ANALISIS KERENTANAN MENGGUNAKAN ALIENVAULT DAN QUALYS PADA *VULNERABILITY OPERATING SYSTEM* BERDASARKAN *FRAMEWORK* STRIDE

ANALYSIS VULNERABILITY USING ALIENVAULT AND QUALYS SOFTWARE IN VULNERABILITY OPERATING SYSTEM BASED ON FRAMEWORK STRIDE

Vreseliana Ayuningtyas[1], Adityas Widjajarto[2], Avon Budiono[3]

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

Abstrak

Perkembangan teknologi informasi yang semakin pesat mengakibatkan keamanan menjadi sangat penting. Di samping kemudahan akses, terdapat juga ancaman terhadap kerentanan pada teknologi informasi. Jumlah serangan siber tahun 2019 menunjukan peringkat ke lima dengan jumlah 1.494.281, data ini di dukung oleh statistik serangan siber yang dikeluarkan oleh Honeynet Project BSSN. Oleh karena itu dibutuhkan software analisis pada kerentanan. Kerentanan merupakan kelemahan pada sistem atau desain yang digunakan saat penyusup mengeksekusi perintah, mengakses data yang tidak sah dan melakukan serangan penolakan layanan. Analisis dilakukan dengan menggunakan salah satu fungsi dari software AlienVault dan Qualys yaitu Vulnerability Assessment. Hasil Vulnerability Scanning yang dilakukan dianalisis, kemudian dihitung dengan rumus risk = vulnerability x threat. Threat didapatkan dari analisis sample walkthrough, sebagai acuan eksploitasi yang sering dilakukan. Hasil estimasi risiko dengan jumlah 73 memiliki risiko tertinggi sebesar 75 sebanyak 5 risiko, kemudian estimasi risiko dianalisis kembali menggunkan framework STRIDE dengan hasil salah satu fungsi tidak mengakomodasi jenis risiko yang ada yaitu Spoofing.

Kata kunci :
vulnerable machine,* kerentanan, ancaman, *framework STRIDE.

Abstract

The rapid development of information technology has made security very important. Besides easy access, there are also threats to vulnerabilities in information technology. The number of cyber attacks in 2019 shows the fifth rank with a total of 1,494,281, this data is supported by the statistics of cyber attacks released by the Honeynet Project BSSN. Therefore a vulnerability analysis software is needed. Vulnerability is a weakness in the system or design used when intruders execute commands, access unauthorized data and carry out denial of service attacks. The analysis was performed using one of the functions of AlienVault and Qualys software, namely Vulnerability Assessment. Vulnerability Scanning results are analyzed, then calculated with the formula risk = vulnerability x threat. Threat is obtained from a sample walkthrough analysis, as a reference for exploitation that is often done. The results of the risk estimation with the number 73 have the highest risk of 75 as many as 5 risks, then the risk estimation is analyzed again using the STRIDE framework with the result that one functions does not accommodate the type of risk that exist, namely Spoofing.

Keywords: ***Security Operation Center (SOC), vulnerable machine, vulnerability, threats, framework STRIDE.***

1. Pendahuluan

Perkembangan Internet dalam teknologi informasi berkembang dengan sangat cepat seiring dengan pertumbuhan penggunanya. Begitu juga tingkat kejahatan dalam teknologi informasi yang merugikan penggunanya baik individu maupun organisai. Pada tahun 2019 jumlah kerentanan meningkat 17,6% sebesar 20.365 (Dima Beker & Sarit Yerus, 2019), data ini didukung oleh statistik kerentanan yang dikeluarkan oleh Research Labs: Application Security, Data Security.

Pada Tugas Akhir ini akan dilakukan analisis terhadap hasil keluaran dari scanning vulnerability pada vulnerable machine yaitu VulnOS, Vulnix dan DC-1 dengan alasan penetration testing yang sudah dijalankan sudah banyak. Software yang digunakan adalah AlienVault dan Qualys, mempunyai salah satu fitur yang akan digunakan yaitu vulnerable assessment dan penggunaannya yang gratis. Dan juga penggunaan framework STRIDE yang merupakan teknis pemodelan yang berbasis ancaman yang dikembangkan oleh Microsoft

2. Tinjauan Pustaka

2.1 Keamanan Infomasi

Keamanan Informasi adalah proteksi peralatan komputer, fasilitas, data dan informasi dari penyalahgunaan pihak-pihak yang tidak sah atau tidak berwenang. Peran Keamanan Informasi untuk suatu organisasi yaitu, dengan memberikan perlindungan informasi dari berbagai macam ancaman agar dapat menjamin kelanjutan bisnis, mengurangi risiko bisnis, meningkatkan Return On Investment (ROI), serta meningkatkan peluang bisnis. (Miftahul Huda, 2020)[1]

