Team name Ping of Death



Penetration Testing Report

## Table of Contents

[General Information 1](#_Toc10038)

[Vulnerabilities Identified as a Result of the Penetration Test 1](#_Toc10039)

[Conclusion 6](#_Toc10040)

General Information

A penetration test was conducted on the "Callobes" machine by the PingOfDeath team. As a result of the assessments, vulnerabilities were identified, risks were evaluated, and preventive measures were recommended.

*Target: Collobes*

**Vulnerabilities Identified as a Result of the Penetration Test**

Initially, *"nmap"* (network mapper) was used to scan the network and identify vulnerabilities. As a result, it was determined that two different ports (22 and 80) were open (Photo 1).

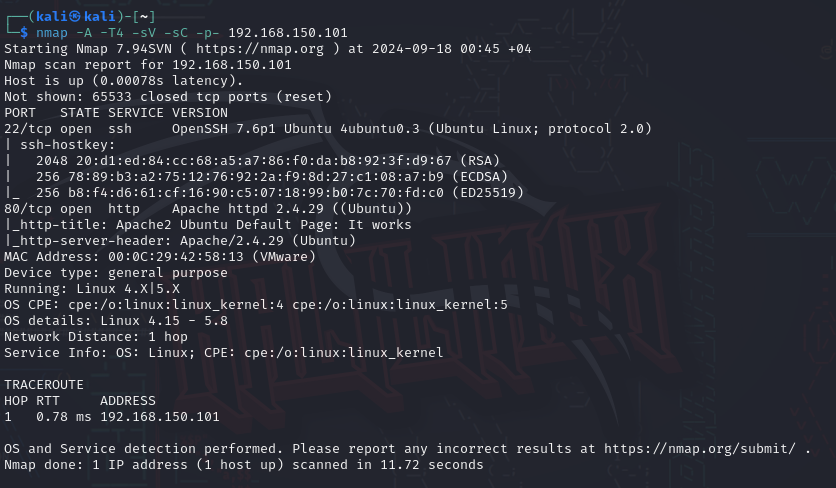


Photo 1

1

Exposure of Sensitive Information to an Unauthorized Actor

**Vulnerability ID: 1**

|  |  |
| --- | --- |
| Vulnerability name | Exposure of Sensitive Information to an Unauthorized Actor |
| CVSS | **Base Score**: 6.5 (Medium Risk) |
| CWE | CWE-200 |
| Severity | High |
| Risk level | High |

CWE-200: Information ExposureThe **Information Exposure** vulnerability refers to systems and applications exposing sensitive information to unauthorized individuals. This vulnerability stems from improper protection of data or other factors that result in the disclosure of confidential information.

Key Aspects of the Vulnerability:

1. **Unauthorized Data Access**: Users or systems may grant unauthorized individuals access to sensitive information, such as user account details, financial information, passwords, and more.
2. **Misconfiguration**: Incorrect configurations or weak security measures in systems and applications can lead to sensitive information being publicly visible.
3. **Data Transmission**: Transmitting data over unencrypted channels allows attackers to intercept and manipulate this information.

Risks:

* **Privacy Breaches**: Attackers gaining access to critical data can compromise the security of both the system and its users.
* **Reputational Damage**: The exposure of sensitive information can harm the reputation of organizations and disrupt customer relationships.
* **Unauthorized Operations**: Attackers can use the disclosed information to gain access to the system or execute malicious operations.

Mitigation Measures:

* **Data Encryption**: Data should be encrypted during both transmission and storage to ensure its protection.
* **Access Control**: Strict access control measures should be implemented to ensure only authorized individuals can access sensitive data.
* **Security Policies**: Clear and effective security policies regarding data protection should be established within the organization.

2

Impact: Unauthorized access to sensitive information poses a serious threat that can lead to data breaches, loss of trust, legal consequences, and financial losses.

Preventive Measures: To prevent this vulnerability, sensitive information should be properly protected, strong authentication and authorization systems should be implemented for user access, and data should be accessible only to authorized individuals.

Finding the machine's user password through sensitive endpoints in robots.txt and obtaining the user flag:

Four endpoints were discovered in the robots.txt file (Photo 2). Among these endpoints, the "shimishao" endpoint was identified using the "dirbuster" tool, which led to the discovery of the "system.log" file (Photo 3). Inside the file, the user's password was found (Photo 4). Finally, by using the obtained information, we successfully logged into the system (Photo 5) and found the user flag (Photo 7).

