Analisa Serangan Terhadap Port 80 Webserver dengan SIEM Wazuh Menggunakan Metode Deteksi dan OSCAR

1st Tri Suryantoro
Magister Teknologi Informasi
Universitas Teknologi Digital Indonesia
Yogyakarta, Indonesia
student.tri_suryantoro@utdi.ac.id

2nd Dini Fakta Sari
Informatika
Universitas Teknologi Digital Indonesia
Yogyakarta, Indonesia
dini@utdi.ac.id

***Abstraks*—Adanya internet di perusahaan menjadikan kegiatan pertukaran data dan informasi menjadi lebih mudah. Kemudahaan mendapatkan data dan informasi perusahaan yang tidak disertai adanya *information security awareness* berimbas munculnya *data leak dan lateral movement.* Perusahaan dituntut memastikan keamanan jaringan yang handal dan aman untuk melindungi aset teknologi informasi dari tindakan peretasan. SIEM membantu perusahaan dan *security officer* untuk memonitor serangan, menemukan *vulnerability* dan menganalisa serangan. Penelitian ini menerapkan pendekatan *network forensic* dengan metode OSCAR dan Deteksi untuk mengetahui efektifitas kinerja SIEM wazuh terhadap serangan port 80 pada webserver. Pengujian serangan tahapan pemindaian port dan pemindaian http direktori, layanan webserver masih terlihat normal atau tidak dijumpainya pesan galat 404 di browser, simpangan deteksi serangan dalam penelitian ini adalah 1,402 detik. Keberadaan SIEM Wazuh, mampu membantu petugas keamanan dalam memonitor keamanan data perusahaan dan mengamankan aset IT perusahaan.**

Katakunci—keamanan jaringan, webserver, siem wazuh, lateral movement, deteksi

I. PENDAHULUAN

Diera saat ini keamanan aset teknologi informasi perusahaan khususnya berkaitan dengan data sudah semestinya dilindungi dan dijaga dari tindakan peretasan. Data dan informasi dapat dirasakan oleh perusahaan dan orang-orang didalamnya ketika data dan informasi dijadikan arah kebijakan untuk membuat kinerja menjadi lebih baik. Data dan informasi memilik kaitan yang sangat erat satu sama lain, tanpa adanya data maka informasi tidak bisa tercipta dan tanpa adanya informasi maka data menjadi tidak berguna. Oleh karena itu perlindungan data dan informasi dalam perusahaan sangatlah penting.

Kemudahaan mendapatkan data dan informasi yang tidak disertai adanya *information security awareness* dapat melahirkan teknik peretasan yang perkembangannya semakin tahun semakin maju. Dilangsir dalam *Cyber Security Monitoring Report* BSSN tahun 2019 berturut turut adanya *data leak* dalam kurun tiga tahun terakhir yaitu 18 Maret 2019 sebanyak 13 juta data pengguna bukalapak, 18 September 2019 sebanyak 7,8 juta data pribadi penumpang malindo air, adanya *cyberattack* ditemukan 117,9 juta serangan dalam bentuk trojan, kemudian 6,4 juta serangan ke server DNS dan 12,5 juta serangan ditujukan ke port 80[1]. Salah satu penyebab kejadian *data leak* ialah *information security awareness*, langsiran penelitian yang dilakukan oleh Robbi Akraman menuliskan terkait keamanan informasi memiliki tingkat kesadaran rata-rata 71%, pada fokus *report for security incidents* memiliki tingkat kesadaran yang buruk yaitu 37% [2].

