Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 3, September 2021, pp. 1643~1653
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i3.pp1643-1653

Vulnerability and risk assessment for operating system (OS) with framework STRIDE: comparison between VulnOS and Vulnix

Adityas Widjajarto, Muharman Lubis, Vreseliana Ayuningtyas
Department of Information System, School of Industrial Engineering, Telkom University, Indonesia

Article Info

Article history:

Received Oct 27, 2020
Revised Jul 28, 2021
Accepted Aug 4, 2021

Keywords:

Assesment
Operating system
Risk
Scanning
Vulnerability

ABSTRACT

The rapid development of information technology has made security become extremely. Apart from easy access, there are also threats to vulnerabilities, with the number of cyber-attacks in 2019 showed a total of 1,494,281 around the world issued by the national cyber and crypto agency (BSSN) honeynet project. Thus, vulnerability analysis should be conducted to prepare worst case scenario by anticipating with proper strategy for responding the attacks. Actually, vulnerability is a system or design weakness that is used when an intruder executes commands, accesses unauthorized data, and carries out denial of service attacks. The study was performed using the AlienVault software as the vulnerability assessment. The results were analysed by the formula of risk estimation equal to the number of vulnerability found related to the threat. Meanwhile, threat is obtained from analysis of sample walkthroughs, as a reference for frequent exploitation. The risk estimation result indicate the 73 (seventy three) for the highest score of 5 (five) type risks identified while later on, it is used for re-analyzing based on the spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of prvilege (STRIDE) framework that indicated the network function does not accommodate the existing types of risk namely spoofing.

Corresponding Author:

Adityas Widjajarto
Department of Information System
Telkom University
Jln. Telekomunikasi No. 1, Bandung, 40257, Indonesia
Email: adtwjrt@telkomuniversity.ac.id

1. INTRODUCTION

The development of the Internet in information technology (IT) is developing very fast along with the growth of its users. Likewise, the level of crime in information technology is detrimental to its users, both individuals, and organizations. Information security is the protection of computer equipment, facilities, data, and information from misuse of unauthorized or unauthorized parties. The role of information security for an organization is to provide information protection from various threats in order to ensure business continuity, reduce business risks, increase return on investment (ROI), and increase business opportunities [1], [2]. Information security is an effort to anticipate fraud through the detection step by step process within an information-based system regardless its boundary and limitation. The aspects that must be met in a system to ensure information security are the information provided is accurate and complete as the right or verified and validated information, which is accountable or held by the right people that can be accessed and used according to the need at the right time, and provides information in the right format or form based on the agreeable manner.

Information security management is an activity to keep information resources safe. Management is not only expected to keep information resources safe, but also expected to keep the implemented system functioning after a disaster or security system breaks. The stages in information management are identifying threats that can attack company information resources and then defining the risks that can be caused by these threats. Next is determining an information security policy and implementing controls to address these risks. Vulnerability scanning detects and identifies known issues of software and tools installed on the host such as older versions of the software in use, active protocol vulnerabilities, and standard passwords. This activity is difficult to do manually; hence this phase is performed using an automated tool which identifies open ports and tries various exploits on the port to identify if a particular process/software is using a port that is vulnerable to exploits based on its process. Some of the tools used to perform vulnerability scanning are Nessus, OpenVas, and Qualys [3].

In 2019 the number of vulnerabilities increased by 17.6% by 20 [4], which is supported by the vulnerability statistics released by Research Labs: application security and data security. Information technology security is needed to increase efficiency in cyberspace security, monitoring, and analysing threats and incidents that exist in information technology security, which the functions that can be used is vulnerability scanning to detects and identifies known problems with software and tools installed on the host [3]. One way to respond quickly to protect the IT assets, maintain awareness of environmental vulnerabilities, and mitigate potential threats is to use it systematically. This is the process for identifying and measuring security vulnerabilities in the organization's environment as a comprehensive program to provide organizations with the knowledge, awareness, and risk background to understand and respond against the environmental threats. Based on the background described above, several problems to be resolved in this study can be formulated by simulating vulnerability scanning with the AlienVault and Qualys (mirroring the scenario) software on the VulnOS, Vulnix, and direct current-1 (DC-1) (for the purpose of shadowing the result) operating systems to help identify vulnerabilities. Comparison of the results of vulnerability scanning in AlienVault and Qualys software and a risk score graph can help identify the types of attacks and threats that often occur. Meanwhile, the STRIDE framework analysis developed by Microsoft is to analyze the threat attack on the walkthrough.

