ANALISIS KERENTANAN MENGGUNAKAN ALIENVAULT DAN QUALYS PADA SECURITY OPERATION CENTER (SOC) BERDASARKAN FRAMEWORK CYBER KILL

ANALYSIS OF VULNERABILITIES USING ALIENVAULT AND QUALYS IN SECURITY OPERATIONS CENTER (SOC) ON CYBER KILL FRAMEWORK

Bobby Abdullah[1], Avon Budiyono, S.T., M.T.[2], Adityas Widjajarto, S.T., M.T [3]

[3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]bobbyabdullah@student.telkomuniversity.ac.id, [2]avonbudi@telkomuniversity.ac.id,
[3]adtwjrt@telkomuniveristy.ac.id

Abstrak

Penerapan *tools open source software Security Information and Event Management* (*SIEM*) adalah salah satu komponen dalam pengimplementasian teknologi pada *Security Operations Center* (SOC). Penelitian ini membandingkan hasil dari *vulnerability scan* antara dua *tools open source software* (AlienVault dan Qualys) dengan parameter uji identifikasi *vulnerabilities* dan waktu yang dibutuhkan untuk melakukan *vulnerability scan*. Langkah-langkah penelitian menggunakan *framework* CYBER KILL. Simulasi dilakukan dengan menerapkan *vulnerability operating system* (VulnOS2, Vulnix, dan DC-1) pada VirtualBox sebagai objek penelitian untuk *scanning* dan AlienVault serta Qualys sebagai manager *scan*. Skenario pengujian yang dijalankan adalah dengan melakukan *vulnerability scan* ketiga *vulnerability operating system* menggunakan *AlienVault* dan *Qualys*. Laporan yang dihasilkan dari *vulnerability scan AlienVault* dan *Qualys* berisi jumlah *vulnerabilities. Potential vulnerability, Information Gathering*, serta informasi dan deskripsi mengenai *vulnerabilities*. Dari hasil penghitungan keakuratan didapatkan hasil bahwa vulnerability memiliki *risk score* yang sama.

Kata kunci : *SIEM, SOC, AlienVault, Qualys, Vulnerability, Open Source, Tools, Framework, Cyber Kill, Cyber*

Abstract

The application of open source software Security Information and Event Management (*SIEM*) is one of the components in implementing technology in the Security Operations Center (SOC). This study compares the results of a *vulnerability* scan between two open-source software tools (AlienVault and Qualys) with the *vulnerability* identification test parameters and the time required to conduct a *vulnerability* scan. Research steps using the CYBER KILL framework. Simulations are carried out by applying the operating system vulnerabilities (VulnOS2, Vulnix, and DC-1) to VirtualBox as research objects for scanning and AlienVault and Qualys as scan managers. The testing scenario that is run is to do a *vulnerability* scan of the three operating system vulnerabilities using AlienVault and Qualys. Reports generated from AlienVault and Qualys *vulnerability* scans contain the number of vulnerabilities. Potential vulnerabilities, Information Gathering, as well as information and descriptions of vulnerabilities. From the results of the calculation of accuracy obtained results has the same risk score.

Keywords: *SIEM, SOC, AlienVault, Qualys, Vulnerability, Open Source, Tools, Framework, Cyber Kill, Cyber.*

1. Pendahuluan

Dalam era globalisasi ini jalur pertukaran informasi digital telah berkembang pesat. Perkembangan ini juga disertai oleh pertambahan jumlah ancaman terhadap keamanan jaringan. Aktivitas- aktivitas ilegal yang dikenal dengan *cyber crime* atau kejahatan *cyber* dalam bentuk *hacking*, virus, *spyware*, trojan dan lain sebagainya terus tumbuh

Dengan jumlah serangan siber terhadap asset-aset organisasi dan perusahaan yang terus meningkat, pengelolaan keamanan informasi di organisasi dan perusahaan pun perlu ditingkatkan. Salah satunya dengan mengadakan fungsi *Security Operation Center (*SOC).