Teknik peretasan keamanan pada port 80 menyebabkan para hacker dengan mudah mengambil alih sistem. Hal ini menimbulkan keterbukaan untuk mengakses data pribadi maupun data penting perusahaan yang seharusnya tidak diketahui oleh orang lain. Hacker merupakan seseorang yang memiliki kemampuan dalam pemrograman serta jaringan komputer. Pesatnya perkembangan teknologi peretasan menjadikan para hacker semakin pintar dalam menjalankan pola kegiatan peretasan, memanfaatkan kelemahan port-port untuk mendapatkan keuntungan pribadi yang dijalankannya. Melihat kondisi ini secepatnya untuk mengamankan port dan apabila di abaikan maka data dan informasi yang di miliki oleh perusahaan dapat mengalami kerugian yang diakibatkan oleh para hacker. *Webserver* memiliki port 80 untuk mendistribusikan layanan permintaan (Request) dalam bentuk halaman web Protokol HTTP dari client yang di kenal dengan browser, dari sinilah celah yang dapat disusupi oleh seorang hacker dengan tanpa disadari pemilik *webserver*. Hal ini digunakan sebagai launch-pad untuk serangan yang lebih luas tanpa disadari sepenuhnya oleh pemilik ataupun pengelola informasi.

Penyelesaian permasalahan ancaman peretasan keamanan di perusahaan dengan mematuhi regulasi keamanan yang berlaku seperti menerapkan *Vulnerability Assesment, Penetration Testing* dan menganalisa serangan, terbukti sebagai penjamin keamanan *cyber* dalam perusahaan[3]. Penelitian ini akan menguji port 80 pada *webserver* dengan SIEM dalam mengatasi masalah keamanan data. Melakukan *monitoring* dan analisa data menggunakan OSCAR (*Obtain Information, Strategies, Collect Evidence, Analyze and Report*), dengan menyederhanakan menjadi *Attacking* dan *Analysis* sesuai dengan kebutuhan jaringan[4], untuk mengetahui efektifitas kinerja SIEM wazuh terkait keamanan data terhadap serangan *hacker*, selain itu penelitian ini diharapkan dapat membantu *security officer* dalam memonitor aset IT, mencermati pola serangan secara *real time*.

II. LANDASAN TEORI

A. Penetrasi Testing

Pengujian penetrasi adalah praktik umum untuk secara aktif menilai pertahanan jaringan komputer atau *webserver* dengan merencanakan dan mengeksekusi semua kemungkinan serangan untuk menemukan dan mengeksploitasi kerentanan [5].

B. Keamanan Jaringan

Keamanan jaringan berkaitan dengan perlindungan sistem informasi. Tindakan ini menjaga terhadap intrusi yang tidak sah, melindungi kegunaan dan integritas jaringan dan data. Serangan *cyber* bisa bersifat pasif seperti *port scaning*, penyadapan dan enkripsi [6]. Tindakan mengamankan yang relevan meliputi beberapa aspek keamanan yaitu: *Confidentiality, Integrity, Availability, Privacy, Authenticity and Trustworthiness, Non-Repudiation, Accountability and Auditability*. [7]

C. Webserver

Webserver adalah sebuah perangkat lunak yang berada di server, berfungsi menerima permintaan (*request*) berupa halaman website melalui protokol http atau https dari *client* (browser) dan mengirimkan kembali (*response*) dalam bentuk halaman website yang umumnya berbentuk tag html. Fungsi *webserver* tidak hanya mengolah data tapi dapat juga mengirimkan data berupa file foto dan video berdasarkan permintaan *client*[5].

D. Lateral Movement

Lateral movement adalah teknik yang digunakan oleh hacker, setelah *compromising* dengan tujuan untuk memperluas akses ke host atau aplikasi yang diretas. Tujuan utama dari teknik ini ialah untuk mengakses informasi berharga dan sensitif yang secara diam-diam tetap tidak terdekteksi selama mungkin, dan bergerak secara literal dengan mengakses lebih banyak sistem dan data sensitif. SIEM cocok untuk mendeteksi serangan siber, membuat profil aktivitas atau secara akurat mendeteksi anomali yang berkaitan dengan gerakan lateral, akibat dari teknik ini ialah peringatan di SIEM akan meningkat terlalu banyak[8]. Tahapan umum *lateral movement* mencakup 3 hal yaitu *reconnaissance* (pengintaian), *credential/privilege gathering* (pengumpulan kredensial/hak akses), dan *gaining access* (mendapatkan akses) [9].

