RESEARCH ARTICLE OPEN ACCESS

ANALYSIS OF SECURITY VULNERABILITY ASSESSMENT IN WEB APPLICATION ENVIRONMENT USING COMMON VULNERABILITY SCORING SYSTEM METHOD

Faisal Ashari Firmansyah*, Syaeful Machfud**
Zaqi Kurniawan***, Ikhsan Rahdiana*****, Ahmad Jurnaidi Wahidin******
*(Faculty of Computer Science, Budi Luhur University, Jakarta, Indonesia)
**(Faculty of Computer Science, STMIK ERESHA, Tangerang, Indonesia)
***(Faculty of Computer Science, Budi Luhur University, Jakarta, Indonesia)
****(Faculty of Computer Science, Budi Luhur University, Jakarta, Indonesia)
*****(Faculty of Computer Science, Budi Luhur University, Jakarta, Indonesia)

----------**********----------

Abstract:

The development of this increasingly advanced era, many companies spend all means to be able to improve security on the side of the system used, the increasing crime in the digital world, one of which is cyber crime such as hacking activities. In order to maintain security in the data, the company needs to test the security of the information system, one of which is by testing the penetration testing. Security vulnerability in a web application system cannot be denied because the web is generally dynamic and accessible to the public, therefore penetration testing is needed to test the extent to which the security level in the system is running. The analysis of security vulnerability assessment in the Web Application Environment in this study uses the Common Vulnerability Scoring System (CVSS) with penetration testing as a testing technique, with the aim of measuring the level of vulnerability in a Common Vulnerability Scoring System (CVSS) system. found that it can be improved its vulnerability level, in this study found at the level of high vulnerability obtained the value of 8.50 using two tools namely nessus and acunetix with the method of penetration testing results obtained have similar vulnerability levels and the findings of vulnerability can be calculated manually using the Common Vulnerability Scoring System (CVSS).

Keywords — CVSS, Vulnerability Assessment, Penetration Testing, System Security, System Vulnerabilities.

----------**********----------

I. INTRODUCTION

Information system security is one of the main problems of information systems. The growth of connectivity from computers via the internet, increasing system extension, and uncontrolled growth in size of system size and complexity has made software security a bigger problem now than in the past. In addition, a business interest is to adequately protect the organization's information assets by following a comprehensive and structured approach to provide protection from the risks faced by an organization in an effort to solve information system security problems and comply with applicable information system security regulations, information security system experts has developed a variety of security assurance methods that include proof of layered design truth, software engineering environment and penetration testing. Penetration testing is a comprehensive method for testing the basis of complete, integrated, operational, and reliable computing consisting of hardware, software and people. This process involves active system analysis for any potential vulnerabilities, including poor or incorrect system configurations, hardware and software weaknesses. Some of the tools used in this penetration test are Nessus and Acunetix from each of these tools which have advantages and

disadvantages in conducting a penetration test that allows the tool to detect all vulnerabilities in the web application that have been tested in terms of security. Vulnerability assessors refer to international standardization scoring, namely the Common Vulnerability Scoring System (CVSS), so that the results expected to be used can correct the vulnerabilities in the system used or to be used.

2. RELATED WORKS

2.1. Penetration Testing

This stage is the most eagerly awaited stage by hackers, the purpose of this stage is exploitation of the system weaknesses (vulnerabilities system) that have been obtained in the previous stages. stages in penetration testing include gaining access, Escalate Privilage, Maintain Access, Clean Up. [4]

2.2 Vulnerability Assessments

Vulnerability Assessments are designed to generate a priority list of vulnerabilities (vulnerabilities / loopholes) and usually the customer (client) has understood it. Customers also know they have a problem, only they need help to identify and prioritize their problems. The more problems identified will be better, of course the "white box" approach (i.e all information related to the target is known) if possible. Submission for an assessment is important, a list of priority vulnerabilities (vulnerabilities / vulnerabilities) found and often also how to fix them. Indications of vulnerability and procedures for handling actions that need to be carried out to deal with, avoid, divide and reduce these vulnerabilities to the extent of tolerance of acceptable risk appetite.