2.1.1. AlienVault

AlienVault merupakan sistem yang menyederhanakan cara mendeteksi dan merespon ancaman yang terus berkembang saat ini. Pendekatan yang unik dan memenangkan penghargaan organisasi digunakan oleh ribuan pelanggan dan menggabungkan beberapa kontrol keamanan platform *all-in-one*, manajemen keamanan terpadu dengan pertukaran informasi mengenai ancaman yang terbuka. Ancaman bersumber dari komunitas intelijen untuk mendeteksi ancaman dan mencari cara yang efektif dan berkesinambungan dan agar dapat dicapai oleh tim IT yang terbatas dengan sumber daya. Fitur-fitur AlienVault yaitu *Asset Discovery, Vulnerability Assessment, Behavioral Monitoring, Intrusion Detection,* dan *SIEM*. (Jonathan Reuvid, 2018) [1]

2.1.1.1. *Vulnerability Assessment*

Fitur ini berfungsi untuk mengetahui serangan baik dari celah kecil yang digunakan penyerang untuk menyusup ke sistem keamanan. *Vulnerability Assessment* memberikan penilaian sebagai bagian dari paket lengkap pemantauan keamanan dan kemampuan manajemen untuk mendeteksi ancaman yang efisien, dan meningkatkan keamanan jaringan.

2.1.2. Qualys

Qualys membantu bisnis dalam menyederhanakan operasi keamanan IT dan menurunkan biaya dengan memberikan intelijen keamanan krisis sesuai permintaan dan mengotomatiskan spektrum penuh audit, kepatuhan dan perlindungan untuk sistem perimeter internet, jaringan internal dan aplikasi web. Solusi Qualys meliputi *Continuous Monitoring, Vulnerability Management, Policy Compliance,* PCI *Compliance, Security Assessment Questionnaire, Web Application Scanning, Web Application Firewall*. (Qualys website, 2020) [3]

2.2.2.1 *Vulnerability Assessment*

Vulnerability Assessment (VA) adalah komponen integral dari *vulnerability management*. VA adalah proses mengidentifikasi kerentanan jaringan dan perangkat sebelum peretas dapat mengeksploitasi sistem.

2.2 *Vulnerability*

Vulnerability adalah kelemahan dalam suatu sistem atau desain yang digunakan saat penyusup mengeksekusi perintah, mengakses data yang tidak sah, dan / atau melakukan serangan penolakan layanan. (Abomhara, Mohamed, and G. M. Kien, 2015) [1]

2.4 STRIDE

STRIDE merupakan teknik pemodelan ancaman berbasis model yang dikembangkan oleh Microsoft. STRIDE juga memandu analisis keamanan melalui beberapa kegiatan yang harus dilakukan agar proses menjadi efektif. Enam jenis ancaman keamanan diantaranya: (Khan, R., McLaughlin, K., Laverty, D., &

Sezer, S., 2018) [2]

1. *Spoofing*

   Serangan *spoofing* terjadi ketika seorang penyerang berpura-pura menjadi seorang yang bukan mereka. *Spoofing* biasanya digunakan untuk mendapatkan akses ke informasi pribadi target, yang menyebarkan malware melalui tautan atau lampiran yang terinfeksi, melewati kontrol akses jaringan, atau mendistribusikan kembali lalu lintas untuk melakukan serangan.
2. *Tampering*

   Terjadi ketika penyerang memodifikasi atau mengedit informasi resmi.
3. *Repudiation*

   Repudiation terjadi ketika seseorang melakukan suatu tindakan dan kemudian mengklaim bahwa mereka tidak benar-benar melakukannya. Biasanya muncul pada operasi seperti transaksi kartu kredit, pengguna membeli sesuatu dan kemudian mengklaim bahwa mereka tidak melakukannya.
4. *Information Disclosure*