E. SIEM Wazuh

Security Information and Event Management (SIEM) merupakan sebuah teknologi yang dapat mendeteksi berbagai ancaman dan insiden dari keamanan dengan mengumpulkan log real-time dan *melakukan analisis* log *history keamanan dari berbagai jenis tipe log yang berasal dari berbagai sumber data perangkat yang berbeda beda [10]*. SIEM wazuh, perangkat sumber terbuka dengan memiliki fungsi utama sebagai deteksi instrusi berbasis host, melakukan analis*a log, pemeriksaan integritas*, deteksi rootkit, peringatan berbasis waktu dan sebagai respons aktif. SIEM wazuh menyedi*akan fitur visibilitas keamana*n yang lebih dalam ke sebuah infrastruktur dengan memantau host di le*vel sistem operasi dan aplikasi*[11]. SIEM wazuh memantau file konfigurasi untuk memastikan mematuhi kebijakan keamanan, standar, atau panduan sistem sesuai *Security Framework*. Agent wazuh melakukan pemindaian berkala untuk mendeteksi aplikasi yang diketahui rentan, atau tidak dikonfigurasi dengan aman. Rangkaian kemampuan yang beragam ini disediakan dengan mengintegrasikan OSSEC, OpenSCAP dan Elastic Stack [11]. OSSEC adalah *open source* HIDS. Perangkat lunak ini melakukan *log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting* dan *active response* [12].

F. Deteksi

Sistem deteksi intrusi menggunakan beberapa metode deteksi berbasis tanda tangan, deteksi berbasis anomali statistik, dan analisis protokol stateful. Sistem deteksi berbasis anomali menampilkan perilaku normal sistem dalam model tertentu. Setiap aktivitas lain yang tidak sesuai dengan model yang disepakati ini dianggap tidak normal dan diperingatkan[13]. Proses dan metodologi yang direkomendasikan dalam buku *Road Map for Digital Forensic Research* ialah *Obtain Information, Startegize, Collect Evidence, Analyze, Report* [7].

G. Persamaan Analisis

Analisis data dalam penelitian ini, mengamati hasil dari respon SIEM wazuh terfokus pada *timestamp*. Kemudian *timestamp* yang diperoleh dilakukan perhitungan untuk dicari nilai standart deviasi. Dengan menggunakan persamaan dibawah ini.

$$SD = \sqrt{\frac{\sum f_1 \, (x_1 - \overline{x})^2}{\sum f_1}} \qquad (1)$$

Berikut keterangan dari persamaan untuk menghitung nilai standar deviasi dari data serangan yang direkam siem.

$\sum f_1 = n =$ Banyaknya data serangan
$f_1 =$ Frekuensi serangan ke-i
$x_1 =$ Nilai tengah serangan ke-i
$\overline{x} =$ Mean atau nilai rata-rata

III. METODOLOGI.

Tahapan penelitian ini melakukan pengujian ke webserver dengan langkah-langkah pengamatan *network existing*, serangan *network environment*, *network forensic* dan analisa data, --menggunakan metode oscar, yang direpresentasikan Figure I Metodologi OSCAR.

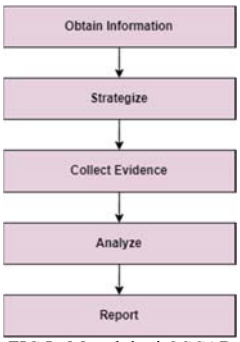

FIG I. Metodologi OSCAR

Representasi Figure I Metodologi OSCAR dalam penelitian ini dijelaskan sebagai berikut:

a. *Obtain Information*, mencari informasi yang mendukung proses forensik, segala informasi yang berhubungan dengan proses investigasi forensik, seperti bentuk topologi jaringan, serangan apa yang terjadi di jaringan dan *environment network*.
b. *Strategize*, merencanakan penyelidikan agar investigator bekerja secara efisien. Investigator melakukan prioritasi terhadap objek apa saja yang bisa dijadikan sebagai barang bukti, proses ini juga menentukan bagaimana proses penanganan barang bukti.
c. *Collect Evidence*, mengumpulan segala macam informasi yang menjadi barang bukti dalam investigasi seperti capture paket, log, dan semua barang bukti yang mengarah ke insiden.
d. *Analyze*, dari hasil prioritasi barang bukti, akuisisi barang bukti di tahap strategize serta pengumpulan barang bukti dari masing-masing sumber, selanjutnya dilakukan analisa terhadap barang bukti.
e. *Report*, segala macam hasil temuan dalam proses analisa sebagai pelaporan dan dokumentasi

