IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 3, June, 2023, pp. 711-716
Journal homepage: http://iieta.org/journals/isi

# Security Vulnerability Analysis and Recommendations for Open Media Vault Cloud Server on Raspberry Pi

Ritzkal Ritzkal[1*], Kodarsyah[2], Puspa Putri Amalia[1], Wildan Mahmud[1], Ade Hendri Hendrawan[3], Bayu Adhi Prakoso[1], Indra Riawan[1]

[1] Informatics Engineering, Universitas Ibn Khaldun, Bogor 16162, Indonesia
[2] National Research and Innovation Agency, Jl. Ir. Djuanda Kota, Bogor 16122, Indonesia
[3] Computer Science, Universitas Dian Nuswantono, Semarang 50131, Indonesia

Corresponding Author Email: ritzkal@ft.uika-bogor.ac.id

https://doi.org/10.18280/isi.280321

**Received:** 23 January 2023
**Accepted:** 12 March 2023

***Keywords:***
*network security, vulnerability, port, Nmap, Nessus*

## ABSTRACT

The Raspberry Pi has been increasingly utilized as a network-attached storage (NAS) server, with Open Media Vault (OMV) software handling file and data storage. Access to the NAS server is provided through a Local Area Network (LAN), where open ports can pose potential security risks, enabling unauthorized intrusion. In this study, the network design method incorporating the PPDIOO model was employed to conduct a vulnerability assessment and to offer security recommendations for the OMV Cloud server running on Raspberry Pi. The analysis was executed using two prominent security tools, Nmap and Nessus. Upon employing Nmap and Nessus in the evaluation, several security vulnerabilities were identified on the OMV Cloud server utilizing Raspberry Pi. Through continuous monitoring and analysis, open ports were detected, including: port 22 (SSH), port 80 (WEB), port 111 (rcpbind), port 139 (netbios-ssn), port 445 (netbios-ssn), port 2049 (NFS), port 3389 (ms-wbt-server), and port 5357 (WSDAPI). Based on the assessment, seven solutions were proposed, addressing three vulnerability categories: high (2%), medium (2%), and informational (96%). This comprehensive examination provides valuable insight into securing the OMV Cloud server, enhancing the overall security of Raspberry Pi-based NAS implementations.

## 1. INTRODUCTION

The Raspberry Pi has been employed as a network-attached storage (NAS) server [1], utilizing the Cloud Open Media Vault (OMV) software to manage file and data storage. Access to the NAS server is provided via a Local Area Network (LAN), where open ports may serve as entry points for unauthorized intrusions, compromising the network's performance and data integrity [2]. Denial of Service (DoS) attacks, which consume memory, CPU, and network resources, also pose a significant threat to both LAN and internet networks [3-5].

Attackers often perform port scanning on the OMV Cloud server running on Raspberry Pi to identify open ports, which subsequently reveal the network vulnerabilities of the server [6]. To ensure the network security of the OMV server, it is crucial to analyze security gaps, conduct testing and monitoring, and provide recommendations for strengthening network security. The following questions have been formulated to address these issues: "How can vulnerability security analysis and monitoring results be obtained for the OMV Cloud server running on Raspberry Pi? What are the vulnerability security recommendations for the OMV Cloud server running on Raspberry Pi?"

Employing the Nmap and Nessus tools for examining security vulnerabilities offers a possible solution to the aforementioned challenges [7]. The Nmap tool can be used to detect active hosts on a network and identify open ports, while the Nessus tool can assess network vulnerabilities and generate security recommendations for the OMV Cloud server [8, 9]. In this study, the Raspberry Pi-based OMV server is analyzed using these tools to derive both vulnerability security analysis results and recommendations.

## 2. RESEARCH METHODS

Figure 1 describes the network design method with the PPDIOO model developed by Cisco. with the following stages: Prepare, Plan, Design, Implement, Operate, and Optimize [10].

### Prepare

At this point, preparations are performed by using a Raspberry Pi to detect the issues with the Open Media Vault cloud server.

