamanan, atau aktivitas mencurigakan pada server web.

d) Pelaporan dan Reaksi: Setelah analisis selesai, hasilnya harus dilaporkan kepada administrator jaringan atau tim keamanan. Laporan tersebut harus berisi temuan, anomali yang ditemukan, serangan yang terdeteksi, serta rekomendasi tindakan yang harus diambil. Berdasarkan laporan tersebut, dapat diambil langkah-langkah untuk memperbaiki kelemahan yang ditemukan, memblokir serangan yang sedang berlangsung, atau mengoptimalkan konfigurasi jaringan dan server web.

Tahapan monitoring ini bertujuan untuk mendeteksi serangan atau aktivitas mencurigakan pada jaringan router dan web server secara proaktif, serta memberikan informasi yang diperlukan untuk meningkatkan keamanan dan kinerja keseluruhan sistem.

3.1.5 Tahap Akuisisi Data

Metodologi yang diusulkan merujuk pada penelitian sebelumnya, yaitu tentang tahapan akuisisi data secara *live forensic* pada *router* untuk mendeteksi serangan DDoS (Pradhana et al., 2021), sehingga tahapan akuisisi pada penelitian ini terdapat pada gambar 3.
Langkah-langkah selama penelitian akan dirinci sebagai berikut.



Gambar 3.3 Tahapan Akuisisi Data Secara Live Forensics.

(Sumber : (Pradhana et al., 2021)

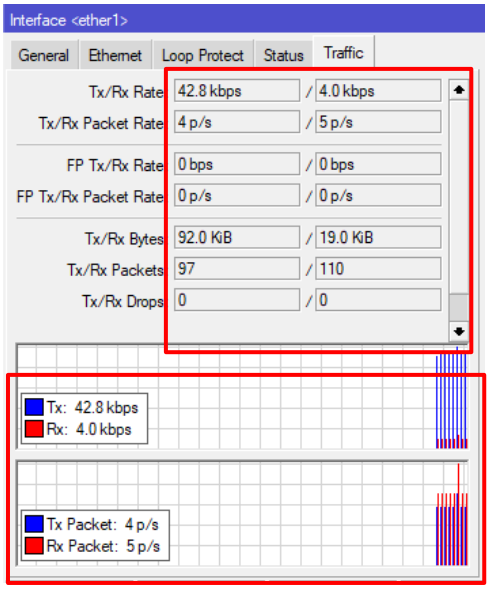
Syarat pertama yang harus terpenuhi saat menggunakan metode *live forensics* ialah sistem harus sedang berjalan/beroprasi (Setiawan et al., 2022). Tujuannya, karena informasi tertentu yang disimpan di jaringan *router* akan hilang jika sistem dimatikan atau direset, maka untuk mendapatkan data dari *router*, penyelidik komputer harus terhubung ke jaringan sebagai klien.

BAB 4
Hasil dan Pembahasan

Pada langkah ini, kita mensimulasikan suatu masalah, selanjutnya akan dilakukan pengamatan *router*, memantau lalu lintas, menganalisis file *log*, analisis forensik, dan hasil analisis. Mengikuti skenario simulasi pada Gambar 2, serangan DDoS dan *web shell* akan dilakukan melalui *file upload* di *web server*.

4.1 Analisis dan Observasi

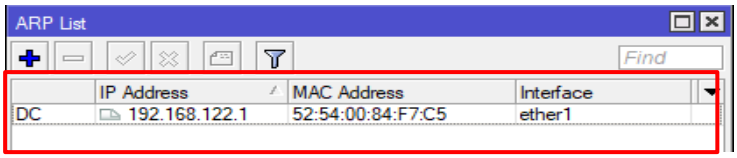
Proses awal ialah melihat *router* pada situasi normal ataupun sedang diserang, yaitu dengan cara menganalisis dan observasi pada *router*. Menu yang ada pada *Interface* dan *Traffic* merupakan bagian dari *Tool Winbox* yang bertujuan digunakan sebagai pemeriksaan *traffic* pada *router*. Ketika proses pemeriksaan terlihat bahwa *router* masih berlajan normal menandakan bahwa *web server* belum mendapatkan serangan. Hal itu dapat dilihat pada *router* grafik *traffic* Tx dan Rx.



Gambar 4.1 Traffic Pada Router Sebelum Terjadi Serangan.

Gambar 4.1 memperlihatkan bahwa *traffic* pada *router* tidak terlalu banyak, sehingga dapat disimpulkan *router* masih dalam keadaan normal.

Mencari informasi IP yang terhubung dengan *router* dapat dilakukan menggunakan *tool* yang ada pada WinBox melalui menu *List Address Resource Protocol* (ARP). Menu ARP list ini menampilkan IP Address, MAC Address, dan Interface.



Gambar 4.2 ARP List Pada Router.

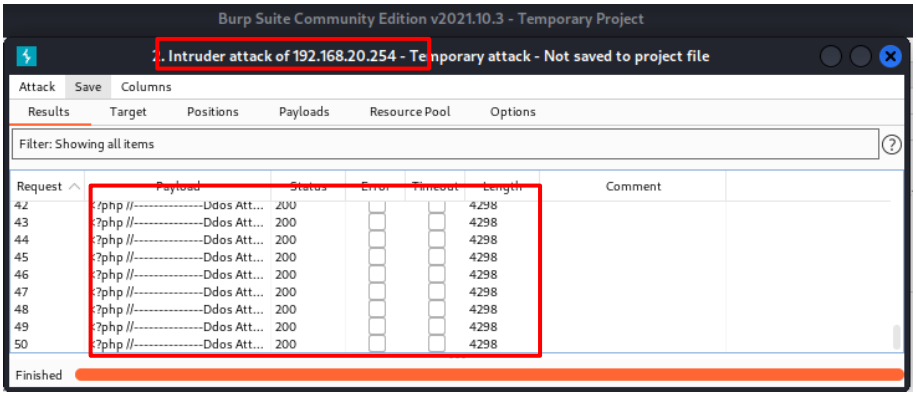
Gambar 4.2 menampilkan alamat IP Router. Alamat IP-nya ialah 192.168.122.1. Setiap IP memiliki Alamat MAC yang unik, yang dapat digunakan untuk mengumpulkan informasi. Karena tidak ada aktivitas, sehingga tidak ada alamat IP yang lain.

Bagian selanjutnya akan mensimulasikan serangan DDoS menggunakan *tool burpsuite* dan serangan *shell web* menggunakan skrip khusus yang berjalan di *server web* melalui unggahan file untuk menentukan apakah serangan berhasil dilakukan atau gagal. Bersamaan dengan itu akan dilakukan pemantauan pada *router* menggunakan aplikasi WinBox dan pemantauan dari komputer *server* menggunakan aplikasi Wireshark, kemudian secara langsung dilakukan juga penarikan data secara *live forensics* sebagai barang bukti yang dianalisis di tahap berikutnya.