2. RESEARCH METHOD

Actually, threat can be defined as the attempt to exploit the benefit from the security weaknesses within certain information based system for certain period of time, which implicated to the negative impact for the environment in the short and long run. Therefore, it can come from two main sources, which are humans both external and internal as well through natural threats namely earthquakes, hurricanes, floods, and fires [5]. Meanwhile, risk is defined as the potential loss, damage, or damage to assets as a result of threats exploiting vulnerabilities such as financial loss, loss of privacy, damage to reputation, legal implications, and even loss of life. It can also be defined as the result of multiplication between vulnerability and threats. On the other hand, penetration testing ensures that the test created is materialized or completed. Given that is part of a larger security program, one must include other safety characteristics to align the test with demand as a driver [6]. A vulnerability machine is an operating system created with weak security vulnerabilities and is usually used for attempted attacks. VulnOS is a suite of vulnerable operating systems packaged in a virtual image to improve penetration testing. VulnOS was created by the author id with the name c4b3rw0lf, with the Linux base operating system and can be downloaded on the Vulnhub website [4]. Vulnerable linux hosts with configuration flaws. Vulnix is made with the name HackLAB: Vulnix and created by the user id reboot user, with the basic operating system Ubuntu server 12.04 and can be downloaded on the vulnhub website while DC-1 is a vulnerable machine that is deliberately created for the purpose of gaining experience in the world of penetration testing. DC-1 is made by DCAU author id with the name DC: 1, with the Debian 32 bit operating system and can be downloaded on the vulnhub website.

STRIDE is a model-based threat modeling technique developed by microsoft that also guides security analysis through the activities that must be carried out for the process to be effective. Six types of security threats include spoofing attacks occur when an attacker pretends to be someone they are not [7]-[9]. It is typically used to gain access to a target's personal information, which spreads malware via infected links or attachments, bypasses network access controls, or redistributes traffic to carry out attacks [10]-[14]. Then, tampering occurs when attackers modify or edit official information and repudiation occurs at the time of someone execute certain action while later on try to claim the otherwise. It usually comes down to the specific activity process such as credit card transactions where users buy something and then claim they did not to obtain certain benefit [15]-[18]. On information disclosure, data breaches or unauthorized access to confidential information and denial of service (DoS) related to creating service interruptions for legitimate users and most recently related to elevation of privilege to gain higher privileged access to system elements

by users with limited authority. On the other hand, internet protocol (IP) as a data routing protocol is the key to the convergence with homogeneous and flat interconnection processes with a simple system design can lead to the lower network management costs [19]. Network development hubs are associated with mobility to ensure network availability for connected entities in motion and resources in storage and compute volumes, especially in parallel computing, network computing, and cloud computing, which in the end should be protected and maintaned in at all cost [20]-[24].

At the review stage, identification will be carried out by designing to describe the planning to solve the problem. The needs used in this research are the vulnerable machine operating systems VulnOS, Vulnix and DC-1, and the software used are AlienVault and Qualys. Meanwhile, at the data collection stage, execution will be carried out with a variable machine and related software, then vulnerability scanning will be carried out and the collected data will be obtained then used for research analysis. At the analysis stage, the output vulnerability scanning will be carried out on AlienVault and Qualys to identify the types of threat attacks that have been collected during the collection stage. The data obtained is then carried out by calculating the risk, which will be analyzed based on the STRIDE framework. In the final stage, the interpretation will consist of a conclusion on the research that has been done and suggestions that can be given from the results of risk analysis on vulnerable machines using the vulnerability scanning feature on AlienVault and Qualys.

The following Tables 1 and 2 is an explanation of the hardware specification and software functions used, including Windows 10 Enterprise, an operating system that provides all the features of Windows 10 Pro, with additional features to help information technology (IT-based) organizations. Windows 10 in this case, is used as the operating system on the main hardware. Meanwhile, Debian as a computer operating system composed of software packages released as free and open software under the majority license of the GNU general public license and other free software licenses. In this analysis, Debian is used as the operating system on VirtualBox on which AlienVault is based. Meanwhile, Ubuntu is an open source operating system distributed Linux based on Debian and has a desktop interface. In this analysis, Ubuntu is used as the operating system on VirtualBox on which VulnOS is based, a series of vulnerable operating systems packaged in virtual images and used to improve penetration testing skills. VulnOS is used as an object that is analyzed by each of the open source SIEM tools. Vulnix is a Linux host that is vulnerable to configuration flaws. The DC-1 is a vulnerable machine designed for the purpose of gaining experience in the world of penetration testing. VirtualBox is virtualization software that can be used to execute additional operating systems within the main operating system. In this analysis, VirtualBox is installed on Windows 10 and used to run several operating systems. AlienVault is a comprehensive security system that includes open source from detection to generating metrics and reports to the executive level. In this analysis, AlienVault is used to analyze the vulnerability of each vulnerable machine. Qualys is a commercial scanner web application, which can be used to find, identify, and assess vulnerabilities so they can be prioritized and fixed before they are targeted and exploited by attackers.