### Plan

The planning step is where the software and hardware specifications for the research are described.

### Design

At the design stage, discuss network topology to understand and simplify the concept of a security system on an Open Media Vault cloud server using Raspberry Pi.

**Implement**

Currently, software installation is being done, first installing Nmap and then Nessus.

**Operate**

At this point, scanning is conducted out on the Open Media Vault cloud server IP using Nmap and Nessus. Nmap scan results will show ports, however Nessus scan results will show the vulnerability category. Furthermore, recommendations are made after an analysis of the Nmap and Nessus tool results.

**Optimize**

In this phase, the network is handled by finding and fixing problems before they have an impact on the network.

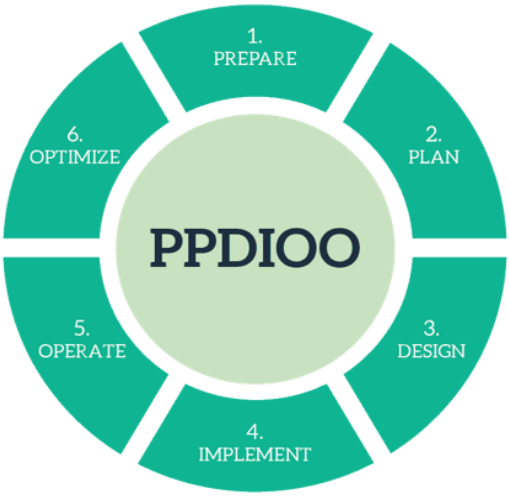


**Figure 1.** Research methodology

## 3. RESULT

At this point, the findings of the study, titled "Vulnerability Security Analysis on the Open Media Vault Cloud Server Using Raspberry Pi," will be discussed.

### 3.1 Prepare

The Open Media Vault cloud server running on a Raspberry Pi was used for this study, and monitoring was done using the programs Nmap and Nessus to identify any vulnerabilities [11].

### 3.2 Plan

The tools used in the research of vulnerability security analysis on the Cloud Open Media Vault server using Raspberry Pi in the Computer System and Network (CSN) Laboratory, are divided into two, namely hardware and software.

The hardware employed in this study is described in Table 1. The Raspberry Pi serves as the initial target server for analysis. Second, use a laptop as a client with Nmap and Nessus installed to do a vulnerability analysis.

The software utilized in this investigation is described in Table 2. In the beginning, the Windows client was used with the Windows 11 Operating System. Secondly, seeing and monitoring the server's ports with the Nmap tool. The third step is to use the Nessus tool to discover any vulnerabilities on the target server.

**Table 1.** Hardware

| No | Device | Amount | Function |
|---|---|---|---|
| 1 | Raspberry Pi | 1 unit | Target server being analyzed |
| 2 | Laptop | 1 unit | Laptop used to perform vulnerability security analysis |

**Table 2.** Software

| No. | Name of Software | Function |
|---|---|---|
| 1 | Windows 11 | Operating system used for research |
| 2 | Nmap | Software used to monitor and view open ports on the Open Media Vault server using Raspberry Pi |
| 3 | Nessus | Software used to scan and see vulnerabilities that exist in the target IP |

### 3.3 Design

At this point, the infrastructure is employed, along with a network topology that follows the configuration of the Cloud Open Media Vault server utilizing a Raspberry Pi. The physical topology and logical topology both display the topology [12].