4.2 Simulasi Serangan

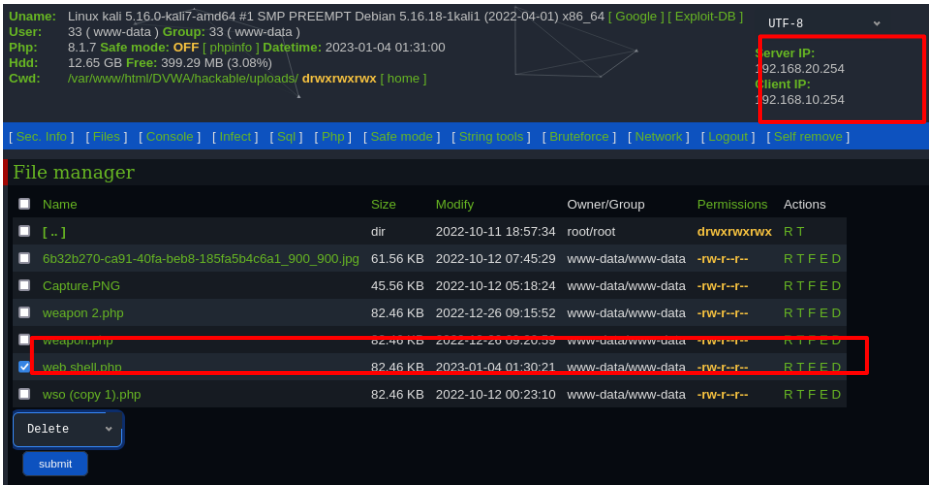
Tahapan simulasi serangan, penyerang melakukan dua jenis serangan yang berbeda mealui kerentanan *file upload* pada *web server* DVWA yang terhubung pada *router*. Serangan pertama yaitu DDoS yang akan menggunakan *tool burpusite* dan serangan kedua menggunakan *web shell* menggunakan *script* php yang dapat mengeksekusi perintah dari jarak jauh.

Serangan pertama yaitu simulasi serangan DDoS menggunakan *tool burpsuite*, meruapakan salah satu *tool* pengujian kerentanan aplikasi yang banyak digunakan oleh para praktisi keaman siber. Simulasi serangan pertama dilihat pada gambar 8.



Gambar 4.3 Simulasi Serangan DDoS.

Gambar 4.3 mendeskripsikan penyerang melakukan *attack* ke 192.168.20.254. Adapun *payload* memiliki arti senjata/*script* yang digunakan untuk menyerang. Kolom status menampilkan respon 200 yang menunjukkan bahwa serangan DDoS dengan *traffic flooding* telah dilaksanakan. Tahapan berikutnya akan dilakukan *monitoring traffic* serta akuisis data log, kemudian akan dilanjutkan kembali pada serangan ke dua yaitu *web shell* yang dapat dilihat pada gambar berikut.

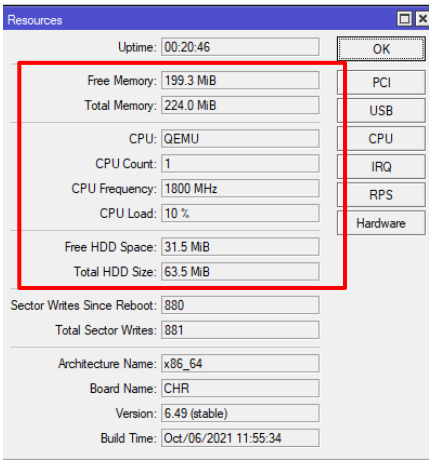


Gambar 4.4 Simulasi Serangan Web Shell.

Pada gambar tersebut tampak bahwa IP 192.168.20.254 merupakan target serangan dan sumber serangan berasal dari 192.168.10.254. Adapun script *web shell*.php merupakan *payload* yang digunakan untuk menyerang. Gambar di atas pada kolom nama menampilkan nama script *web shell*.php yang menunjukkan bahwa serangan *web shell* melalui *file upload* berhasil dilakukan, setelah serangan *web shell* berhasil dilaksanakan. Tahapan selanjutnnya akan dilakukan *monitoring traffic* dan akusisi data pada *router* melalui WinBox dan komputer *server* menggunakan Wireshak.

4.3 *Monitoring* Trafik dan Akuisisi

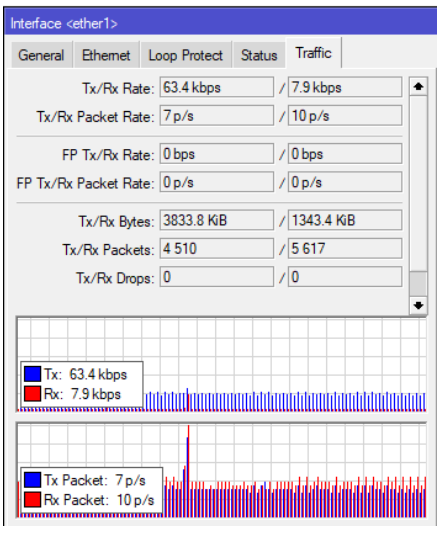
Setelah melakukan pengamatan dan simulasi terhadap serangan yang diluncurkan, tindakan selanjutnya ialah melakukan *monitoring* serangan pada *router*. Pada proses ini, trafik lalu lintas *router* akan ditangkap menggunakan aplikasi WinBox melaui komputer investigator dan *wireshark* menggunakan komputer *server*. Setelah itu, dilanjutkan dengan analisis dan mencatat aktivitas yang ditemukan pada *router* yang dipantau.



Gambar 4.5 Pemantauan Resource Router saat serangan DDoS.

Gambar 4.5 menunjukkan telah terjadi lonjakan penggunaan CPU dan memori. Hal ini terjadi akibat meningkatnya aktivitas yang diikuti dengan lintas data pada *router* yang mengganggu aktivitas yang sedang dilakukan. Kegiatan ini dapat mengakibatkan *router* mengalami beban kelebihan dan memulai ulang sistem.

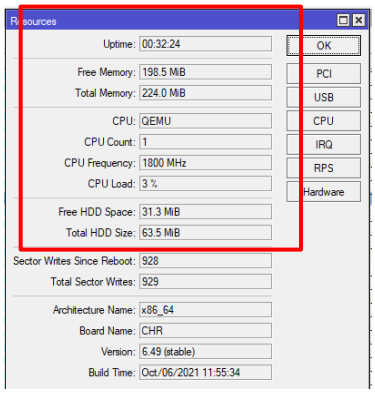
Gambar 4.5 meperlihatkan terjadinya peningkatan pada penggunakan CPU Load yang normalnya 1% atau 2% meningkat menjadi 10%. Peningkatan ini disebabkan oleh meningkatnya aktivitas *traffic* pada *router* yang jika diteruskan dapat mengakibatkan kelebihan beban pada *router* dan *web server*. Shingga, *router* dapat mengalami *restart* dan *web server* tidak dapat diakses oleh pengguna lain.



Gambar 4.6 Pemantauan Traffic Router Saat Serangan DDoS.

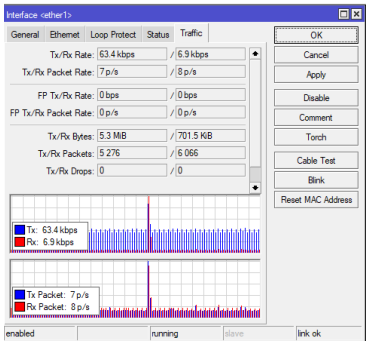
Selain peninggatan pada penggunaan CPU Load dan Memori pada *router* di menu *resource* Winbox, dapat dilihat juga pada menu *interface* juga terjadi peningkatan *traffic*

pada paket Rx Rate dan Rx Bytes yang lebih tinggi dari sebelumnya. Informasi ini menjelaskan Gambar 4.6.



