Journal of Production, Enterprise, and Industrial Applications
Vol. 2, Issue 2, pp. 1–6 (2024)
doi: http://doi.org/10.25124/jpeia.v2i2.8721

RESEARCH ARTICLE

Implementasi dan Analisis Sistem Forensik Digital pada Linux Vulnerable Machine Menggunakan *Framework* Forensics Zachman

Leonardo Taufan Sontani, Avon Budiono* and Adityas Widjajarto

Fakultas Rekayasa Industri, Universitas Telkom, Bandung, 40257, Jawa Barat, Indonesia
*Corresponding author: avonbudi@telkomuniversity.ac.id

Abstrak

Berdasarkan saran dari Badan Siber dan Sandi Negara, pengumpulan, dokumentasi, dan pencatatan informasi kebocoran data perlu dilakukan dalam 24 jam pertama sejak insiden terjadi. Penelitian ini melakukan aktivitas digital forensik terhadap perangkat Linux dengan menggunakan *framework* Zachman dan membandingkan tiga aplikasi forensik berdasarkan kemampuannya untuk melakukan forensic digital. Penilaian pada perbandingan aplikasi forensik dilakukan berdasarkan keberhasilannya dalam melakukan aktivitas forensik. Sedangkan penilaian data keluaran log dilakukan berdasarkan informasi yang terkait dengan penyerangan dengan tiap informasi. Berdasarkan hasil analisis data pada perbandingan aplikasi forensik, FTK Imager mendapat nilai tertinggi yaitu 7. Pencarian data yang terhapus sulit dilakukan pada FTK Imager karena FTK Imager tidak mencantumkan nama file pada temuan data terhapus. Berdasarkan hasil analisis data perbandingan kelengkapan informasi log, access.log mendapatkan nilai 14 dengan mencatat pemindaian dengan Nikto, akses ke robots.txt, dan akses ke aplikasi *database* MongoDB.

Key words: Forensik digital, *Framework*, FORZA, Typhoon, Log.

Pendahuluan

Berdasarkan data dari Badan Siber dan Sandi Negara [1], total anomali lalu lintas internet di Indonesia mencapai 976 juta serangan. Meski jumlah tersebut menurun 40% dari tahun 2021 dengan 1,6 miliar serangan, jumlah tersebut masih lebih tinggi apabila dibandingkan dengan tahun 2019 dengan 290 juta serangan, dan tahun 2020 dengan temuan 495 juta serangan. Berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 24 ayat (1), (2), (3), pemilik sistem elektronik tidak hanya harus menjalankan prosedur pengamanan sistem elektronik, pemilik sistem juga harus menyediakan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan, serta melaporkan ke pihak yang berwajib apabila terjadi kegagalan atau gangguan sistem yang serius akibat terjadinya serangan dari pihak luar.

Tinjauan Pustaka

Forensik Digital

Forensik digital adalah metode pengamanan, identifikasi, ekstraksi, interpretasi, dan dokumentasi dari bukti komputer, yang tetap memerhatikan integritas bukti dan proses hukum yang ada. Forensik digital dapat disamakan dengan menganalisis tempat kejadian perkara. Tujuan adanya forensik yaitu untuk mengembalikan, menganalisis, dan menampilkan bukti komputer yang bisa ditampilkan di pengadilan.

FORZA

Framework Zachman, atau disingkat sebagai FORZA, adalah *framework* yang menggabungkan antara peran, tanggung jawab, beserta prosedur menjadi satu. Layer terhubung satu sama lain berdasarkan enam kategori pertanyaan:

1. Apa (atribut data)
2. Kenapa (motivasi)
3. Bagaimana (prosedur)
4. Siapa (orang)
5. Dimana (lokasi), dan
6. Kapan (waktu)

Bukti Digital

Berdasarkan Casey [2], bukti digital adalah informasi pembuktian yang tersimpan atau terkirim dalam bentuk digital yang dapat digunakan sebagai barang bukti pada persidangan.

Metodologi Penelitian

Pada alur pengujian skenario penyerangan, tahap pertama adalah menjalankan virtual machine target yang digunakan sebagai objek penelitian. Tahap kedua adalah menjalankan *virtual machine attacker* sebagai penyerang untuk melakukan implementasi *attack tools*. Tahap ketiga melakukan implementasi *attack tools* berdasarkan salah satu

Table 1. A

Singkatan	Deskripsi	
	Nama	**Pemakaian Pertama Pada Halaman**
FORZA	Forensics Zachman	4
SOP	Standard Operating Procedure	5
SWGDE	Scientific Working Group on Digital Evidence	5
RFC	Request For Comments	7
SHA	Secure Hashing Algorithm	21
CVE	Common Vulnerabilities and Exposures	28
CVSS	Common Vulnerabilities and Scoring System	28
OSVDB	Open Source Vulnerability *Database*	37

walkthrough. Kemudian tahap keempat dilakukan klasifikasi *attack tools* berdasarkan *vulnerability*. *Tools* didapat berdasarkan data walkthrough.

