SKANIKA: Sistem Komputer dan Teknik Informatika
Volume 8, Nomor 1, Januari 2025, Halaman 133-144 E-ISSN: 2721-4788

Analisis Deteksi Penyusup pada Layanan *Open Journal System* Menggunakan Metode *Network Forensic Development Life Cycle*

Hero Wintolo[1*], Imam Riadi[2], Anton Yudhana[3]
[1]Fakultas Teknologi Industri, Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Fakultas Sains dan Teknologi Terapan, Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Fakultas Teknologi Industri, Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
E-mail: [1]2437083004@webmail.uad.ac.id, [2]imam.riadi@is.uad.ac.id, [3]eyudhana@ee.uad.ac.id
(*: corresponding author)

Abstrak

Penelitian ini bertujuan mendeteksi penyusup pada komputer *server* yang digunakan untuk layanan *Open Journal System* (OJS). Komputer *server* ini terhubung ke jaringan internet melalui sambungan *router*, sehingga rentan terhadap serangan dari luar. Dalam penelitian ini, *tools* yang digunakan adalah *tripwire*, yang diinstal pada komputer *server* sebagai objek utama. *Tripwire* berfungsi sebagai alat pendeteksi perubahan pada sistem *file* yang mengindikasikan aktivitas mencurigakan serta mencatat *hash file* yang valid dan memverifikasi integritas *file* terhadap catatan ini secara berkala. Sistem ini dioperasikan oleh manajer jurnal dari komputer yang terhubung ke *server* dalam satu *network address* yang memberikan layanan OJS. Metode yang digunakan dalam penelitian ini adalah *Network Forensic Development Life Cycle(*NFDLC), yang terdiri atas beberapa tahapan, yaitu inisiasi, akuisisi, implementasi, operasi, dan disposisi. Setiap tahapan diterapkan secara sistematis untuk memfasilitasi proses analisis forensik terhadap serangan yang terjadi. Hasil penelitian menunjukkan bahwa metode NFDLC efektif dalam menganalisis dan mendeteksi penyusup pada jaringan. Berdasarkan analisis forensik menggunakan *tools tripwire*, ditemukan adanya kehilangan 12 data dalam 7 insiden serangan yang teridentifikasi pada layanan OJS. Penelitian ini berhasil membuktikan bahwa metode NFDLC dan *tools tripwire* efektif dalam mendeteksi serta menganalisis penyusup yang mencoba mengakses komputer *server* layanan OJS.

Kata kunci: Deteksi, Penyusup, OJS, *tripwire*, NFDLC

Abstract

This study aims to detect intruders on a server computer used for Open Journal System (OJS) services. The server is connected to the internet via a router, making it vulnerable to external attacks. In this research, the tool used is Tripwire, installed on the server computer as the main object. Tripwire functions as a change detection tool for the file system, identifying suspicious activities and recording valid file hashes, verifying file integrity against this record periodically. The system is operated by journal managers from computers connected to the server within the same network address providing OJS services. The method used in this research is the Network Forensic Development Life Cycle (NFDLC), which consists of several stages: initiation, acquisition, implementation, operation, and disposition. Each stage is applied systematically to facilitate the forensic analysis of attacks. The research results show that the NFDLC method is effective in analyzing and detecting intruders in the network. Based on forensic analysis using Tripwire, 12 data losses were found in 7 attack incidents identified on the OJS service. This study successfully demonstrates that the NFDLC method and Tripwire tool are effective in detecting and analyzing intruders attempting to access the OJS service server computer.

***Keywords**: 3 Detection, Intruder; OJS, Tripwire, NFDLC*

1. PENDAHULUAN

Tindak kejahatan dalam bentuk gangguan keamanan di OJS perlu diantisipasi karena gangguan ini semakin meningkat, baik dari segi kuantitas atau kualitas. Komputer yang memiliki layanan tata kelola jurnal menggunakan OJS perlu dilindungi dari tindakan gangguan kejahatan yang disebabkan oleh serangan dari orang-orang yang tidak bertanggungjawab karena menyimpan dokumen yang mendukung kinerja dosen dan mahasiswa dalam bentuk artikel yang dikirimkan, dinilai, dan diterbitkan, baik untuk keperluan pribadi atau perguruan tinggi. Kejahatan yang dilakukan oleh para penyerang memberi dampak pada OJS dan menyebabkan kerugian finansial serta merusak reputasi perguruan tinggi, institusi, dan perusahaan yang

menawarkan layanan OJS tersebut. Para penulis, *editor* dan *reviewer* yang terlibat aktif pada OJS tentu akan sangat kehilangan data dengan format doc/docx atau pdf yang tersimpan dalam jurnal yang berada pada sebuah OJS yang terkena serangan, hal ini juga membuat tata kelola dari jurnal harus memberikan totalitasnya dalam pelayanan, sebagai contoh semua dokomen artikel yang diunggah oleh para penulis dan *reviewer* harus diunduh dan disimpan terlebih dahulu agar meminimalisir dampak kehilangan saat serangan terjadi.

Pengelola OJS dengan menggunakan cara unduh dan simpan untuk setiap dokumen yang masuk akan menambah pekerjaaan menjadi lebih banyak dalam menata kelola jurnalnya. Tata kelola jurnal di perguruan tinggi di Indonesia sudah banyak yang menggunakan OJS, dimana perangkat lunak ini diinstalasi dan konfigurasi pada sebuah web *server* yang dikenal secara publik. Kemudahan dalam proses instalasi dan penggunaannya membuat OJS menjadi pilihan utama dalam pengelolaan jurnal. Hingga artikel ini ditulis, OJS sudah memiliki versi sebanyak 3 versi. OJS versi pertama memiliki antar muka yang sederhana, minim fitur, tidak mendukung banyak *plugin* dan integrasi yang modern. OJS versi kedua hadir untuk memperbaiki yang menjadi kekurangan dari versi pertamanya tetapi masih saja meninggalkan kesan antarmuka yang kaku dan kurang *user friendly*. OJS terakhir versi tiga hadir dengan antar muka yang lebih baik dari versi kedua banyak *plugin*, integrasi dengan layanan pihak ketiga, serta lebih fleksibel dalam penyesuaian.