Table 1. Hardware specification

Component	Hardware	Specification
Core Hardware Specification	Processor	Intel® Core™ i7-7500U dual-core 2.7GHz (8 CPUs), ~ 2.9GHz
	Memory	8192MB RAM
	Hard Disk	1 TB
	System Type	64-bit Operating System, x64-based processor
	Operating System	Windows 10 Enterprise 64-bit (10, Build 17134)
1st VM VirtualBox specification	Processor	Intel® Core™ i7-7500U dual-core 2.7GHz (1 CPUs), ~ 2.9GHz
	Memory	4096MB RAM
	Hard Disk	32 GB
	System Type	64-bit Operating System
	Operating System	Debian GNU/Linux 8 (jessie) 64-bit
2nd VM VirtualBox specification	Processor	Intel® Core™ i7-7500U dual-core 2.7GHz (8 CPUs), ~ 2.9GHz
	Memory	786 MB
	Hard Disk	32 GB
	System Type	64-bit Operating System
	Operating System	Ubuntu 14.04.6 LTS 64-bit / VulnOS v2
3rd VM VirtualBox specification	Processor	Intel® Core™ i7-7500U dual-core 2.7GHz (8 CPUs), ~ 2.9GHz
	Memory	512 MB
	Hard Disk	32 GB
	System Type	64-bit Operating System
	Operating System	Ubuntu Server 12.04 86xbit / Vulnix
4th VM VirtualBox specification	Processor	Intel® Core™ i7-7500U dual-core 2.7GHz (8 CPUs), ~ 2.9GHz
	Memory	512 MB
	Hard Disk	32 GB
	System Type	64-bit Operating System
	Operating System	Debian 86xbit / DC-1

Table 2. Software specification

Type	Software	Version
Operating System	Windows 10 Enterprise 64-bit	10, Build 17134
	Debian	8 Jessie 64-bit
	Ubuntu	14.04.6 LTS 64-bit
Vulnerability Operating System	VulnOS	2
	Vilnix	1
	DC-1	1
Virtual Machine	VirtualBox	6.1.2
Software	AlienVault	5.7.4
	Qualys	-

The STRIDE threat model categorizes threats based on spoofing, tampering, repudiation, information disclosure and elevation of privilege. Each of the six threat classifications is a method of attack that can exploit the information assurance component and each has the security properties of an officer to deal with the threat. The identified vulnerabilities and threats are then analyzed how the threats will directly affect each asset owned [25]. There are six security objectives maintained, namely confidentiality, integrity, availability, authenticity, secure lifecycle, and non-repudiation. The risk of each element will depend on the type of attack carried out. Using this information and knowledge of the potential severity of the attack, we can determine the risk score. In the picture below, it is explained that the topology in this study consists of 1 router connected to the internet, 1 laptop host, 1 software on the server, and 3 vulnerable machines namely VulnOS, Vulnix, DC-1 while the latter is not shown in this study but used for shadow experiment. Internet router is connected to the host laptop that has VirtualBox installed. The internet router provides an IP address which is used as a link between the AlienVault and Qualys software and vulnerable machines on the same network.

Figure 1 shows the network topology, which influence significantly the output of the vulnerability assessment on AlienVault as a risk factor for each vulnerability found within the system, which is in accordance with the common vulnerability scoring system (CVSS) v3.0 provided by the national vulnerability database (NVD) as can be seen in Table 3. CVSS is a standard IT vulnerability score, and this method provides a score ranging from 0 to 10. The common vulnerability scoring system (CVSS) provides a way to capture the main characteristics of vulnerabilities and generate a numerical score that reflects their severity. The numerical scores can then be translated into qualitative representations (such as low, moderate high, and serious) to help organizations properly assess and prioritize their vulnerability management processes.

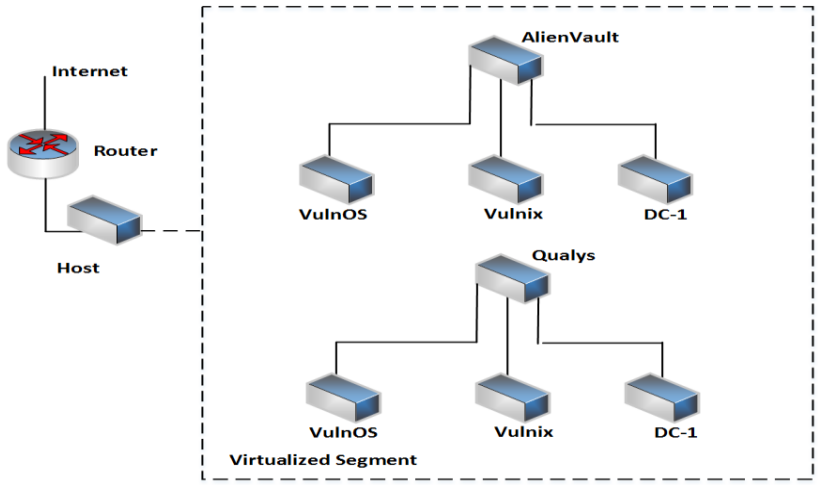


Figure 1. Network topology

Table 3. Severity range

Severity	v3 Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Serious	9.0-10.0