2.3 Vulnerability Metrics

Metrics are constituent components or characteristics of vulnerabilities that can be measured quantitatively or qualitatively. These atomic values are grouped together in three separate regions: base groups, temporal groups, and environmental groups. The base group contains all the intrinsic and fundamental qualities for each given vulnerability that does not change from time to time or in a different environment. The temporal group contains characteristics of vulnerability that depend on time and change as the age of vulnerability. Finally, environmental groups contain vulnerability characteristics related to implementation and the environment. The adjusted final score represents the threat of vulnerability thatappears at a specific time point for certain environmental conditions. The metric group is shown in Figure II-2.

The authors acknowledge that many other metrics can be included in the CVSS. They also realize that there is no perfect scoring system for everyone. Specific constituent metrics used in CVSS are identified as the best compromise between completeness, ease of use and accuracy. They represent the author's cumulative experience as well as extensive testing of real-world vulnerabilities in the end-user environment. [5]

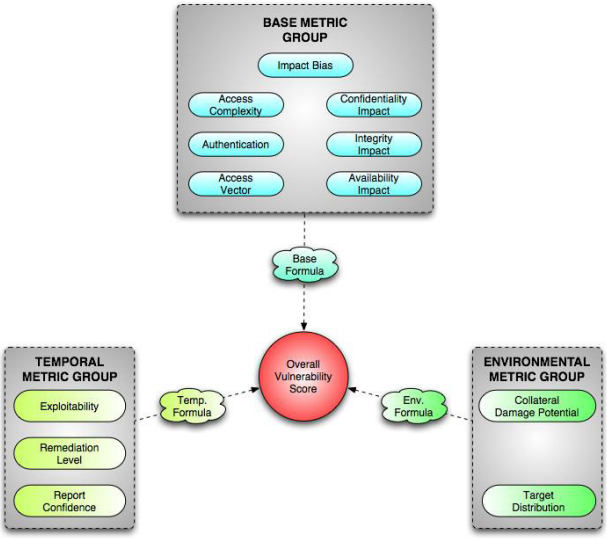

Figure 1 : *Flow diagram CVSS*

2.4 Base Metric Scoring

The base score provides the basis for the overall vulnerability score. The most significant metrics in the assessment process are three impact metrics. This metric dictates the overall effect the vulnerability will have on the target system and therefore has the strongest bearing on the final score. [7]

```
AccessVector     = case AccessVector of
                   local:          0.7
                   remote:         1.0
AccessComplexity = case AccessComplexity of
                   high:           0.8
```

```
                low:            1.0
Authentication  = case Authentication of
                required:       0.6
                not-required:   1.0
ConfImpact      = case ConfidentialityImpact of
                none:           0
                partial:        0.7
                complete:       1.0

ConfImpactBias  = case ImpactBias of
                normal:         0.333
                confidentiality: 0.5
                integrity:      0.25
                availability:   0.25
IntegImpact     = case IntegrityImpact of
                none:           0
                partial:        0.7
                complete:       1.0
IntegImpactBias = case ImpactBias of
                normal:         0.333
                confidentiality: 0.25
                integrity:      0.5
                availability:   0.25
AvailImpact     = case AvailabilityImpact of
                none:           0
                partial:        0.7
                complete:       1.0
AvailImpactBias = case ImpactBias of
                normal:         0.333
                confidentiality: 0.25
                integrity:      0.25
                availability:   0.5
BaseScore = round_to_1_decimal(10 * AccessVector
                    * AccessComplexity
                    * Authentication
                    * ((ConfImpact * ConfImpactBias)
                    + (IntegImpact * IntegImpactBias)
                    + (AvailImpact * AvailImpactBias)))
```

2.5 Temporal Metric Scoring

The temporal score adjusts the base score by including factors that can change over time. The temporal score will be less than or equal to the base score; that is, temporal metrics only function to reduce the base score to a maximum of 33%. This is shown at the end of the assessment section. [8]

Temporal Metric Formula

```
Exploitability  = case Exploitability of
                unproven:       0.85
                proof-of-concept: 0.9
                functional:     0.95
                high:           1.00

RemediationLevel = case RemediationLevel of
                official-fix:   0.87
                temporary-fix:  0.90
                workaround:     0.95
                unavailable:    1.00
ReportConfidence = case ReportConfidence of
                unconfirmed:    0.90
                uncorroborated: 0.95
                confirmed:      1.00
TemporalScore = round_to_1_decimal(BaseScore *
Exploitability
                    * RemediationLevel
                    * ReportConfidence)
```