Pengelola yang melakukan tata kelola artikel yang akan diterbitkan menggunakan layanan OJS mempertimbangkan bahwa layanan ini menyediakan solusi penting untuk meningkatkan keamanan dan efisiensi pengelolaan jurnal, termasuk pengarsipan, proses editorial, dan pelacakan manuskrip secara terintegrasi [1] dibandingkan dengan membuat aplikasi berbasis web secara mandiri. Keamanan yang menjadi bagian penting dari sistem yang memberi layanan terbuka seperti OJS ini perlu dijaga dan dievaluasi setiap saat. Salah satu cara melakukan evaluasi yaitu dengan menerapkan metode *vulnerability assessment*, yang memiliki tujuan untuk mengidentifikasi kerentanan yang dapat dimanfaatkan oleh penyerang, sehingga data dan layanan lebih terlindungi [2]. Langkah-langkah seperti pencegahan akses tidak sah, mitigasi *defacement*, dan penggunaan *plugin* validasi unggahan diterapkan untuk melindungi data serta mengurangi risiko serangan[3] pada layanan ini. Selain itu, pendekatan sistematis diterapkan untuk memberikan pandangan komprehensif tentang strategi keamanan dan implementasi yang mendukung perlindungan OJS[4]. Dalam konteks pengumpulan metadata penelitian, metode web *scraping* pada OJS dengan teknik CSS *selector* dan *library beautifulsoup* turut meningkatkan keamanan dan efisiensi dengan akses data yang terstruktur serta hemat *bandwidth*, meskipun terbatas pada antarmuka standar OJS [5].

Layanan OJS ini dapat bekerja dengan baik jika didukung dengan sistem operasi dan layanan standar pengelolaan aplikasi berbasis *web* menggunakan *web server*. Peningkatan keamanan sangat dibutuhkan oleh pengelola web *server* untuk menanggulangi berbagai jenis serangan. Selain *web server*, serangan juga dapat ditujukan pada peralatan jaringan komputer. Sebagai contoh peralatan *switch* yang memiliki *feature* untuk membuat *Virtual Local Area Network*(VLAN) menggunakan *Spanning Tree Protocol*(STP) dapat mengalami serangan BPDU *config* dan *take over root bridge* sehingga memengaruhi nilai prioritas dan MAC *address* yang mengakibatkan terjadinya perubahan root ID dan bridge ID pada jaringan, untuk mengantisipasi hal tersebut diperlukan konfigurasi tambahan seperti VLAN trunking sehingga untuk keamanan jaringan menjadi lebih baik [6]. Serangan berbasis aplikasi seperti injeksi SQL, *cross-site scripting*(XSS), dan *forgery* pada *web server* dapat diidentifikasikan sebagai risiko utama gangguan keamanan data, dengan menggunakan *tools burp suite*, *nessus*, dan *wapiti*, serta dilakukan pengujian keamanan yang proaktif akan dapat membantu memitigasi risiko ini serta melindungi data dari gangguan keamanan [7]. Pada *web server* yang menerapkan *Web Application Firewall* (WAF) berbasis *modSecurity* terbukti efektif dalam melindungi *web server* dari serangan seperti *command execution* dengan respons yang diberikan berupa pesan *error* terhadap serangan, sehingga meningkatkan keamanan aplikasi *web* secara signifikan[8]. Serangan ke *web server* dalam bentuk *Distributed Denial of Service* (DDoS) seperti *slowloris* menjadi ancaman serius karena dapat menurunkan performa *web server* hingga 78%. Namun, efektivitas

deteksi serangan ini menggunakan *Host-Based Intrusion Detection System* (HIDS) mencapai 92,84%, dan *firewall* pada *layer* jaringan mampu menghentikan serangan dengan tingkat keberhasilan hingga 98,91% sehingga *firewall* menjadi solusi yang sangat efektif dalam melindungi *web server* dari ancaman DDoS [9].

Keamanan *web server* yang dirancang untuk memberikan rasa aman bagi para pengguna yang mendapatkan pelayanan sesuai dengan kebutuhannya yang memiliki peran sangat penting dalam kehidupan sehari-hari. Salah satu teknologi yang dapat digunakan untuk meningkatkan keamanan *web server* yaitu kontainer seperti *docker*. Tingkat keamanan pada *docker* yang dapat ditingkatkan secara signifikan melalui penggunaan profil *AppArmor* terbukti berhasil melindungi kontainer dari serangan dunia nyata, termasuk *privilege escalation* dan *container escape*, yang sebelumnya sulit diatasi, sehingga pendekatan keamanan *web server* menjadi lebih kuat [10]. Sedangkan pada penerapan forensik memori pada *web server* yang menggunakan *Apache*2 mampu mengidentifikasi artefak penting, seperti konfigurasi, koneksi, permintaan, dan respons yang tersimpan dalam memori, bahkan setelah struktur aslinya dihapus, sehingga memberikan solusi efektif untuk investigasi digital pada web *server* [11]. Metode analisis *log server* juga berperan dalam mendeteksi aktivitas mencurigakan, seperti potensi serangan atau manipulasi data, dengan memanfaatkan teknik monitoring untuk mengidentifikasi pola akses tidak biasa dan risiko keamanan, yang memperkuat sistem perlindungan *server* secara Keseluruhan [12].

Upaya membangun keamanan di bidang teknologi informasi mencakup perlindungan terhadap perangkat keras dan perangkat lunak terus ditingkatkan. Pada perangkat lunak yang digunakan untuk sistem ujian dengan memanfaatkan perangkat keras komputer *web server* pada layanan ujian online dengan menerapkan algoritma *Rijndael* dan *Remote Desktop Protocol* (RDP) memungkinkan enkripsi kunci *login* dapat dimanfaatkan untuk menjaga kerahasiaan informasi serta pembatasan akses selama ujian, sehingga mencegah kecurangan dan meningkatkan integritas proses ujian[13]. Kementerian Pendidikan dan Kebudayaan, memberikan layanan keamanan data gambar melalui implementasi algoritma RC4 dan metode *steganografi* EOF. Sistem ini dirancang untuk mengenkripsi dan menyembunyikan data dalam media video, melindungi informasi rahasia dari akses tidak sah [14] yang digunakan untuk ujian yang berisifat *online*. Lebih luas lagi, untuk membangun keamanan yang kokoh dalam organisasi menjadi krusial untuk menghadapi ancaman dari dalam (*insider threats*) pada sebuah perangkat lunak berbasis web. Ancaman ini sering kali datang dari pengguna sah yang memanfaatkan kerentanan sistem, sehingga pendekatan pencegahan seperti pengendalian akses berbasis atribut, analisis perilaku, dan deteksi anomali sangat diperlukan untuk melindungi organisasi dari risiko ini [15].