Pada alur skenario penyerangan, tahap pertama adalah melakukan pemindaian semua perangkat yang terhubung di jaringan virtual menggunakan perangkat lunak Netdiscover dan Nikto. Tahap kedua adalah memindai *port* terbuka yang ada pada *Typhoon*. Tahap ini menggunakan aplikasi Nikto. Tahap ketiga adalah mengakses web server dan membuka robots.txt melalui browser. Tahap keempat adalah mengakses MongoAdmin. Pada MongoAdmin, ditemukan basis data kredensial yang dapat digunakan untuk melakukan SSH pada perangkat *Typhoon*. Setelah mendapatkan kredensial dari MongoAdmin, tahap kelima adalah melakukan SSH ke Typhoon. *User* dan kata sandi yang digunakan menggunakan kredensial yang ditemukan pada MongoAdmin.

Setelah SSH dilakukan, tahap keenam adalah mencari versi kernel Linux dan Ubuntu yang digunakan. Hal ini dilakukan untuk mencari titik kelemahan dari *Typhoon*. Ditemukan bahwa Typhoon menggunakan Ubuntu versi 14.04. Dengan informasi tersebut, tahap ketujuh adalah membuat tab baru pada OS penyerang, dan mencari exploit yang dapat digunakan pada Ubuntu 14.04. Pencarian ini dapat dilakukan dengan Searchsploit. Pada tahap kesembilan, pada *Typhoon* dilakukan pengunduhan *file exploit* menggunakan Wget. File exploit ini kemudian dikompilasi dan dieksekusi untuk mendapatkan akses *root*. Pada tahap kesebelas, dilakukan penghapusan log. Penghapusan log ditujukan sebagai simulasi anti-forensik yang umum dilakukan untuk menghapus jejak penyerang.

Aktivitas pertama untuk aktivitas forensik digital adalah pembuatan dan preservasi *image*. Pada aktivitas ini dimulai dengan melakukan *mounting storage* pada mesin virtual. Mounting dilakukan dengan menyalakan *read-only* agar tidak ada data yang berubah pada penyimpanan *Typhoon*. Kemudian dengan menggunakan *command-line*, dilakukan *cloning* pada penyimpanan *Typhoon* dengan FTK *Imager*. Aktivitas kedua adalah pembacaan *image*. Pada aktivitas ini, dilakukan pemeriksaan data yang ada pada *image*. Aktivitas ketiga adalah melakukan Ekspor dan Hashing.

Singkatan dan Akronim

Dapat dilihat pada tabel 1 berikut.

Hasil dan Pembahasan

Perbandingan Vulnerability dan Risk dengan Temuan Pemindaian Keamanan

Pada tabel 2 tersebut, ditemukan bahwa Nessus Essentials tidak menemukan adanya vulnerability pada Robots.txt. Selain itu, kedua perangkat lunak tidak menemukan adanya kerentanan pada V2. Pada Nessus Essentials, ditemukan banyak vulnerability dan threat yang tidak dieksploitasi menjadi risk. Ini karena Nessus Essentials ditujukan untuk pengujian keamanan yang lebih umum dibandingkan dengan Nikto. Nessus menemukan banyak kerentanan pada Man-In-The Middle, dimana kerentanan tersebut hanya dapat dieksploitasi dengan mendengarkan lalu lintas jaringan dan membajak komunikasi antar perangkat. Selain itu, Nikto hanya digunakan sebagai pemindai kerentanan pada server web, sehingga tidak menguji kerentanan pada sisi lainnya.

Table 2. B

No.	Eksploitasi	Identifikasi	Ditemukan	
			Nessus Essentials	**Nikto**
1	MongoDB Service Without Authentication Detection	V1	✓	✓
2	Linux Kernel 3.13.0 $<$ 3.19 - 'overlayfs' Local Privilege Escalation	V2	x	x
3	Penggunaan Robots.txt Untuk Menyembunyikan Layanan Internal	V3	x	✓

Analisis Eksperimen Implementasi Forensik Berdasarkan *Framework* FORZA

Pada subbab ini, dilakukan analisis eksperimen implementasi forensik berdasarkan *framework* FORZA. Pada *framework* FORZA, terdapat tiga lapisan yang dipertanyakan dan dibentuk oleh tim forensik. Pada *Technical Presentation Layer*, dilakukan pengumpulan informasi dari pemimpin kasus kepada ahli forensik digital. Ahli forensik digital harus melakukan sejumlah tindakan:

- Why: Mengapa forensik ini dilakukan dan apa saja tugas yang perlu dilakukan Forensik ini dilakukan atas dugaan terjadinya serangan pada server dan kebocoran data pada sistem Typhoon. Tugas yang perlu dilakukan penyelidik adalah membuktikan ada atau tidaknya serangan dan kebocoran data yang terjadi pada sistem.
- What: Hipotesis alasan perangkat bisa diserang, dan log apa yang perlu diselidiki Perangkat server diduga menggunakan Linux versi lawas dan aplikasi tidak diperbarui, sehingga memiliki banyak kerentanan yang terbuka dan tidak diamankan. Log yang perlu dikumpulkan:

  - Log akses pada Apache (access.log)
  - Log galat pada Apache (error.log)
  - Log otentikasi user pada Linux (auth.log)
  - Log MongoDB (mongod.log)

Table 3. A

No.	Perangkat Terhubung	Alamat IP
1	Windows PC	192.168.56.1
2	Linux Desktop 1	192.168.56.128
3	Linux Desktop 1	192.168.56.129
4	Server Typhoon	192.168.56.130

- Log Sejarah Bash (.bash-history)

- Where: Lokasi geografis forensik ini dilakukan beserta alamat IP perangkat terhubung Forensik dilakukan pada Bekasi, Indonesia. Perangkat yang terhubung pada jaringan server adalah sebagai berikut: 3
- Who: Pihak yang perlu dilibatkan dan diwawancara pada forensik ini Pada forensik ini, pemilik server perlu dilibatkan dan diwawancarai mengenai kejadian dugaan kebocoran data.
- When: Waktu kejadian ini diduga terjadi Penyerangan pada sistem diduga terjadi pada 10 Februari 2022. Waktu belum ditemukan.
- How: Metode penyelidikan forensik Pada forensik ini, direncanakan untuk melakukan akuisisi data pada perangkat komputer dengan menyalin *image* secara penuh. Penyelidikan akan dilakukan dengan menggunakan tiga aplikasi, yaitu *Autopsy*, FTK *Imager*, dan OSForensics. Karena perangkat telah dimatikan, media penyimpanan akan dipasang secara *read-only* pada mesin virtual Ubuntu untuk mengakuisisi data.

1. Data Acquisition Layer

   Data acquisition layer dilakukan pada bagian Collection, Transport, Storage, dan Examination. Ada sejumlah pertanyaan yang harus dapat dijawab oleh penyelidik forensik digital:

   - Why: Tugas dari spesialis forensik digital Tugas yang perlu dilakukan penyelidik adalah membuktikan ada atau tidaknya serangan dan kebocoran data yang terjadi pada sistem.
   - What: Temuan di lapangan Perangkat fisik semua komputer dan jaringan yang terhubung ditemukan dalam posisi sudah dimatikan. Pemeriksaan lebih lanjut dibutuhkan.
   - Who: Pernyataan staf internal dan terduga mengenai kebocoran data ini Berdasarkan hasil penyelidikan, diduga serangan ini dilakukan melalui jaringan internal.
   - How: Melakukan akuisisi forensik dan penyitaan. Akuisisi dan penyimpanan dilakukan menggunakan FTK *Imager* dan dd. Data yang diambil merupakan *full image* dari perangkat beserta dengan hasil checksum SHA-256 dari file dan penyimpanan itu sendiri. Sedangkan barang yang disita merupakan file mesin virtual dari Typhoon.
   - Where: Akuisisi data forensik jaringan Karena semua komputer dan jaringan telah dimatikan, data forensik jaringan tidak dilakukan.
   - When: Timeline akuisisi forensik dan rantai penjagaan barang bukti Berita acara akuisisi forensik dan barang bukti akan disimpan pada penyimpanan terpisah beserta dengan checksum yang dihasilkan pada bukti tersebut.

2. Data Analysis Layer

   Pada data analysis layer, data yang sudah dikumpulkan akan dibawa ke laboratorium forensik digital untuk analisis lebih lanjut yang dilakukan oleh analis forensik digital. Lapisan ini akan dilakukan pada tahap Examination. Pertanyaan yang harus dijawab oleh analis forensik digital:

Table 4. C

No.	Kejadian	Alamat IP Sumber	Waktu
1.	Server dipindai dengan Nikto	192.168.56.128	2 Februari 2022 18:48 WIB
2.	Diaksesnya robots.txt	192.168.56.128	2 Februari 2022 18:54 WIB
3.	Diaksesnya *database* MongoDB	192.168.56.128	2 Februari 2022 18:55 WIB
4.	Dilakukan akses SSH	192.168.56.128	10 Februari 2022 9:13 WIB
5.	192.168.56.128 mengunduh dan menjalankan exploit	Lokal	
6.	Dilakukan pembacaan data	Lokal	

   - Why: Menemukan bukti peretasan dan kebocoran data yang terjadi pada sistem, dan
   - What: Membuat daftar kejadian berdasarkan bukti yang ditemukan. Berdasarkan barang bukti yang didapatkan dari dokumen di atas, ditemukan bahwa:
   - Who: Mendapatkan informasi pengguna, informasi akun, dan informasi lainnya Akun pengguna yang terdapat pada perangkat server adalah typhoon dan admin. Typhoon merupakan akun biasa tanpa izin apapun sedangkan admin adalah akun dengan izin akses penuh pada perangkat server.
   - When: Membuat kronologi kejadian dari peretasan.