(1). Physical topology of the Open Media Vault cloud server

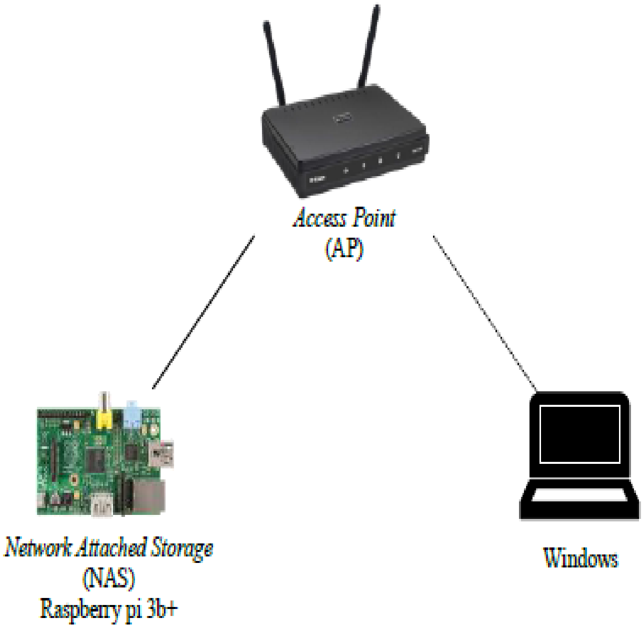


**Figure 2.** Physical topology

Based on Figure 2, the physical network topology illustrates the design of the Cloud Open Media Vault server network structure using Raspberry Pi.

(2). Topologi logika server cloud Open Media Vault

Based on Figure 3, the logical topology describes the IP addressing on the computer network structure on the Cloud Open Media Vault server, where the Cloud Open Media Vault server as a target with LAN IP 192.168.0.xx. where the LAN IP will be tested.

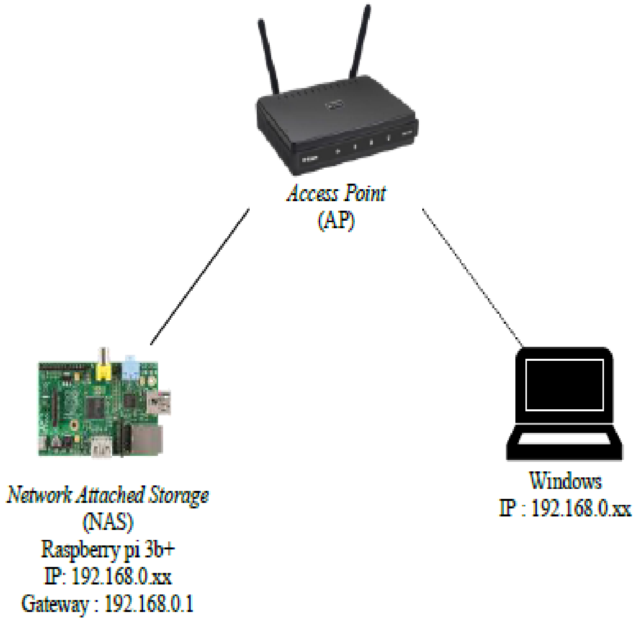


**Figure 3.** Logic topology

### 3.4 Implement

Using Raspberry-Pi, the study was carried out on the Open Media Vault cloud server network. The installation procedure is carried out during the implementation stage [13, 14], including:

1. Installation of Nmap

Nmap will be used to scan and keep an eye on network ports. The steps for installing Nmap are as follows.

a. Download the installation for Nmap. On the official Nmap website, the file may be downloaded without charge.

b. Launch the installer for Nmap.

d. Select Continue Installation by clicking I Agree.

d. Examine all of Nmap's features.

e. Select C: Program Files(x86) as the installation directory location and then click next.

f. Wait while the installation process is running.

g. The installation has been finished.

2. Nessus installation

Nessus will be used for scanning and viewing vulnerabilities in the target IP. The following is the Nessus installation process:

a. Download the Nessus installer file

b. Open the installer file

c. Click next

d. Click install

e. After the install process is complete, open the Nessus application, the page will open in the default browser with the address https://localhost:8834/#/

f. Create a Nessus account by entering an email address and password

g. The account has been successfully created, then log in with the email and password used when creating the account

h. Enter the Nessus page

i. Select New Scan

j. Select Basic Network Scan

k. Fill in name with the target server name, and Targets with the target IP.

l. Save

m. Click the Launch icon

n. Wait 10-12 minutes for the scanning process.