Membangun keamanan pada teknologi informasi yang tangguh memerlukan pemanfaatan analisis forensik terhadap serangan yang sebelumnya dilakukan oleh para *intruder*. Analisis forensik jaringan, sebagai bagian dari forensik digital, berfokus pada pengawasan dan analisis lalu lintas jaringan untuk mengumpulkan bukti setelah terjadinya serangan siber. Berbagai metode telah dikembangkan untuk mendukung proses ini. Salah satu pendekatan inovatif adalah *framework* berbasis metode *Obtain*, *Strategize*, *Collect*, *Analyze*, *Report*(OSCAR), yang dirancang untuk meningkatkan proses investigasi dengan mengidentifikasi aktivitas berbahaya, mengumpulkan data penting, serta menyusun laporan hasil analisis guna mendukung penyelidikan kejahatan siber [16]. Penggunaan metode lainnya untuk forensik digital adalah *Network Forensic Development Life Cycle* (NFDLC) digunakan untuk mengidentifikasi karakteristik bukti digital dari serangan DDoS pada router, dengan memanfaatkan alat seperti *wireshark* untuk analisis log aktivitas dan alamat IP penyerang [17]. Metode forensik digital lainnya yaitu *Trigge*r, *Acquire*, *Analysis*, *Report*, *Action* (TAARA) yang diterapkan untuk merekonstruksi serangan *ransomware Ryuk* melalui analisis log aktivitas jaringan. Proses ini melibatkan alat-alat seperti *wiresha*rk, *networkminer*, dan TCPDUMP untuk mengumpulkan serta menganalisis bukti digital[18] secara terperinci . Terakhir yang akan dihadapi dalam bentuk serangan ICMP-Flood berbasis DDoS, menggunakan analisis forensik jaringan diterapkan pada lingkungan komputasi *cloud* dan *edge* dengan melalui *packet filtering firewall* di lapisan 3 TCP/IP serta *circuit-level gateway firewall* di lapisan 4 TCP/IP untuk mitigasi dan pemulihan *server* yang terganggu [19]. Pendekatan pembuktikan bahwa analisis forensik merupakan elemen penting

dalam memperkuat keamanan siber sekaligus mengidentifikasi dan mengatasi ancaman dengan cara yang terstruktur dan efektif untuk menanggulangi gangguan pada *end device* yang dapat berbentuk *personal computer*, *cloud computing* [20], web *server* serta *server* yang digunakan dalam penelitian ini yang memberikan layanan OJS pada masyarakat.

Dari uraian terkait metode yang digunakan untuk melakukan analisis forensik, belum pernah digunakan untuk melakukan analisis forensik terhadap layanan OJS. Penelitian sebelumnya menggunakan metode ini untuk analisis forensic dengan menggunakan *tools wireshark*. Sehingga kebaruan dalam penelitian ini selain terlihat pada obyek penelitian, juga terlihat pada *tools* yang digunakan yaitu *tripwire*.

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah Metode NFDLC yang dapat dilihat pada Gambar 1. Metode ini memiliki urutan dalam proses digital forensik yang secara terurut yang harus dilakukan dengan rincian yaitu:

a. Inisiasi
   Fokus utama dalam tahap ini yaitu penilaian risiko awal pada peralatan *end device* dan *intermediary device* terhadap kemungkinan terjadinya serangan. Tahap ini akan sangat membantu dalam pengambilan keputusan perangkat lunak dan perangkat keras yang digunakan serta kerentanannya terhadap sebuah serangan.
b. Akuisisi
   Tahap ini digunakan untuk mengumpulkan data yang digunakan dalam penyelidikan sehingga membutuhkan beberapa *tools* yang berupa perangkat lunak. Dengan standar yang telah ditetapkan pada *tools* yang digunakan, maka bukti-bukti yang didapat akan dapat dimanfaatkan pada proses selanjutnya.
c. Implementasi
   Tools yang digunakan untuk mengumpulkan data yang nantinya dapat digunakan sebagai bukti telah terjadinya tindakan kejahatan mulai digunakan dan tentu saja hal ini dilakukan pendokumen yang nantinya dapat dimanfaatkan tanpa harus mengulang lagi dari awal.
d. Operasi
   Tahapan ini merupakan sebuah tahapan yang harus dilakukan karena bentuk serangan yang telah didokumenkan pada tahap sebelumnya harus dilakukan analisis menggunakan tools yang dalam penelitian ini menggunakan *tripwire*. Pada tahapan ini setiap analisis atas sebuah serangan harus tercatat dengan baik, hal ini sebagai bentuk persiapan dan antisipasi jika terjadi serangan yang sama dengan dampak yang sama atau bahkan tingkat kerusakan yang lebih parah.
e. Disposisi
   Selanjutnya yang terakhir dilakukan tahap disposisi, dimana dokumen yang telah disiapkan dan dibuat dalam rangka memberi informasi perangkat yang menjadi sasaran serangan dikirimkan kepada pimpinan tertinggi yang menjadi penanggungjawab pada institusi dimana perangkatnya telah diserang.

Gambar 1. Metode NFDLC yang digunakan dalam penelitian ini

Seperti yang terlihat pada Gambar 1, metode NFDLC ini banyak digunakan untuk melakukan digital forensik terhadap berbagai kejadian yang terkait dengan gangguan keamanan pada jaringan komputer. Gangguan ini sering juga dikenal sebagai serangan siber, menyasar obyek yang sebagian besar yaitu *end device* yang berupa komputer dengan fungsi sebagai *web server*, *mail server* dan *cloud computing* bahkan *mobile computing*. Selain *end device*, serangan juga dapat menyasar pada *intermediary device* yang berupa *switch*, *router* dan perangkat wifi.

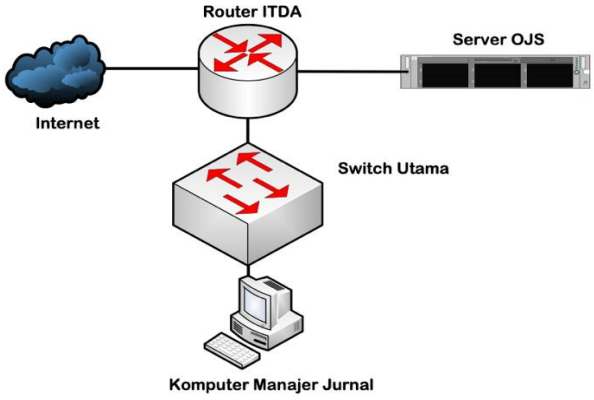
Tahapan-tahapan dalam metode NFDLC ini diterapkan untuk menganalisis deteksi penyusup pada layanan OJS yang didalamnya ada banyak jurnal yang diakses secara publik dan *open access*, meskipun pada sever yang ada layanan OJS juga ada perangkat lunak lainnya untuk memberikan layanan akademik pada sivitas academica.

3. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan melalui beberapa tahapan yang sesuai dengan metode yang digunakan dan mengikuti penelitian yang sudah menggunakan metode NFDLC. Persiapan yang dilakukan guna menunjang keberhasilan dalam penelitian ini yaitu dengan melakukan persiapan pasca serangan pertama. Sesuai dengan metode yang digunakan sebagai digital forensik, persiapan dilakukan setelah terjadinya serangan pertama yang mengakibatkan hilangnya data pada OJS tanpa diketahui penyebabnya, sehingga pengujian dilakukan secara riil dalam menghadapi serangan gelombang kedua yang terjadi pada bulan Agustus 2024.

3.1 Tahap Inisiasi

Tahap pertama adalah proses inisiasi, di mana dilakukan konfigurasi *end device*. Perangkat ini berupa komputer *web server* yang berfungsi sebagai *server* OJS serta komputer yang digunakan oleh manajer jurnal untuk mengelola jurnal yang tersimpan di *server* tersebut. Proses konfigurasi ini bertujuan untuk memastikan bahwa sistem dapat berjalan dengan baik dan mendukung pengelolaan jurnal secara efektif. Selain komputer *web server* dan komputer manajer jurnal, terdapat juga perangkat tambahan yang digunakan sebagai *intermediary device*, seperti *router* dan *switch*. Perangkat-perangkat ini berfungsi untuk menghubungkan berbagai komponen jaringan agar komunikasi antar perangkat dapat berjalan dengan lancar. Gambar 2 menunjukkan skema lengkap dari konfigurasi peralatan yang digunakan dalam penelitian ini, termasuk penempatan *end device* dan *intermediary device*.



Gambar 2. Konfigurasi jaringan yang digunakan

Proses konfigurasi perangkat dan jaringan ini merupakan langkah awal yang sangat penting untuk menjamin bahwa infrastruktur teknis yang dibutuhkan dalam pengelolaan jurnal berbasis OJS dapat berfungsi secara optimal dan mendukung tujuan penelitian ini. Konfigurasi peralatan yang digunakan dalam penelitian yang terlihat pada Gambar 2 meliputi dua perangkat *end device* dalam bentuk komputer *web server* dan *Personal Computer*(PC), dua perangkat *intermediary device* dalam bentuk *router* dan *switch* yang digunakan untuk menghubungkan *end device* dengan jaringan intrernet. OJS yang diletakan pada komputer *web server* yang memberikan pelayanan kepada manajer jurnal, *editor* jurnal, mitra bestari, penulis artikel, dan pembaca artikel yang berasal dari luar yang terhubung melalui jaringan internet serta dari dalam kampus yang tentu saja telah melalui *Domain Name System*(DNS) yang berada diluar jaringan kampus. PC yang memiliki alamat jaringan yang sama dengan OJS digunakan untuk melakukan *remote* ke OJS menggunakan *tools tripwire*. Peralatan yang digunakan dalam penelitian ini selangkapnya dapat dilihat pada Tabel 1.

Tabel 1. Alat dan Bahan

No	Alat dan Bahan	Jumlah	Keterangan
1	Komputer *server*	1	Prosesornya 2x Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz 16 Cores, RAM HP SmartMemory DDR4 2,133 MHz 64 GB
2	Komputer manajer jurnal	1	Intel® Core™ i5-10400 Processor (Cache 12M, hingga 4,30 GHz), LED 19.5" (K202HQL) Acer Monitor Resolution : (HD)1366 x 768@60 Hz, RAM 4GB DDR4 SDRAM, HDD 1TB, 7200RPM
3	*Swicth* 8 *port*	1	D-Link DGS-108
4	*Router* Mikrotik	1	Mikrotik Ethernet Router RB750Gr3 hEX
5	Koneksi Internet	1	200 mbps
6	Perangkat lunak *tripwire*	1	IP360
7	*Open Journal System*	1	Versi 2.4.8.1

Alat dan bahan yang tersaji pada Tabel 1 secara kuantitas jumlahnya satu untuk setiap peralatan yang digunakan meski dengan komposisi menjadi satu dalam obyek penelitian sebagai contoh peralatan nomor 6 diletakkan didalam peralatan nomor 1, serta peralatan nomor 7 diletakan juga pada peralatan nomor 1. Alat dan bahan terdiri dari perangkat keras dan perangkat lunak, serta perangkat jaringan yang digunakan untuk memberikan layanan OJS. Peralatan perangkat keras yang ada perangkat lunaknya yang dioperasikan oleh manager jurnal ada pada peralatan nomor 1 dan 2. Peralatan nomor 6 digunakan pada tahap selanjutnya setelah inisiasi adalah tahap akuisisi. Tahap inisiasi ini merupakan tahapan yang penting sebelum melakukan tahap akuisisi. Semua peralatan yang telah disiapkan nantinya akan digunakan sebagai tempat kejadian perkara dalam sebuah tindakan kriminal yang dalam hal ini dilakukan menggunakan jaringan internet.

3.2 Tahap Akuisisi

Peralatan dalam bentuk perangkat keras dan perangkat lunak yang disiapkan pada tahap inisasi selanjutnya digunakan untuk tahap akusisi. Tahapan ini digunakan untuk mengumpulkan data dengan menggunakan perangkat lunak yang telah diletakan didalam *web sever* sebagai perangkat utama untuk menghasilkan data primer yaitu *tripewire*. Waktu yang dibutuhkan untuk menunggu terjadinya serangan agak lama dan tidak bisa dipastikan waktunya. Hal yang pasti setelah terjadi serangan pertama sebelum dilakukan penelitian ini, pengelola sudah mengembalikan data yang hilang saat terjadi serangan di gelombang pertama, dimana pada saat itu ada keluhan dari pengelola jurnal terkait gambar pada layanan OJS yang hilang. Pada akhirnya serangan yang ditunggu itu terjadi lagi sebanyak 3 kali yang dapat dilihat pada Tabel 2.

