

Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas

Afif Saktiansyah, Muhammad Muharrom

Universitas Bina Sarana Informatika, Jakarta, Indonesia

Article Info

Article history:

Received January 17, 2022

Revised January 26, 2022

Accepted February 01, 2022

Keywords:

Assessment Techniques
Implementation of Vulnerability
OpenVas Software
Vulnerability Analysis

ABSTRACT

Vulnerability Assessment is an important method for identifying and analyzing security vulnerabilities within a network system. This research aims to identify security vulnerabilities within the PT. Dutakom Wibawa Putra network using OpenVAS as a research tool. In the vulnerability analysis phase, OpenVAS is utilized to scan the PT. Dutakom Wibawa Putra network and identify existing vulnerabilities. Subsequently, an evaluation is conducted on the identified vulnerabilities, including risk assessment and necessary mitigation recommendations. The outcomes of this study provide a clear overview of the security vulnerabilities present in the PT. Dutakom Wibawa Putra network. This research using method analysis of vulnerability assessment technique implementation on network using OpenVas, several significant vulnerabilities that could impact the security of the network and systems have been identified. The findings of this analysis report can serve as a foundation for developing improved security strategies and implementing effective mitigation measures. In conclusion, this study successfully applies Vulnerability Assessment techniques to the PT. Dutakom Wibawa Putra network using OpenVAS. The identified vulnerability analysis results offer valuable insights into security weaknesses that need to be addressed. It is hoped that this research can serve as a reference for PT. Dutakom Wibawa Putra and similar organizations in enhancing their network security through the implementation of effective Vulnerability Assessment techniques.

Copyright ©2023 The Authors.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Afif Saktiansyah,
Universitas Bina Sarana Informatika, Jakarta, Indonesia.
Email: afifsaktiansyah4@gmail.com

How to Cite: M. Muharrom and A. Saktiansyah, Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas, *International Journal of Engineering and Computer Science Applications (IJECSA)*, vol. 2, no. 2, pp. 53-62, Sep. 2023. doi: [10.30812/ijecsa.v2i2.3297](https://doi.org/10.30812/ijecsa.v2i2.3297).

1. INTRODUCTION

In the ever-evolving digital era, companies like PT Dutakom Wibawa Putra need to keep their networks secure to protect sensitive data, maintain operational continuity, and prevent potentially damaging cyber-attacks. Vulnerability Assessment is a proactive approach to identifying security vulnerabilities in networks and computer systems. Through this technique, companies can identify security gaps that may be exploited by unauthorized parties or attackers to gain illegal access to systems or steal confidential information. PT Dutakom Wibawa Putra has chosen OpenVas (Open Vulnerability Assessment System) as one of the tools to perform vulnerability analysis on their network. OpenVas is a popular open-source software used to identify and analyze vulnerabilities in IT infrastructure. However, the implementation of Vulnerability Assessment techniques using OpenVas may face several challenges and issues that need to be addressed. Some of the background issues that may arise in the implementation of Vulnerability Assessment techniques using OpenVas include Configuration Complexity, Proper configuration of OpenVas requires a deep understanding of the networks, operating systems, and protocols involved.

Misconfiguration can result in inaccurate analysis results or even cause disruptions in network operations. The effectiveness of OpenVas in detecting certain vulnerabilities may vary depending on the version and updates available. The reliability and accuracy of vulnerability detection is also an important factor in assessing the quality of the analysis performed. Handling False Positive (a result that incorrectly states a vulnerability exists when it does not) and False Negative (failing to detect a vulnerability that actually exists) are common problems in vulnerability analysis. It is important for PT Dutakom Wibawa Putra to evaluate OpenVas ability to reduce these errors and optimize the accuracy of the analysis results. Resource Provision: The implementation of Vulnerability Assessment techniques using OpenVas requires sufficient computing resources to run the analysis efficiently [1]. PT Dutakom Wibawa Putra has limited resources, it is necessary to evaluate to ensure that the existing system can properly handle the analysis workload without disrupting network operations. By understanding the background of the problems that may arise, PT. Dutakom Wibawa Putra can identify and overcome the obstacles associated with the implementation of the Vulnerability Assessment technique using OpenVas. Thus, the company can improve their network security and protect valuable digital assets.