Analisis Bukti Digital Eksploitasi dengan Log

Pada pemindaian menggunakan Netdiscover, tidak ditemukan log apapun pada perangkat. Ini karena Netdiscover tidak mengakses aplikasi apapun pada perangkat server untuk memindai alamat IP yang ada pada jaringan. Pada pemindaian menggunakan Nikto, empat log mendeteksi adanya aktivitas, yaitu access.log, error.log, auth.log, dan Syslog. Berikut adalah log yang ditemukan dari keempat log tersebut. Pada access.log, ditemukan bahwa alamat IP 192.168.56.128 melakukan akses ke halaman utama dan menemukan informasi bahwa perangkat Nikto digunakan. Selain itu, pada access.log juga ditemukan bahwa Nikto menemukan sebuah entri pada robots.txt. Pada catatan error.log, ditemukan satu entri aktivitas yang relevan. Pada pemindaian Error.log pada Apache mencatat klien 192.168.56.128 mencoba melakukan request terhadap folder bernama RVNA. Pada auth.log, ditemukan sejumlah entri yang mencoba mengotentikasi dirinya yang bersumber dari 192.168.56.128. Pada log ini juga terdeteksi penggunaan dari Nikto. Pada Syslog, banyak entri yang tercatat pada pemindaian Nikto dilakukan. Ditemukan bahwa alamat IP 192.168.56.128 mencoba melakukan login melalui IMAP, POP3, dan SMTP. Ketiga protokol ini merupakan protokol email. Namun tidak ditemukan penggunaan Nikto pada pemindaian ini.

Pada akses robots.txt, dua log berhasil menemukan sumber alamat IP yaitu access.log dan syslog, tetapi hanya access.log yang mengetahui apa yang alamat IP itu lakukan. Pada syslog, hanya ditemukan bahwa alamat IP 192.168.56.128 terhubung dengan Typhoon. Namun access.log mencatat bahwa alamat IP 192.168.56.128 melakukan akses ke robots.txt. Pada akses MongoAdmin, ada tiga log yang mencatat aktivitas tersebut. Log tersebut adalah access.log, error.log, dan mongod.log. Namun mongod.log hanya mencatat bahwa koneksi dibuka dan tidak disertai informasi apapun. Access.log dan error.log mencatat akses terhadap MongoAdmin, dengan keduanya

Table 5. D

No	Tindakan	Bobot	Total Temuan	Nilai
1.	Pemindaian Nikto	1	3	3
2.	Akses robots.txt	1	3	3
3.	Akses Mongo Admin	2	4	8
4.	Akses masuk SSH	3	0	0
5.	Penggunaan eksploit	3	0	0

Table 6. E

No	Tindakan	Bobot	Total Temuan	Nilai
1.	Pemindaian Nikto	1	2	2
2.	Akses robots.txt	1	0	0
3.	Akses Mongo Admin	2	2	4
4.	Akses Masuk SSH	3	0	0
5.	Penggunaan Eksploit	3	0	0

Table 7. F

No	Tindakan	Bobot	Total Temuan	Nilai
1.	Pemindaian Nikto	1	0	0
2.	Akses robots.txt	1	0	0
3.	Akses Mongo Admin	2	0	0
4.	Akses Masuk SSH	3	4	12
5.	Penggunaan Eksploit	3	0	0

Table 8. G

No	Tindakan	Bobot	Total Temuan	Nilai
1.	Pemindaian Nikto	1	0	0
2.	Akses robots.txt	1	0	0
3.	Akses Mongo Admin	2	0	0
4.	Akses Masuk SSH	3	0	0
5.	Penggunaan Eksploit	3	2	6

mencatat alamat IP pengakses. Namun, access.log mencatat informasi bahwa alamat IP tersebut mengakses basis data credentials yang tersimpan. Pada saat penyerang masuk melalui SSH, hanya auth.log yang mencatat aktivitas tersebut. Auth.log mencatat bahwa alamat IP 192.168.56.128 masuk menggunakan kata sandi melalui SSH. Pada pengunduhan dan eksekusi dari exploit, tidak ada log yang mencatat aktivitas ini. Bash History hanya mencatat perintah apa yang dilakukan oleh user tersebut, tetapi tidak mencatat tanggal atau informasi apapun.