Gambar 4.7 Pemantauan Resource Router Saat Serangan Web Shell.

Gambar 4.7 menunjukkan telah terjadi peningkatan penggunaan CPU dan memori, menurut laporan tersebut. Hal ini karena peningkatan aktivitas *router* terkait data yang terhambat oleh serangan yang sedang berlangsung menandakan adanya serangan yang sedang dilakukan.

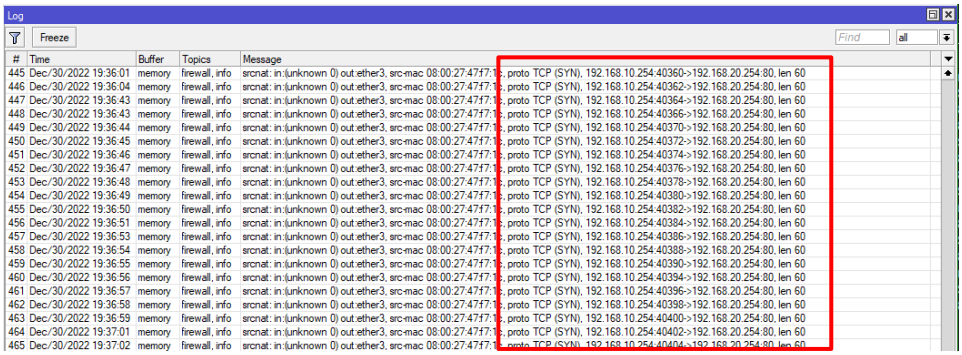


Gambar 4.8 Pemantauan Traffic Router Saat Serangan Web Shell.

Peningkatan *traffic* saat dilakukan serangan *web shell* juga terjadi, dapat dilihat pada Tx dan Rx yang meningkat saat sebelum terjadinya serangan, menandakan bahwa serangan berhasil dilakukan. Informasi ini dapat dilihat pada menu WinBox di *interface* bagian *tab traffic* pada Gambar 4.8.

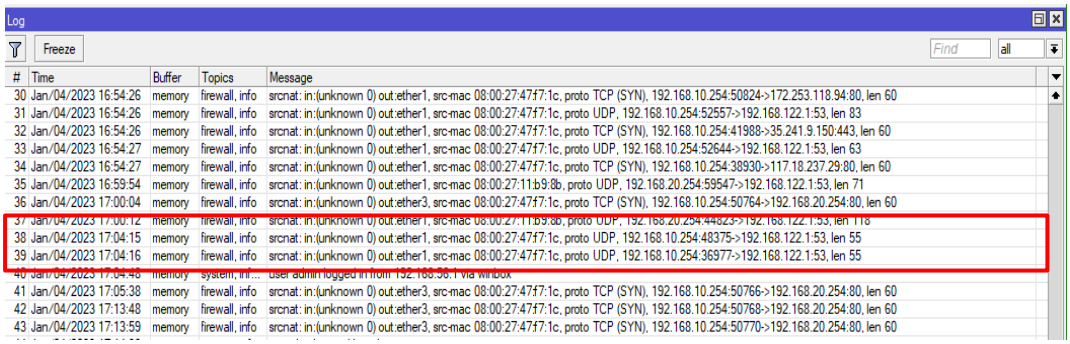
Memperkuat hasil analisis maka diperlukannya data, setelah serangan berhasil dijalankan akan dilakukan penarikan data oleh inverstigator menggunakan metode *live forensics*. Syarat agar dapat menjalankan metode *live forensics*, kondisi perangkat harus dalam keadaan hidup atau *running*, karena jika *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*. Proses akuisisi data ini dilakukan untuk mengumpulkan bukti digital dan artefak serangan guna laporan investigasi forensik dan dapat memberikan rekomendasi perbaikan. Data yang didapatkan dari proses akusisi dan pemeriksaan forensik ini berupa *Log Resource*, *Traffic log*, dan *ARP list* dapat dilihat pada Gambar 4.9.



Gambar 4.9 Monitoring Data Log Activity Router saat serangan DDoS.

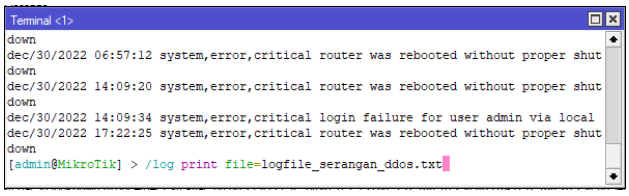
Router memiliki *log activity* yang dapat diakses melalui WinBox. Berikut ialah informasi yang didapatkan ketika terjadi serangan DDoS pada *log activty* pada *router* yaitu Time berisi bulan-tanggal-tahun, Buffer, Topics berisi info, Firewall, dan Message berisi interface, mac address, protocol, IP,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



Gambar 4.10 Monitoring Data Log Activity Router saat serangan Web Shell.

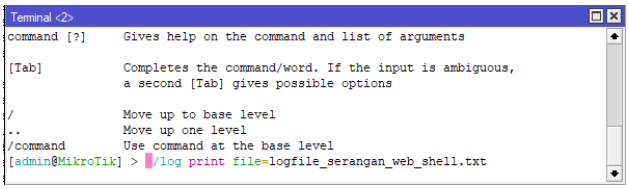
Pada Gambar 4.10 *Log Activity* pada *router* saat dilakukan serangan *Web Shell* sama seperti saat serangan sebelumnya, yaitu DDoS menampilkan informasi berupa Time (Bulan/tanggal/Tahun dan Waktu), Buffer, Topics (Firewall, info), Message (*interface*, *mac address*, *protocol*, IP Address, dan Port).

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 4.11.



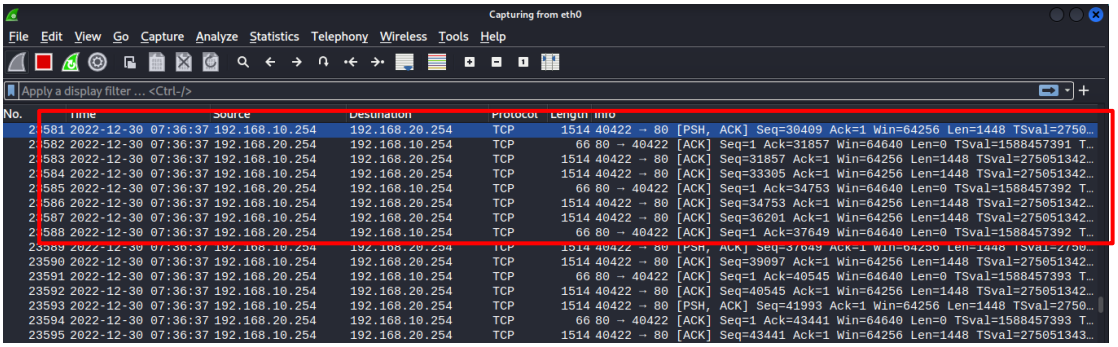
Gambar 4.11 Hasil Akuisisi Data Log Activity Router pada serangan DDoS.

Gambar 4.11 memperlihatkan proses akuisisi *log* Traffic pada *router* saat terjadi serangan DDoS 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.