Open Vulnerability Assessment System (OpenVas) is a Vulnerability Scanner maintained and distributed by Greenbone Network. It is intended to be a complete vulnerability scanner with a variety of built-in tests and a web interface designed to make setting up and running vulnerability scans quick and easy while providing a high level of user configuration [2]. According to [3] OpenVas is one of the software that has the ability to perform comprehensive scanning in handling system Vulnerability against the system security standards that have been implemented in the field. In conducting security assessments, OpenVas identifies and analyzes security vulnerabilities that exist in IT infrastructure. This research aims to identify security vulnerabilities within the PT. Dutakom Wibawa Putra network using OpenVAS as a research tool.

2. RESEARCH METHOD

This research uses the OpenVas Data research method. This research in which data collection [4] activities are a series of activities carried out through observation and recording, using certain instruments in accordance with the characteristics of the facts to be studied or investigated 5. Therefore, data collection activities can also be referred to as activities to measure or reveal facts [6] under investigation, becoming relevant data needed to test the truth of research hypotheses. In this regard, data collection activities use more inductive thinking processes, namely measuring and observing specific facts which then become general data, and can be used to test research hypotheses. Researchers here use objects at the company PT Dutakom Wibawa Putrat about analyzing the implementation of the Vulnerability Assessment Technique on the PT Dutakom Wibawa Putra network using OpenVas. When conducting research, researchers use the following collection techniques a. Observation is an observation that shows a study or learning that is carried out deliberately, purposefully, sequentially, and according to the objectives to be achieved in an observation that records all events and phenomena called observation results, which are described in detail, thoroughly, precisely, accurately, useful and objectively in accordance with the observations made. This data collection method involves direct interaction between the interviewer and the respondent, which allows the collection of in-depth and contextual information. c. Documentation comes from the word document which means library material, which can be in the form of recordings, such as sound / cassettes, videos, films, drawings and photographs. Documents mean all original records/authentic records that can be proven/made into legal evidence.

Vulnerability Assessment depends on discovering different types of system or network vulnerabilities, which means the assessment process includes the use of various tools, scanners and methodologies to identify vulnerabilities, threats and risks [2]. The goal is to find security holes that can be exploited by attackers to access or tamper with sensitive information [7]. This technique involves the use of tools and methods such as automated scanning, penetration testing, code analysis, and configuration checks to identify weaknesses that may exist. The results of a Vulnerability Assessment help organizations to take appropriate steps in improving security and protecting their systems from threats [8]. Here are some important points of the Vulnerability Assessment technique

[9] is preparation, determination of method, vulnerability scanning, risk evaluation, prioritization of vulnerabilities, remediation and follow-up, tracking and reporting, and monitoring and updating.