Meski begitu, tidak semua log dapat digunakan sebagai barang bukti yang kuat. Penilaian akan dilakukan berdasarkan apakah log mencatat alamat IP, terdapat waktu percobaan tersebut dilakukan, tercatat dengan jelas aktivitas apa yang dilakukan oleh penyerang, dan apakah ada bukti jelas bahwa log mencatat percobaan peretasan. Penyerangan dapat dipecah menjadi tiga bagian, yaitu pemindaian, mendapatkan akses dengan eksploitasi, dan eskalasi izin. Ketiga tindakan tersebut memiliki bobot yang berbeda sebagai barang bukti di pengadilan. Oleh karena itu, diberikan nilai bobot pada tiap jenis tindakan, dengan pemindaian mendapatkan bobot 1, akses dengan eksploitasi dengan bobot 2, dan eskalasi izin dengan bobot 3. Catatan log memiliki empat data penting yang dapat digunakan untuk membuktikan legitimasi bahwa peretasan benar terjadi. Empat data tersebut adalah dicatatnya alamat IP yang melakukan akses, tercatat waktu kejadian (timestamp), tercatat informasi aktivitas yang terkait dengan kronologi kejadian, dan apabila barang bukti tersebut merupakan tindakan kriminal berupa peretasan.

Pada access.log yaitu log akses aplikasi web Apache, tercatat tiga aktivitas yang dilakukan pada simulasi penyerangan. Aktivitas tersebut adalah Pemindaian Nikto, Akses Robots.txt, dan Akses MongoAdmin. Pada pemindaian Nikto, ditemukan alamat IP, timestamp, dan aktivitas pemindaian yang dilakukan oleh Nikto. Berdasarkan temuan, ditemukan bahwa Nikto mencoba melakukan HTTP request terhadap halaman web server. Log juga mencatat bahwa pemindaian dilakukan dengan menggunakan Nikto. Meski begitu, pemindaian Nikto tidak dapat menjadi alat bukti kuat tanpa bukti peretasan lainnya karena pemindaian bukanlah tindakan kriminal. Pada akses robots.txt, ditemukan juga alamat IP, timestamp, dan informasi bahwa penyerang melakukan akses terhadap robots.txt. Ditemukan bahwa alamat IP 192.168.56.128 pada 23:17 melakukan akses kepada halaman robots.txt menggunakan browser Mozilla Firefox. Meski begitu, robots.txt merupakan file teks yang bersifat publik yang digunakan untuk menyembunyikan halaman dari mesin pencari.

Pada akses MongoAdmin, ditemukan juga alamat IP, waktu kejadian, dan aktivitas yang dilakukan. Pada pencatatan ini, ditemukan bahwa alamat IP 192.168.56.128 melakukan akses pada dua halaman, yaitu /mongoadmin/ dan /mongoadmin/?db=credentials. MongoAdmin adalah aplikasi basis data internal dan tidak seharusnya diakses oleh pihak luar. Dan dengan diaksesnya salah satu credentials *database* yang ada pada MongoAdmin, dapat dibuktikan bahwa penyerang mengambil informasi kata sandi yang bukan haknya. Dengan menjumlah semua informasi yang didapat dari access.log, maka access.log mendapatkan nilai 14. Access.log berhasil mencatat akses aplikasi web MongoAdmin yang dapat dijadikan sebagai barang bukti atas kebocoran data. Pada error.log yaitu log pencatatan galat pada Apache, ditemukan log pada dua aktivitas. Log tersebut yaitu pemindaian Nikto dan Akses MongoAdmin. Pada pemindaian Nikto, hanya ditemukan informasi waktu dan alamat IP yang relevan. Log ini tidak mendeskripsikan apapun mengenai aktivitas yang dilakukan oleh Nikto, dan hanya waktu dan alamat IP saja yang berkaitan dengan aktivitas pemindaian Nikto. Pada akses MongoAdmin, hanya tercatat informasi alamat IP, timestamp, dan informasi bahwa kode yang dipakai pada aplikasi web sudah usang dan perlu diperbarui. Log ini tidak menginformasikan aktivitas akses dari MongoAdmin. Dengan menjumlah hasil temuan pada Error.log, nilai 6 didapatkan. Catatan log yang dihasilkan oleh Error.log tidak dapat menjelaskan apa yang terjadi pada insiden kebocoran data, sehingga tidak dapat digunakan sebagai barang bukti yang kuat. Pada auth.log yaitu log masuk user pada Linux, tercatat satu aktivitas yaitu masuknya IP 192.168.56.128 melalui SSH. Pada log tersebut, tercatat waktu dengan zona waktu GMT+3, alamat IP, dan informasi lengkap tentang apa yang dilakukan. Pada log tersebut dijelaskan bahwa alamat IP tersebut masuk ke user typhoon melalui SSH. Apabila alamat IP tidak memiliki hak apapun untuk mengakses user typhoon atau pada server tersebut, bukti SSH ini dapat digunakan sebagai barang bukti bahwa penyerang dengan sengaja dan tanpa hak mengakses sistem elektronik orang lain. Berdasarkan hasil di atas, maka didapatkan nilai auth.log yaitu 12. Auth.log mencatat masuknya user ke dalam sistem yang merupakan barang bukti penting apabila user tersebut tidak memiliki izin atas akses tersebut.