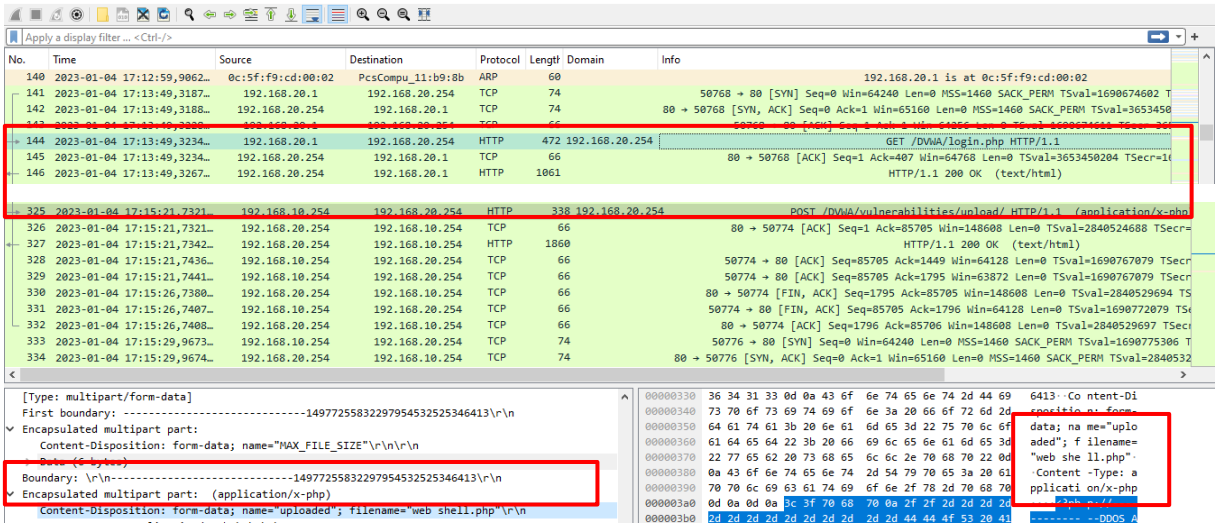
Gambar 4.12 Hasil Akuisisi Data Log Activity Serangan Web Shell.

Gambar 4.12 ialah proses akuisisi data *log traffic* yang ada pada *router* saat dilakukan serangan *Web Shell*. Tujuan dilakukannya akuisisi ini ialah karena data pada *router* akan menghilang saat dilakukan *restart* atau saat *router* dimatikan. Maka, perlu dilakukan penyimpanan alat bukti berupa *log traffic router* melalui terminal pada WinBox dengan format .txt, sehingga jika diperlukan untuk analisis lebih lanjut data masih dapat ditampilkan.



Gambar 4.13 Akuisisi Data Log Traffic Wireshark Serangan DDoS.

Serangan pertama yang dilakukan ialah DDoS bersamaan 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 4.13.



Gambar 4.14 Akuisisi Data Log Traffic Wireshark Serangan Web Shell.

Pada Gambar 4.14 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 mencari informasi yang diperlukan dalam proses penyelidikan.

4.4 Analisis Forensik dan karakteristik serangan

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 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 mengenali karakteristik artefak serangan sehingga dapat memberikan rekomendasi perbaikan.

Setelah dilakukan simulasi serangan, investigator melakukan penarikan aktivitas data log di router melalui aplikasi Winbox yang dapat dilihat hasil akuisisi log pada gambar 4.9 dan 4.10.

Pada Gambar 4.9 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 4.10 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 4.13 dan 4.14

Gambar 16 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 upaya untuk melakukan serangan DDoS. Gambar 4.14 meperlihatkan 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 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.

Dari hasil pengujian yang dilakukan maka didapatkan hasil dari Karakteristik Serangan File Upload Yang menyebabkan serangan DDOS. Pemantauan dilakukan melalui jaringan Router menggunakan aplikasi winbox secara live-realtime.

Tabel 4.1 Karakteristik Serangan File Upload-DDOS pemantauan dari router

Nama Karakteristik	**Evidence**
IP Penyerang	192.168.10.254
Port yang dilalui penyerang	80
Mac Penyerang	08:00:27:47:f7:1c

IP Korban	192.168.20.254
Mac Korban	08:00:27:47:f7:1c
Direktory Serangan	**Tidak Diketahui**
Ekstensi File	**Tidak Tiketahui**
Time stamp	2022-12-30 : 07:36
Traffic pada router	Meningkat 10 %
Script File	**Tidak Diketahui**

Dari tabel 4.1 didapatkan karakteristik serangan file upload yaitu Ip penyerang 192.168.10.254, Port yang dilalui penyerang 80, Mac Penyerang 08:00:27:47:f7:1c, IP Korban 192.168.20.254, Mac Korban 08:00:27:47:f7:1c, Direktory Serangan tidak diketahui, Ekstensi File tidak diketahui, Time stamp 2022-12-30 : 07:36, Traffic pada router meningkat 10%, script file tidak diketahui. Alasan tidak diketahui untuk direktory serangan, ekstensi file, time stamp, dan script file adalah karena pada router hanya dapat membaca hingga layer 3, sedangankan direktory serangan, ekstensi file, dan script file ada pada layer aplikasi yaitu layer 7.

Tabel 4.2 Karakteristik Serangan File Upload-DDOS pemantauan dari Web Server.

Nama Karakteristik	**Evidence**
IP Penyerang	192.168.10.254
Mac Penyerang	08:00:27:47:f7:1c
Port Yang dilalui Penyerang	80
IP Korban	192.168.20.254
Mac Korban	08:00:27:47:f7:1c
Direktory Serangan	/DVWA/vulnerabilities/upload
Ekstensi File	php
Time stamp	2022-12-30 : 07:36
Traffic pada Web Server	Meningkat 200 Request

Script File	<?php //--------------Watching webshell!-------------- if(array_key_exists('watching',$_POST)){ $tmp = $_SERVER['SERVER_NAME'].$_SERVER['PHP_SELF']."\n".$_POST['pass']; @mail('test@testmail.com', 'root', $tmp); // Edit or delete! } //-----------------Password---------------------- $□ = "fa769dac7a0a94ee47d8ebe021eaba9e"; $□ = true; $□ = 'UTF-8'; $□ = 'FilesMan'; .... ?>

Karakteristik Serangan File Upload Yang menyebabkan serangan DDOS. Pemantauan dilakukan melalui jaringan Web Server menggunakan aplikasi wireshark secara live-realtime. Dari tabel 4.2 didapatkan karakteristik serangan file upload yaitu Ip penyerang 192.168.10.254, Port yang dilalui penyerang 80, Mac Penyerang 08:00:27:47:f7:1c, IP Korban 192.168.20.254, Mac Korban 08:00:27:47:f7:1c, Direktory Serangan /DVWA/vulnerabilities/upload, Ekstensi File .php, Time stamp 2022-12-30 : 07:36, Traffic pada web server meningkat 200 Request, script file berawalan <?php dan diakhiri dengan karakter ?>.

Karakteristik Serangan File Upload Yang menyebabkan **serangan Web Shell**. Pemantauan dilakukan melalui jaringan **Router** menggunakan aplikasi winbox secara live-realime.

Tabel 4.3 Karakteristik Serangan File Upload-Web Shell pemantauan dari router.