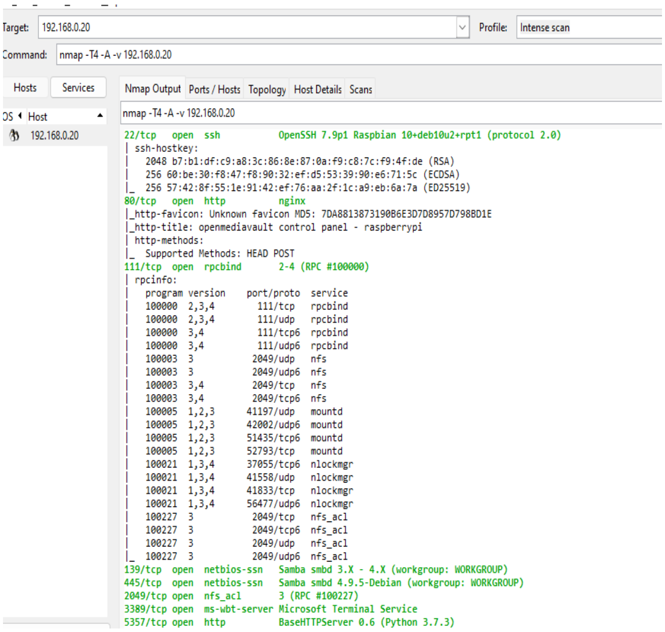
### 3.5 Operate

a. Network scan using Nmap

Nmap is used for the network scan, and it shows the open ports and information about the ports as well as the topology of the target IP, which is 192.168.0.xx.

Figure 4 displays the port, status, service, and version of a Nmap scan of IP 192.168.0.x. Seven ports are open on the Raspberry-Pi-powered Cloud Cloud Open Media Vault server, including ports 22, 80, 111, 139, 445, 2049, and 5357. These ports' duties are as follows:

- Port 22 is a Secure Shell (SSH) port
- Port 80 is a web server port
- Port 111 is a rcpbind port
- Port 139 is a netbios ssn port
- Port 445 is a netbios ssn port
- Port 2049 is a nfs-acl port
- Port 3389 is ms-wbt-server port
- Port 5357 is a Web Services for Devices (WSDAPI) port



Target: 192.168.0.20
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.0.20

192.168.0.20

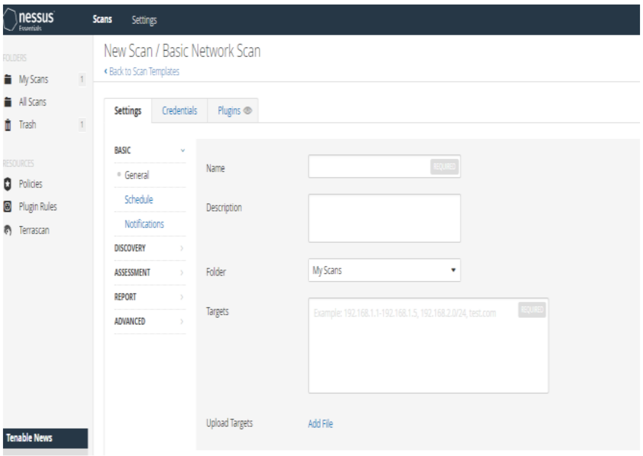
```
nmap -T4 -A -v 192.168.0.20
22/tcp   open  ssh          OpenSSH 7.9p1 Raspbian 10+deb10u2+rpt1 (protocol 2.0)
| ssh-hostkey:
|   2048 b7:b1:df:c9:a8:3c:86:8e:87:0a:f9:c8:7c:f9:4f:de (RSA)
|   256 60:be:30:f8:47:f8:90:32:ef:d5:53:39:90:e6:71:5c (ECDSA)
|_  256 57:42:8f:55:1e:91:42:ef:76:aa:2f:1c:a9:eb:6a:7a (ED25519)
80/tcp   open  http         nginx
|_http-favicon: Unknown favicon MD5: 7DA8813873190B6E3D7D8957D798BD1E
|_http-title: openmediavault control panel - raspberrypi
| http-methods:
|_  Supported Methods: HEAD POST
111/tcp  open  rpcbind      2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      41197/udp   mountd
|   100005  1,2,3      42002/udp6  mountd
|   100005  1,2,3      51435/tcp6  mountd
|   100005  1,2,3      52793/tcp   mountd
|   100021  1,3,4      37055/tcp6  nlockmgr
|   100021  1,3,4      41558/udp   nlockmgr
|   100021  1,3,4      41833/tcp   nlockmgr
|   100021  1,3,4      56477/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
2049/tcp open  nfs_acl      3 (RPC #100227)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
5357/tcp open  http         BaseHTTPServer 0.6 (Python 3.7.3)
```