Sebuah studi tentang pencurian data yang dirilis oleh IBM pada tahun ini mengungkapkan bahwa kerugian akibat pencurian data dari tahun ke tahun naik sebesar 12%, dengan kerugian rata-rata sebesar US$3,92 juta. Laporan yang sama juga mengatakan, rata-rata waktu yang dibutuhkan untuk mengidentifikasi kebobolan, mulai dari hari pertama sampai serangan itu diketahui, adalah 206 hari. Atmojo (2017)

Security Operation Center adalah suatu tim yang terorganisir dan mempunyai kemampuan dalam bidang keamanan siber yang bertugas memantau dan meningkatkan postur keamanan organisasi dengan mencegah, mendeteksi, menganalisis, dan menanggapi insiden keamanan siber dengan menggunakan teknologi dan proses yang telah disusun dengan baik. Madani (2011)

Penelitian dilakukan dengan menggunakan *software* AlienVault dan Qualys untuk mendeteksi serangan sehingga diketahui sejauh mana AlienVault dan Qualys dapat mengakomodasi *framework*

Penelitian ini menghasilkan usulan dan perbandingan mengenai *tools* sesuai metode dalam *framework* CYBER KILL. Hasil usulan dan perbandingan tersebut dapat membantu SOC untuk bekerja secara maksimal dalam melindungi serta menangani celah maupun serangan siber pada suatu sistem.

2. Dasar Teori

2.1 Definisi Security Operation Center

Security Operation Center (SOC) adalah salah satu komponen pendukung keamanan IT dalam sebuah perusahaan. Lebih spesifik, *Cyber* SOC adalah serangkaian aktifitas yang terdiri dari pengamanan *cyberspace*, memonitor dan menganalisa ancaman dan insiden, serta secara proaktif dan responsif melakukan manajemen terhadap insiden. Secara fungsi, SOC membantu perusahaan dalam melakukan identifikasi, mengelola dan meremediasi terhadap serangan. Singkatnya tujuan akhir dari SOC adalah untuk meningkatkan postur keamanan IT dari perusahaan dengan mendeteksi dan merespon ancaman dan serangan sebelum berdampak pada bisnis. Atmojo (2017)

2.2 Vulnerability

Risk dapat dikatakan sebagai potensi kehilangan, atau kerusakan suatu sistem yang diakibatkan dari *threat* yang mengeksploitasi *vulnerability*. Menurut (Kumar, 2016) penentuan hasil resiko dapat menggunakan formula *Risk = Vulnerability x Threat*

2.3 Threat

Threat merupakan aksi yang terjadi baik dari dalam maupun dari luar sistem yang dapat mengganggu keberlangsungan sistem. *Threat* terhadap sistem dapat digolongkan menjadi 2 macam yaitu aktif dan pasif (Bodnar dan Hopwood, 2006). Yang termasuk dalam ancaman aktif yaitu kecurangan dan kejahatan siber, sedangkan yang termasuk dalam ancaman pasif adalah bencana alam, kesalahan manusia, dan kegagalan sistem atau lingkungan (Bodnar dan Hopwood, 2006). Dengan adanya ancaman-ancaman tersebut, maka harus dilakukan usaha untuk melindungi sistem yang dapat dicapai melalui mitigasi.

2.4 Risk

Risk dapat dikatakan sebagai potensi kehilangan, atau kerusakan suatu sistem yang diakibatkan dari *threat* yang mengeksploitasi *vulnerability*. Menurut (Kumar, 2016) penentuan hasil resiko dapat menggunakan formula *Risk = Vulnerability x Threat.*