Nama Karakteristik	**Evidence**
IP Penyerang	192.168.10.254
Port yang dilalui penyerang	80
Mac Penyerang	08:00:27:47:f7:1c
IP Korban	192.168.20.254
Mac Korban	08:00:27:47:f7:1c
Direktory Serangan	**Tidak Diketahui**
Ekstensi File	**Tidak Tiketahui**
Time stamp	2022-12-30 : 07:36
Traffic pada router	**Meningkat 10 %**
Script File	**Tidak Diketahui**

Penyerang menggunakan alamat IP 192.168.10.254 dan memanfaatkan port 80. Alamat MAC dari penyerang tercatat sebagai 08:00:27:47:f7:1c. Korban dari serangan memiliki alamat IP 192.168.20.254 dengan alamat MAC yang sama, yaitu 08:00:27:47:f7:1c. Meskipun demikian, informasi terkait direktori, ekstensi file, dan skrip tidak dapat diidentifikasi. Timestamp dari serangan adalah 2022-12-30 pada pukul 07:36. Terdapat peningkatan lalu lintas pada router sebesar 10%, namun skrip file yang digunakan penyerang tidak dapat diidentifikasi. Hal ini disebabkan oleh keterbatasan router yang hanya mampu membaca hingga layer 3, sementara direktori, ekstensi file, dan skrip terletak pada layer aplikasi (layer 7).

Karakteristik Serangan File Upload Yang menyebabkan **serangan Web Shell**. Pemantauan dilakukan melalui jaringan **Web Server** menggunakan aplikasi wireshark secara live dan realtime.

Tabel 4.4 Karakteristik Serangan File Upload-Web Shell pemantauan dari Web Server.

Nama Karakteristik	**Evidence**
IP Penyerang	192.168.10.254
Mac Penyerang	08:00:27:47:f7:1c
Port Yang dilalui Penyerang	80
IP Korban	192.168.20.254
Mac Korban	08:00:27:47:f7:1c
Direktory Serangan	/DVWA/vulnerabilities/upload
Ekstensi File	php
Time stamp	2022-12-30 : 07:36
Traffic pada Web Server	Tetap
Script File	<?php //----------Watching webshell!---------- if(array_key_exists('watching',$_POST)){ $tmp = $_SERVER['SERVER_NAME'].$_SERVER['PHP_SELF']."\n".$_POST['pass']; @mail('test@testmail.com', 'root', $tmp); // Edit or delete! } //----------Password---------- $□ = "fa769dac7a0a94ee47d8ebe021eaba9e"; $□ = true; $□ = 'UTF-8'; $□ = 'FilesMan'; .... ?>

Karakteristik Serangan File Upload Yang menyebabkan serangan DDOS. Pemantauan dilakukan melalui jaringan Web Server menggunakan aplikasi wireshark secara live-realtime. Dari tabel 4.4 didapatkan karakteristik serangan file upload yaitu Ip

penyerang 192.168.10.254, Port yang dilalui penyerang 80, Mac Penyerang 08:00:27:47:f7:1c, IP Korban 192.168.20.254, Mac Korban 08:00:27:47:f7:1c, Direktory Serangan /DVWA/vulnerabilities/upload, Ekstensi File .php, Time stamp 2022-12-30 : 07:36, Traffic pada web server meningkat 200 Request, script file berawalan <?php dan diakhiri dengan karakter ?>.

4.5 Evaluasi Perbandingan Analisis Log Router dan Log Wireshark.

Evaluasi yang dilakukan bertujuan untuk melakukan validasi agar barang bukti yang didapatkan bisa dilakukan verifikasi, dilihat akurasinya, dan kualitas temuan yang diapatkan guna menjelaskan integritas data .

Tabel 4.5 Perbandingan Analisis Log Router dan Log Wireshark.

Evidence	**Log Activity Winbox**		**Log Traffic Wireshark**	
	Ddos	**Web Shell**	**Ddos**	**Web Shell**
IP Penyerang	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan
Mac Penyerang	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan
IP korban	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan
Mac korban	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan
Timestamp	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan
Port	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan	Berhasil didapatkan
File serangan	Tidak ditemukan	Tidak ditemukan	Berhasil didapatkan	Berhasil didapatkan

Tabel 4.5 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 (Dye, 2008). *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.*

4.6 Standarisasi penemuan artefak serangan

Dalam standarisasi penemuan artefak serangan pada riset ini, rujukan utama berakar pada Bab 2, khususnya di halaman 20, yang mengulas poin-poin esensial terkait Serangan File Upload secara komprehensif. Rujukan tambahan dari studi-studi sebelumnya terkait serangan DDoS memberikan lanskap yang lebih luas dalam konteks keamanan jaringan (Zidane, 2021). Lebih lanjut, data primer yang diperoleh dari hasil penelitian ini sendiri menambah dimensi khusus yang bersumber dari analisis yang tajam terhadap metode Live Forensics untuk mengidentifikasi Serangan File Upload. Kombinasi integral dari sumber-sumber ini memperkuat landasan penelitian ini, memberikan wawasan mendalam, dan membentuk landasan kokoh guna membuat standarisasi penemuan artefak serangan file upload yang menyebabkan serangan DDOS dan Web shell pada penelitian ini yang dapat dilihat pada tabel 4.6

Tabel 4.6 Standarisasi artefak Serangan file upload-DDOS.

No	Karakteristik serangan File Upload yang menjadi serangan DDOS
1	Direktory Serangan biasanya menuju pada upload file. Misalnya, /www/file/upload/
2	Ekstensi file berbentuk .php
3	Script File diawali dengan tanda **<?php** dan di akhiri **?>** contoh : **<?php** **.....** **.....** **?>**

3	Traffick Resource pada router meningkat
4	Traffick Resource pada komputer server meningkat
5	Web Server menjadi lambat dan tidak dapat diakses

Selanjutnya untuk Standarisasi artefak serangan web shell memiliki rujukan utama berakar pada Bab 2, khususnya di halaman 20, yang mengulas poin-poin esensial terkait Serangan File Upload secara komprehensif, penelitian tentang deteksi serangan web shell (Waliulu & Jumame, 2020), (Anwar et al., 2023) dan hasil riset yang dilakukan pada penelitian ini sehingga mengahsilkan standarisasi artefak serangan web shell melalui file upload dapat dilihat pada Standarisasi artefak Serangan *file upload*-Web Shell pada Tabel 4.7.

Tabel 4.7 Standarisasi artefak Serangan file upload-Web Shell.

No	Karakteristik serangan File Upload yang menjadi serangan DDOS
1	Direktory Serangan biasanya menuju pada upload file. Misalnya, /www/file/upload/
2	Ekstensi file berbentuk .php
3	Script File diawali dengan tanda **<?php** dan di akhiri **?>** contoh : **<?php** **.....** **.....** **?>**
3	Terdapat file script tidak dikenali di dalam sever dengan ekstensi php.
4	File dalam database tiba-tiba hilang
5	Web Server menjadi lambat dan tidak dapat diakses
6	Nama file dalam database tiba-tiba berubah

4.7 Rekomendasi perbaikan

Berdasarkan analisis, data Log Activity dan Log Traffic dilakukan komparasi. Dalam Log Activity dan 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.

4.7.1. Rekomendasi perbaikan serangan File upload DDOS

Berdasarkan hasil penelitian yang telah dilakukan bersumber pada tabel 4.1 dan 4.2 didukung oleh rekomendasi perbaikan dari berbagai sumber, berikut adalah sejumlah rekomendasi untuk serangan file upload yang menjadi serangan DDOS pada riset ini dapat dilihat pada tabel 4.8.