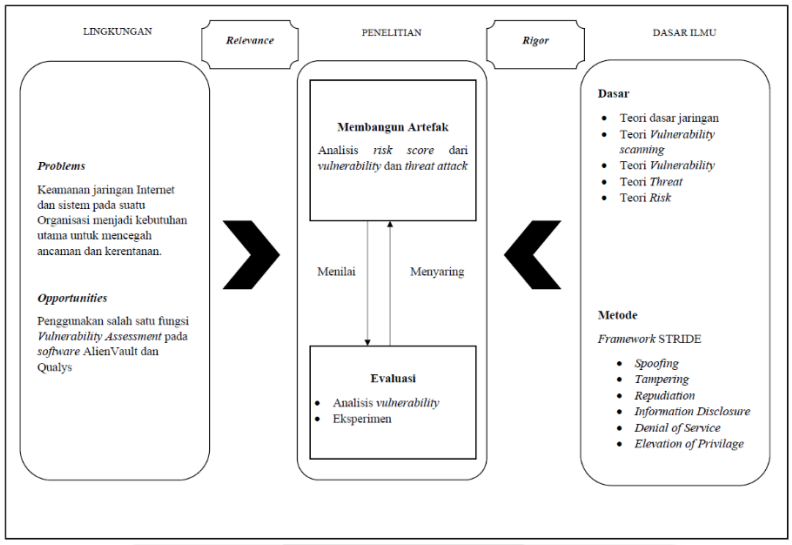
   Pelanggaran data atau akses tidak sah ke informasi rahasia.
5. *Denial of Service (DoS)*

   Gangguan layanan untuk pengguna sah.
6. *Elevation of Privilege*

   Mendapatkan akses hak istimewa yang lebih tinggi ke elemen sistem oleh pengguna dengan otoritas terbatas.

3. Pembahasan

3.1. Metode Konseptual



Gambar 1 Metode Konseptual

Gambar diatas menjelaskan penelitian Analisis Kerentanan mengunakan AlienVault dan Qualys berdasarkan Framework STRIDE pada Vulnerable Machine. Pada lingkup lingkupan terdapat “Problem” yaitu masalah yang dihadapi saat ini keamanan jaringan Internet dan sistem pada organisasi menjadi kebutuhan utama dalam mencegah ancaman dan kerentanan lalu “Opportunities” pada analisis ini yaitu penggunaan salah satu fungsi vulnerability assessment pada software AlienVault dan Qualys. Pada lingkup penelitian terdapat “Membangun Artefak” yang mendeskripsikan aktivitas yang dilakukan pada penelitian ini adalah analisis risk score dari vulnerability dan threat attack “Evaluasi” sebagai gambaran apa saja yang dibutuhkan pada penelitian ini yaitu menganalisis hasil reporting vulnerability dan juga perhitungan risk score.

Pada lingkup “Dasar Ilmu” terdapat dasar sebagai garis besar materi yang menjadi acuan yaitu Teori Dasar Jaringan, Teori Vulnerability Scanning, Teori Vulnerability, Teori Threat, dan juga Teori Risk, lalu metode yang digunakan adalah framework STRIDE dengan fitur Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service dan Elevation of Privilege.

4. Analisis dan Hasil

4.1 Analisis Pengujian

Keluaran *vulnerability assessment* pada AlienVault yaitu faktor risiko untuk setiap kerentanan yang ditemukan dalam sistem, yang sesuai dengan *Common Vulnerability Scoring System* (CVSS) v3.0 yang diberikan oleh *National Vulnerability Database* (NVD). CVSS merupakan standar nilai kerentanan TI, dan metode ini memberikan skor berkisar 0 hingga 10.

4.1.1 Hasil Pengujian VulnOS

Pengujian ini merupakan *scan vulnerability assessment* yang dijalankan pada *software* AlienVault pada *vulnerable machine* VulnOS.

Tabel 1 *Vulnerability* VulnOS dengan AlienVault

Script ID	Vuln ID	*Vulnerability*	CVSS	*Severity*
108438	V1.A1	*Drupal core critical remote code execution*	7,5	*High*
105611	V1.A2	SSH *weak encryption algorithms supported*	4,3	*Medium*
105610	V1.A3	SSH *weak MAC algorithms supported*	2,6	*Medium*
80091	V1.A4	TCP *timestamps*	2,6	*Medium*

Pengujian ini merupakan *scan vulnerability assessment* yang dijalankan *software* Qualys pada *vulnerable machine* VulnOS.

Tabel 2 *Vulnerability* VulnOS dengan Qualys

Script ID	Vuln ID	*Vulnerability*	CVSS	*Severity*
11827	V2.A1	*HTTP Security Header not Detected*	4,3	*Medium*
38738	V2.A2	*SSH Server Public Key too Small*	5	*Medium*
38739	V2.A3	*Deprecated SSH Cryptographic Settings*	6,4	*Medium*
82054	V2.A4	*TCP Sequence Number Approximation*	5	*Minimal*

4.1.2 Hasil Pengujian Vulnix

Pengujian ini merupakan *scan vulnerability assessment* yang dijalankan pada *software* AlienVault pada *vulnerable machine* Vulnix.