Table 9. G

No	Tindakan	Bobot	Total Temuan	Nilai
1.	Pemindaian Nikto	1	2	2
2.	Akses robots.txt	1	0	0
3.	Akses Mongo Admin	2	0	0
4.	Akses Masuk SSH	3	0	0
5.	Penggunaan Eksploit	3	0	0

Pada Bash History yaitu log yang mencatat setiap perintah yang dilakukan oleh seorang user, hanya ditemukan satu log yaitu penggunaan eksploit. Pada temuan ini, tidak ada timestamp dan informasi yang dapat digunakan sebagai bukti kuat bahwa perintah dilakukan oleh penyerang. Pada data Bash History, ditemukan alamat IP yang digunakan untuk mengunduh sebuah file bernama 37292.c yang kemudian dijalankan. Apabila file 37292.c tidak ditemukan, maka Bash History tidak dapat digunakan sebagai barang bukti yang kuat. Dengan data yang ditemukan, maka nilai dari Bash History adalah 6. Bash History hanya mencatat perintah yang dilakukan oleh user, dan tidak mencatat perintah yang dilakukan setelah eksploitasi sistem berhasil dilakukan. Tidak adanya timestamp juga menjadikan log ini sulit digunakan sebagai barang bukti karena tidak diketahui kapan sistem dieksploitasi oleh penyerang. Pada Syslog atau log pencatatan sistem, hanya didapatkan log pada satu objek tindakan. Objek tersebut yaitu Pemindaian Nikto. Pada Pemindaian Nikto, Syslog mencatat banyak data yang berasal dari alamat IP 192.168.56.128. Meski keluaran data Syslog memiliki alamat IP dan timestamp, informasi yang diberikan oleh Syslog tidak memiliki informasi yang jelas mengenai apa yang dilakukan oleh penyerang. Dengan membaca log tersebut, hanya diketahui bahwa alamat IP 192.168.56.128 mencoba melakukan otentikasi masuk email dengan Dovecot dan Postfix. Meski aktivitas tersebut abnormal karena rentang waktunya yang sangat berdempetan, data keluaran log ini tidak dapat menjadi bukti kuat bahwa alamat IP tersebut melakukan penyerangan pada sistem.

Analisis Fungsi Forensik Dari Perangkat Lunak Autopsy, FTK *Imager*, dan OSForensics

Pada aplikasi *Autopsy*, fitur pembuatan dan preservasi *image* tidak dapat dilakukan. Sedangkan pada FTK *Imager* dan OSForensics, pembuatan dan preservasi *image* dapat dilakukan. Kedua aplikasi memiliki aplikasi esensial yang dibutuhkan dalam penelitian ini, tetapi OSForensics memiliki lebih banyak fitur seperti restorasi *image* ke disk, membangun ulang penyimpanan RAID, membuat *image* dari perangkat Android, dan lainnya. Sedangkan FTK *Imager* dapat membuat *memory dump* yang menangkap data yang ada di memori RAM untuk menganalisa program yang berjalan di latar belakang pada saat ini. Ketiga program dapat melakukan pembacaan *image*. FTK *Imager* dan *Autopsy* dapat melihat langsung isi dokumen yang ada di dalam *image*, sedangkan untuk OSForensics, membaca file yang ada di *image* berada di menu *File System Browser*. FTK *Imager* dan *Autopsy* juga dapat membaca isi dari file tanpa harus membukanya satu persatu. Walau tidak digunakan dalam penelitian ini, *Autopsy* dan OSForensics dapat menganalisa data yang ada di *image* secara otomatis. Namun kedua program ini tidak dirancang untuk sistem operasi Linux, sehingga banyak fitur analisa yang tidak dapat digunakan. FTK *Imager* tidak memiliki fitur analisa apapun.

Autopsy dapat melakukan pencarian data terhapus di direktori tempat dokumen tersebut dihapus, atau terpisah melalui File View ¿ Deleted Files. File yang terhapus dan belum tertimpa masih memiliki nama. Meski begitu, pembukaan hasil dari pencarian data terhapus pada Autopsy tidak sesuai dengan file yang seharusnya. Pada FTK *Imager*, data yang terhapus dapat ditemukan, namun FTK *Imager* tidak menemukan nama file yang sudah terhapus tersebut. FTK *Imager* juga tidak dapat melihat dokumen terhapus langsung dari direktori asalnya. Pencarian data terhapus pada OSForensics tidak berhasil menemukan banyak dokumen yang dicari. Tidak ada daftar data yang terhapus seperti kedua aplikasi sebelumnya, semua harus dicari berdasarkan keyword. Berdasarkan percobaan pencarian, tidak ada data yang berhasil ditemukan menggunakan OSForensics. Pembuatan hash pada Autopsy dapat dilakukan dengan mudah bahkan pada file terhapus. Pembuatan hash pada FTK *Imager* juga dapat dilakukan dengan beberapa klik, termasuk pada file terhapus. Begitu pula dengan OSForensics. Namun OSForensics tidak memiliki metode mudah untuk melakukan ekspor file.