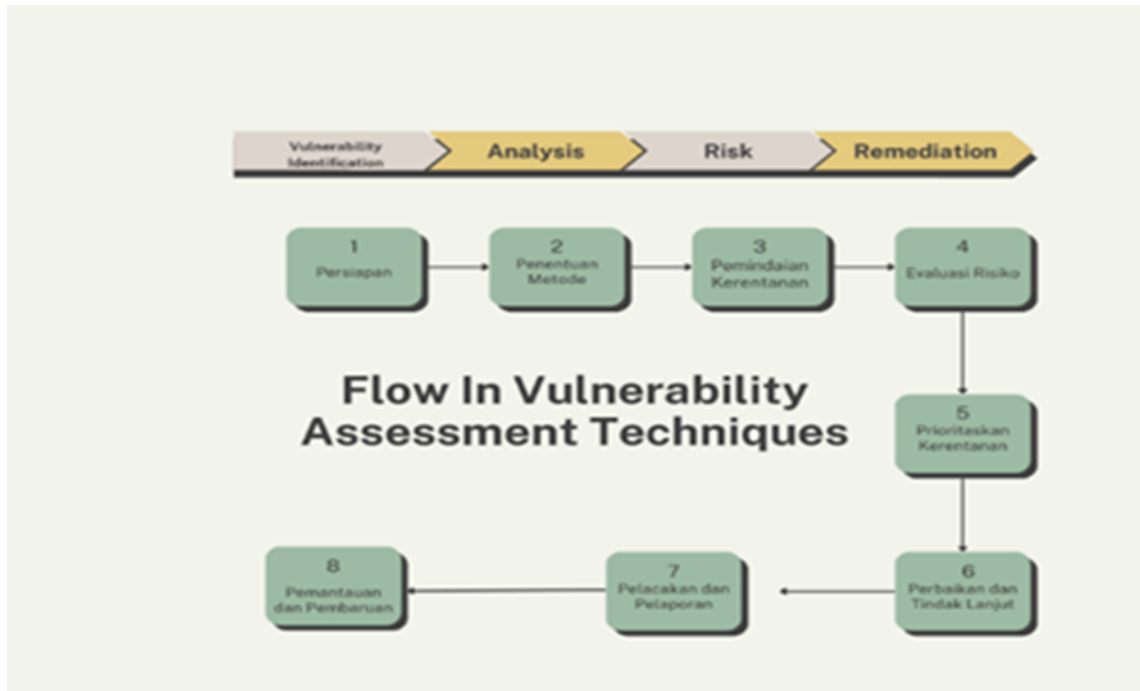


Figure 1. Flow of Vulnerability Assessment Technique

Open Vulnerability Assessment System (OpenVas) is a Vulnerability Scanner managed and distributed by Greenbone Network [10]. It is intended to be a complete vulnerability scanner with a variety of built-in tests and a Web interface designed to make setting up and running vulnerability scans quick and easy while providing a high level of user configurability. Overall, OpenVas is a powerful and flexible tool for performing Vulnerability Assessment, providing critical information to improve system security and protect organizations from security threats.

Metasploit is currently the world's leading penetration testing tool, and one of the largest open source projects in information security testing. metasploit has totally revolutionized the way we perform security testing on our systems. the reason why metasploit is so popular is because of the wide variety of tasks it can perform to ease the work of penetration testing to make systems more secure. In the context of computer security, exploitation refers to using weaknesses in a computer system or software to gain unauthorized access, take over, or perform other malicious actions. Metasploit provides an organized framework with pre-developed exploits, allowing users to try out those exploits in a controlled and safe scenario. Metasploit has a text-based and graphical interface that makes it easy for users to run its tools. Using Metasploit, users can perform weakness scans, exploit discovered vulnerabilities, attempt illegal access, and perform various actions to test and improve the security of their own systems [11].

Basically, data analysis in data analysis research is mostly done while in the field with various data collection activities. Thus, after completing the field what the researcher must do is make a complete research report, and it is also an implementation process that starts from data reduction, data presentation to conclusion like Figure 1. Data Reduction In data reduction, the author summarizes the data needed, selects important data and focuses on the research title so that the data can be summarized and provides a clear view and makes it easier to conduct research. 2. Data Presentation Data presentation is a series of complete data in a systematic format into a simple, selective and easy to understand format. This aims to identify meaningful patterns, draw conclusions and take action. 3. Conclusion Drawing Furthermore, researchers draw conclusions and verification, by drawing conclusions by describing the results that have been obtained [12].