Tabel 4.8 Rekomendasi perbaikan serangan File upload-DDOS.

No	Karakteristik serangan File Upload yang menjadi serangan DDOS	Rekomendasi Perbaikan
1	Direktory Serangan biasanya menuju pada upload file. Misalnya, /www/file/upload/	Memastikan integritas direktory file upload hanya dapat diakses oleh orang yang berhak.
2	Ekstensi file berbentuk .php	- Batasi ekstensi file untuk data yang diperlukan saja, misal upload file hanya memerlukan gambar maka izinkan ekstensi file gambar saja. - Buat validasi input agar ekstensi file tidak dapat di baypass saat dilakukan intercept oleh penyerang.
3	Script File diawali dengan tanda **<?php** dan di akhiri **?>** contoh :	Batasi input isi data file yang boleh di unggah dan yang tidak, dengan cara

	<?php **.....** **.....** **?>**	Validasi isi file yang boleh dan yang tidak boleh diupload, dalam kasus ini karakter isi file dengan tanda **<?php** dan di akhiri **?>**
4	Traffick Resource pada router meningkat	Setting firewall para router dengan cara
5	Traffick Resource pada komputer server meningkat	Membuat rule firewall filter dengan action drop terhadap alamat ip asal "Indiksiddos" dengan tujuan alamat ip "seranganddos". Misalnya : add chain=detect-ddos action=add-src-to-address-list address-list= seranganddos address-list-timeout=10
6	Web Server menjadi lambat dan tidak dapat diakses	Memasang SIEM seperti wazuh pada web server kemudian melakukan setting konfigurasi WAZUH dengan membuat rule Blocking serangan dan Aktif respon. Berikut ini script firewall-drop.sh pada WAZUH. <command> <name>firewall-drop</name> <executable>firewall-drop.sh</executable> <expect>srcip</expect> <timeout_allowed>yes</timeout_allowed> </command>

4.7.2. Rekomendasi perbaikan serangan File upload Web Shell

Berdasarkan hasil penelitian yang telah dilakukan bersumber pada tabel 4.3 dan 4.4 didukung oleh rekomendasi perbaikan dari berbagai sumber, berikut adalah sejumlah rekomendasi untuk serangan file upload yang menjadi serangan web shell pada riset ini dapat dilihat pada tabel 4.9.

Tabel 4.9 Rekomendasi perbaikan serangan File upload-Web Shell.

No	Karakteristik serangan File Upload yang menjadi serangan WEB SHELL	Rekomendasi Perbaikan
1	Direktory Serangan biasanya menuju pada upload file. Misalnya, /www/file/upload/	Memastikan integritas direktory file upload hanya dapat diakses oleh orang yang berhak.
2	Ekstensi file berbentuk .php	- Batasi ekstensi file untuk data yang diperlukan saja, misal upload file hanya memerlukan gambar maka izinkan ekstensi file gambar saja. - Buat validasi input agar ekstensi file tidak dapat di baypass saat dilakukan intercept oleh penyerang.
3	Script File diawali dengan tanda **<?php** dan di akhiri **?>** contoh : **<?php** **.....** **.....** **?>**	Batasi input isi data file yang boleh di unggah dan yang tidak, dengan cara Validasi isi file yang boleh dan yang tidak boleh diupload, dalam kasus ini karakter isi file dengan tanda **<?php** dan di akhiri **?>**
4	Terdapat file script tidak dikenali di dalam sever dengan ekstensi php.	Hapus Script yang tidak dikenali atau lakukan scanning menggunakan virus total.

5	File dalam database tiba-tiba hilang.	Selalu backup rutin file pada web server secara otomatis bisa menggunakan perintah cron job. Untuk membuat perintah cron job pada web server agar backup otomatis, Anda dapat mengikuti langkah-langkah berikut: 1. Buka Terminal atau SSH ke Web Server. Akses server Anda melalui terminal atau SSH dengan menggunakan kredensial yang sesuai. 2. Buka Tabel Cron Job. Ketik perintah berikut untuk membuka tabel cron job untuk pengeditan: crontab -e Jika Anda ingin mengedit cron job untuk pengguna tertentu, tambahkan nama pengguna setelah opsi -e. Misalnya, crontab -e -u username. 3.Tambahkan Perintah untuk Backup. Anda dapat menambahkan perintah untuk backup ke file cron job. Contoh di bawah ini menunjukkan bagaimana Anda dapat menjadwalkan backup MySQL menggunakan mysqldump: 0 2 * * * /usr/bin/mysqldump -u username -ppassword nama_database > /path/ke/direktori/backup.sql 4.Simpan dan Keluar. Setelah menambahkan perintah, tekan Ctrl + X, kemudian Y untuk menyimpan perubahan, dan Enter untuk keluar.

		5.Verifikasi dan Lihat Daftar Cron Job: Anda dapat menggunakan perintah berikut untuk memeriksa apakah cron job telah ditambahkan dengan benar: crontab -l

Melihat dari sudut pandang keamanan, serangan ini disebabkan oleh kerentanan *file upload* yang tidak menerapkan keamanan dalam pembatasan file (NKD, 2019). Dampak terburuk yang dapat terjadi ialah ketika situs *web* mengizinkan mengunggah skrip sisi *server*, seperti file PHP, Java, atau Python, dan juga dikonfigurasi untuk 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*.

Rekomendasi untuk perbaikan pada serangan DDoS ialah dengan melakukan *setting* pada *firewall* pada *router* yaitu melakukan pembatasan akses ketika terjadi pengiriman paket SYN ke *web server* secara berlebihan. Untuk serangan *Web Shell* rekomendasi perbaikan dapat dilakukan pada *web server* yaitu dengan cara melakukan pembatasan ekstensi tertentu saja pada file yang dapat di-*upload*, kemudian melakukan pembatasan ukuran file agar penyerang tidak dapat melakukan *upload* file yang besar.

BAB 5
Kesimpulan dan saran

5.1 Kesimpulan

Karakteristik serangan DDoS melalui file upload yaitu Traffick Resource pada router meningkat, Traffick Resource pada komputer server meningkat, Terdapat IP yang sama melakukan pengiriman paket atau permintaan yang berulang-ulang dalam satu waktu dalam kasus ini penyerang melakukan upload file, Web Server menjadi lambat dan tidak dapat diakses. Karakteristik serangan Web Shell melalui file upload yaitu Terdapat file script tidak dikenali di dalam sever dengan ekstensi .php, File dalam database tiba-tiba hilang, Muncul file baru yang tidak dikenali didalam database, Nama file dalam database tiba-tiba berubah. Namun, terdapat keterbatasan dalam kemampuan router untuk mendeteksi file terkait serangan. Hal ini disebabkan oleh fakta bahwa router beroperasi di layer 3, yang memungkinkannya hanya untuk membaca header paket guna menentukan tujuan paket. Kemampuan untuk membaca isi dari file teks, seperti script, gambar, video, audio, dan sejenisnya tidak dimungkinkan oleh router. Dalam simulasi serangan DDoS dan web shell yang dimonitor menggunakan aplikasi Winbox, file-file terkait serangan tidak dapat diidentifikasi. Namun, pada log Wireshark yang berjalan di komputer server, semua bukti terkait dapat diidentifikasi dengan jelas. Hasil akhir dari penelitian ini adalah mengenali karakteristik serangan file upload dan memberikan rekomendasi perbaikan pada *web server* sehingga mencegah serangan selanjutnya terjadi. Berdasarkan penelitian yang dilakukan, penulis menyimpulkan bahwa penggunaan metode *live forensics* untuk mengenali karakteristik artefak serangan dapat dilakukan. Penelitian ini fokus pada objek serangan *file upload* yang adapat menyebabkan serangan DDoS dan *Web Shell*. Pendekatan penelitian menggunakan data hasil eksperimen kualitatif, yaitu data dari *router* menggunakan aplikasi Winbox dan komputer *server* menggunakan Wireshark dengan hasil dapat mengetahui IP pelaku penyerang, tanggal, waktu, protokol yang digunakan, jenis serangan, dan asal *script* yang digunakan penyerang.