Tabel 3 *Vulnerability* Vulnix dengan AlienVault

Script ID	Vuln ID	*Vulnerability*	CVSS	*Severity*
103674	V1.B1	OS *end of life detection*	10	*Serious*
100072	V1.B2	*Check if Mailserver answer to VRFY and EXPN request*	5	*High*
901202	V1.B3	*Check for rlogin service*	7.5	*High*
100080	V1.B4	*Check for rsh service*	7.5	*High*
802236	V1.B5	*Finger service remote information disclosure vulnerability*	5	*High*
105042	V1.B6	SSL/TLS: *OpenSSL CCS man in the middle security bypass vulnerability*	6,8	*High*
103936	V1.B7	SSL/TLS*: OpenSSL TLS 'heartbeat' extension information disclosure vulnerability*	5	*High*
80091	V1.B8	TCP *timestamps*	2,6	*Medium*

Pengujian ini merupakan *scan vulnerability assessment* yang dijalankan *software* Qualys pada *vulnerable machine* Vulnix.

Tabel 4 *Vulnerability* Vulnix dengan Qualys

QID	Vuln ID	*Vulnerability*	CVSS	*Severity*
42430	V2.B1	*OpenSSL memory leak*	5	*Critical*
38142	V2.B2	SSL *server allows anonymous authentication*	5,1	*Critical*
66002	V2.B3	NFS *exported filesystems list*	5	*Serious*
31003	V2.B4	*Finger service discloses logged users*	5	*Serious*

38141	V2.B5	SSL *server may be forced to use weak encryption*	5,4	*Serious*
38601	V2.B6	*Remote login service open*	7,5	*Medium*
38020	V2.B7	*Remote shell service open*	7,5	*Medium*
38628	V2.B8	UDP *constant* IP *identification field fingerprint*	5	*Medium*
38734	V2.B9	SSH *server public key too small*	5	*Medium*
38739	V2.B10	*Deprecated* SSH *cryptographic settings*	6,4	*Medium*

4.1.3 Hasil Pengujian DC-1

Pengujian ini merupakan *scan vulnerability assessment* yang dijalankan *software* AlienVault pada *vulnerable machine* DC-1.

Tabel 5 *Vulnerability* DC-1 dengan AlienVault

Script ID	Vuln ID	*Vulnerability*	CVSS	*Severity*
103674	V1.C1	*OS end of life detection*	10	*Serious*
108438	V1.C2	*Drupal core critical remote code execution*	7,5	*High*
105610	V1.C3	*Drupal Core* SQL *Injection Vulnerability*	7,5	*High*
108440	V1.C4	*Cleartext Transmission of Sensitive Information via* HTTP	4,8	*Medium*
105611	V1.C5	SSH *Weak* MAC *Algorithms Supported*	4,3	*Medium*
80091	V1.C6	TCP *timestamps*	2,6	*Medium*

Pengujian ini merupakan *scan vulnerability assessment* yang dijalankan *software* Qualys pada *vulnerable machine* DC-1.

Tabel 6 *Vulnerability* DC-1 dengan Qualys

QID	Vuln ID	*Vulnerability*	CVSS	*Severity*
13054	V2.C1	*Drupal core database abstraction API SQL Injection*	7,5	*Urgent*
11511	V2.C2	*Drupal multiple remote security*	7,5	*Critical*
11828	V2.C3	*Web configuration file exposed*	5	*Critical*
13074	V2.C4	*Drupal core password hashing API denial of service*	5	*Medium*
86728	V2.C5	*Web server uses plain-text form based authentication*	5	*Medium*
11	V2.C6	*Hidden* RPC *services*	5	*Medium*
11827	V2.C7	HTTP *security header not detected*	4,3	*Medium*
86729	V2.C8	*AutoComplete attribute not disabled for password in form based authentication*	2,6	*Medium*
38738	V2.C9	SSH *server public key too small*	5	*Medium*
38739	V2.C10	*Deprecated* SSH *cryptographic settings*	6,4	*Medium*
12087	V2.C11	*Expose php set to on in php.ini*	5	*Minimal*

4.1.4 Analisis hasil *Walkthrough* VulnOS*

Dari analisis yang sudah dilakukan didapatkan hasil *score exploit*, selanjutnya hasil akan dianalisis kembali dengan melihat *port* maupun keterangan pada *vulnerability* masing-masing *vulnerable machine*. Tabel V-14 berikut adalah *attack threat* yang ada pada *vulnerable machine* VulnOS.