A. *Pengamatan Network Existing*

Tahapan penelitian dalam pengamatan *network existing* yang akan digunakan untuk simulasi pengujian serangan, sebagai pemicu respon SIEM. Luaran pengamatan *network existing* dalam penelitian ini ialah membuat peta skema serangan. Pengujian serangan ke port 80 di server *webserver* direpresentasikan Figure II Skema serangan port 80 webserver. Kemudian untuk mendukung penelitian ini menggunakan perangkat dan peralatan yang direpresentasikan pada Table I Kebutuhan hardware dan software.

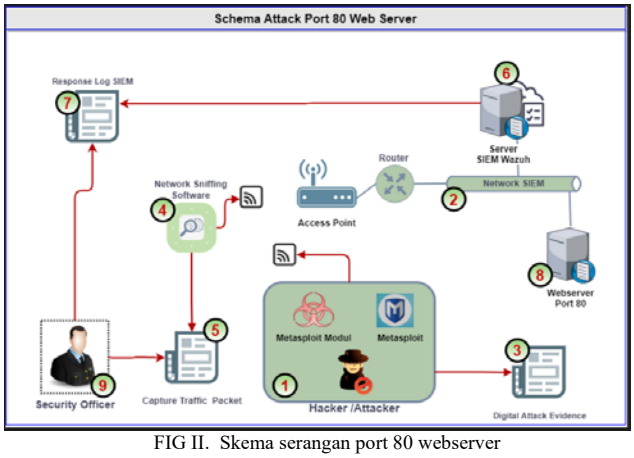

FIG II. Skema serangan port 80 webserver

TABLE I. KEBUTUHAN HARDWARE DAN SOFTWARE

Hardware	Software
Server HPE ProLiant ML150 Gen9, RAM 32G HDD 1T, 12Core, Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz Speed: 2397 MHz	a) XCP-ng Virtualization Platform b) OS CentOS 7 c) Kalilinux OS versi 2022.2 d) Apache httpd 2.4.6 & PHP 5.4.16 e) Metasploit f) Colasoft capsa sniffer versi 11

B. *Serangan Network Environment*

Tahapan setelah melakukan pengamatan network existing yang meliputi penyiapan dan konfigurasi *hardware* serta *software*, maka dilakukan penyerangan terhadap port 80 pada *webserver*. Serangan yang dilakukan dalam penelitian ini adalah serangan berupa *reconnaissance* (pengintaian) menggunakan *tools* nmap dan modul pemindaian exploit[14]. Perlengkapan tahapan serangan ini dipresentasikan pada Tabel II Perlengkapan serangan *reconnaissance.*

TABLE II. PERLENGKAPAN SERANGAN RECONNAISSANCE

No	Tools	Modul
1	Nmap versi 7.92	Scanner
2	Metasploit-framework	auxiliary/scanner/http/files_dir

C. *Skenario Serangan*

Pada penelitian ini dibuat proses skenario serangan, untuk memperjelas bagaimana pada tahapan awal *hacker* melakukan serangan dan apakah proses serangan tersebut dapat dideteksi oleh SIEM wazuh, software sniffer dan *collect evidence*. Representasi skenario serangan dan alur akusisi data, dipresentasikan pada Figure III Skenario serangan dan akusisi data.