3. RESULT AND ANALYSIS

The object of implementing the Vulnerability Assessment technique with OpenVas. PT Dutakom Wibawa Putra has implemented the Vulnerability Assessment technique as a step to maintain company network security. The following are the steps taken in implementing the Vulnerability Assessment technique: 1. Preparation: a) Identify the assets to be evaluated. b) Define the scope of the evaluation and the objectives to be achieved. c) Gather information about the assets to be evaluated, including network architecture, operating systems, applications used, and relevant configurations. 2. Determine the method: a) Select the appropriate evaluation method, such as automated scanning, manual analysis, or a combination of both. b) Use the OpenVas tool and technique to be used in the evaluation. 3. Vulnerability Scanning: a) Perform a vulnerability scan using the selected tool or manual method. b) Identify vulnerabilities and security holes present in the evaluated system, network, or application. c) Record the scan results, including the vulnerabilities found, severity, and detailed information related to the vulnerabilities. 4. Risk Evaluation: a) Review the vulnerabilities found and analyze the level of risk associated with each vulnerability. b) Consider the potential impact and probability of exploitation of the vulnerabilities. c) Determine the level of risk associated with each vulnerability. 5. Prioritize Vulnerabilities: a) Based on the established level of risk, prioritize vulnerabilities that need to be addressed immediately. b) Determine the sequence of corrective actions based on the level of urgency and risk associated with each vulnerability. 6. Remediation and Follow-up: a) Develop corrective recommendations for each identified vulnerability. b) Implement corrective actions, such as system patching, reconfiguration, policy changes, etc. c) Be sure to monitor and verify that the remedial action has successfully mitigated the risk associated with the vulnerability. 7. Tracking and Reporting: a) Track all steps taken in the vulnerability remediation process. b) Create a vulnerability evaluation report that includes the scan results, risk level, remediation recommendations, and actions taken. c) Report the results of the vulnerability evaluation to relevant stakeholders, such as the security team, management, or the owner of the asset being evaluated. 8. Monitoring and Updates: a) Continue to monitor system and network security on a regular basis. b) Update the vulnerability evaluation according to changes in infrastructure, applications, or emerging security threats. c) Be sure to update evaluation tools and techniques as needed and technology evolves. By following flow of Figure 2, it can perform Vulnerability Assessment techniques in a structured and effective manner, helping to improve system and network security using OpenVas.

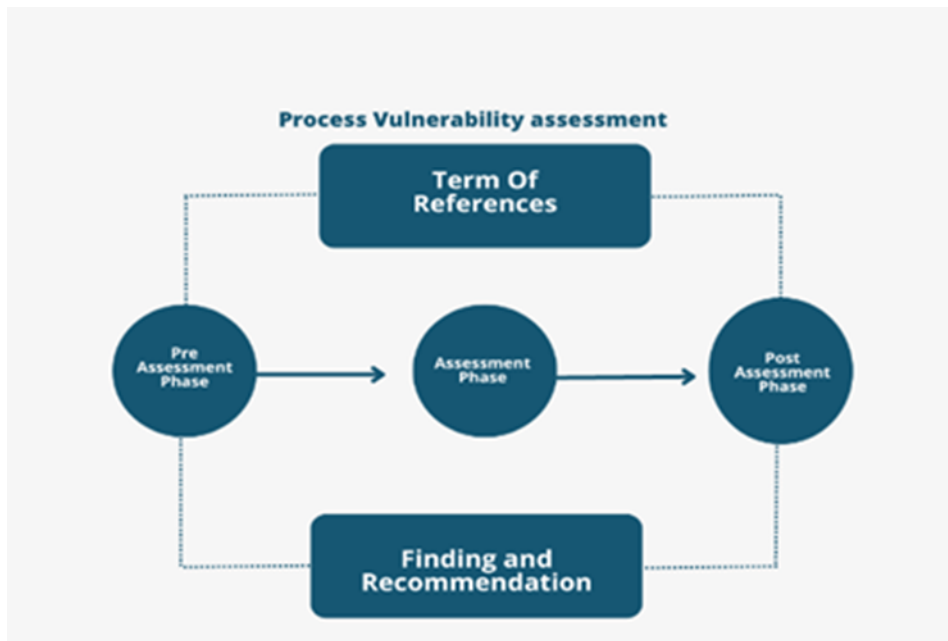


Figure 2. Process Vulnerability Assessment

Software Implementation Stages In the application of this software, there are several stages consisting of of: A. Installation of linux times B. Installation of OpenVas C. OpenVas configuration. A. In the installation of kali linux after downloading from the Webstie www.kali.org, select the language, then select the location; United States; Asia; Indonesia; configure the location; configure the keyboard after completion, wait for the process. select network; if there is no wifi select no; configure hostname; domain; set up users and passwords; select the hard drive partition and adjust it to your needs; after that the process display will appear finish the