2.5 AlienVault OSSIM (Open Source Security Information Management)

Menurut *Alien Vault*, (2012) *OSSIM* adalah aplikasi *SIEM* yang berbasis *open source*. *OSSIM* berberupa sebuah sistem operasi berbasis *Debian* yang di dalamnya sudah terinstalasi berbagai aplikasi untuk keperluan *network monitoring*, *HIDS*, *NIDS*. Selain menggunakan aplikasi-aplikasi yang sudah ada, di dalam *OSSIM* ditambahkan modul-modul buatan tim pengembang, sehingga *OSSIM* menjadi aplikasi *SIEM* yang lebih *powerful*. Pada dasarnya *OSSIM* ini berupaya mengintegrasikan beberapa perangkat lunak dan *existing tools* lainnya untuk bekerjasama melakukan suatu penyimpanan, melakukan korelasi dan manajemen perangkat. Sehingga dapat menghasilkan kumpulan *event, log* dan informasi kondisi keamanan jaringan dari sebuah *single console*.

2.6 Qualys

Qualys merupakan sebuah berbasis *Cloud* yang menawarkan banyak pelayanan yang salah satunya adalah *Vulnerabilty Management*. *Qualys* dijalankan melalui *Web Service*. *Qualys* dapat dijalankan dengan mudah dengan cara registrasi terlebih dahulu, menggunakan *e-mail* dan akan menerima *username* beserta *password* untuk dapat mengakses *Qualys* sesuai kebutuhan.

2.7 Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) merupakan suatu kerangka nilai pengukuran untuk menilai tingkat kerentanan serta keparahan dalam suatu sistem. (Mell et al., 2006) Dikemabangkan oleh *Forum of Incident Response and Security Teams (FIRST), CVSS* menggunakan algoritma dalam menentukan tiga peringkat keparahan : *Base, Temporal,* dan *Environmental.* Skor dengan numerik dimulai dari 0.0 hingga 10.0 merupakan nilai yang paling parah.

2.8 The Cyber Kill Chain

Berdasarkan *paper* yang dikeluarkan oleh *Lockheed Martin*, *Intrusion Kill Chain* dibagi menjadi 7 tahapan yakni *Reconnaissance*, *Weaponization*, *Delivery*, *Exploitation*, *Installation*, *Command and Control* (C2), dan *Actions* on *Objectives*.

1 *Reconnaissance Reconnaissance* merupakan tahap pertama dari intrusi yang paling sering dilakukan. Terdapat berbagai macam teknik untuk melakukan *reconnaissance*, yang paling umum *reconnaissance* ini dikelompokkan kedalam 2 tipe yakni Aktif dan Pasif. *Reconnaissance* secara aktif akan melibatkan *attacker* untuk menyentuh atau terhubung langsung dengan target serangan guna mendapatkan informasi yang lebih lengkap dan spesifik misal seperti informasi

kerentanan atau *vulnerability* pada sistem target. Berbeda dengan tipe aktif, tipe pasif tidak melibatkan target serangan secara langsung. Informasi yang dibutuhkan untuk melakukan serangan pada tahap ini didapatkan biasanya dari pihak ketiga seperti mesin pencari, media sosial, dan beberapa *website* penyedia informasi.

2 *Weaponization* Tergantung dari jumlah dan kualitas informasi yang berhasil didapatkan dari proses *reconnaissance*, *attacker* akan mulai menyusun skenario serangan yang paling cocok terhadap targetnya, dan tahap ini disebut *weaponization*. Tahapan ini lebih banyak terjadi pada sisi *attacker* sehingga cukup sulit dideteksi sampai serangan tersebut dijalankan. Fase ini sangat bergantung pada informasi hasil *reconnaissance* sehingga untuk mengurangi tingkat keberhasilan dari *attacker* dapat dilakukan pembatasan informasi apa saja yang mungkin dapat diketahui oleh *attacker* pada fase *reconnaissance*. Dan juga memastikan bahwa setiap *vulnerability* yang terdapat pada jaringan internal dilakukan *patch* sebelum berhasil dieksploitasi oleh *attacker*.

3 Delivery
Skenario yang telah disiapkan sebelumnya pada fase *weaponization* kemudian dijalankan pada fase *delivery*. *Payload* ataupun *exploit* yang telah dipilih sebelumnya akan dikemas sedemikian hingga dan dikirmkan ke target dengan berbagai cara misal saja seperti lewat *email*, *usb flash-drive* yang sengaja dijatuhkan didekat lokasi target, atau melalui *website* yang telah disusupi *payload* dan mengarahkan target untuk mengunjungi *website* tersebut.