Kesimpulan

Analisis perbandingan vulnerability dan risk dengan temuan pemindaian kerentanan menunjukkan bahwa pemindaian kerentanan tidak dapat menemukan semua vulnerability yang ada pada sistem. Pada analisis kelengkapan informasi log, ditemukan bahwa access.log mendapatkan nilai tertinggi dengan hasil 14 dari 20. Access.log menemukan tiga kejadian dengan informasi yang lengkap. Sedangkan nilai terendah didapatkan oleh Syslog dengan hasil 2 dari 20. Syslog mencatat aktivitas yang relevan saat kejadian, namun tidak memiliki informasi yang lengkap. Pada analisis fungsi forensik dari perangkat lunak, ditemukan bahwa FTK *Imager* memiliki nilai tertinggi dengan skor total 7. FTK *Imager* berhasil melakukan fungsi fungsi forensik digital yang dibutuhkan untuk analisis ini.

Daftar Pustaka

1. Badan Siber dan Sandi Negara. Lanskap Keamanan Siber Indonesia. Jakarta: Direktorat Operasi Keamanan Siber, Badan Siber dan Sandi Negara; 2022.
2. Casey E. Digital Evidence and Computer Crime. Great Britain: Academic Press; 2004.
3. APJII. Profil Internet Indonesia 2022; 2022. https://apjii.or.id/survei2022x.
4. Aldrich J. R. A. Fisher on Bayes and Bayes' Theorem. Bayesian Analysis. 2008;1:161-70.
5. Alkhowaiter W. The Power of Instagram in Building Small Business. Social Media Strategy and Digital Business. 2016:60.
6. Badan Siber dan Sandi Negara. Laporan Tahunan Monitoring Keamanan Siber 2021; 2021.
7. Badan Siber dan Sandi Negara. Panduan Menghadapi Insiden Data Breach;. https://cloud.bssn.go.id/s/QKwjMjJ4rwoneJ9.
8. Berry MW, Kogan J. Text Mining: Applications and Theory. USA: John Wiley and Sons, Ltd.; 2010.
9. Brown N. Overlay Filesystem;. https://www.kernel.org/doc/html/latest/filesystems/overlayfs.html?highlight=overlayfs.
10. CNN Indonesia. 225 Juta Serangan Siber Masuk Indonesia Sepanjang 2018; 2019. https://www.cnnindonesia.com/teknologi/20190207210646-185-367347/225-juta-serangan-siber-masuk-indonesia-sepanjang-2018.
11. Cloudflare. What is a computer port? — Ports in networking;. https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/.
12. Cooper C. Wanna Cry: Lessons Learned 1 Year Later; 2018. https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later.