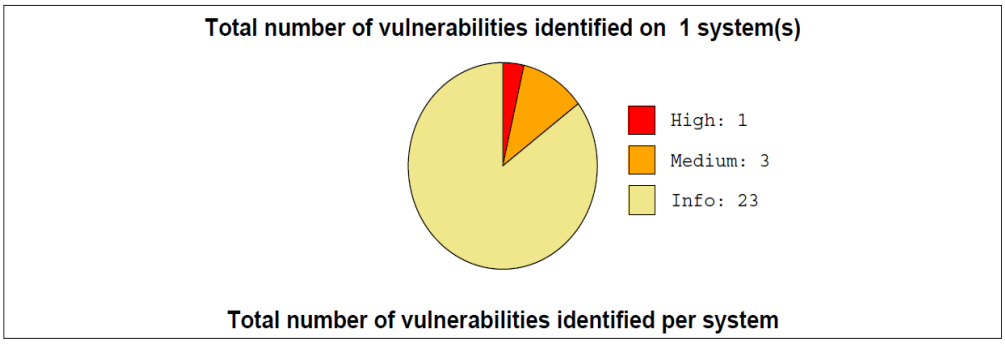
3. RESULTS AND DISCUSSION

3.1. Experiment VulnOs with AlienVault

Table 4 represents the number of vulnerabilities detected on VulnOs scanned using AlienVault with the number detected were 3 vulnerabilities with medium severity, 1 vulnerability with high severity and found 23 info, while Figure 2 shows its visualization. Therefore, A1 in here shows the types of vulnerabilities that were found when scanning, namely drupal core critical remote code execution with script ID 108438, CVSS 7.5, port 80, and severity in the high category. This host runs drupal and is vulnerable to code vulnerabilities for remote access. Meanwhile, A2 shows the types of vulnerabilities found while scanning, namely SSH weak encryption algorithms supported with script ID 105611, CVSS 4.3, port 22, and medium severity. The remote secure shell connection (SSH) server is configured to allow weak encryption algorithms. The vulnerability exists in SSH messages which use cipher-block chaining (CBC) mode which allows an attacker to recover plaintext from ciphertext blocks. On the other hand, A3 shows the types of vulnerabilities found when scanning, namely SSH weak message authentication code (MAC) algorithms supported with script ID 105610, CVSS 2.6, port 22, and medium severity. The remote SSH server is configured to allow weak MD5 and 96-bit MAC algorithms. Therefore, A4 shows the types of vulnerabilities found when scanning, namely TCP timestamps with script ID 80091, CVSS 2.6, and medium severity. The remote host implements TCP timestamps which allow it to be used to calculate uptime.

Table 4. First experiment severity range with 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



HostIP	HostName	Serious	High	Med	Low	Info
192.168.0.102	VulnOS	--	1	3	--	23

192.168.0.102	VulnOS

Figure 2. VulnOS vulnerability with AlienVault

3.2. Experiment Vulnix with AlienVault

Table 5 represents the number of vulnerabilities detected on Vulnix scanned using AlienVault while Figure 3 show its visualization. In this case, the number detected were 14 vulnerabilities with medium severity, 14 vulnerabilities with high severity, 2 vulnerabilities with serious severity and found 37 info. B1 shows the types of vulnerabilities found when scanning, namely OS end of life detection with script ID 103674, CVSS 10, and serious category severity. The operating system on remote host has reached the end of its useful life and should not be used again. Therefore, B2 shows the types of vulnerabilities found when scanning, namely check if mailserver answer to verify and expand requests with script ID 100072, CVSS 5, port 25, and severity high category. The mailserver on this host answers VRFY and EXPN requests automatically. Meanwhile, B3 shows the types of vulnerabilities found when scanning, namely check for login service with script ID 901202, CVSS 7.5, port 513, and severity high category. This remote host is running the rlogin service. Rlogin files are easy to abuse and could potentially allow anyone to log in without