**Figure 4.** Nmap scanning result

The Nessus scan findings for IP 192.168.0.xx revealed a vulnerability; descriptions of each information are shown on the colored icons; the red icon indicates a high vulnerability, the orange symbol a medium vulnerability, and the blue icon a low vulnerability [15-17]. In order to make it simpler to assess the outcomes of data processing, information is also received in the form of data descriptions that are then processed in a table. The following is a table of vulnerability data from the scan results using Nessus based on the level of vulnerability category [18].

b. Network scan using Nessus

When a network scan is performed using Nessus, the vulnerabilities discovered by the target IP (192.168.0.xx) will be displayed. The network scan conducted by Nessus on the Open Media Vault Cloud server is depicted in the following figure.



New Scan / Basic Network Scan

‹ Back to Scan Templates

Name: REQUIRED

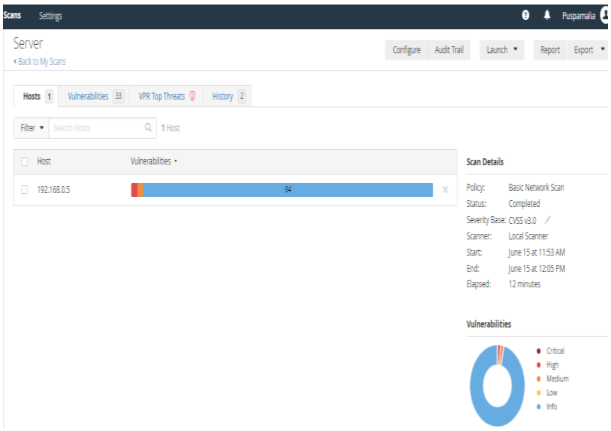
Description:

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED

Upload Targets: Add File

**Figure 5.** Nessus scanning process



Server

‹ Back to My Scans

1 Host

| Host | Vulnerabilities |
|---|---|
| 192.168.0.5 | 64 |

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: June 15 at 11:53 AM
End: June 15 at 12:05 PM
Elapsed: 12 minutes

Vulnerabilities

**Figure 6.** Nessus scanning results

The Nessus scanning procedure is shown in Figure 5, where the Name column contains the server's name and the Target column contains the IP of the target server. Figure 6 displays the results of Nessus scanning and the target's percentage of vulnerability [19, 20]. Table 3 describes vulnerability.

c. Rekomendation

At this stage explains the proposed remedy to solve the vulnerability problem from the data that has been evaluated in the previous analysis stage, where the data collected is the vulnerability of the target IP with several categories, namely High, Medium, and Info [21].

Table 4 is a vulnerability in the high category, with the description Samba 4.13.x<4.13.17/4.14.x<4.14.12/4.15.x<4.15.5 Multiple Vulnerabilities with a recommendation description Upgrade samba to Version 4.13.17, 4.14.12/4.15.5.