Tabel 2. Hasil dan Analisis

No	Indikasi dan Akibat
1	Pemberi layanan domain itda.ac.id memberikan informasi dan laporan kepada Kepala Pusat Layanan Teknologi Informasi bahwa telah terjadi pelanggaran *Agreed Upon Procedures* (AUP) melalui email tanggal 21 Agustus 2023 pada domain: a. https://slot777.itda.ac.id/ b. https://elib.itda.ac.id/fileta/slot-gacor/ c. https://www.itda.ac.id/cache/slot-gacor/ d. https://ejournals.itda.ac.id/public/bandar-toto-macau/ e. https://ofes.itda.ac.id/tembak-ikan/ f. https://ofes.itda.ac.id/sd/
2	Terhapusnya seluruh data Elena, E-journals dan Senatik pada 23 Maret 2024
3	Terhapusnya seluruh directory public pada 10 Agustus 2024

Hasil dan analisis terkait kejadian serangan yang terangkum dalam tabel diatas telah mengakibatkan keadaan yang terjadi pada nomor 2 di Tabel 2, sehingga dalam tahapan yang dilakukan pada metode NFDLC selanjutnya yaitu implementasi dengan cara memasang perangkat lunak *tripware* pada komputer *web server* yang dapat di *remote* dari komputer manajer jurnal. Penggunaan *tools* ini juga menjadi penting dalam tahap akuisisi, karena pada penelitian lainnya

yang menggunakan metode NFDLC, *tools* yang sering digunakan oleh para peneliti pada tahap ini adalah *wireshark*.

Gambar 3. Proses instalasi, konfigurasi, dan eksekusi *tripwire*

3.3 Tahap Implementasi

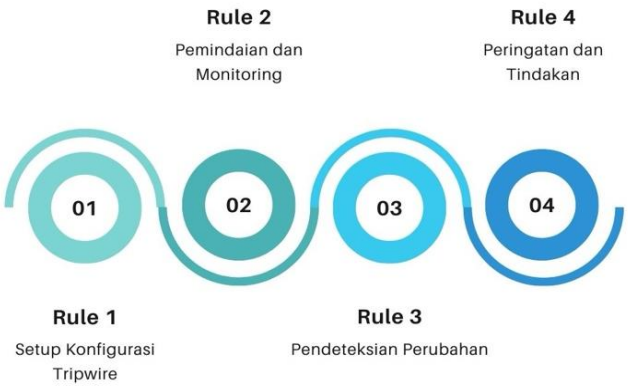
Sebelum melakukan tahapan implementasi, diperukan pesiapan yang detail untuk melakukan instalasi, konfigurasi, dan implementasi dari perangkat lunak *tripwire* yang tampak pada Gambar 3. Perangkat lunak yang digunakan sebagai *tools* dalam penelitian ini diletakan menjadi satu dengan perangkat lunak OJS pada *web server*. Proses pertama hingga keempat yang terlihat pada Gambar 3 dilakukan di computer *server*, sedangkan proses ke lima dapat dilakukan pada computer manager jurnal.

Proses selanjutnya yang dilakukan dalam penelitian ini terkait pada tahap implementasi yaitu dengan menggunakan *tripwire* untuk memantau *folder* OJS didalam *server*. Konfigurasi *tripwire* pada OJS dilakukan dengan urutan yang dapat dilihat pada Tabel 3.

Tabel 3. Konfigurasi Tripwire untuk Sistem OJS

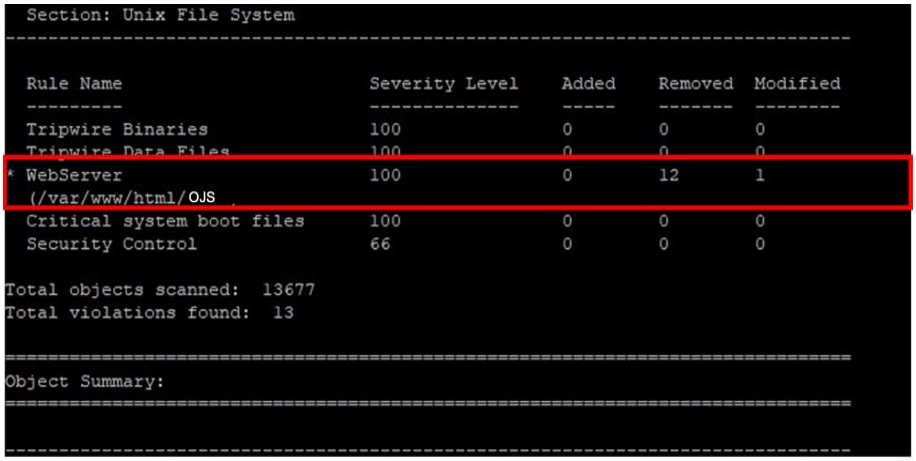
No	Sasaran	Deskripsi	Keterangan
1	Direktori OJS	Direktori atau *folder* OJS merupakan direktori yang digunakan untuk instalasi, konfigurasi dan tata kelola jurnal	/var/www/html/ojs
2	Frekuensi pemindaian	Proses pemindaian pada direktori OJS dilakukan dalam interval waktu yang ditentukan	24 jam
3	Status *folder*	Pemindaian yang dilakukan untuk memantau berubahan yang ada pada *folder* OJS terkait (ditambah, diubah, atau dihapus)	Ditambah= ada *file* atau *folder* yang ditambahkan Diubah = ada *file* atau *folder* yang mengalami perubahan Diubah = ada *file* atau *folder* yang berkurang
4	Pesan perubahan	Bertambah dan berkurangnya *file* atau *folder* dikirimkan ke pemangku kepentingan pada tata kelola server	Melalui email atau bisa menggunkan *file log system*

Tripwire sebagai *tools* yang digunakan dalam penelitian ini untuk mendapatkan bukti forensik dari tindakan kejahatan yang menyasar komputer *server* layanan OJS perlu dilakukan pengaturan agar dapat optimal dalam melakukan proses pemindaian. Seperti yang tampak pada Gambar 4, Tripwire diatur untuk mendeteksi perubahan *folder* dalam OJS menggunakan 4 langkah.



Gambar 4. Diagram pengaturan *tripwire*

Tahapan implementasi dilakukan untuk mempersiapkan diri jika terjadi jenis serangan yang sama, sehingga akan didapatkan bukti forensik yang dapat digunakan pada langkah berikutnya di metode NFDLC yang dapat dilihat pada Gambar 5. Pada kejadian serangan pertama terhadap layanan OJS yang kami kelola, perangkat lunak ini belum dipasang sehingga kejadian hilang dokumen dalam bentuk doc dan pdf pada OJS sehingga data akibat dari serangan bersumber pada para *editor* bahkan *author*.