Tabel 7 *Walkthrough* VulnOS

Threat ID	*Attack Threat*	*Walkthrough*										*Score Exploit*
		1	2	3	4	5	6	7	8	9	10	
T1.1	*General enumeration*	V	V	V	V	V	V	V	V	V	V	10
T1.2	*Exploit research*	V	-	-	V	-	V	V	-	-	V	5
T1.3	*SMB/RPC enumeration*	V	V	V	V	V	V	V	V	-	V	9
T1.4	*Admin access*	V	-	-	-	-	-	-	-	-	-	1
T1.5	*SQLMap*	V	V	V	V	V		V	-	-	V	8

T1.6	*Password cracking*	V	V	-	V	V	V	V	-	-	V	7
T1.7	*SSH*	V	V	V	V	V	V	V	V	V	-	9
T1.8	*TTY Shell*	V	-	-	-	V	-	-	-	-	-	2
T1.9	*Execution Bypass*	-	V	-	-	-	-	-	-	-	-	1
T1.10	*Compiling Exploits*	-	V	-	-	V	-	-	-	-	V	3
T1.11	*Chmod*	-	-	V	-	-	-	-	-	-	-	1
T1.12	*Web enumeration*	-	-	-	V	-	V	-	V	V	-	4
T1.13	*Transfer file*	-	-	-	-	V	V	-	-	-	V	3
T1.14	*Pop3*	-	-	-	-	-	-	V	-	-	-	1
T1.15	*Fingerprinting*	-	-	-	-	-	-	-	V	-	-	1

4.1.5 Analisis hasil *Walkthrough* Vulnix*

Dari analisis yang sudah dilakukan didapatkan hasil *score exploit*, selanjutnya hasil akan dianalisis kembali dengan melihat *port* maupun keterangan pada *vulnerability* masing-masing *vulnerable machine*. Tabel berikut adalah *attack threat* yang ada pada *vulnerable machine* Vulnix.

Tabel 8 *Walkthrough* Vulnix

Threat ID	*Attack Threat*	*Walkthrough*										*Score Exploit*
		1	2	3	4	5	6	7	8	9	10	
T2.1	*Network discovery*	V	-	V	-	-	-	V	-	-	-	3
T2.2	*Port scanning*	V	V	V	V	V	V	-	V	V	V	9
T2.3	*ARP scanning*	-	-	-	-	-	-	-	V	-	-	1
T2.4	*Finger scanning*	V	-	V	-	V	-	V	-	V	V	6
T2.5	*NFS enumeration*	V	V	V	V	V	V	V	V	V	V	10
T2.6	*SSH Enumeration*	V	V	-	-	V	-	-	-	-	-	3
T2.7	*Users enumeration*	-	V	V	-	V	-	V	-	V	V	6
T2.8	*Netcat*	-	-	V	-	-	-	-	-	-	-	1
T2.9	*SMTP Enumeration*	-	-	V	-	V	-	-	-	V	V	4
T2.10	*Bruteforce*	V	V	V	-	V	-	-	-	-	-	6
T2.11	*Edit /etc/passwd*	-	V	-	-	-	-	-	-	-	-	1
T2.12	*Added a new user with specified ID to had access*	-	V	V	V	V	V	-	V	V	-	7
T2.13	*Created .ssh in the remote home directory*	-	V	V	V	V	V	V	V	V	V	9
T2.14	*Sudo -l shows that vulnix allowed to edit /etc/exports file*	V	V	V	V	V	V	V	V	V	V	10
T2.15	*Disable rootsquashing*	-	V	V	-	-	V	V	V	V	-	6
T2.16	*User remote acces*	V	-	V	V	V	-	V	V	V	V	9
T2.17	*Remote write access*	-	V	V	V	-	V	-	-	V	V	6
T2.18	*Copy /bin/bash to the remote root directory*	V	-	-	-	-	-	-	-	-	-	1
T2.19	*Root access*	V	V	V	V	-	V	V	V	V	V	9
T2.21	*System reboot required*	V	V	V	V	-	V	V	V	-	-	7
T2.22	*./bash -p*	-	-	-	-	-	-	V	-	-	-	1

4.1.6 Analisis hasil *Walkthrough* Vulnix*

Dari analisis yang sudah dilakukan didapatkan hasil *score exploit*, selanjutnya hasil akan dianalisis kembali dengan melihat *port* maupun keterangan pada *vulnerability* masing-masing *vulnerable machine*. Tabel berikut adalah *attack threat* yang ada pada *vulnerable machine* DC-1.