a password. B4 shows the types of vulnerabilities that were found when scanning, namely check for rsh service with script ID 1000080, CVSS 7.5, port 514, and severity category high. This remote host runs the remote shell (RSH) service, which is a computer program that can execute shell commands as a user even with another computer. B5 shows the types of vulnerabilities found when scanning, namely finger service remote information disclosure vulnerability with the script ID 802236, CVSS 5, port 79, and severity in the high category. These hosts run finger services and are vulnerable to information disclosure vulnerabilities. B6 shows the types of vulnerabilities found when scanning, namely secure socket layer/transport layer security (SSL/TLS): OpenSSL CCS man in the middle security bypass vulnerability with script ID 105042, CVSS 6.8, port 995, and severity high category. OpenSSL is vulnerable to bypass security vulnerabilities. B7 shows the types of vulnerabilities found when scanning, namely SSL/TLS: OpenSSL TLS 'heartbeat' extension information disclosure vulnerability with script ID 105042, CVSS 6.8, port 993, and severity high category. OpenSSL is vulnerable to bypass security vulnerabilities. B8 shows the types of vulnerabilities found when scanning, namely transmission control protocol (TCP) timestamps with script ID 80091, CVSS 2.6, and medium category severity, which the host implements TCP timestamps.

Table 5. Second experiment severity range with 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

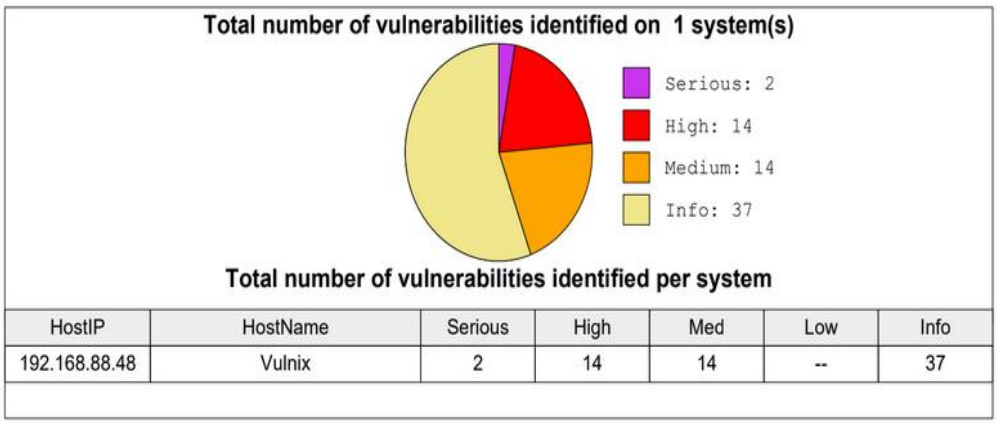


Figure 3. Vulnix vulnerability with AlienVault

3.3. Walkthrough analysis with VulnOS

Table 6 shows the walkthrough analysis in each phases to identify the threat attack or the exploit score to be used in the multiplication with the vulnerability score namely CVSS in Table 7 that present the risk value obtained. An example of the V1.A1 vulnerability is drupal core critical remote code execution with a value of 7.5. Then it will be multiplied by the possibility of the threat is T1.1, namely general enumeration is 10, T1.2 is research exploit is 5, T1.5 is SQLMap is 8, and T1.12 is web enumeration is 4. The risk value will then be used as a graph so that It is easy to see which types of exploits and vulnerabilities are common. Penetration or testing is the art or measure of uncovering risks and vulnerabilities and digging deep to detect how much a target can compromise in any kind of legitimate attack. It also tries to find additional security risks that often don't show up in vulnerability scans. Penetration testing will involve exploiting servers, networks, firewalls, computers, to find vulnerabilities, and draw attention to practical threats involved with the identified vulnerabilities. Apart from the defined purpose, the penetration test approach can also be used to evaluate and measure the suspicious power mechanism of the system on how capable or strong the system

is in protecting against various types of unexpected malicious attacks. In this case, the Table 8 shows the risk analysis of VulnOS by using STRIDE framework to understand the categorization of the threats.

Table 6. VulnOS walkthrough

Threat ID	Attack Threat	Walkthrough										Exploit Score
		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

Table 7. VulnOS estimation risk analysis

Vuln ID	CVSS	Threat ID	Score Exploit	Risk ID	Risk
V1.A1	7,5	T1.1	10	R1.A1	75
		T1.2	5	R1.A2	37,5
		T1.5	8	R1.A3	60
		T1.12	4	R1.A4	30
V1.A2	4,3	T1.7	9	R1.A5	3
		T1.6	9	R1.A6	38,7
		T1.11	1	R1.A7	4,3
V1.A.3	2,6	T1.10	3	R1.A8	7,8
		T1.7	9	R1.A9	23,4
V1.A4	2,6	T1.12	4	R1.A10	10,4