installation Then wait a few minutes until the display appears to boot to the desktop; enter username and password Desktop Display Kali Linux 13. Desktop display Kali Linux is as in Figure 3.



Figure 3. KaliLinux desktop

Make sure your Kali Linux is installed and updated with the latest version. Open the terminal on Kali Linux [14]. Update the existing package list by running the following command: `sudo apt update`. After the update process is complete, run the following command to install the required package: `sudo apt install OpenVas`, during the installation process, it will appear like this, After completion you will be asked to select the appropriate configuration. Select the options that suit your needs. You can use the default values for most options. The results of the completed installation are shown in Figure 4.

```
(root@Sysadmin)-[~/home/sysadmin]
# sudo apt install openvas
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openvas is already the newest version (22.4.1).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

Figure 4. Done OpenVas Installation

Scanning process on the first target, Office A, as the target to identify the vulnerability. Enter the ip address 192.168.57.103 which will be configured into OpenVas as below When a request is made to OpenVas to identify which will be the target of vulnerability identification all scanning tools will run everything. If the scanning process has been completed, the conclusion of the Vulnerability Assessment results can be seen. If it is said to be critical or High, the result that appears is High. The High status occurs because OpenVas finds critical gaps in the target system for which vulnerabilities are identified. The scanning results are shown in Figure 5.

Vulnerability	Severity	QoD	Host		Location	Created
			IP	Name		
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.5.107		1524/tcp	Mon, Apr 26, 2021 4:05 PM UTC
The rexec service is running	10.0 (High)	80 %	192.168.5.107		512/tcp	Mon, Apr 26, 2021 4:00 PM UTC
rlogin Passwordless Login	10.0 (High)	80 %	192.168.5.107		513/tcp	Mon, Apr 26, 2021 3:56 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.5.107		8787/tcp	Mon, Apr 26, 2021 4:03 PM UTC
Twiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.5.107		80/tcp	Mon, Apr 26, 2021 4:01 PM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.5.107		1099/tcp	Mon, Apr 26, 2021 4:04 PM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.5.107		general/tcp	Mon, Apr 26, 2021 3:59 PM UTC

Figure 5. Scanning Result

After the process of Figure 5, it can be seen in the task details that the Office A network has several dangerous gaps in the High category. The vulnerability occurs on port 445 on the TCP connection with a quality of detection of 98 percent. This vulnerability can exploit and can control the system. This vulnerability can be exploited by attackers to send special network messages created for the system running this server service.

High (CVSS: 7.5) 80/tcp

NVT: wpoison (nasl version) (OID: 1.3.6.1.4.1.25623.1.0.11139)

Summary

This script attempts to use SQL injection techniques on CGI scripts
More info at : http://en.wikipedia.org/wiki/SQL_injection

Vulnerability Detection Result

The following URLs seem to be vulnerable to various SQL injection techniques :