4 Exploitation
Exploitation adalah tahapan selanjutnya setelah *exploit* atau *payload* berhasil dikirimkan, diterima dan dijalankan oleh target. *Exploit* akan dijalankan dan mengeksploitasi *vulnerability* yang ada pada target menyebabkan perangkatnya ter-*compromise*. *Exploit* ini bisa diberikan langsung pada tahap *delivery* ataupun hanya berupa *dropper* dimana *exploit* yang sesungguhnya akan *didownload* dari Internet saat *dropper* tersebut dijalankan oleh target

5 Installation
Instalasi dari *Remote Access Trojan* (*RAT*) dan *backdoor* pada target membuat *attacker* memiliki akses berkelanjutan pada sistem target untuk melancarkan serangan lanjutan ataupun mengincar target lainnya. *Attacker* yang terlatih dan berpengalaman akan dengan mudah menyembunyikan RAT dan *backdoor* yang diinstallnya untuk menghindari deteksi, *RAT* dan *backdoor* jenis ini biasanya merupakan varian yang telah dimodifikasi

6 Command and Control (C2)
Command and *Control* (C2) dipakai oleh *attacker* untuk mengontrol sistem target yang telah ter-*compromise* secara penuh. *Command and Control* ini bisa diimplementasikan pada berbagai protokol tergantung dari kemampuan *attacker*, *Command and Control* yang umum adalah via protokol yang tidak terenkripsi seperti *HTTP*, *DNS*, *ICMP*, dan *IRC*. Beberapa *attacker* yang terlatih akan memakai jalur komunikasi terenkripsi untuk menghindari pendeteksian seperti *HTTPS* dan *SSH*.

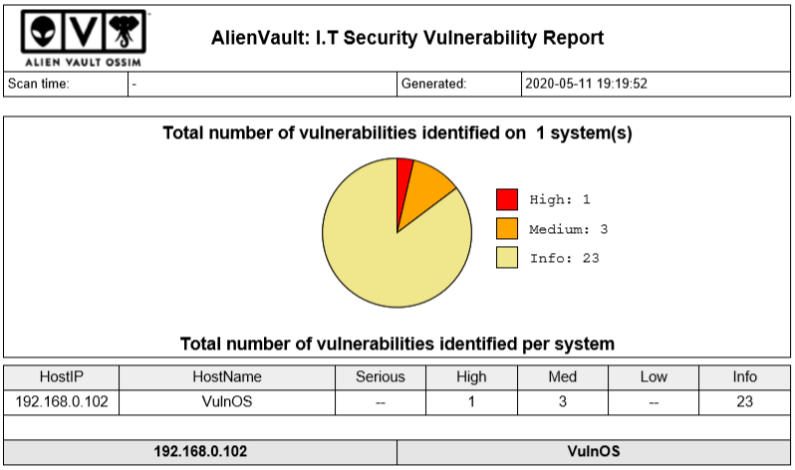
7 Action on Objectives
Setiap *attacker* pasti memiliki tujuan saat melancarkan serangannya, entah itu hanya untuk melatih kemampuan atau yang lebih serius lagi seperti pencurian informasi dan *cyberterrorism*. Ketika *attacker* telah berhasil mencapai targetnya maka *security analyst* yang melakukan *NSM* dan *CSM* sebagai *defender* dapat dikatakan gagal dalam menjalankan tugasnya. Oleh karena itu salah satu tugas *security analyst* adalah untuk mencegah *attacker* mendapatkan tujuannya, medeteksi serangannya dan memutus serangan tersebut pada fase atau tahap yang tepat sesuai *Intrusion Kill Chain*

3. Pengujian dan Analisis

3.1 Pengujian

1. Pengujian Menggunakan AlienVault

Proses *scanning* dengan menggunakan *tools OSSIM* yang menghasilkan daftar *vulnerabilities, CVSS Base Score, CVSS Base Vector,* dan Vulnerability ID.