Tabel 9 *Walkthrough* DC-1

Threat ID	*Attack Threat*	*Walkthrough*										*Score Exploit*
		1	2	3	4	5	6	7	8	9	10	
T3.1	*Network discovery*	-	V	-	V	V	-	-	-	-	-	3
T3.2	*General Enumeration*	V	V	V	V	V	V	V	V	V	V	10
T3.3	*Web Enumeration*	V	V	V	V	V	V	V	V	V	V	10
T3.4	*Checking robot.txt*	V	V	-	V	V	-	V	V	-	V	7

T3.5	*Exploit Research*	V	-	-	-	V	V	-	-	-	-	3
T3.6	*Kernel exploit*	V	-	-	V	V	-	-	-	-	-	3
T3.7	*TTY shell*	V	-	V	V	-	V	-	-	V	V	6
T3.8	*Enumeration (nikto)*	-	-	-	-	V	-	-	-	-	-	1
T3.9	*-exec "/bin/sh*	-	V	V	-	-	V	-	-	V	-	4
T3.10	*Root access*	V	V	V	V	V	-	V	V	V	-	8
T3.11	*SQLMap*	-	-	V	-	-	-	-	-	-	-	1
T3.12	*Password Cracking*	-	-	V	-	-	-	-	-	-	-	1

4.2 Hasil Analisis

4.2.1 Hubungan STRIDE dengan Risiko VulnOS

Setelah dilakukan analisis hubungan antara *attack threat* dengan *vulnerability* pada masing-masing *vulnerable machine*. Kemudian didapatkan dua hasil analisis yaitu hubungan antara STRIDE dengan *threat* yang ditemukan pada *tools* yang digunakan, dan juga grafik risiko dari hasil perkalian CVSS dengan *score exploit*.

Tabel 10 Hubungan STRIDE dengan Risiko VulnOS

Risk ID	STRIDE					
	Spoofing	*Tampering*	*Repudiation*	*Information Disclosure*	*Denial of Service*	*Elevation of Privilage*
R1.A1				V		
R1.A2				V		
R1.A3			V			
R1.A4					V	
R1.A5						V
R1.A6						V
R1.A7						V
R1.A8					V	
R1.A9						V
R1.A10			V			
R2.A1					V	
R2.A2				V		
R2.A3						V
R2.A4						V
R2.A5						V
R2.A6			V			

Tabel 10 diatas adalah hasil analisis *risk* yang didapatkan dari kemungkinan *threat* dari *vulnerability* pada *vulnerable machine* VulnOS dengan AlienVault dan Qualys menggunakan STRIDE.

Tabel 11 Hubungan STRIDE dengan Risiko Vulnix

Risk ID	STRIDE					
	Spoofing	*Tampering*	*Repudiation*	*Information Disclosure*	*Denial of Service*	*Elevation of Privilage*
R1.B1				V		
R1.B2					V	
R1.B3				V		
R1.B4					V	
R1.B5				V		
R1.B6						V
R1.B7					V	
R1.B8						V
R1.B9						V
R1.B10		V				
R1.B11						V
R1.B12				V		
R2.B1					V	
R2.B2						V

R2.B3				V		
R2.B4					V	
R2.B5				V		
R2.B6					V	
R2.B7						V
R2.B8				V		
R2.B9						V
R2.B10		V				
R2.B11				V		
R2.B12				V		
R2.B13						V
R2.B14						V

Tabel 11 adalah hasil analisis *risk* yang didapatkan dari kemungkinan *threat* dari *vulnerability* pada *vulnerable machine* Vulnix dengan AlienVault dan Qualys menggunakan STRIDE.

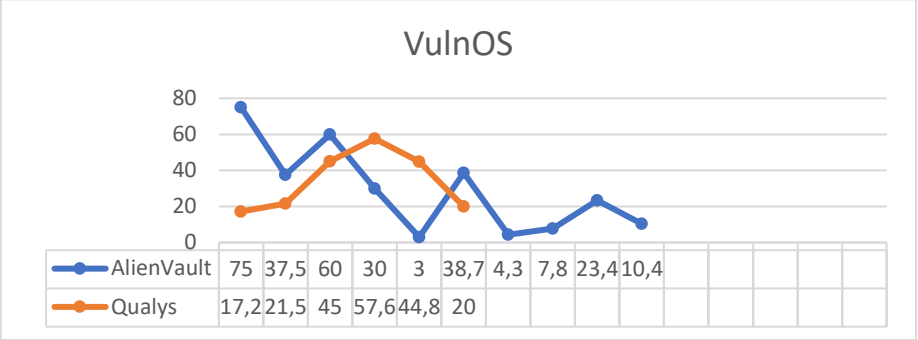
Tabel 12 Hubungan STRIDE dengan Risiko DC-1