Table 8. Risk analysis of VulnOS with STRIDE

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	-	-	-

3.4. Walkthrough analysis with Vulnix

Similar like previous analysis, Table 9 shows the exploit score while Table 10 shows the risk value obtained by multiplying the vulnerability score CVSS and the exploit score. For example, the V1.B1 vulnerability is OS end of life detection with a value of 10. Then it will be multiplied by the possible threat is T2.1, namely Netdiscover is 3 and T2.3 is ARP scanning is 1. The risk value will then be used as a graph for easy viewing, which types of exploitation and vulnerability occur frequently. The assurance of an IT product means that the product meets its security objectives, that the security measures implemented by the product will be able to counter the threat as it occurs [26]-[28]. The frequency of penetration testing responds to many factors, from industry type to network technology and regulatory compliance. If there is some kind of industry compliance regulation, then penetration testing should also be run as essential to meet those needs. It is often recommended that penetration tests be scheduled if any of the following occurs, such as significant

disruption to the network or infrastructure, increased media awareness and attention that could increase the likelihood of an attack, adding offices or changing office locations to the network, the latest industry regulations require additional compliance, patches security functions, and new applications or infrastructure are added to the application system. Interestingly, the most common factors can be attributed to the lack of consistent procedures for analysing and collecting data errors generated during software development, which is extremely difficult and time-consuming [29], [30]. One solution provided for complexity is through the use of network knowledge software SDN existing solutions, only the logic of network devices [31]-[33].

Table 9. Vulnix walkthrough

Threat ID	Attack Threat	Walkthrough										Exploit Score
		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
T2.1	Network discovery	V	-	V	-	-	-	V	-	-	-	3

Table 10. Vulnix estimation risk analysis

Vuln ID	CVSS	Threat ID	Score Exploit	Risk ID	Risk
V1.B1	10	T2.1	3	R1.B1	30
		T2.3	1	R1.B2	10
V1.B2	5	T2.9	4	R1.B3	20
V1.B3	7,5	T2.2	9	R1.B4	67,5
V1.B4	7,5	T2.5	10	R1.B5	75
		T2.6	3	R1.B6	22,5
V1.B5	5	T2.4	6	R1.B7	30
V1.B6	6,8	T2.19	9	R1.B8	61,2
		T2.6	3	R1.B9	20,4
		T2.8	1	R1.B10	6,8
V1.B7	5	T2.20	10	R1.B11	50
V1.B8	2,6	T2.1	3	R1.B12	7,8

After every process was done, the risk analysis was conducted like before by cetegorizing the threats as can be seen in Table 11. User education is central to implementing a cybersecurity policy, with key elements in a realistic context of simulation related to the dynamics of a cyber attack, the ongoing development of the infrastructure, existing vulnerabilities and the need to be aware of their potential impact [34], [35]. The main function of an ideal network management system is to improve the operational capacity of the network by maintaining the best performance of the network operation, which could be through predicting the result based on positive and negative indicators and advanced planning [36], [37]. Therefore, organizations must meet the necessary and specific rigorous requirements to achieve the safety-stability boundary in the prevention of worst-case scenarios [38]. Considering that the complexity and heterogeneity of networks built in a company's specific environment have simultaneously reduced the efficiency of network administrators [39], vulnerabilities assessment and analysis regularly can support the employees in giving the confidence in order to prepare themselves through training and understanding for proper control and handling

activity. It is doubtful that some modeling and analysis could accurately and clearly predict how such an attack would occur on the network infrastructure, resulting in a shutdown or disruption, followed by a collision as the consequences [40], [41]. But at the very least, it can presents a depiction and alternative solution for prediction and preparation for the organization. In general, awareness and preparation for asset sustainability and performance often become the target attack through creating failures in the process of securing the assets. Thus, it should be noted that infrastructure is extremeily critical in order to provide the increased level of convenience of connectivity by decreasing the susceptibility to cyber attack through routine and regular vulnerability assessment [42], [43].

Table 11. Risk analysis of Vulnix with STRIDE

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	-	-

4. CONCLUSION

In this study, there are several limitations and drawbacks which can be used as a reference and also a consideration for further research. It can also assist organizations with their considerations before implementing the AlienVault software in the Vulnerability assessment. The suggestions generated in this study are is being as: the use of large resources in the application of the AlienVault software, so that it also requires large resources for the server used. By having VA, of course one way to quickly respond in guarding the IT assets to sustain the business process and awareness over security vulnerabilities in the environment, which in the further, support the decision making to mitigate the potential threats through quantification of the risk as the regular virtual support. Consideration is needed in choosing open source security information and event management (SIEM) software using cloud services so that large resource requirements for servers are not needed so that the data obtained is more complete and easy to analyze.