File sharing between Windows and Linux-based machines is done via the Samba service. This flaw impacts a read/write Out-of-Bounds (OOB) Heap vulnerability that was present in Samba versions prior to 4.13.17. On affected Samba installations that make use of the vfs fruit VFS module, this vulnerability enables remote attackers to execute arbitrary code as root. Samba must be updated to the most recent version, 4.13.17, 4.14.12, or 4.15.5, in order to prevent Out of Bounds (OOB) vulnerabilities [22].

If the server manager does not follow up and repair the vulnerability, it will become critical. A vulnerability with the Significant category denotes a high risk. where critical represents the highest level of vulnerability [23, 24].

Table 5 is a vulnerability in the medium category, with the description SMB Signing not required with the recommendation [25] enforce message signing in the host's configuration. In Windows, this can be found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing' [26]. See the 'see also' link for more details.

With Windows workstations connected to a network, Samba can reduce the complexity of multiple Linux (UNIX) operating system platforms. To connect all Linux (Unix) machines to Windows machines [27], Samba enables Unix or Linux servers to communicate with Microsoft Windows protocols on a single network. The SMB protocol allows digital signature of SMB packets in order to prevent man-in-the-middle attacks that change SMB packets while they are in transit [28]. The use of digital signatures in a highly secure network helps prevent "session hijacking," which involves client PCs and servers.

Vulnerability with the Medium category indicates that the vulnerability is medium risk, if the server manager does not follow up (fix), the vulnerability will become High. Where High is a higher vulnerability category than the Medium [29].

Table 6 is a vulnerability with the Info category, Vulnerability with the Info category shows vulnerability information, but if the server manager does not follow up (fix), the vulnerability will become Low. Where Low is a higher vulnerability category than the Info category [30].

**Table 3.** Nessus scanning result

| No. | Kategori | Tampilan |
|---|---|---|
| 1. | High | Detect unsupported samba versions |
| 2. | Medium | SMB Signing not required |
| 3. | Info | HyperText Transfer Protocol (HTTP) Information<br>RPC portmapper (TCP)<br>SMB Use Host SID to Enumerate Local Users<br>SHH Algorithms and Languages Supported<br>SSH Password Authentication Accepted<br>SSH Server Type and Version Information<br>RPC Services Enumeration<br>Nessus SYN scanner<br>Service Detection<br>Common Platform Enumeration (CPE)<br>Device Type<br>Ethernet Card Manufacturer Detection<br>Ethernet MAC Addresses<br>FTP Server Detection<br>Host Fully Qualified Domain Name (FQDN) Resolution<br>ICMP Timestamp Request Remote Date Disclosure<br>Inconsistent Hostname and IP Address<br>Nessus Scan Information<br>NFS Server Superfluous<br>nginx HTTP Server Detection<br>OS Identification<br>OS Security Patch Assessment Not Available<br>Patch Report<br>Samba Version<br>Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)<br>SSH Protocol Versions Supported<br>Target Credential Status by Authentication Protocol-No Credentials Provided<br>TCP/IP Timestamps Supported<br>Traceroute Information<br>WMI Not Available |

**Table 4.** High category recommendation

| No. | Vulneranility | Category | Solution | Port |
|---|---|---|---|---|
| 1 | Samba 4.13.x<4.13.17/4.14.x<4. 14.12/4.15.x<4.15.5 Multiple Vulnerabilities | High | Upgrade samba ke Versi 4.13.17, 4.14.12/4.15.5 | - |

**Table 5.** Medium category recommendation

| No. | Vulnerability | Category | Solution | Port |
|---|---|---|---|---|
| 1 | SMB Signing not required | Medium | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | - |

**Table 6.** Info category recommendations

| No. | Vulnerability | Category | Solution | Port |
|---|---|---|---|---|
| 1 | Nessus SYN scanner | Info | Protect targets with IP filters | 22, 80, 111, 139, 445, 2049 |
| 2 | Inconsistent Hostname and IP Address | Info | Fix reverse DNS or hosts file | - |
| 3 | NFS Server Superfluous | Info | Disable this Service | 2049 |
| 4 | Patch Report | Info | Upgrade samba to Version 4.13.17, 4.14.12 / 4.15.5 | - |
| 5 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) | Info | Disable SMBv1 according to vendor instructions in Microsoft KB2696547. Also, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over NetBIOS API, block TCP port 137/139 and UDP port 137/138 on all network boundary devices | 445 |

### 3.6 Optimize

In this final stage, server maintenance is performed, such as updating Samba to the most recent version, before the issue affects the network and poses a security risk to the Raspberry Pi-based Open Media Vault cloud server.