Gambar 1 Hasil AlienVault

Gambar 1 merupakan hasil pengujian vulnerability machine VulnOS menghasilkan vulnerabilities dengan tingkat keparahan High dengan 1 vulnerability, Medium dengan 3 vulnerability, serta 23 Info

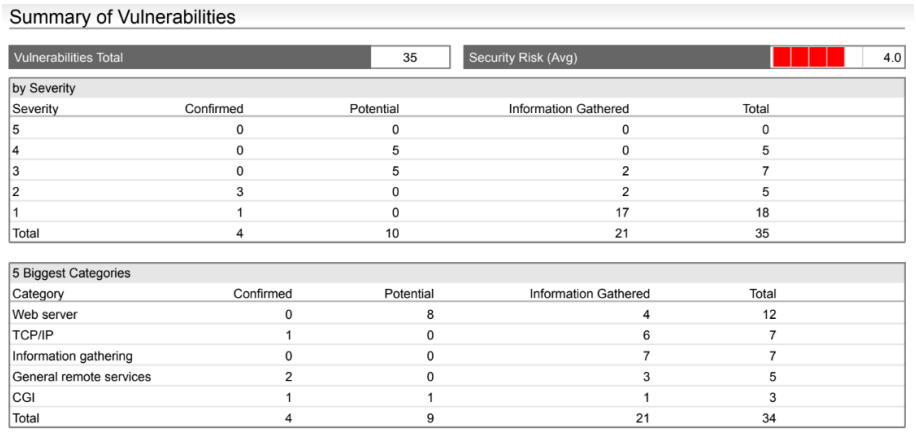
Tabel 1 Daftar Vulnerability denga AlienVault

VulnOS2				
Severity	***Vulnerabilities***	***CVSS Base Vector***	***CVSS Base Score***	***Vulnerability ID***
Serious	-	-	-	-
High	*Drupal Core Critical Remote Code Execution Vulnerability (port 80/tcp)*	AV:N/AC:L/Au:N/C:P/I:P/A:P	7.5	$V.AV_{x1}$
Medium	*SSH Weak Encryption Algorithms Supported* (port 22/tcp)	AV:N/AC:M/Au:N/C:P/I:N/A:N	4.3	$V.AV_{x2}$
	SSH Weak MAC Algorithms Supported (port 22/tcp)	AV:N/AC:H/Au:N/C:P/I:N/A:N	2.6	$V.AV_{x3}$
	TCP timestamps (*port* 0/tcp)	AV:N/AC:H/Au:N/C:P/I:N/A:N	2.6	$V.AV_{x4}$
Low	-	-	-	

Tabel 1 berisi daftar daftar vulnerability dengan tingkat keparahan, cvss base vector, cvss base score, dan vulnerability id untuk dilakukan analisis

2. Pengujian Menggunakan Qualys

Proses *scanning* dengan menggunakan *tools Qualys Vulnerability Management* yang menghasilkan daftar *vulnerabilities*



Summary of Vulnerabilities

Vulnerabilities Total	35	Security Risk (Avg)	4.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	5	0	5
3	0	5	2	7
2	3	0	2	5
1	1	0	17	18
Total	4	10	21	35

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Web server	0	8	4	12
TCP/IP	1	0	6	7
Information gathering	0	0	7	7
General remote services	2	0	3	5
CGI	1	1	1	3
Total	4	9	21	34

Gambar 2 Hasil Qualys

Gambar 2 merupakan hasil pengujian vulnerability machine VulnOS menghasilkan vulnerabilities dengan tingkat keparahan Medium (2) dengan 3 vulnerability, dan Minimal (1) dengan 1 vulnerability