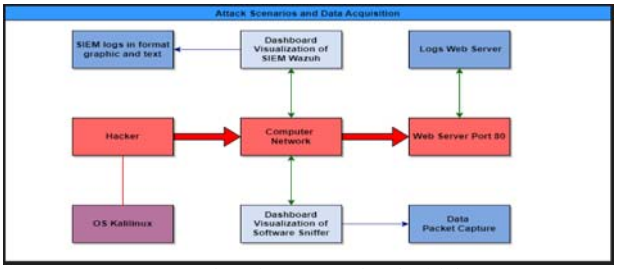

FIG III. Skenario serangan dan akusisi data

Dalam Fig III Skenario serangan dan akusisi data dilakukan penyerangan sesuai dengan skenario sebagai berikut, *hacker* melakukan serangan pemindaian port menggunakan *software* kalilinux *tools* Nmap ke target *webserver* dengan tujuan port 80, diperolehnya port ini adalah untuk mendapatkan akses yang lebih dalam atau seorang penyerang telah berada pada tahapan *priviledge escalation*[15], setelah *hacker* menemukan port tersebut *available*, kemudian secara bersamaan diambil dan dilakukan pengamatan di SIEM wazuh, dashboard sniffer, server webserver dan *collect evidence* serta melakukan pengamatan log SIEM wazuh, data packet capture sniffer dan data log webserver.

D. *Analisa Data Serangan*

Proses analisa penelitian ini, mengikuti metodologi OSCAR, dari metodologi OSCAR yang digunakan dalam penelitian ini yaitu *attacking*, *collect evidence* dan *analysis*. Representasi rangkuman serangan terhadap metodologi yang dipergunakan dipresentasikan pada Tabel III Rangkuman serangan pengenalan SIEM.

TABLE III. RANGKUMAN SERANGAN PENGENALAN SIEM

Modul	Respon SIEM	Respon Webserver
auxiliary/scanner/http/ dir_scanner	Gambaran respon SIEM	Gambaran respon webserver

IV. PEMBAHASAN

Analisa dan pembahasan penelitian pengamatan *network existing*, serangan *network environtment*, implementasi skenario serangan dan analisa data serangan, dijelaskan dibawah ini.

A. *Pengamatan Network Existing*

Hasil proses pengamatan *network existing* diperoleh IP gateway jaringan yaitu 192.168.18.1 dan subnet segment jaringan 255.255.255.0 atau segment 24. Representasi data proses observasi dipresentasikan pada Tabel IV Data segment IP *newtork existing* dan untuk data *capture* dipresentasikan pada Figure IV Capture segment network existing.