2.6 CVSS Vulnerability Sample

Apache Chunked-Encoding Memory Corruption Vulnerability (CVE-2002-0392) In June 2002, a vulnerability was found in the means used by the Apache web server to handle requests that were encoded using chunk coding. The Apache Foundation reports that successful exploits can cause denial of service in some cases, and on the other hand, arbitrary code execution with privileges from web servers. Because vulnerabilities can be exploited remotely, the Access Vector is "Remote". "Low" Access Complexity because there are no additional circumstances that need to be in place for this exploitation to succeed; the attacker only needs to make the exploit message right for the apache web listener. Authentication is not required to trigger vulnerabilities (each Internet user can connect to a web server) and so the Authentication metric is "Not Required". [6]

3. DESIGN OF RESEARCH DESIGN

In this study the author uses the Penetration Testing method to simulate external or internal cyber attacks with the aim of penetrating the security of an organization's information system network so that a system security vulnerability assessment can be done with CVSS. Using a variety of different technical tools and approaches, an examiner or hacker tries to exploit a system gap with the aim of obtaining important sensitive data.

3.1 Methods in Web Application Penetration Testing

Application penetration testing web activities have 3 motives in the process, namely:

1. Passive Penetration Testing

In this case what is done is mapping and testing the controls that are in the web application, login and configuration, so that we can map the target system.

2. Active Penetration Testing
   In this case what is being done is testing the security of the system by manipulating inputs, taking access, and testing existing vulnerabilities.
3. Aggressive Penetration Testing
   Exploit vulnerabilities, reverse engineer software and systems. embed the backdoor, download the code, try to take over the information on the server.

3.2 Sample Selection Method

Sampling techniques are part of the research population used to estimate the results of a study. While sampling technique is part of statistical methodology relating to the methods of sampling. Definition of sampling or sampling method according to the interpretation of some experts. Some of them are as follows;
Sampling technique is a sampling technique Sampling technique is a way to determine a sample whose number is in accordance with the sample size that will be used as the actual data source, taking into account the characteristics and distribution of the population in order to obtain a representative sample.

3.3 Testing Techniques

This testing technique for the CVSS method will be carried out by one example of the level of vulnerability which is high but uses two different applications so that the results obtained are the same. Therefore CVSS needs to be proven whether the level of vulnerability has the same scoring value as well, of course. The results obtained in the test will be calculated using the CVSS method with the standardization that has been determined. Thus the average value will be obtained from the test.

4. RESEARCH RESULT DISCUSSION

4.1 Network Topology Selection

The selection of target vulnerability includes a web server that uses apache version 2.2 and a web application using PHP (Hypertext Prepocessor) vesi 5 and the network topology is convergence, then vulnerability analysis is performed in each environment. From the topology seen on the web server and application server connected to each other through a switch this is needed so that between servers can communicate with each other.

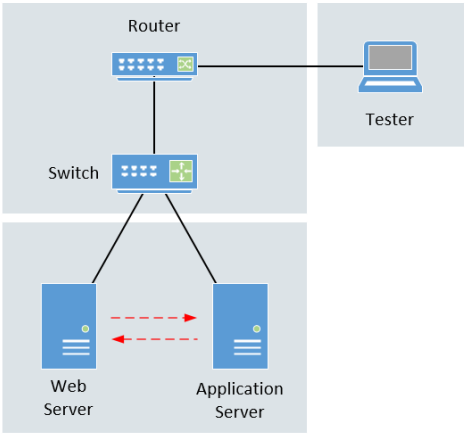

figure 2 : *Topology Testing*

Then for testing by scanning the target using the Nessus application and accunetix, there will be a number of security loopholes that will be assessed for the level of vulnerability up to repair evaluation. As seen in Figure 4 is a vulnerability finding from the scan using nessus.