```

/Templatize.asp?item='UNION'
/Templatize.asp?item='
/Templatize.asp?item='%22
/Templatize.asp?item=9%2c+9%2c+9
/Templatize.asp?item='bad_bad_value
/Templatize.asp?item=bad_bad_value'
/Templatize.asp?item='+OR+'
/Templatize.asp?item='WHERE
/Templatize.asp?item=%3B
/Templatize.asp?item='OR

```

An attacker may exploit this flaws to bypass authentication or to take the control of the remote database.
Solution: Modify the relevant CGIs so that they properly escape arguments
See also : <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

Solution

Modify the relevant CGIs so that they properly escape arguments.

Vulnerability Detection Method

Details: wpoison (nasl version) (OID: 1.3.6.1.4.1.25623.1.0.11139)
Version used: \$Revision: 421 \$

Figure 6. Description of the High result of the OpenVas Vulnerability Assessment

In the Figure 6, the results of the report explain the existence of a high level vulnerability on port 80, then the medium level and low level. Vulnerabilities that are at a high level must be immediately mitigated to secure the system that has been carried out Vulnerability Assessment using openvas which is shown in Figure 7.

Service (Port)	Threat Level
80/tcp	High
139/tcp	Log
3389/tcp	Medium
general/SMBClient	Log
135/tcp	Medium
general/icmp	Log
general/tcp	Log
8443/tcp	Medium

Figure 7. Assessment Report

At this stage, it will be tested whether or not the vulnerability can be exploited or not. If the Vulnerability Assessment stage has been carried out, the previous stage up to the vulnerability report is sufficient. However, if the process is up to penetration testing, simulation testing must be carried out in accordance with the findings of vulnerabilities in the system identified vulnerabilities to prove whether or not the vulnerability is potentially dangerous on the target machine. In addition, the vulnerability must also be successfully exploited. To start proving the findings of the Windows XP vulnerability that has been identified, then go directly to the exploitation process. The tool used is Metasploit which is shown in Figure 8 [15].

```

dBBBBBb dBBBp dBBBBBBp dBBBBBb
+ dB'
dB'dB'dB' dBBp dBp dBp BB
dB'dB'dB' dBp dBp dBp BB
dB'dB'dB' dBBBBp dBp dBBBBBB

          dBBBBBBp dBBBBBb dBp dBBBBBp dBp dBBBBBBp
          dB' dBp dB' dBp
          dBp dBBBB' dBp dB' dBp dBp dBp
          dBp dBp dBp dB' dBp dBp dBp
          dBBBBBp dBp dBBBBBBp dBBBBBp dBp dBp

To boldly go where no
shell has gone before

=[ metasploit v6.3.20-dev-80e10886fe5feed734b3638899f0e2e11407a6c0]
+ --=[ 2319 exploits - 1215 auxiliary - 412 post ]
+ --=[ 1268 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

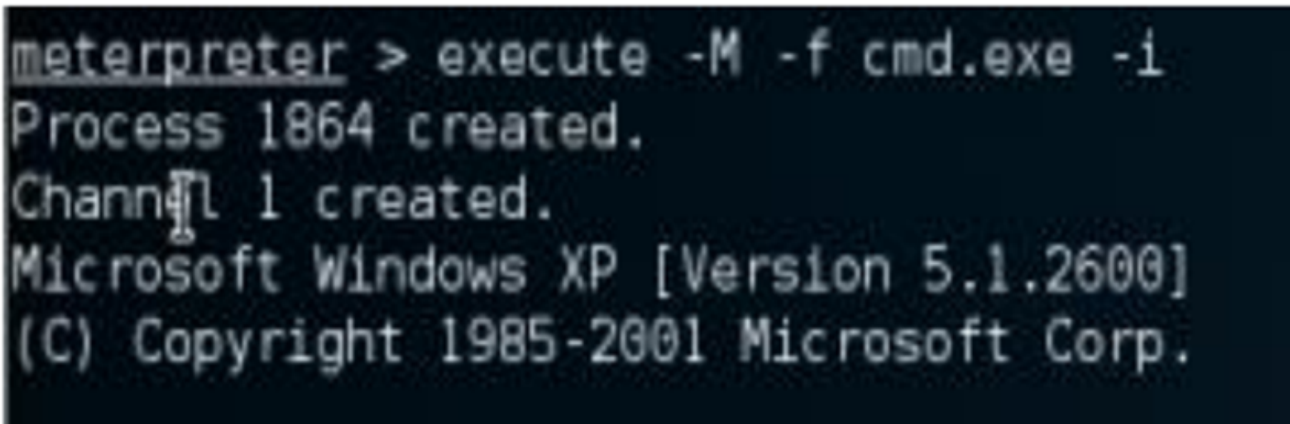
Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Figure 8. Metasploit Console