Tabel 2 Daftar Vulnerability dengan Qualys

Severity	***Confirmed Vulnerability***	***CVSS Base Score***	***Vulnearbility ID***
5 (Urgent)	-	-	-
4 (Critical)	-	-	-
3 (Serious)	-	-	-
2 (Medium)	HTTP *Security Header Not Detected*	*4.3*	*V.Qu$_{x1}$*
	SSH *Server Public Key Too Small*	*5.0*	*V.Qu$_{x2}$*
	Deprecated SSH *Cryptographic Settings*	*6.4*	*V.Qu$_{x3}$*
1 (Minimal)	TCP *Sequence Number Approximation Based Denial of Service*	*5.0*	*V.Qu$_{x4}$*

Tabel 2 berisi daftar daftar vulnerability dengan tingkat keparahan, cvss base vector, cvss base score, dan vulnerability id untuk dilakukan analisis

3.2 Hasil Analisis Menggunakan Technical Aspect Cyberkill Chain

- *Reconnaissance* pada tahap ini adalah pengumpulan informasi dari potential target, informasi didapat melalui pengintaian atau dari berbagai situs penyedia informasi publik yang selanjutnya akan diteruskan kedalam tahap *Weaponize*

Tabel 3 Teknik Reconnaissance

Teknik *Reconnaissance*	Tipe *Reconnaissance*	Teknik yang digunakan
Identifikasi target	Active	*Sql mapping, Fingerprinting, General enumeration*

  - Teknik identifikasi target dilakukan untuk mengetahui informasi objek yang dijadikan target untuk dieksploitasi dengan menggunakan tipe *Reconnaissance* aktif yang berarti akan melibatkan attacker untuk terhubung langsung dengan target. Dengan teknik yang digunakan Sql maping, dan *Fingerprinting* akan mudah terdeteksi.
  - Mitigasi yang dapat dilakukan berupa pengimplementasian firewall, disertai dengan ACL yang baik dan terdokumentasi. Penambahan perangkat IPS juga menjadi solusi yang baik untuk melakukan pemblokiran secara otomatis saat terdeteksi adanya serangan ini.

- *Weaponize* merupakan tahap dimana *attacker* akan melakukan desain backdoor.
  - Attacker melakukan *web enumeration* dengan mengeksploitasi vulnerability *HTTP Security Header not Detected* dan *Drupal core critical remote code execution.*
  - Mitigasi yang dapat dilakukan adalah memastikan bahwa semua vulnerability yang terdapat pada jaringan internal dilakukan patching sebelum berhasil dieksploitasi oleh attacker.

- Attacker melakukan *Execution Bypass* untuk dapat masuk kedalam Drupal dengan mengeksploitasi vulnerability Drupal *Core Critical Remote Code Execution Vulnerability*
  - Delivery merupakan tahap yang beresiko tinggi untuk *attacker* karena pada tahap ini akan

meninggalkan jejak dari *attacker* itu sendiri
- Mitigasi yang bisa dilakukan untuk mencegah dan mendeteksi serangan pada tahap delivery ini adalah dengan mengimplementasikan IDS dan IPS.

- *Exploitation Exploit* akan dijalankan dan mengeksploitasi *vulnerability* yang ada pada target menyebabkan perangkatnya ter-*compromise*.

Tabel 4 Exploitation

Kategori Exploit	*Tipe Exploit*	*Tipe Vulnerability*
Operating System Exploit	TCP *Sequence Number Approximation*	Denial of Service
Network Level Exploit	Protocol exploit for TCP, UDP, SSH, SMTP	Privilege Escalation
Application/Software Exploit	Web Application Exploit	Drupal

  - Operating System Exploit adalah serangan yang ditujukan untuk memperoleh modul kernel dari Operating System melalui vulnerability Denial of Service
  - Network Level Exploit serangan dengan mengeksploitasi protokol TCP, UDP, SSH, dan SMTP untuk mendapatkan privilege escalation
  - Application/Software Exploit serangan dengan memanfaatkan Web Application Exploit (Drupal) untuk masuk kedalam sistem target.
  - Mitigasi yang bisa dilakukan untuk mengurangi tingkat keberhasilan pada fase ini adalah dengan mengimplementasikan Host-based IDS/IPS (HIDS/HIPS), menerapkan *application whitelisting*, dan *patch management* yang baik pada drupal.