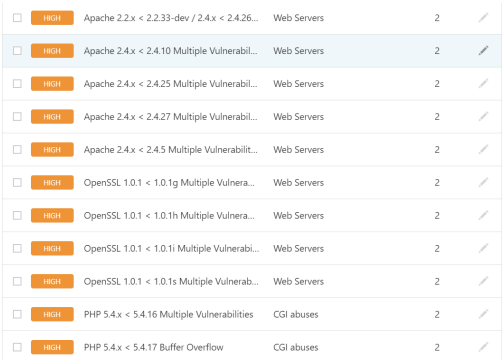

Figure 3 : *Result Testing*

In Figure 4 is a scan of the Nessus application in which there are vulnerabilities in the system with high vulnerability levels which means that there is a need for improvements in the system so that alerts on the system are safe from vulnerabilities. Then in some of the findings the vulnerability above is not the same and the way to fix it is different.

4.2 Vulnerability Level Testing

In testing the effectiveness of the target is an application that is paired on a virtual machine with the aim of minimizing the level of error when an error occurs in the application, thus a snapshot system can be used if a system crash occurs.

Figure 4 : *High Vulnerability info*

4.3 Vulnerability Level Testing

At this time the vulnerability level uses CVSS as a standardization for calculating the level of security in a system, because the target has the same level of vulnerability, namely high.

Serverity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Thus the vulnerability scoring at high level is 7.0-8.9, this calculation needs to be proven by the available CVSS formula.

Table 2 CVSS Formula

BASE METRIC	EVALUATION	SCORE
Access Vector	[Remote]	(1.00)
Access Complexity	[Low]	(1.00)
Authentication	[Not-Required]	(1.00)
Confidentiality	[Partial]	(0.70)
Impact		
Integrity Impact	[Partial]	(0.70)
Availability Impact	[Complete]	(1.00)
Impact Bias	[Availability]	(0.25)
BASE FORMULA		
Round (10 * 1.0 * 1.0 * 1.0 * (0.7 * 0.25) +(0.7 * 0.25) + (1.0 * 0.5)) = (8.50)		

It has been seen that the results obtained if the high vulnerability level has a score of 8.50 where the minimum level of 7.0-8.9 is still included in that category.

4. CONCLUSION

Based on the problems, literature study, research review, review of research objects and research methodology, the Common Vulnerability Scoring System (CVSS) is a method to provide an assessment of vulnerability in a system, it can be concluded as follows:Secara keseluruhan perhitungan skoring kerentanan pada suatu sistem dapat menggunakan *Common Vulnerability Scoring System* (CVSS) sebagai standarisasi pada level kerentanan *high*.

1. From the results of the analysis, this can be used for the adequacy of the security control aspects of a system, thus the system used is safe from attack because the vulnerability has been detected the level of vulnerability and how to improve it.
2. By obtaining the results of the vulnerability assessment scoring can easily fix these vulnerabilities, because the information obtained is very detailed starting from the application, impact and solution findings.

REFERENCES

[1] Christian Mainka, J. S. (2012). Penetration Testing Tool for Web Services Security. *IEEE Eighth World Congress on Services*.

[2] Farkhod Alisherov A., a. F. (2011). Methodology for Penetration Testing. *International Journal of of Grid and Distributed Computing*.

[3] Goel, J. N. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *International Conference on Recent Trends in Computing*.

[4] Gupta, A. (2013). Vulnerability Assessment and Penetration Testing. *International Journal of Engineering Trends and Technology- Volume4Issue3- 2013*.

[5] Kaur, M. G. (2017). Penetration Testing – Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science*.

[6] Keramati, M. a. (2013). CVSS-based Security Metrics for Quantitative Analysis Of Attack Graphs. *International Conference on Computer and Knowledge Engineering (ICCKE 2013)*.

[7] Klíma, T. (2017). Methodology of Information . *Acta Informatica Pragensia, 2016, 5(2): 98–117*.

[8] McDonald, J. D. (2016). Improving Penetration Testing Methodologies for Security-Based Risk Assessment . *Cybersecurity Symposium*.

[9] Muhammad Zunnurain Hussain, M. Z. (2017). Penetration Testing In System Administration. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 06*.

[10] Salas, M. (2014). Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security. *Electronic Notes in Theoretical Computer Science*.