To run the exploit on the smb application enter the command below: root@kali:~# msfconsole — msf > use exploit/windows/smb/ms08 After entering the SMB vulnerability database then enter the target ip address to be exploited RHOST 192.168.57.103 and then exploited. The results of the exploitation above show the system that provides the results entered and then entered the meterpreter. After entering the meterpreter session, the command prompt program will be executed on windows xp in order to fully control the entire system [16]. The results of exploiting the vulnerability from metasploit are shown in Figure 9.



```
meterpreter > execute -M -f cmd.exe -i
Process 1864 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

Figure 9. Vulnerability Exploitation Results From Metasploit

Find the main problem in the network and fix it by update software, Set security policies, improve network settings, Train employees on threats, adhere to standard security guidelines, collaborate with internal security team, create a clear action plan, review security check tools used, and suggest further research for continuous security. In conclusion, while this study has shed light on the effectiveness of OpenVas in identifying vulnerabilities within the PT. Dutakom Wibawa Putra network, it is essential to consider the specific context and evolving nature of cybersecurity [1] [2].

4. CONCLUSION

In conclusion, the implementation of the Vulnerability Assessment technique using OpenVas on the PT. Dutakom Wibawa Putra network has provided valuable insights into the security posture of the company's network infrastructure. However, it is essential to acknowledge certain limitations of this study and suggest directions for future research. Firstly, it's important to note that the effectiveness of Vulnerability Assessment using OpenVas may vary depending on the specific network environment and configurations. This study focused on a particular case, and the results may not be directly applicable to all scenarios. Future research should explore the adaptability and performance of OpenVas in diverse network environments to provide a more comprehensive understanding of its capabilities and limitations. Secondly, the Vulnerability Assessment analysis identified vulnerabilities that require immediate attention. Still, it is crucial to recognize that the remediation process and the implementation of security measures are equally critical. Future research should delve deeper into the remediation phase, including the development of strategies and best practices for addressing the vulnerabilities discovered. Furthermore, the study highlighted the importance of regular scanning and monitoring processes to keep up with evolving vulnerabilities. Future research can focus on optimizing the frequency and scope of scans, as well as improving the automation of these processes to enhance network security further. In conclusion, while this study has shed light on the effectiveness of OpenVas in identifying vulnerabilities within the PT. Dutakom Wibawa Putra network, it is essential to consider the specific context and evolving nature of cybersecurity. Future research should continue to explore and refine Vulnerability Assessment techniques and contribute to the ongoing efforts to strengthen network security in an ever-changing threat landscape.

5. ACKNOWLEDGEMENTS

We would like to thank those who have supported this research.

6. DECLARATIONS

AUTHOR CONTRIBUTION

All authors contributed to the writing of this article.

FUNDING STATEMENT

-

COMPETING INTEREST

The authors declare no conflict of interest in this article.

REFERENCES

- [1] T. Astriani, "Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 8, no. 4, pp. 2041–2050, dec 2021. [Online]. Available: <https://jurnal.mdp.ac.id/index.php/jatisi/article/view/1232>