- Installation pada tahap ini attacker sudah melakukan *backdoor* pada sistem dan akan memiliki akses berkelanjutan untuk melancarkan serangan lanjutan.
  - Attacker melakukan *password cracking* untuk mendapat *privilege user* dengan mengeksploitasi *vulnerability* SSH *Weak Encryption Algorithms Supported*
  - Sistem deteksi tingkat lanjut dapat diimplementasikan untuk memitigasi serangan pada tahap ini. Implementasi yang biasa dilakukan adalah dengan melakukan monitoring pada *event logs* dan *registry* sistem. *Application whitelisting* juga bisa dipakai untuk mencegah *backdoor* pada sistem

- Command and Control (C2) pada tahap ini *attacker* memberikan intruksi jarak jauh kepada target melalui protocol SSH.
  - Attacker melakukan SSH untuk melakukan remote access dengan mengeksploitasi vulnerability SSH *Weak* MAC *Algorithms Supported, dan* SSH *Server Public Key Too Small*
  - IDS dan IPS dapat mendeteksi traffic komunikasi dari C2. Beberapa jenis malware akan melakukan koneksi outbound untuk menghubungi pemiliknya, koneksi atau komunikasi ini biasa disebut dengan istilah callback atau homecalling.

- Actions on Objectives pada tahap ini ketika *attacker* telah berhasil mencapai targetnya yaitu user root, maka security analyst yang melakukan *Network Security Monitoring* dan *Continuous Security Monitoring* sebagai *defender* dapat dikatakan gagal dalam menjalankan tugasnya.

4. Kesimpulan

Setelah dilakukan analisis kerentanan menggunakan AlienVault dan Qualys pada Security operation center berdasarkan *framework* cyber kill didapat kesimpulan sebagai berikut :

- Pengimplementasian sebagian fungsi pada technology SOC menggunakan AlienVault dan Qualys pada fitur *vulnerability* scaning yang bertujuan untuk mengetahui jenis jenis *vulnerability* pada vulnerable machine

- Dari penelitian menggunakan software open source AlienVault dan Qualys bahwa hasil yang didapatkan oleh peneliti memiliki hasil daftar *vulnerability* yang cenderung sama dengan tipe *vulnerability* Drupal Core

- Hasil *vulnerability* scaning dengan *AlienVault* dan *Qualys* dapat mengakomodasi *framework Cyber Kill Chain*. Mengacu pada hasil report dari *vulnerability* scan, threat, serta risk dan menghasilkan solusi berupa mitigasi pada setiap fase dari *Cyber Kill Chain*

- Fitur yang dapat digunakan dalam penelitian ini adalah *vulnerability* scanning dikarenakan objek bersifat offline sehingga information dan event management tidak bekerja secara maksimal

Daftar Pustaka:

[1] AlienVault. (2012, 04 25). *AlienVault OSSIM Review – Open Source SIEM*. Retrieved from https://resources.infosecinstitute.com: https://resources.infosecinstitute.com/alienvault-ossim-review-open-source-siem/

[2] Ammann, P., Wijesekera, D., & Kaushik, S. (2002). *Scalable, Graph-Based Network Vulnerability Analysis *.*

(2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case.*

[3] Bahrami, P., Dehghantanha, A., Dargahi, T., Parizi, R., Choo, K., & Javadi, H. (2019). Cyber kill chain-based taxonomy of advanced persistent *threat* actors: Analogy of tactics, techniques, and procedures. *Journal of Information Processing Systems, 15*(4), 865-889.

[4] Becker, J., Niehaves, B., & Janiesch, C. (2010). Socio-Technical Perspectives on Design Science in IS Research. *Information Systems and eBusiness Management, Vol.9, issue 1*, 109-131.