Gambar 5. Monitoring *server* dengan *tripwire* saat penyusup melakukan kegiatan penghapusan

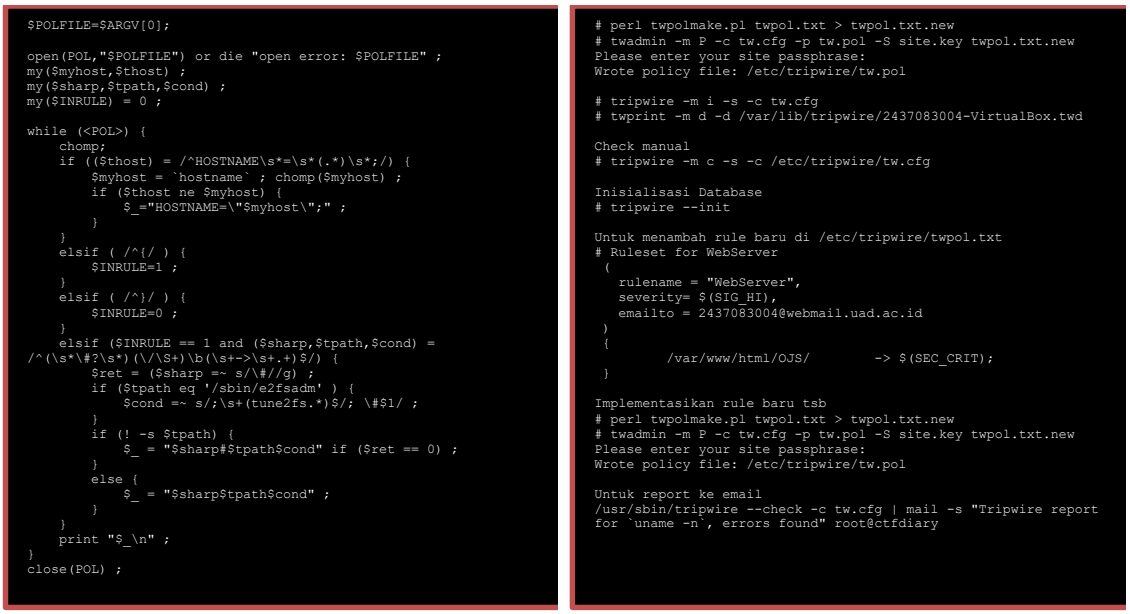
Perangkat lunak *tripwire* yang dapat dilihat pada Gambar 5 diletakan pada komputer *web server* yang didalamnya ada perangkat lunak OJS dan dikendalikan melalui komputer manager jurnal, hal ini dilakukan karena komputer *web server* yang dipasang OJS tidak boleh dioperasikan secara langsung untuk menghindari kesalahan prosedur yang dapat menggangu *web server*. Sebagai *tools* yang digunakan dalam penelitian ini, *tripwire* berbeda dengan *wireshark* yang sering digunakan sebagai *tools* dalam penelitian dengan menggunakan metode NFDLC. Cara kerja *wireshark* menangkap data paket langsung dari jaringan dan menampilkan informasi secara detail (protokol, sumber, tujuan, dll.). Sedangkan *tripwire* bekerja dengan cara mencatat hash file yang valid dan memverifikasi integritas *file* terhadap catatan ini secara berkala. *Wireshark* digunakan untuk mengidentifikasi serangan jaringan, sedangkan *tripwire* untuk mendeteksi tanda-tanda manipulasi data akibat aktivitas berbahaya. *Tools tripewire* dapat diunduh pada *web site* dengan alamat https://www.tripwire.com dapat diinstalasikan pada perangkat *end device* yaitu *web server* yang memberikan layanan OJS. Pengoperasian dari perangkat lunak yang sudah dinstalasi dan dikonfigurasi dapat dilakukan dengan mudah dengan cara *remote*. Perangkat lunak ini dapat membaca dokumen yang ditambahkan, dimodifikasi dan dihapus dari *web server* penyedia layanan OJS.

3.4 Tahap Operasi

Tahap keempat dalam metode NFDLC adalah operasi, yang dalam penelitian ini digunakan untuk mengumpulkan bukti forensik dari serangan terhadap OJS. Pada penelitian ini, *tripwire* digunakan sebagai alat forensik untuk memantau aktivitas *server*, dan berhasil merekam serangkaian kejadian serangan yang mengakibatkan hilangnya data di OJS. Sebagaimana diperlihatkan pada gambar di atas, *tripwire* mencatat kejadian dengan *Rule Name* "*web server*," dan menunjukkan 12 pada kolom "*Removed*" yang mengindikasikan bahwa sebanyak 12 data telah dihapus oleh penyerang dari *web server* yang ada aplikasi OJS. Informasi ini menjadi bukti penting adanya penghapusan data yang disengaja oleh pihak penyerang. Dengan mencatat setiap tindakan serangan tersebut, dapat dihitung bahwa dari 12 percobaan serangan, semuanya berhasil terekam oleh *tripwire* seperti yang terlihat pada Gambar 5 yang diberi garis kotak berwarna merah **memperlihatkan bahwa serangan telah dicatat**. Data yang dihasilkan dari pemindaian tersebut digunakan sebagai parameter untuk evaluasi kuantitatif sensivitas menggunakan tingkat deteksi (*Detection Rate*=DR). Tingkat deteksi yang digunakan untuk mengukur seberapa efektif *tripwire* dalam mendeteksi perubahan yang terjadi pada *folder* yang dimonitor dengan menggunakan satuan persentase dari perubahan file yang benar-benar terdeteksi oleh *tripwire* dibandingkan dengan total perubahan yang terjadi.

$$DR = \frac{Perubahan\ yang\ terdeteksi}{Jumlah\ semua\ perubahan} x\ 100\% = \frac{12}{12} x100 = 100\%$$