- [2] D. Laksmiati, "Vulnerability Assessment Pada Situs www.Hatsehat.com Menggunakan Openvas," *Akrab Juara : Jurnal Ilmu-ilmu Sosial*, vol. 5, no. 3, pp. 240–246, 2023.
- [3] F. Wibowo, H. Harjono, and A. P. Wicaksono, "Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS," *Jurnal Informatika*, vol. 6, no. 2, pp. 212–217, sep 2019. [Online]. Available: <http://ejournal.bsi.ac.id/ejurnal/index.php/ji/article/view/5925>
- [4] E. D. Sikumbang, "Penerapan Data Mining Penjualan Sepatu Menggunakan Metode Algoritma Apriori," *Jurnal Teknik Komputer Amik BSI*, vol. 4, no. 1, pp. 156–161, 2018.
- [5] M. T. M. A. Nur and F. Darmawan, Irfan Rokhman, "Implementasi Risk assessment pada Divisi Teknologi Informasi Di PT. XYZ Menggunakan Iso 27005:2008," in *e-Proceeding of Engineering*, 2020, pp. 2111–2118.
- [6] M. Melladia, D. E. Putra, and L. Muhelni, "Penerapan Data Mining Pemasaran Produk Menggunakan Metode Clustering," *Jurnal Teknik Informasi dan Komputer (Tekinkom)*, vol. 5, no. 1, pp. 160–167, jun 2022. [Online]. Available: <https://jurnal.murnisadar.ac.id/index.php/Tekinkom/article/view/458>
- [7] E. Z. Darajat, E. Sedyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *JURNAL SISTEM INFORMASI BISNIS*, vol. 12, no. 1, pp. 36–44, sep 2022. [Online]. Available: <https://ejournal.undip.ac.id/index.php/jsinbis/article/view/47792>
- [8] R. Sahtyawan, "Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment And Penetration Testing)," *Journal of Information System Management (JOISM)*, vol. 1, no. 1, pp. 18–22, jul 2019. [Online]. Available: <https://jurnal.amikom.ac.id/index.php/joism/article/view/18>
- [9] D. Aryanti, Nurholis, and J. Nashar Utamajaya, "Analisis Kerentanan Keamanan Website Menggunakan Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja," *Jurnal Syntax Fusion*, vol. 1, no. 03, pp. 15–25, sep 2021. [Online]. Available: <http://fusion.rifainstitute.com/index.php/fusion/article/view/53>
- [10] A. M. Tania, D. Setiyadi, and F. Khasanah, Nidaul, "Keamanan Website Menggunakan Vulnerability Assessment," *INFORMATICS FOR EDUCATORS AND PROFESSIONAL : Journal of Informatic*, vol. 2, no. 2, pp. 171 – 180, 2018.
- [11] Mira Orisa and M. Ardita, "Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web," *Jurnal Mnemonic*, vol. 4, no. 1, pp. 16–19, feb 2021. [Online]. Available: <https://ejournal.itn.ac.id/index.php/mnemonic/article/view/3213>
- [12] D. M. Paramita and A. N. Fajar, "Analysis of Network Performance Management Dashboard," *International Journal of Mechanical Engineering and Technology (IJMET)*, vol. 10, no. 03, pp. 952–963, 2019. [Online]. Available: http://edocs.ilkom.unsri.ac.id/4362/2/ManjarI_MonicaAdhelia.09011181621009.pdf
- [13] P. Cisar and R. Pinter, "Some ethical hacking possibilities in Kali Linux environment," *Journal of Applied Technical and Educational Sciences JATES*, vol. 9, no. 4, pp. 129–149, 2019. [Online]. Available: <http://doi.org/10.24368/jates.v9i4.139http://jates.org>

-
- [14] M. Kyei and M. Asante, "Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools," *International Journal of Computer Applications*, vol. 176, no. 32, pp. 26–33, jun 2020. [Online]. Available: <http://www.ijcaonline.org/archives/volume176/number32/kissi-2020-ijca-920365.pdf>
- [15] R. Seema and N. Ritu, "Penetration Testing Using Metasploit Framework : an Ethical Approach," *International Research Journal of Engineering and Technology(IRJET)*, vol. 06, no. 08, pp. 538–542, 2019. [Online]. Available: https://www.academia.edu/40379823/IRJET-_PENETRATION_TESTING_USING_METASPLOIT_FRAMEWORK_AN_ETHICAL_APPROACH
- [16] F. Heiding, E. Süren, J. Olegård, and R. Lagerström, "Penetration testing of connected households," *Computers and Security*, vol. 126, no. March, pp. 1–13, mar 2023. [Online]. Available: <https://linkinghub.elsevier.com/retrieve/pii/S016740482200459X>