5.2 Saran

Pada penelitian ini beberapa saran yang dapat diambil dalam rangka melaksanakan pengujian lebih lanjut dalam penelitian ini. Pengujian yang lebih komprehensif dapat memberikan pemahaman yang lebih mendalam tentang efektivitas dan keandalan metode

live forensics dalam mengenali serangan file upload pada web server. Dalam konteks ini, berikut adalah beberapa saran untuk memperluas pengujian selanjutnya:

a) Perluasan Pengujian pada Skala yang Lebih Besar: Melakukan pengujian pada skala yang lebih besar dapat membantu dalam menguji kehandalan dan skalabilitas metode live forensics dalam mengenali serangan file upload. Hal ini dapat melibatkan menggunakan berbagai jenis web server dengan tingkat lalu lintas yang tinggi dan variasi serangan yang lebih kompleks.
b) Pengujian pada Lingkungan yang Berbeda: Melakukan pengujian pada lingkungan yang berbeda dapat memberikan wawasan tentang kinerja metode live forensics dalam skenario yang beragam. Misalnya, pengujian dapat dilakukan pada lingkungan cloud, lingkungan virtualisasi, atau infrastruktur yang terdistribusi. Hal ini akan membantu dalam memvalidasi efektivitas metode live forensics di berbagai konteks.
c) Perbandingan dengan Metode Lain: Melakukan perbandingan kinerja dan efektivitas metode live forensics dengan metode deteksi serangan file upload lainnya. Misalnya, membandingkan dengan metode berbasis tanda tangan, analisis perilaku, atau metode deteksi berbasis mesin learning. Perbandingan ini dapat memberikan wawasan lebih lanjut tentang keunggulan dan kelemahan relatif dari masing-masing metode.

Daftar Pustaka

Ahmad, M. S., Riadi, I., & 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), 1–8. https://doi.org/10.33096/ilkom.v9i1.103.1-8

Aji, S., Fadlil, A., & Riadi, I. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 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., & Murniyanti, E. (2018). *Implementasi Web Application Firewall Menggunakan Reverseproxy*. *5*(3), 1–7.

Anwar, S., Informatika, F., Telkom, U., Karimah, S. A., Informatika, F., Telkom, U., Jadied, E. M., Informatika, F., & Telkom, UUse the "Insert Citation" button to add citations to this document.

. (2023). *Deteksi ARP Spoofing pada Jaringan Wireless Menggunakan Metode String Matching dengan Algoritma Boyer Moore dan Brute Force*. *10*(3), 3450–3454.

Arviana, G. N. (2021). *Kenali Apa Itu Aplikasi Web dan Kelebihannya Dibanding Aplikasi Mobile*. https://glints.com/id/lowongan/aplikasi-web-adalah/#.Y5z8vnbP3tQ

Bacudio, A. G., Yuan, X., Bill Chu, B. T., & Jones, M. (2011). An Overview of Penetration Testing. *International Journal of Network Security & Its Applications*, *3*(6), 19–38. https://doi.org/10.5121/ijnsa.2011.3602

BSSN. (2021a). *Laporan Tahunan Monitoring Keamanan Siber 2021*.

BSSN. (2021b). *Laporan Tahunan Monitoring Keamanan Siber Terkait Serangan 2021*.

Bugcrowd. (2022). *Remote Code Execution (RCE)*. https://www.bugcrowd.com/glossary/remote-code-execution-rce/

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

Carvajal, L., Varol, C., & Chen, L. (2013). Tools for collecting volatile data: A survey study. *2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering, TAEECE 2013*, *May 2019*, 318–322. https://doi.org/10.1109/TAEECE.2013.6557293

Chen, T., Liu, Y. X., & Huang, L. (2022). ImageGP: An easy-to-use data visualization web

server for scientific researchers. *IMeta*, *1*(1), 1–6. https://doi.org/10.1002/imt2.5

Collie, J. (2015). Tracing Forensic Artifacts from USB-Bound Computing Environments on Windows Hosts. *Athens Journal of Sciences*, *3*(1), 17–30. https://doi.org/10.30958/ajs.3-1-2

Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2020). Evaluation of live forensic techniques in ransomware attack mitigation. *Forensic Science International: Digital Investigation*, *33*. https://doi.org/10.1016/j.fsidi.2020.300979

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

Dye, M. a. (2008). Network fundamentals: CCNA exploration companion guide. In Tonya Simpson (Ed.), *Cisco Networking Academy series CN - QA76.3 .D94 2008*. Paul Boger.

Eisenstein, E. M., Ben-Yehuda, Y., Shemesh, N., & Kharasch, S. (2012). Investigation of unexplained infant deaths in Israel: Time for a different approach. *Israel Medical Association Journal*, *14*(11), 695–700.

Fachri, F., Fadlil, A., Riadi, I., Dahlan, A., Jln Soepomo, Y., & Artikel, I. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test. *JURNAL INFORMATIKA*, *8*(2). http://ejournal.bsi.ac.id/ejurnal/index.php/ji

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

Fitri Nova, Pratama, M. D., & 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), 1–7. https://doi.org/10.30630/jitsi.3.1.59

Freiling, F., Groß, T., Latzo, T., Müller, T., & ... (2018). Advances in forensic data acquisition. *IEEE Design & …*. https://ieeexplore.ieee.org/abstract/document/8424163/

Garfinkel, S. (2007). Anti-forensics: Techniques, detection and countermeasures. *ICIW 2007: 2nd International Conference on i-Warfare and Security*, *4*(March), 77–84.

Guo, H., Jin, B., & Shang, T. (2012). Forensic investigations in Cloud environments. *Proceedings - 2012 International Conference on Computer Science and Information Processing, CSIP 2012*, 248–251. https://doi.org/10.1109/CSIP.2012.6308841

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

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

Hassan, N. A. (2019). Digital Forensics Basics - A Practical Guide Using Windows OS. In N. A. Hassan (Ed.), *Digital Forensics Basics* (1st ed.). Appress. https://doi.org/10.1007/978-1-4842-3838-7_1

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

Huang, J., Li, Y., Zhang, J., & Dai, R. (2019). UChecker: Automatically Detecting PHP-Based Unrestricted File Upload Vulnerabilities. *Proceedings - 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2019, June 2019*, 581–592. https://doi.org/10.1109/DSN.2019.00064

Kompas.com. (2022). *Apa Itu Router? Definisi, Fungsi, dan Jenis, dan Bedanya dengan Modem*. https://tekno.kompas.com/read/2022/08/29/14450017/apa-itu-router-definisi-fungsi-dan-jenis-dan-bedanya-dengan-modem

Koprawi, M. (2020). Dampak dan Pencegahan Serangan File Inclusion: Perspektif Developer. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, *5*(1), 40–43. 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), 9–18.