TABLE IV. DATA SEGMENT IP NETWORK EXISTING

Network	IP Network
Wireless	Gateway 192.168.18.1
IP Dynamic	192.168.18.0/24

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e429:9bfd:3312:4df6%18
   IPv4 Address. . . . . . . . . . . : 192.168.18.232
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.18.1
```

Fig IV. Data segment network existing

B. *Serangan Network Environment*

1) *Nmap*

Pengujian serangan menggunakan nmap diketahui bahwa posisi webserver memiliki IP 192.168.18.62, dan dalam proses pemindaian port pada server tersebut diperoleh port 80 dalam keadaan open atau *vulnerability*. Proses pemindaian dengan tools nmap direpresentasikan pada Figure V Data pengujian serangan nmap.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.18.62
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 11:17 EDT
Nmap scan report for 192.168.18.62
Host is up (0.0049s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
25/tcp   open  smtp    Postfix smtpd
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 86:CA:BC:49:59:32 (Unknown)
Service Info: Host:  webserver62.localdomain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

FIG V. Data pengujian serangan nmap

2) *auxiliary/scanner/http/files_dir*

Pengujian serangan untuk mengidentifikasi keberadaan direktori (*http directory scanner*), menggunakan tools metasploit-framework dengan modul auxiliary/scanner/http/files_dir dengan target port jaringan 80, diperoleh SIEM wazuh merespon dalam bentuk visualisasi grafik dan teks. Visualisasi grafik direpresentasikan pada Figure VI Kompilasi visualisasi siem wazuh

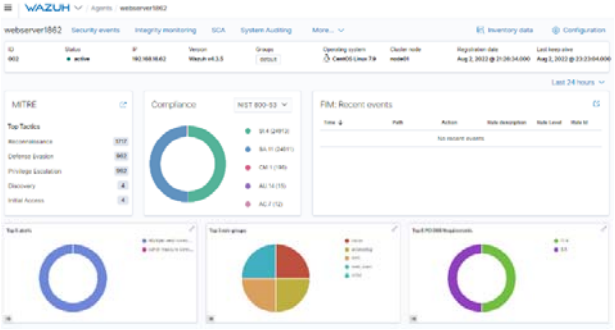

FIG VI. Kompilasi visualisasi SIEM Wazuh

Data pengamatan respon SIEM wazuh direpresentasikan pada Figure VII Data teks SIEM wazuh.

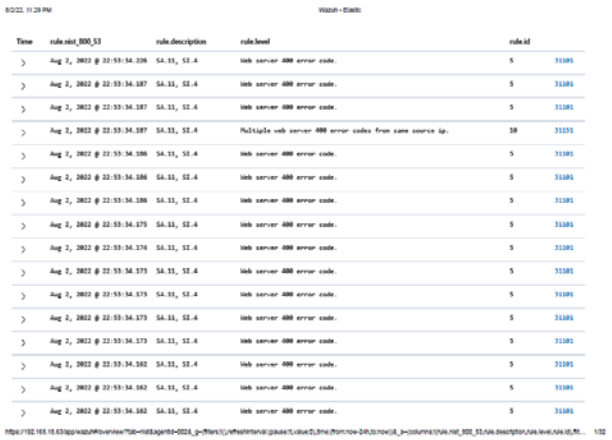

FIG VII. Data teks SIEM Wazuh

Kemudian data serangan untuk pengamatan log serangan port 80 di webserver, teramati error code 404. Representasi dari log webserver dapat dilihat pada Figure VIII Log serangan pengamatan port 80 webserver. Dan pengamatan paket serangan teramati pada software sniffer packet capture yang direpresentasikan pada Figure IX Visualisasi packet capture.

FIG. VIII. Log serangan pengamatan port 80 webserver

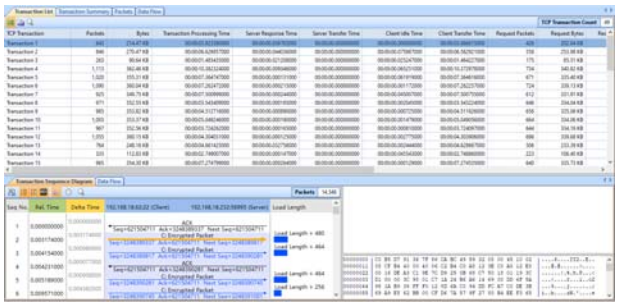

FIG IX. Visualisasi packet capture

Pengamatan dari sisi penyerang atau hacker, diperoleh dua direktori terdeteksi yaitu dengan kode 200 dan 302. Data perolehan direpresentasikan pada Figure IX. Log serangan hacker target port 80 webserver.

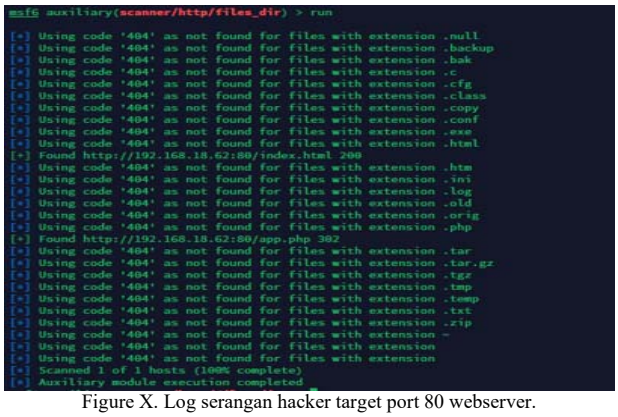

Figure X. Log serangan hacker target port 80 webserver.

Rangkuman serangan network environment untuk tipe serangan pemindaian http directory scanner mengunakan modul auxiliary/scanner/http/dir_scanner dan pemindaian kerentanan port server webserver, direpresentasikan pada Tabel V Data rangkuman serangan pengenalan siem dan Tabel VI Data korelasi serangan dan SIEM wazuh

TABLE V. DATA RANGKUMAN SERANGAN PENGENALAN SIEM

Respon SIEM	Respon Webserver
SIEM Wazuh merespon dengan visualisasi berupa grafik dan teks dengan notifikasi error code webserver 404	Visualisasi webserver masih terlihat normal tidak menampilkan halaman website tidak tersedia (error code 404)