REFERENCES

[1] D. Nathans, "Designing and Building a Security Operations Center," *British Library Cataloguing-in-Publication Data, Syngress*, 2015, pp. 1-9, doi: 10.1016/C2013-0-19158-1.
[2] G. Sadowsky, J. X. Dempsey, A. Greenberg, B. J. Mack, and A. Schwartz, "*Information Technology Security Handbook*," *International Bank for Reconstrcution and Dev./The World Bank*, 2003.
[3] S. Jetty, "Network Scanning Cookbook Practical Network Security using Nmap and Nessus 7," *Packt Publishing Ltd*, pp. 10-11, 2018.
[4] D. Beker and S. Yerus, "The State of Vulnerabilities 2019," July 2020. [Online]. Available: from: https://www.imperva.com/blog/the-state-of-vulnerabilities-in-2019/.
[5] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks," *Journal of Cyber Security and Mobility*, vol. 4, pp. 65-88, 2015, doi: 10.13052/jcsm2245-1439.414.
[6] J. S. Tiller, "CISO's Guide to Penetration Testing: A Framework to Plan, Manage and Maximize Benefits," *CRC Press Taylor & Francis Group*, 2012, doi: 10.1201/b11306.
[7] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1-6, doi: 10.1109/ISGTEurope.2017.8260283.
[8] D. R. Miller, S. Harris, A. A. Harper, S. VanDyke, and C. Blask, "Security Information and Event Management (SIEM) Implementation," *The McGraw-Hill Companies*, 2011.
[9] J. Reuvid, "Managing Cybersecurity Risk: Cases Studies and Solutions," *Legends Team Group*, 2018.
[10] A. Katherine, J. Seale, T. Mcdonald, H. Pardue, W. Glisson, and M. Jacobs, "MedDevRisk: Risk Analysis Methodology for Networked Medical Devices," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018, doi: 10.24251/HICSS.2018.414.

[11] S. Schinagl, K. Schoon, and R. Paans, "A Framework for Designing a Security Operations Centre (SOC)," *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 2253-2262, doi: 10.1109/HICSS.2015.270.
[12] A. Michail, "Security Operation Centers a Business Perspective," *Utrecht University MSc in Business Informatics*, 2015.
[13] E. Conrad, S. Misenar and J. Feldman, "CISSP Study Guide," *Newnes*, 2012, doi: 10.1016/C2011-0-07337-4.
[14] J. Fruhlinger, "Threat Modelling Explained: A Process for Anticipating Cyber Attacks," *IDG Community, Inc*, 2020. [Online]. Available: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html. [Retrieved at December 2021].
[15] I. Kamil, M. L. Julham, and A. R. Lubis, "Management Maintenance System for Remote Control based on Microcontroller and Virtual Private Server," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 16, no. 3, pp. 1349-1355, 2019, doi: 10.11591/ijeecs.v16.i3.pp1349-1355.
[16] R. Fauzi, M. Hariadi, S. M. S. Nugroho, and M. Lubis. "Defense Behavior of Real Time Strategy Games: Comparison between HFSM and FSM," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 13, no. 2, pp. 634-642, Februaary 2019, doi: 10.11591/ijeecs.v13.i2.pp634-642.
[17] H. A. A. Julham, A. R. Lubis, and M. Lubis, "Development of Soil Moisture Measurement with Wireless Sensor Web-Based Concept," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 13, no. 2, pp. 514-520, February 2019, doi: 10.11591/ijeecs.v13.i2.pp514-520.
[18] A. Almaarif and M. Lubis. "Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website," *International J. on Advance Sc. Eng. And Inf. Tech*, vol. 10, no. 5, pp. 1874-1880, 2020, doi: 10.18517/ijaseit.10.5.8862.
[19] M. Abdurohman and B. S. Nugroho, "Technical Specification for Effective Next Generation Network Interconnection in Indonesia," *International J. on Advance Sc. Eng. And Inf. Tech.* vol. 10, no. 3, pp. 1153-1162, 2020, doi: 10.18517/ijaseit.10.3.5753.
[20] B. Muruganantham, P. Shamili, S. G. Kumar, and A. Murugan, "Quantum Cryptography for Secured Communication Network," *International Journal of Electrical & Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 407-414, 2020, doi: 10.11591/ijece.v10i1.pp407-414.
[21] D. Moussaoui, M. Feham, B. A. Bensaber, and B. Kadri, "Securing Vehicular Cloud Networks," *International Journal of Electrical & Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4154-4162, 2019, doi: 10.11591/ijece.v9i5.pp4154-4162.
[22] M. Lubis, R. Fauzi, A. R. Lubis, and R. Fauzi, "A Case Study of Universities Dormitory Residence Management System (DRMS) in Indonesia," in *IEEE Int. Conf. Cyber and IT Service*, 2018, doi: 10.1109/CITSM.2018.8674313.
[23] R. Johari, I. Kaur, R. Tripathi, and K. Gupta, "Penetration Testing in IoT Network," *2020 5th International Conference on Computing, Communication and Security (ICCCS)*, 2020, pp. 1-7, doi: 10.1109/ICCCS49678.2020.9276853.
[24] S. Karmokar, M. M. Mohin, M. K. Islam, M. R. Alam, and M. M. Rahman, "Quantitative Vulnerability Assessment: An Approach to Reduce Biases in Disaster Vulnerability Assessment," *Current World* Environment, vol. 14, no. 3, pp. 383-399, 2019, doi: 10.5194/isprs-archives-XLII-4-703-2018.
[25] L. Chang, G. Chen, S. Cao, and C. Zheng, "Vulnerability Assessment of Regional Water Resources," *IOP Conference Series Earth and Environmental Science* vol. 508, p. 012026, April 2020, doi: 10.1088/1755-1315/508/1/012026.
[26] A. Bialas, "Vulnerability Assessment of Sensor Systems," *Sensors*, vol. 19, no. 11, pp. 2518, 2019, doi: 10.3390/s19112518.
[27] K. Mahajan and A. M. Kim, "Vulnerability Assessment of Alberta's Provincial Highway Network," *Transportation Research Interdisciplinary Perspectives*, vol. 6, p. 100171, July 2020, doi: 10.1016/j.trip.2020.100171.
[28] C. Szymula and N. Besinovic, "Passenger-centered Vulnerability Assessment of Railway Networks," *Transportation Research Part B* Methodological, vol. 136, pp. 30-61, June 2020, doi: 10.1016/j.trb.2020.03.008.
[29] R. Adebiaye, "Mitigating Vulnerability Risk in Cybersecurity using Predictive Measures," *International Journal of Advanced Scientific Research & Development*, vol. 4, no. 10, pp. 12-27, October 2017, doi: 10.26836/ijasrd/2017/v4/i10/4106.
[30] D. Rogowski, "Software implementation of common criteria related design patterns," *2013 Federated Conference on Computer Science and Information Systems*, 2013, pp. 1147-1152.
[31] D. Magin, R. Khondoker, and K. Bayarou, "Security Analysis of OpenRadio and SoftRAN with STRIDE Framework," *The 24th international conference on computer communications and applications (ICCCN 2015).* IEEE, vol. 38, 2015.
[32] J. Straub, "Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks," *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, 2020, pp. 148-153, doi: 10.1109/SmartCloud49737.2020.00035.
[33] M. Brett and J. Parker, "A Framework to Understand Local Government Network Environment From Cyber Security Perspective. Developing an Open Source Tool Kit for Local Government," *Exploring Cyber Security in Local Government*, March 2019, doi: 10.6084/m9.figshare.9963722.v1.
[34] G. Subaşu, L. Roşu, and I. Bădoi, "Modeling and simulation architecture for training in cyber defence education," *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2017, pp. 1-4, doi: 10.1109/ECAI.2017.8166396.