## 4. CONCLUSION

The monitoring and analysis process can be carried out using the PPDIOO model's stages and the Nmap and Nessus tools. Based on the results of the monitoring and analysis, vulnerabilities on the Open Media Vault cloud server using the Raspberry Pi can be found with three categories, namely, high, medium, and info. Where the resulting suggestions can be used as a guide for server upkeep and repair to close security holes on the Raspberry Pi-powered Open Media Vault cloud server.

## REFERENCES

[1] Sholeh, A.N., Wardaya, M.S.S. (2019). Analysis and Vulnerability Testing of Library Information Systems. Independent Journal: Science, Arts, and Technology, 3(1): 116-131.

[2] Prasetyo, S.E., Lee, R.C. (2021). Network security analysis on Pay2home using penetration testing method. In Combines-Conference on Management, Business, Innovation, Education and Social Sciences, 1(1): 710-718.

[3] Anugrah, I., Rahmanto, R.H. (2017). Local area network security system using de-militarized zone technique. PIKSEL: Computer Science Research Embedded and Logic Systems, 5(2): 91-106. https://doi.org/10.33558/piksel.v5i2.271

[4] Al-Munawar, N., Sediyono, A. (2017). Characteristics of computer power consumption with changes in Distributed Denial of Service (Ddos) Attack Level. In Proceedings of the National Seminar of Scholars, pp. 141-147. https://doi.org/10.25105/semnas.v0i0.2174

[5] Siregar, J.J. (2013). Security exploitation analysis of web denial of service attack. Comtech: Computer, Mathematics and Engineering Applications, 9: 1199-1205. https://doi.org/10.21512/comtech.v4i2.2597

[6] Utami, A.S.P., Lidyawati, L., Ramadhan, Z. (2013). Design and performance analysis of network intrusion prevention system using Snort Ids and Honeyd. Reka Elkomika, 1(4).

[7] Putra, S.A., Budiono, A., Hediyanto, U.Y.K.S. (2023). Vulnerability assessment of student final project proposal web using Acunetix and NMAP. Eproceedings of Engineering, 10(2): 1615-1622.

[8] Sudirman, D., Yaqin, A.N. (2021). Network penetration and security audit using Nmap. SATIN-Information Science and Technology, 7(1): 32-44. https://doi.org/10.33372/stn.v7i1.702

[9] Suharyanto, C.E., Maulana, A. (2020). Designing network attached storage (NAS) using Raspberry Pi for micro, Small and Medium Enterprises (MSMES). Journal of Computer Science and Technology, 5(2): 271-278. https://doi.org/10.33480/jitk.v5i2.1215

[10] Saputra, A., Muhamad Akbar, M.I.T., Solikin, I., Kom, M. (2016). Development of Wireless Local Area Network (WLAN) Using Ppdioo Method. Faculty of Computer Science, Binadarma University.

[11] Bayu Rendro, D., Nugroho Aji, W. (2020). Analysis of monitoring computer network security systems using Nmap software (Case Study at SMK Negeri 1 Kota Serang). Prosisko: Journal of Research Development and Observation of Computer Systems, 7(2): 108-115.

[12] Anonymous. (2010). Computer Network System for Beginners, Yogyakarta, Andi, Madcoms.

[13] Kamilah, I., Ritzkal, R., Hendrawan, A.H. (2019). Analysis of security vulnerabilities in the laboratory

attendance server in the informatics engineering study program. Proceedings of Semnastek.