Lucas, M. W. (2009). *Cisco Routers for the Desperate*.

Ma, C., & Chi, Y. (2022). Evaluation Test and Improvement of Load Balancing Algorithms of Nginx. *IEEE Access*, *10*, 14311–14324. https://doi.org/10.1109/ACCESS.2022.3146422

Maheswari, K. U., & Shobana, G. (2021). The state of the art tools and techniques for remote digital forensic investigations. *2021 3rd International Conference on Signal Processing and Communication, ICPSC 2021*, *May*, 464–468. https://doi.org/10.1109/ICSPC51351.2021.9451718

National Security Agency. (2020, April). *Detect and Prevent Web Shell Malware*. *April*, 1–17. https://media.defense.gov

NKD, F. (2019). *Web security : Unrestricted File Upload Mengancam Keamanan Website*. https://www.logique.co.id

Oleg Afonin, D. N. & Y. G. (2015). *Countering Anti-Forensic Efforts – Part 1*. https://www.forensicfocus.com/articles/countering-anti-forensic-efforts-part-1/

OWASP Foundation. (2023). *Unrestricted File Upload*. https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Paligu, F., & Varol, C. (2020). Browser forensic investigations of whatsapp web utilizing indexeddb persistent storage. *Future Internet*, *12*(11), 1–17. https://doi.org/10.3390/fi12110184

Piantadosi, V., Scalabrino, S., & Oliveto, R. (2019). Fixing of security vulnerabilities in open source projects: A case study of apache HTTP server and apache tomcat. *Proceedings - 2019 IEEE 12th International Conference on Software Testing, Verification and Validation, ICST 2019*, 68–78. https://doi.org/10.1109/ICST.2019.00017

Pooj, K., & Patil, S. (2016). Understanding File Upload Security for Web Applications. *International Journal of Engineering Trends and Technology*, *42*(7), 342–347. https://doi.org/10.14445/22315381/ijett-v42p261

portswigger. (2021). *File upload vulnerabilities*. https://portswigger.net/web-security/file-upload

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

Rahman, S., & Khan, M. N. A. (2015). Review of Live Forensic Analysis Techniques. *International Journal of Hybrid Information Technology*, *8*(2), 379–388. https://doi.org/10.14257/ijhit.2015.8.2.35

Rasool, A., & Jalil, Z. (2020). A review of web browser forensic analysis tools and techniques. In *Researchpedia Journal of Computing*. researchgate.net. https://www.researchgate.net/profile/Researchpedia-Journal-Of-Computing/publication/358975880_A_Review_of_Web_Browser_Forensic_Analysis_Tools_and_Techniques/links/62204299e474e407ea1e17bc/A-Review-of-Web-Browser-Forensic-Analysis-Tools-and-Techniques.pdf

Riadi, I., & Aristianto, E. I. (2016). An Analysis of Vulnerability Web Against Attack Unrestricted Image File Upload. *Computer Engineering and Applications Journal*, *5*(1), 19–28. https://doi.org/10.18495/comengapp.v5i1.161

Riadi, I., Herman, H., & 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), 1–9. https://doi.org/10.29099/ijair.v6i2.311

Riadi, I., Luthfi, A., & 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*, *15*(2), 406–410. https://doi.org/https://sites.google.com/site/ijcsis/ ISSN 1947-5500

Riadi, I., Sunardi, S., & Kadim, A. A. (2019). Monitoring Log Aplikasi Mobile Native Menggunakan Framework Grr Rapid Response. *Jurnal Buana Informatika*, *10*(1), 1. https://doi.org/10.24002/jbi.v10i1.1909

Savoldi, A., Gubian, P., & Echizen, I. (2010). Uncertainty in live forensics. *IFIP Advances in Information and Communication Technology*, *337 AICT*, 171–184. https://doi.org/10.1007/978-3-642-15506-2_12

scalefocus. (2022). *Why Penetration Testing Is Not Enough to Secure Your Business*. https://www.scalefocus.com/blog/why-penetration-testing-is-not-enough-to-secure-your-business

Setiawan, N., Pratama, A. R., & Ramadhani, E. (2022). Jurnal Sistem dan Teknologi Informasi Metode Live Forensics untuk Investigasi Serangan Formjacking pada Website E-Commerce. *Sistem Teknologi Informasi Indonesia*, *7*(1), 1–9. http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

shilvirichiyanti. (2020). pengertian cyber crime. *Pengaruh Penanganan Cybercrime Dalam Perkembangan Teknologi Informasi*.

Susanto, M. F., Nurcahyo, A., & ... (2022). Website Threat Monitoring Untuk Pemantauan dan Analisis Ancaman Pada Web Server. *IRWNS*, *1*(2), 13–14. https://jurnal.polban.ac.id/

Teknologi.id. (2022). *Alasan Meningkatkan Keamanan Website*. WSEAS Transactions on …. https://teknologi.id

Triawan Adi Cahyanto, Rizal, M. A., Ari Eko Wardoyo, Taufiq Timur Warisaji, & Daryanto. (2022). Live Forensic to Identify the Digital Evidence on the Desktop-based WhatsApp. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *6*(2), 213–219. https://doi.org/10.29207/resti.v6i2.3849

Umar, R., Riadi, I., & Kusuma, R. S. (2021). Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method. *IJID (International Journal on*

Informatics for Development), *10*(1), 53–61. https://doi.org/10.14421/ijid.2021.2423

Waliulu, R. F., & Jumame, S. T. (2020). Desain dan Implementasi Deteksi WebShell Malicious Web Shell (Backdoor Trap). *Jurnal Sistem Informasi Bisnis*, *10*(2), 188–194. https://doi.org/10.21456/vol10iss2pp188-194

Wang, R., Dong, D., Lei, F., Ma, J., Wu, K., & Lu, K. (2023). *Roar: A Router Microarchitecture for In-network Allreduce*. 423–436. https://doi.org/10.1145/3577193.3593711

Web Dev. (2020). *7 Layar OSI*. https://newtonindonesia.co.id/7-layar-osi/

Wireshark. (2022). *Wireshark*. https://www.wireshark.org/

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

Yatsenko, I. (2022). Problems of concluding an expert opinion based on the results of a forensic veterinary examination of a live animal and ways to solve them. *Law. Human. Environment*, *13*(4), 71–88. https://doi.org/10.31548/law2022.04.008

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

Zhou, C., Lu, P., Praquin, M., Chien, T. C., Kaufman, R., Cao, X., Xia, M., Mong, R. S. K., Pfaff, W., Pekker, D., & Hatridge, M. (2023). Realizing all-to-all couplings among detachable quantum modules using a microwave quantum state router. *Npj Quantum Information*, *9*(1), 1–9. https://doi.org/10.1038/s41534-023-00723-7

Zidane, M. (2021). Klasifikasi Serangan Distributed Denial-Of-Service (DDOS) Menggunakan Metode Data Mining Naïve Bayes memperoleh gelar Sarjana Komputer Disusun oleh : *Universitas Brawijaya*, *6*(1), 63.