[35] A. A. Algarn, "Most Successful Vulnerability Discoverers: Motivation and Methods," *International Conference on Security and Management (SAM)*, 2013, p. 1.
[36] A. Widjajarto, M. Lubis, and M. K. R. Syahputra, "Optimization Pesrformance Management with FCAPS and ITILv3: Opportunities and Obstacles," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 17, no. 1, pp. 281-290, January 2020, doi: 10.11591/ijeecs.v17.i1.pp281-290.
[37] A. Shukla, B. Katt, and L. O. Nweke, "Vulnerability Discovery Modelling with Vulnerability Severity," *2019 IEEE Conference on Information and Communication Technology*, 2019, pp. 1-6, doi: 10.1109/CICT48419.2019.9066187.
[38] T. M. Shahrani, A. N. Ramdhania, M. Lubis, and A. Almaarif, "Implementation of Building Construction and Environmental Control for Data Centre based on ANSI/TIA-942 in Networking Content Company," *Journal of Physics: Conference Series*, vol. 1361, p. 012074, 2019.
[39] F. Lubis and M. Lubis, "Network Fault Effectiveness and Implementation at Service Industry in Indonesia," *Journal of Physics: Conference* Series, vol. 1566, p. 012080, November 2019.
[40] K. Tai, A. Kizhakkedath, J. Lin, R. L. K. Tiong, and M. S. Sim, "Identifying Extreme Risks in Critical Infrastructure Interdependencies," *Int. Symposium for Next Generation Infrastructure*, 2013, doi: 10.14453/isngi2013.proc.44.
[41] A. Atef and O. Moselhi, "Understanding the Effect of Interdependency and Vulnerability on the Performance of Civil Infrastructure," *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction*, vol. 30. p. 1, 2013.
[42] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 25-30, doi: 10.1109/ISI.2016.7745438.
[43] YAO Xin-qiang, SUN Bai-tao, Zai-lin Yang, and CAO Jing-quan, "A New Method For Vulnerability Analysis And Application In Rural Dwellings," *2019 13th Symposium on Piezoelectrcity, Acoustic Waves and Device Applications (SPAWDA)*, 2019, pp. 1-4, doi: 10.1109/SPAWDA.2019.8681872.