[5] Ben Rothke, C. C. (2012). *Building a Security Operations Center (SOC)*. Retrieved from https://www.academia.edu: https://www.academia.edu/33355557/Building_a_Security_Operations_Center_SOC

[6] Bhatt, S., Manadhata, P., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE Security and Privacy, 12*(5), 35-41.

[7] Bidou, R. (n.d.). *Security Operation Center Concepts & Implementation.*

[8] Bryant, B., & Saiedian, H. (2017, 6 1). A novel kill-chain *framework* for remote security log analysis with SIEM software. *Computers and Security, 67*, 198-210.

[9] Daimi, K. (2017). *Computer and network security essentials.* Springer International Publishing.

[10] Eric M. Hutchins∗, M. J. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lockheed Martin Whitepaper*, 4-5.

[11] Ganame, A., Bourgeois, J., Bidou, R., & Spies, F. (n.d.). *A Global Security Architecture for Intrusion Detection on Computer Networks.*

[12] Hevner, A. R., Ram, S., March, S. T., & Park, J. (2004). Design Science in Information Systems Research. *MIS Quarterly Vol. 28 No. 1*, 75-105.

[13] Hevner, A., & Chatterjee, S. (2010). *Design Research in Information System : Theory and Practice.* New York: Springer.

[14] Hildenbrand, T., Rothlauf, R., Geisser, M., Heinzl, A., & Kude, T. (2008). Approach to Collaborative Software Development. *International Conference on Complex, Intelligent and Software Intensive Systems* (pp. 523-528). Barcelona: IEEE.

[15] Kiwia, D., Dehghantanha, A., Choo, K., & Slaughter, J. (2018, 7 1). A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *Journal of Computational Science, 27*, 394-409.

[16] P., P. (2018, 12 24). *What is a SOC (SecurityOperations Center)?* Retrieved from https://securityaffairs.co: https://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html

[17] Phillips, C., & Swiler, L. (1999). *A Graph-Based System for Network-Vulnerability Analysis.*

[18] Raj, P., & Jagadeesan, M. (n.d.). *A Framework Design to Improve and Evaluate the Performance of Security Operation Center (SOC) MSc Internship Cyber Security.*

[19] Scanner, I. (1995). *Analysis. Of An Algorithm For Distributed Recognition And Accountability*. Springer-Verlat.

[20] Tarnowski, I. (n.d.). *How to use cyber kill chain model to build cybersecurity?*

[21] Toto A. Atmojo, C. C. (2017, 08 01). *Strategi Pengembangan Security Operation System*. Retrieved from https://www.ciocommunity.org: https://www.ciocommunity.org/news/read/200/Strategi-Pengembangan-Security-Operation-System

[22] Yadav, T., & Mallari, R. (2016, 6 10). Technical Aspects of Cyber Kill Chain.

[23] ELK. (2012, 04 25). *ELK OSSIM Review – Open Source SIEM*. Retrieved from https://resources.infosecinstitute.com: https://resources.infosecinstitute.com/ELK-ossim-review-open-source-siem/

[24] Becker, J., Niehaves, B., & Janiesch, C. (2010). Socio-Technical Perspectives on Design Science in IS Research. *Information Systems and eBusiness Management, Vol.9, issue 1*, 109-131.

[25] Eric M. Hutchins∗, M. J. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lockheed Martin Whitepaper*, 4-5.

[26] P., P. (2018, 12 24). *What is a SOC (SecurityOperations Center)?* Retrieved from https://securityaffairs.co: https://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html

[27] Mokodompit, M. P., & Nurlaela, N. (2017). Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X). *Jurnal Sistem Informasi Bisnis, 6*(2), 97. https://doi.org/10.21456/vol6iss2pp97-104

[28] Patsos, D., Mitropoulos, S., & Douligeris, C. (2010). Expanding topological *vulnerability* analysis to intrusion detection through the incident response intelligence system. *Information Management and Computer Security, 18*(4), 291–309. https://doi.org/10.1108/09685221011079207