Keberhasilan ini menunjukkan efektivitas metode forensik yang digunakan dalam mendeteksi dan mencatat tindakan penyerang, sekaligus menyediakan dasar yang kuat untuk proses investigasi lebih lanjut dan langkah-langkah mitigasi yang dapat diambil untuk mencegah insiden serupa di masa mendatang. *Log history* yang terlihat pada Gambar 5 dapat dibuka dan dibaca karena adanya konfigurasi yang dilakukan pada *tripwire* seperti yang ditampilkan pada Gambar 6.



```
$POLFILE=$ARGV[0];

open(POL,"$POLFILE") or die "open error: $POLFILE" ;
my($myhost,$thost) ;
my($sharp,$tpath,$cond) ;
my($INRULE) = 0 ;

while (<POL>) {
    chomp;
    if (($thost) = /^HOSTNAME\s*=\s*(.*)\s*;/) {
        $myhost = `hostname` ; chomp($myhost) ;
        if ($thost ne $myhost) {
            $_="HOSTNAME=\"$myhost\";" ;
        }
    }
    elsif ( /^{/ ) {
        $INRULE=1 ;
    }
    elsif ( /^}/ ) {
        $INRULE=0 ;
    }
    elsif ($INRULE == 1 and ($sharp,$tpath,$cond) =
/^(\s*\#?\s*)(\/\S+)\b(\s+->\s+.+)$/) {
        $ret = ($sharp =~ s/\#//g) ;
        if ($tpath eq '/sbin/e2fsadm' ) {
            $cond =~ s/;\s+(tune2fs.*)$/; \#$1/ ;
        }
        if (! -s $tpath) {
            $_ = "$sharp#$tpath$cond" if ($ret == 0) ;
        }
        else {
            $_ = "$sharp$tpath$cond" ;
        }
    }
    print "$_\n" ;
}
close(POL) ;
```

```
# perl twpolmake.pl twpol.txt > twpol.txt.new
# twadmin -m P -c tw.cfg -p tw.pol -S site.key twpol.txt.new
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol

# tripwire -m i -s -c tw.cfg
# twprint -m d -d /var/lib/tripwire/2437083004-VirtualBox.twd

Check manual
# tripwire -m c -s -c /etc/tripwire/tw.cfg

Inisialisasi Database
# tripwire --init

Untuk menambah rule baru di /etc/tripwire/twpol.txt
# Ruleset for WebServer
 (
   rulename = "WebServer",
   severity= $(SIG_HI),
   emailto = 2437083004@webmail.uad.ac.id
 )
 {
        /var/www/html/OJS/        -> $(SEC_CRIT);
 }

Implementasikan rule baru tsb
# perl twpolmake.pl twpol.txt > twpol.txt.new
# twadmin -m P -c tw.cfg -p tw.pol -S site.key twpol.txt.new
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol

Untuk report ke email
/usr/sbin/tripwire --check -c tw.cfg | mail -s "Tripwire report
for `uname -n`, errors found" root@ctfdiary
```

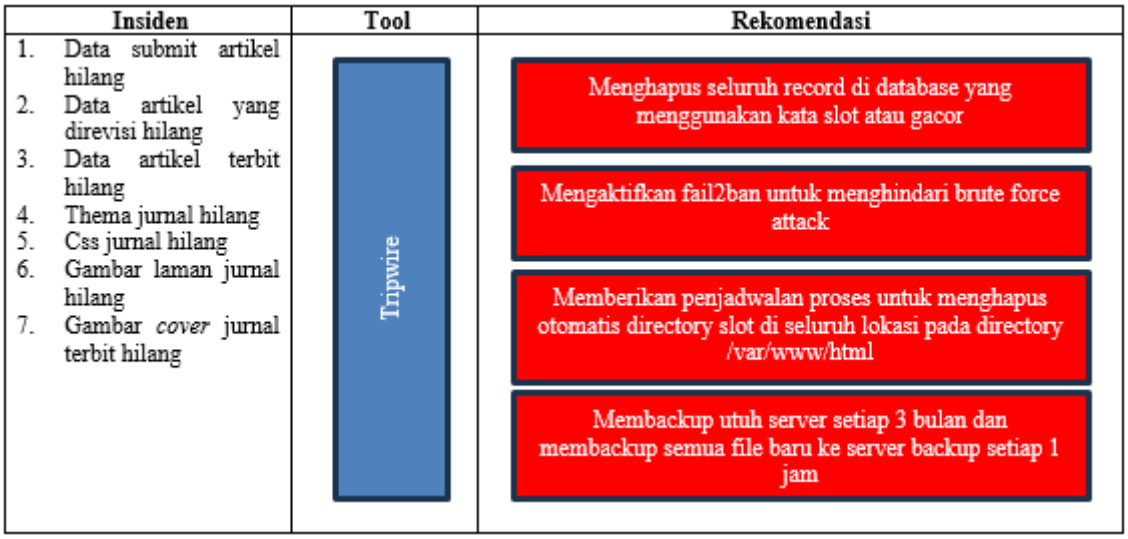
(a) (b)

Gambar 6. *Tripwire Policy File Customize Tool* (a), (b)

Tripwire Policy File adalah *file* konfigurasi yang berisi aturan atau kebijakan yang digunakan untuk memantau dan memverifikasi integritas *folder* OJS . *Tripwire* memungkinkan administrator untuk menyesuaikan kebijakan pemantauan ini sesuai dengan kebutuhan spesifik sistem yang dipantau pada OJS.

3.5 Tahap Disposisi

Tahap terakhir dari metode yang digunakan dalam penelitian ini adalah disposisi, yang dilakukan dengan pendokumentasian insiden, seperti yang ditunjukkan pada Gambar 7 bagian insiden. Gambar tersebut menampilkan catatan hilangnya data, dengan total 7 insiden yang teridentifikasi. Disposisi ini mencakup informasi detail mengenai insiden-insiden tersebut serta bukti forensik yang diperoleh menggunakan alat keamanan *tripwire*. Data insiden dan bukti forensik yang telah dikumpulkan dikirimkan kepada pimpinan sebagai bagian dari proses disposisi. Tujuan pengiriman ini dokumen ini untuk memberikan gambaran menyeluruh mengenai insiden yang terjadi, serta sebagai bahan pertimbangan penting bagi pimpinan dalam mengambil keputusan strategis terkait mitigasi dan langkah pemulihan. Dengan adanya disposisi yang baik, pimpinan dapat lebih cepat merespon kejadian serangan dan merencanakan tindakan yang lebih tepat untuk mencegah terulangnya insiden serupa di masa mendatang. Dengan menyertakan Gambar 7 pada nota dinas yang dikirmkan pada pimpinan perguruan tinggi, akan sangat membantu Tindakan pencegahan dan penanggulangan yang harus dilakukan untuk menghadapi serangan yang sama.



Gambar 7. Resume dan Rekomendasi

Metode yang digunakan dalam penelitian ini telah diterapkan pada kasus serangan terhadap OJS, di mana terdapat bukti forensik hilangnya data pada *web server* tersebut. Meskipun metode ini terbukti sukses dalam mengidentifikasi serangan, pengembangan lebih lanjut diperlukan, khususnya dalam hal mitigasi dan penanganan pasca-serangan. Penanganan tersebut akan membantu mencegah dampak yang lebih besar dan memastikan keamanan data setelah serangan terjadi.