Risk ID	STRIDE					
	Spoofing	*Tampering*	*Repudiation*	*Information Disclosure*	*Denial of Service*	*Elevation of Privilage*
R1.C1				V		
R1.C2				V		
R1.C3				V		
R1.C4			V			
R1.C5					V	
R1.C6				V		
R1.C7			V			
R1.C8			V			
R1.C9			V			
R1.C10				V		
R1.C11			V			
R1.C12				V		
R2.C1					V	
R2.C2					V	
R2.C3				V		
R2.C4			V			
R2.C5					V	
R2.C6			V			
R2.C7						V
R2.C8			V			
R2.C9				V		
R2.C10			V			
R2.C11				V		
R2.C12						V
R2.C13				V		
R2.C14				V		
R2.C15				V		
R2.C16			V			
R2.C17						V
R2.C18				V		

Tabel 11 adalah hasil analisis *risk* yang didapatkan dari kemungkinan *threat* dari *vulnerability* pada *vulnerable machine* Vulnix dengan AlienVault dan Qualys menggunakan STRIDE.

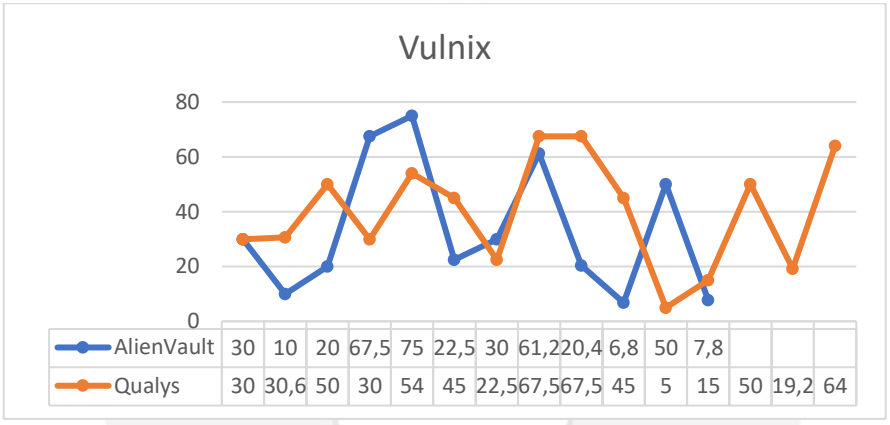
4.3 Hasil Analisis Risiko

Setelah dilakukan analisis estimasi risiko yang dilakukan dapat diketahui nilai risiko yang menjelaskan jenis *vulnerability* yang berisiko dan *threat attack* yang sering dilakukan.



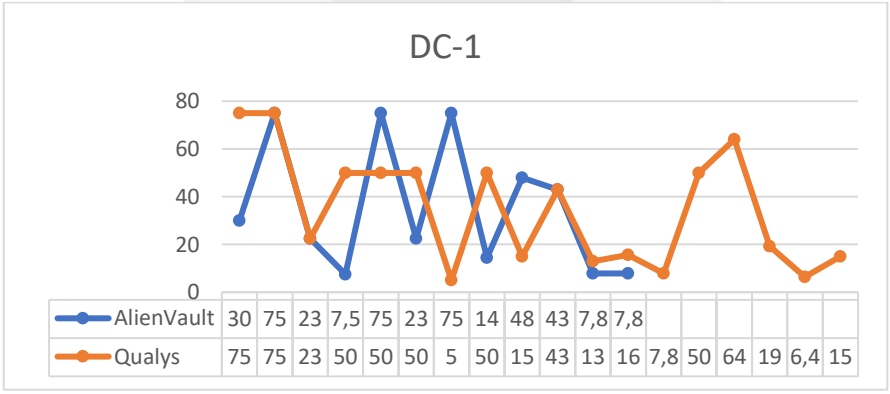
Gambar 2 Grafik Hasil Risiko VulnOS

Gambar 2 merupakan grafik risiko VulnOS pada *software* AlienVault dan Qualys dengan total 16 risiko beserta nilainya yang di dapatkan dari nilai kerentanan dan ancaman yang sering terjadi. Dari 16 risiko terdapat 1 risiko dengan nilai tertinggi.



Gambar 3 Grafik Hasil Risiko Vulnix

Gambar 3 merupakan grafik risiko Vulnix pada *software* AlienVault dan Qualys dengan total 27 risiko beserta nilainya yang di dapatkan dari nilai kerentanan dan ancaman yang sering terjadi. Dari 27 risiko terdapat 1 risiko dengan nilai tertinggi.



Gambar 4 Grafik Hasil Risiko DC-1

Gambar 4 merupakan grafik risiko VulnOS pada *software* AlienVault dan Qualys dengan total 30 risiko beserta nilainya yang di dapatkan dari nilai kerentanan dan ancaman yang sering terjadi. Dari 30 risiko terdapat 5 risiko dengan nilai tertinggi.