C. *Analisa Data Serangan*

Analisa akusisi data SIEM Wazuh adalah nilai standart deviasi serangan. Nilai standar deviasi diperoleh dengan mengolah data figure VII menggunakan persamaan 1, nilai lama serangan diperoleh dengan menghitung waktu akhir serangan dikurangi waktu awal dari setiap waktu serangan yang terdeteksi atau terekam oleh SIEM wazuh. Kemudian untuk data deskripsi SIEM diperoleh dari *rule.description* SIEM. Dan untuk isian kolom waktu deteksi SIEM diperoleh dari atribut *time* SIEM pada figure VII. Dalam penelitian ini diperoleh nilai standart deviasi serangan 1,402 detik, proses nilai ini diperoleh dari 30 lamanya serangan dari serangan yang terdeteksi oleh SIEM. Rekapitulasi perhitungan nilai standart deviasi serangan, direpresentasikan pada Tabel VI Rekapitulasi standart deviasi serangan tahap *reconnaissance*.

TABLE VI. REKAPITULASI STANDART DEVIASI SERANGAN TAHAP RECONNAISSANCE

No	Waktu Deteksi SIEM Wazuh	Lama Serangan (detik)	Deskripsi SIEM
1	Aug 2, 2022 @ 22:53:33.129	25	Webserver 400 error code
2	Aug 2, 2022 @ 22:53:33.159	30	
3	Aug 2, 2022 @ 22:53:33.189	25	
4	Aug 2, 2022 @ 22:53:33.220	25	
5	Aug 2, 2022 @ 22:53:33.250	26	
6	Aug 2, 2022 @ 22:53:33.280	26	
7	Aug 2, 2022 @ 22:53:33.311	26	
8	Aug 2, 2022 @ 22:53:33.341	26	
9	Aug 2, 2022 @ 22:53:33.372	26	
10	Aug 2, 2022 @ 22:53:33.405	23	
11	Aug 2, 2022 @ 22:53:33.432	30	
12	Aug 2, 2022 @ 22:53:33.462	26	
13	Aug 2, 2022 @ 22:53:33.492	26	
14	Aug 2, 2022 @ 22:53:33.522	26	
15	Aug 2, 2022 @ 22:53:33.553	26	
16	Aug 2, 2022 @ 22:53:33.583	26	
17	Aug 2, 2022 @ 22:53:33.613	26	
18	Aug 2, 2022 @ 22:53:33.644	26	
19	Aug 2, 2022 @ 22:53:33.674	26	
20	Aug 2, 2022 @ 22:53:33.704	26	
21	Aug 2, 2022 @ 22:53:33.737	23	
22	Aug 2, 2022 @ 22:53:33.764	26	
23	Aug 2, 2022 @ 22:53:33.795	28	
24	Aug 2, 2022 @ 22:53:33.825	26	
25	Aug 2, 2022 @ 22:53:33.855	26	
26	Aug 2, 2022 @ 22:53:33.885	26	
27	Aug 2, 2022 @ 22:53:33.915	26	
28	Aug 2, 2022 @ 22:53:33.945	26	
29	Aug 2, 2022 @ 22:53:33.974	26	
30	Aug 2, 2022 @ 22:53:34.007	26	
STDDEV		1,402	

V. KESIMPULAN

A. *Kesimpulan*

Dari penelitian yang dilakukan dapat diambil kesimpulan, layanan webserver masih terlihat normal atau tidak dijumpainya pesan galat 404 di browser ketika serangan terjadi. Penerapan metode deteksi dan OSCAR mampu mendeteksi adanya serangan pada port 80 webserver dengan indikasi adanya notifikasi di SIEM wazuh. Hasil analisa dalam proses akusisi data, diperoleh nilai standar deviasi waktu serangan 1,402 detik. Semakin rendah nilai standar deviasi, maka semakin mendekati rata-rata, sedangkan jika nilai standar deviasi semakin tinggi, artinya semakin lebar rentang variasi data serangan yang terjadi. Berdasarkan pengujian keamanan Port 80 atau *Service HTTP (Hyper Text Transfer Protocol)*. Adanya hasil kerentanan yang diperoleh dan adanya serangan yang terjadi, dapat mengancam keamanan data dan informasi jika tidak dilakukan perbaikan.

B. Saran