Langkah-langkah mitigasi yang disarankan mencakup tindakan pencegahan yang lebih komprehensif serta pemulihan sistem yang lebih cepat dan efektif. Selain itu, rekomendasi terkait mitigasi dan penanganan pasca serangan telah disusun dan dapat ditemukan pada kolom Rekomendasi di Gambar 7 yaitu menghapus seluruh *record* di database yang menggunakan kata slot atau gacor, mengaktifkan fail2ban untuk menghindari *brute force attack*, memberikan penjadwalan proses untuk menghapus otomatis direktori slot di seluruh lokasi pada direktori /var/www/html, membackup utuh *web server* setiap 3 bulan dan membackup semua *file* baru ke *server* backup setiap 1 jam. Dengan demikian, metode ini tidak hanya berguna untuk mengatasi insiden yang sudah terjadi, tetapi juga untuk memperkuat pertahanan sistem di masa mendatang dan meminimalkan risiko serangan yang serupa di kemudian hari.

4. KESIMPULAN DAN SARAN

Penelitian kami pada layanan OJS menggunakan metode NFDLC dan *tools tripwire* menunjukkan bahwa metode ini dapat diterapkan secara efektif pada *platform* OJS. Hasil analisis forensik menunjukkan adanya hilangnya 12 data, dengan tingkat keberhasilan deteksi serangan sebesar 100%. Ini membuktikan bahwa kombinasi metode NFDLC dan *tripwire* mampu mendeteksi serangan secara akurat dan memberikan bukti forensik yang dapat diandalkan. Selain keberhasilan ini, penelitian juga mengidentifikasi beberapa area yang memerlukan pengembangan lebih lanjut. Salah satunya adalah pentingnya memastikan bahwa seluruh proses penanganan insiden terdokumentasi dengan baik dan terstruktur. Dokumentasi yang lebih rinci akan sangat berguna untuk mencegah dan menangani insiden serupa di masa depan, serta meningkatkan respons dan langkah mitigasi yang lebih cepat. Dokumentasi yang baik juga berperan penting dalam meningkatkan keamanan data di layanan OJS, karena dapat membantu mengidentifikasi pola serangan dan memperkuat sistem terhadap serangan di kemudian hari. Sebagai saran dari keberlanjutan penelitian ini yaitu pada pengembangan metode NFDLC di masa mendatang dapat mencakup penyempurnaan proses mitigasi dan pemulihan pasca serangan, sehingga keamanan layanan dapat ditingkatkan lebih lanjut.

DAFTAR PUSTAKA

[1] S. M. Haider, and M. Kashif, "Open Journal System," *ANNALS: Abbasi Shaheed Hospital and Karachi Medical & Dental Collage*, vol. 24, no. 2, pp. 59-61, 2019.

[2] I. Riadi, A. Yudhana, and Yunanri, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 7, no. 4, pp. 853-860, 2020.

[3] L. Verma, "Ojs security analysis: Issues, reasons, and possible solutions," *DESIDOC Journal of Library and Information Technology*, vol. 41, no. 5, pp. 391–396, 2021.

[4] Y. Arta, *et al*., "Analisa Web Server Untuk Kebutuhan Open Journal System Menggunakan Secure Tunnel Web Server Analysis for Open Journal System Needs Using Secure Tunnel," *Cogito Smart Journal*, vol. 8, no. 2, pp. 537-548, 2022.

[5] A. Purnomo, "Impementasi Web Scraping Pada OJS Dengan Metode CSS Selector," *RESOLUSI: Rekayasa Teknik Informatika dan Informasi*, vol. 3, no. 2, 63-68, 2022.

[6] Y. Indrianingsih, H. Wintolo, and E. Y. Saputri, "Spanning Tree Protocol (STP) Based Computer Network Performance Analysis on BPDU Config Attacks and Take Over Root Bridge Using the Linear Regression Method," *Jurnal Online Informatika*, vol. 6, no. 2, pp. 155-262, 2021.

[7] P. S. S. K. Gandikota, *et al.*, "Web Application Security through Comprehensive Vulnerability Assessment," *Procedia Computer Science*, Elsevier B.V., vol. 230, 2023, pp. 168–182.

[8] H. Alamsyah, "Penerapan Sistem Keamanan WEB Menggunakan Metode WEB Aplication Firewall," *Jurnal Amplifier: Jurnal Ilmiah Bidang Teknik Elektro dan Komputer*, vol. 11, no. 1, pp. 37-42, 2021.

[9] S. Suharti, A. Yudhana, and I. Riadi, "Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 3, pp. 567–582, 2022.

[10] H. Zhu and C. Gehrmann, "Lic-Sec: An enhanced AppArmor Docker security profile generator," *Journal of Information Security and Applications*, vol. 61, 2021.

[11] J. N. Hilgert, R. Schell, C. Jakobs, and M. Lambertz, "About the applicability of Apache2 web server memory forensics," *Forensic Science International: Digital Investigation*, vol. 46, pp. 1-11, 2023.

[12] D. Downs, "Spanning Student Networks: Designing Undergraduate Research Journal Websites to Foster Student–Student Mentoring," *Computer Composition*, vol. 60, pp. 2021.

[13] Z. Alamsyah, G. Purnama Insany, F. Jihad Taqwana, and K. dan Desain, "Perancangan dan Implementasi Aplikasi Keamanan Ujian Online Menggunakan Algoritma Rijndael dan Remote Desktop Protocol," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 7, no. 2, pp. 119–132, 2024.

[14] A. Fikriyan and S. Mulyati, "Sistem Pengamanan Data Gambar Menggunakan RC4 dan EOF Pada Media Video Mp4 Berbasis Java Desktop Pada Kementerian Pendidikan dan Kebudayaan," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 4, no. 2, pp. 91–98, 2021.

[15] U. Inayat, *et al*., "Insider threat mitigation: Systematic literature review," *Ain Shams Engineering Journal*, vol. 15, no. 12, pp. 1-18, 2024.
[16] A. Shah, "Evaluating Network Forensics Applying Advanced Tools," *International Journal of Advanced Engineering, Management and Science*, vol. 9, no. 4, pp. 01–09, 2023.
[17] R. H. W. Murti, I. Riadi, N. Anwar, and T. Ismail, "Forensik Jaringan Terhadap Serangan DDOS Menggunakan Metode Network Forensic Development Life Cycle," *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)*, vol. 11, no. 3, pp. 107-112, 2023.
[18] R. Surya Kusuma, R. Umar, and I. Riadi, "Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 6, no. 2, pp. 133-140, 2021.
[19] A. Yudhana, I. Riadi, and S. Suharti, "Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing," *International Journal of Safety and Security Engineering*, vol. 12, no. 5, pp. 577–588, 2022.
[20] S. Ali, *et al*., "Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing," *Egyptian Informatics Journal*, vol. 27, pp. 1-15, 2024.