5 Kesimpulan dan Saran

5.1 Kesimpulan

Setelah dilakukannya pengujian dan analisis beberapa sampel kerentanan menggunakan framework STRIDE, dapat disimpulkan sebagai berikut:

1. Hasil reporting Vulnerability Assessment Qualys memiliki keterangan yang lebih lengkap dan jumlah kerentanan yang terdeteksi lebih banyak.
2. Serangan maupun kerentanan yang dilihat oleh AlienVault maupun Qualys, dapat diakomodasikan dengan framework STRIDE dengan fitur Spoofing, Tampering, Information Disclosure, Denial of service, dan juga Elevation of Privilege dibuktikan dengan contoh vulnerability yang ditemukan dan dianalisis. Beberapa fitur yang tidak dapat mengakomodasi risiko pada vulnerable machine Vulnix, VulnOS dan DC-1 pada software AlienVault dan Qualys adalah Spoofing.
3. Jenis vulnerable machine dengan kerentanan terbanyak adalah sistem operasi Vulnix.
4. Nilai risiko dengan jumlah tertinggi merupakan jenis eksploitasi yang sering dilakukan dan vulnerability dengan nilai tertinggi. Pada analisis kali ini ada beberapa risiko yang tinggi 5 dari diantaranya R1.A1 dengan vulnerability Drupal core critical remote code execution dan threat General enumeration; R1.B5 dengan vulnerability Check for rsh service dan threat NFS enumeration; R1.C5 dengan vulnerability Drupal core critical remote code execution dan threat Web enumeration; R2.C1 dengan vulnerability Drupal core database abstraction API SQL Injection dan threat Web enumeration; dan R2.C2 dengan vulnerability Drupal multiple remote security dan threat Web enumeration.
5. *Framework* yang akurat dalam analisis estimasi risiko adalah MITRE ATT&CK, dengan taktik dan teknik yang rinci pada matriksnya.

5.2 Saran

Pada penelitian ini, terdapat beberapa keterbatasan maupun kekurangan. Keterbatasan dan kekurangan ini bida dijadikan acuan dan juga pertimbangan untuk penelitian selanjutnya maupun bagi organisasi yang ingin mengimplementasikan salah satu fungsi *software* AlienVault dan Qualys yaitu *Vulnerability Assessment*. Adapun saran yang dihasilkan dalam penelitian ini sebagai berikut:

1. Penggunaan resource yang besar dalam penerapan software AlienVault, sehingga membutuhkan resource yang besar juga untuk server yang digunakan.
2. Perlu adanya pertimbangan dalam memilih open source software SIEM, seperti penelitian diatas Qualys menggunakan layanan cloud sehingga kebutuhan resource yang besar untuk server tidak diperlukan.
3. Perlu dipertimbangkan dalam memlilih open source software SIEM agar data yang diperoleh lebih lengkap dan mudah di analisis.

Daftar Pustaka:

[1] David Nathans (2015): Designing and Building A Security Operations Center. British Library Cataloguing-in-Publication Data, 1 – 9.
[2] Khan, R., McLaughlin, K., Laverty, D., dan Sezer, S. (2018): STRIDE-based Threat Modeling for Cyber-Physical Systems. Innovative Smart Grid Technologies Conference Euripa (ISGT-Europa), 3.
[3] Miftahul Huda (2020): Keamanan Informasi.Nulisbuku.com, 125.
[4] Katherine A. Seale, J. Todd Mcdonald, Harold Pardue, William Glisson, Michael Jacobs (2018): MedDevRisk: Risk Analysis Methodology for Networked Medical Devices. Conference Paper, 9 - 11.
[5] Jonathan Reuvid (2015): Managing Cybersecurity Risk: Cases Studies and Solutions. Legends Team Group, 44.
[6] Abomhara, M., Kien, G.M (2015): Cyber security and the internet of things: vulnerabilities. threats, intruders and attacks. J. Cyber Secur, 65-88.
[7] Khan, R., McLaughlin, K., Laverty, D., dan Sezer, S. (2018): STRIDE-based Threat Modeling for Cyber-Physical Systems. Innovative Smart Grid Technologies Conference Euripa (ISGT-Europa), 3.
[8] Larry Osterman (2007): Threat Modeling Again, STRIDE, https://blogs.msdn.microsoft.com/larryosterman/2007/09/04/threat-modeling-again-stride/ ., *download*(diturunkan/diunduh) pada 25 November 2019.
[9] AlienVault (2012): AlienVault OSSIM Review – Open Source SIEM. Retrieved from https://resources.infosecintitute.com/alienvault-ossim-review-open-source-siem/ ., *download(*diturunkan/diunduh) pada 30 Agustus 2019.