[14] Firdaus, D.S., Ritzkal, R., Hendrawan, A.H. (2019). Analysis of security vulnerabilities on the Open Media Vault cloud server at the Faculty of Engineering, Ibn Khaldun University Bogor. Semnastek Proceedings.

[15] Jetty, S., Rahalkar, S. (2019). Securing network infrastructure: discover practical network security with Nmap and Nessus 7. Packt Publishing Ltd.

[16] Aristian, A., Cholil, W. (2022). Vulnerability analysis of the Lia Palembang language institute website using Nessus, Netsparker and Acunetic. Journal of Education and Counselling (JPDK), 4(4): 2459-2473. https://doi.org/10.31004/jpdk.v4i4.5821

[17] Juardi, D. (2017). Review of internet network security vulnerability using Nessus. Syntax Journal of Informatics, 6(1): 11-19.

[18] Hendrawan, A.H., Setiawan, F.A., Mulyo, A.S. (2014). Network security analysis with the security lifecycle method at Ibn Khaldun University Bogor. Proceedings of Lppm Uika Bogor.

[19] Dwiyatno, S. (2020). Analysis of monitoring computer network systems using Nmap Software. Prosisko: Journal of Research Development and Observation of Computer Systems, 7(2): 108-115. https://doi.org/10.30656/prosisko.v7i2.2522

[20] Julianto, C. P. (2022). Security gap testing on website using ISSAF framework, Doctoral Dissertation, ATMA Jaya University Yogyakarta.

[21] Mulya, B.W.R., Tarigan, A. (2018). Ranking the security risks of the poor city polytechnic computer network system using CVSS and FMEA. ILKOM Scientific Journal, 10(2): 190-200.

[22] Cahyanto, T.A., Oktavianto, H., Royan, A.W. (2016). Analysis and implementation of honeypot using dionaea as network security support. Indonesian Journal of Information Systems and Technology, 1(2).

[23] Zein, M.A., Hediyanto, U.Y.K.S., Almaarif, A. (2023). Security hardening of virtual private server operating systems at Xyz Educational Institutions Based on Nist Sp 800-123. Scientific Journal of Research and Learning Informatics, 8(1): 230-241.

[24] Tan, T., Soewito, B. (2022). Cyber-attack risk management using the NIST cybersecurity framework. Journal of Information System, Applied, Management, Accounting and Research, 6(2): 411-422.

[25] Popescu, M., Capotă, C., Țene, I., Găină, M., Halunga, S. (2023). Vulnerabilities of windows systems through Wi-Fi infrastructure. In Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI, 12493: 704-711. https://doi.org/10.1117/12.2643121

[26] Newman, Z., Meyers, J.S., Torres-Arias, S. (2022). Sigstore: Software signing for everybody. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, pp. 2353-2367. https://doi.org/10.1145/3548606.3560596

[27] Kaur, B., Chopra, S., Singh, G. (2023). Comparison of linux and windows and their server configuration. Trends In Interdisciplinary Research Volume II, 68. https://www.bhumipublishing.com/wp-content/uploads/2023/06/trends-in-interdisciplinary-research-volume-ii-1.pdf#page=74

[28] Franzen, F., Steger, L., Zirngibl, J., Sattler, P. (2022). Looking for honey once again: Detecting RDP And SMB honeypots on the Internet. In 2022 IEEE European Symposium on Security and Privacy Workshops (Euros&PW), pp. 266-277.

[29] Setiawan, M.F., Saedudin, R.R., Herdianto, U.Y.K. (2022). Closing security gaps using the hardening method case study: Cloudfri closing security vocations using the hardening method case study: Cloudfri. Eproceedings of Engineering, 9(2): 656-663.

[30] Kartolo, R., Negara, E.S. (2022). Analysis of private cloud computing performance using reability, maintainability, availability and security methods. Journal of Inovtek Polbeng-Seri Informatika, 7(1): 136-146.