13. Databoks. Berapa Pengguna Media Sosial Indonesia; 2019. https://databoks.katadata.co.id/datapublish/2019/02/08/berapa-pengguna-media-sosial-indonesia.
14. Denholm T. Explaining OverlayFS – What it Does and How it Works;. https://www.datalight.com/blog/2016/01/27/explaining-overlayfs-%E2%80%93-what-it-does-and-how-it-works/.
15. EC-Council. Computer Hacking Forensics Investigator Version 3; 2009.
16. Fadilah AR, Saepudin D, Ummah I. Analisis dan Perbandingan Metode Support Vector Machine dan Naive Bayes untuk E-mail Spam Filtering. 2014.
17. Falahah, Nur DD. Pengembangan Aplikasi Sentiment Analysis Menggunakan Metode Naïve Bayes (Studi Kasus Sentiment Analysis dari Media Twitter). 2015.
18. Farhadloo M, Rolland E. Fundamentals of Sentiment Analysis and Its Applications. In: Sentiment Analysis; 2016. p. 3-6.
19. Feldman R, Sanger J. The Text Mining Handbook: Advanced Approaches to Analyzing Unstructured Data. New York: Cambridge University Press; 2007.
20. Google. Introduction to robots.txt;. Accessed: n.d. https://developers.google.com/search/docs/advanced/robots/intro.
21. Hu Y, Manikonda L, Kambhampati S. What We Instagram: A First Analysis of Instagram Photo Content and User Types; 2014. p. 1-4.
22. Internet Engineering Task Force (IETF). The Secure Shell (SSH) Protocol Architecture; 2006. https://datatracker.ietf.org/doc/html/rfc4251.
23. Internet Engineering Task Force (IETF). The Syslog Protocol; 2009. https://datatracker.ietf.org/doc/html/rfc5424.
24. Ieong RSC. FORZA: Digital Forensics Investigation Framework. In: Digital Forensic Research Conference. Lafayette; 2006. .
25. Jaakonmäki R, Müller O, von Brocke J. The Impact of Content, Context, and Creator on User Engagement in Social Media Marketing. In: International Conference on System Sciences. Hawai: HICSS; 2017. p. 1152.
26. Jansen W, Ayers R. Guidelines on PDA Forensics. Gaithersburg: National Institute of Standards and Technology; 2004.
27. Kannan S, Gurusamy V. Preprocessing Techniques for Text Mining. 2014:1-6.
28. Kaspersky. Cyberthreat Real-Time Map; 2019. https://cybermap.kaspersky.com/stats/#country=144&type=ids&period=m.
29. Khan A, Baharudin B, Lee LH, Khan K. A Review Machine Learning Algorithms for Text-Documents Classification. Journal of Advances in Information Technology. 2010;4.
30. Kietzmann JH, Hermkens K, McCarthy I, Silvestre B. Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media. Business Horizons. 2011:241-51.
31. King R. Sentiment analysis gives companies insight into consumer opinion. Business Week: Technology. 2011.
32. Kircaali YC. Typhoon: 1.02 Vulnhub Walkthrough; 2020. https://www.yckircaali.com/typhoon-1-02-vulnhub-walkthrough/.
33. Kompas com. Kronologi Kasus Kebocoran Data WNI, Dijual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS; 2021. https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan.
34. Liputan6. Bagaimana Kondisi Keamanan Siber di Indonesia selama Kuartal Kedua 2019?; 2019. https://cybermap.kaspersky.com/.
35. National Institute of Standards and Technology (NIST). Secure Hash Standard (SHS); 2015. FIPS PUB 180-4.
36. National Institute of Standards and Technology (NIST). Digital Evidence;. Accessed: n.d. https://www.nist.gov/digital-evidence.
37. O'Reilly and Associates. Managing System Logs; 2001. https://docstore.mik.ua/orelly/linux/run/ch08_03.html.
38. Paass G. A Brief Survey of Text Mining. January 2015. 2015.
39. Pandora FMS. Log Monitoring: What should we do before we start?; 2021. https://pandorafms.com/blog/log-monitoring/.
40. Patterson BL. Sentiment Analysis as a Measure of Social Media Engagement:1-2. N.d.
41. Perez S. Instagram Officially Announces Its New Business Tools; 2016. https://techcrunch.com/2016/05/31/instagram-officially-announces-its-new-business-tools/.
42. Perreault MC, Mosconi E. Social Media Engagement: Content Strategy and Metrics Research Opportunities. In: International Conference on System Sciences. Finlandia: HICSS; 2018. p. 3568.
43. PortSwigger. Clickjacking (UI redressing);. N.d. https://portswigger.net/web-security/clickjacking.
44. PortSwigger. Cross-site scripting;. N.d. https://portswigger.net/web-security/cross-site-scripting.
45. Primartha R. Security Jaringan Berbasis CEH. Bandung: Penerbit INFORMATIKA; 2018.
46. Ratnasari CI, Kusumadewi S, Rosita L. Model Natural Language Processing untuk Perumusan Keluhan Pasien. In: Seminar Nasional Informatika Medis (SNIMed) V; 2014. p. 11-8.
47. Riza H, Darmawan D, Utoyo I, Lahey T, Izza J, Lim E, et al. Data and Cyber Security. Jakarta Selatan: Perkumpulan Basis Data Indonesia; 2020.
48. Scientific Working Group on Digital Evidence. Forensics Science Communications; 2000. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.
49. Sipayung EM, Maharani H, Zefanya I. Perancangan Sistem Analisis Sentimen Komentar Pelanggan Menggunakan Metode Naive Bayes Classifier. Jurnal Sistem Informasi. 2016;8(1):958-65.
50. Smura M. Comparative Research on Engagement in Social Media Platforms. Finlandia: Helsinki Metropolia University of Applied Sciences; 2016.
51. Statista. Global Social Networks Ranked by Number of Users; 2019. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
52. Tech Terms. Disk Image; 2008. https://techterms.com/definition/diskimage.
53. Telkom University. About Telkom University; 2019. https://telkomuniversity.ac.id/about/?lang=en.
54. The Next Web. How One Guy Stopped the WannaCry Ransomware in Its Tracks After It Spread to 150 Countries; 2017. https://thenextweb.com/security/2017/05/15/how-one-guy-stopped-the-wannacry-ransomware-in-its-tracks-after-it-spread-to-150-countries/.
55. Ubuntu. CVE-2015-1328; 2015. https://ubuntu.com/security/CVE-2015-1328.
56. Webopedia. Image; 2006. https://www.webopedia.com/definitions/image/.