Solusi perbaikan yang disarankan adalah seorang system administrator sebaiknya melakukan *hardening system* webserver untuk menghindari kerentanan sistem dan meminimalisir dampak serangan, melakukan pengujian ulang serta melakukan penghitungan ulang nilai kerentanan, dan optimalisasi tugas *security officer* utk mengamati setiap notifikasi SIEM perlu dilakukan secara berkala, menggunakan sistem operasi dan kernel yang stabil dan backup data secara berkala. Penelitian yang dilakukan mengenai evaluasi keamanan pada port 80, dikemudian hari dapat dikembangkan dalam bentuk pengujian keamanan port 80 menggunakan *Hacking Methodology* diantaranya *Reconnaissance, Enumeration, Exploitation, Privilege Escalation, Post Exploitation, Covering Tracks* dan *Report Writing.*

REFERENCES

[1] Pusat Operasi Keamanan Siber Nasional BSSN, "Indonesia Cyber Security Monitoring Report 2019," 2020. [Online]. Available: https://cloud.bssn.go.id/s/nM3mDzCkgycRx4S/download

[2] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," *J. Sist. Inf. Bisnis*, vol. 8, no. 2, p. 115, 2018, doi: 10.21456/vol8iss2pp115-122.

[3] R. Sahtyawan, "Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment and Penetration Testing)," *J. Inf. Syst. Manag.*, vol. 1, no. 1, pp. 18–22, 2019, doi: 10.24076/joism.2019v1i1.18.

[4] F. Paramita, O. Alvina, R. E. Sentia, and A. Kurniawan, "Analisis Unauthorized Access Point Menggunakan Teknik Network Forensics," *J. Telemat.*, vol. 14, no. 2, pp. 63–72, 2021.

[5] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[6] I. Priyadarshini, "Introduction On Cybersecurity," in *Cyber Security in Parallel and Distributed Computing Concept, Techniques, Applications and Case studies*, 2019, no. March, pp. 3–37. doi: 10.1002/9781119488330.ch6.

[7] C. Arfanudin, B. Sugiantoro, and Y. Prayudi, "Analisis Serangan Router Dengan Security Information and Event Management Dan Implikasinya Pada Indeks Keamanan Informasi," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 1, pp. 1–7, 2019.

[8] Palo Alto Networks, "What is lateral movement in cyber security?," 2022. https://www.paloaltonetworks.com/cyberpedia/what-is-lateral-movement (accessed Jul. 26, 2022).

[9] crowdstrike.com, "Lateral Movement," 2022. https://www.crowdstrike.com/cybersecurity-101/lateral-movement/ (accessed Jul. 26, 2022).

[10] W. Abidian, "Security Information and Event Management (Studi Kasus : Jaringan Uii) (Studi Kasus : Jaringan Uii)," Universitas Islam Indonesia, 2021. [Online]. Available: https://dspace.uii.ac.id/handle/123456789/29642

[11] M. D. Pratama, F. Nova, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos," vol. 3, no. 1. pp. 1–7, 2022.

[12] M. Syani and A. M. Ropi, "Analisis Dan Implementasi Network Security System Menggunakan Teknik Host-Based Intrusion Detection System (Hids) Berbasis Cloud Computing," *Semin. Nas. Telekomun. dan Inform. (SELISIK 2018)*, no. September, p. 2, 2018.

[13] S. M. Zeinali, "Analysis of Security Information and Event Management (Siem) Evasion an Detection Methods," Tallinn University of Technology, 2016.

[14] N. I. Aspriantama, "Pengujian Keamanan Sistem Informasi Uajy Menggunakan Penetration Testing," 2021, [Online]. Available: http://e-journal.uajy.ac.id/id/eprint/24753

[15] I. Syarifudin, "Pentesting dan Analisis Keamanan Web Paud Dikmas," *Pentesting Dan Anal. Keamanan Web Paud Dikmas*, no. April, p. 2, 2018.