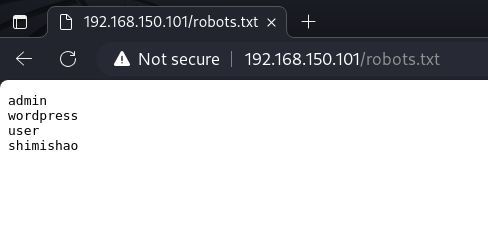
****

Photo 2

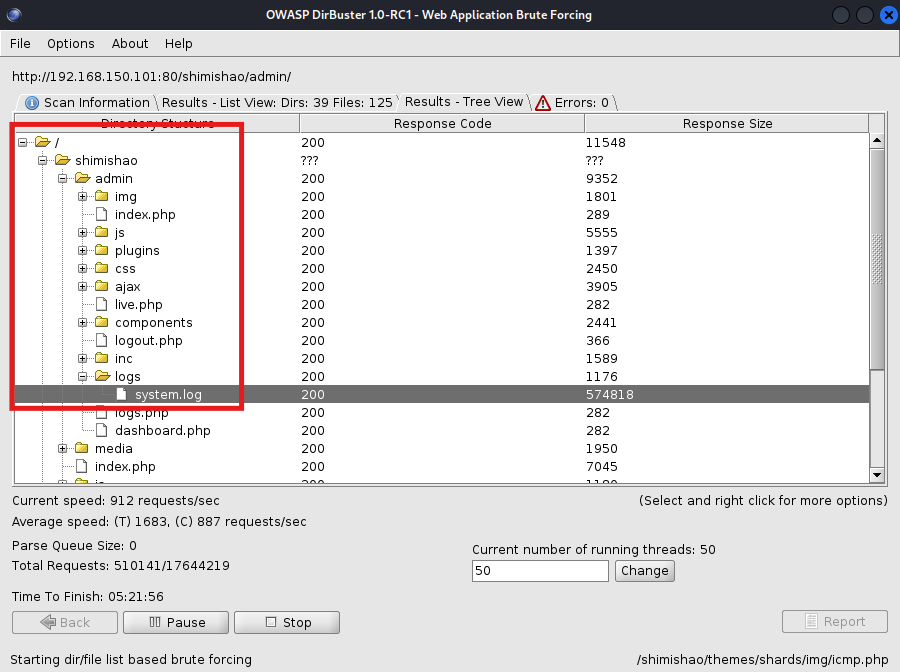


Photo 3

3

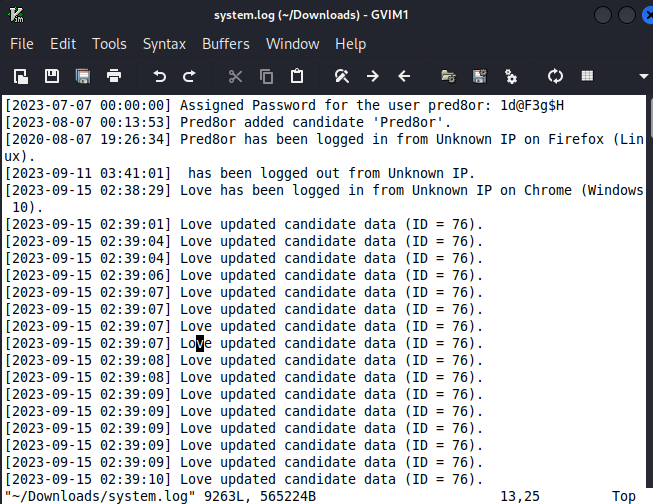


Photo 4

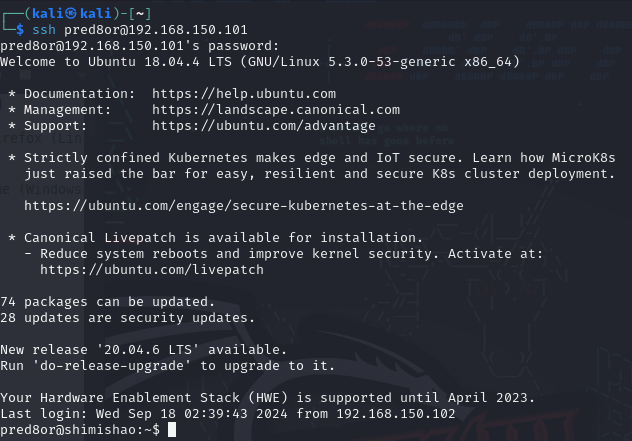


Photo 5

4

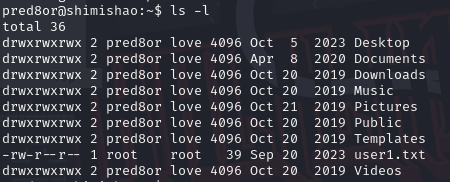


Photo 6

IMG_256

Photo 7

Detecting the misconfiguration in "pkexec policy" with LinPeas: LinPeas:

LinPeas is a script used to detect security vulnerabilities on Linux systems (Photo 8). This script assesses the system's security status by checking permissions, owners, active services, scheduled tasks, and other security weaknesses. It detected a misconfiguration in the "pkexec policy" (Photo 9). The "pkexec policy" is designed to enhance security by ensuring that only authorized users can execute certain commands. A misconfiguration in this policy can lead to significant vulnerabilities. The discovered vulnerability in the "pkexec policy" allowed us to escalate privileges to the root user (Photo 10).



Photo 8

5

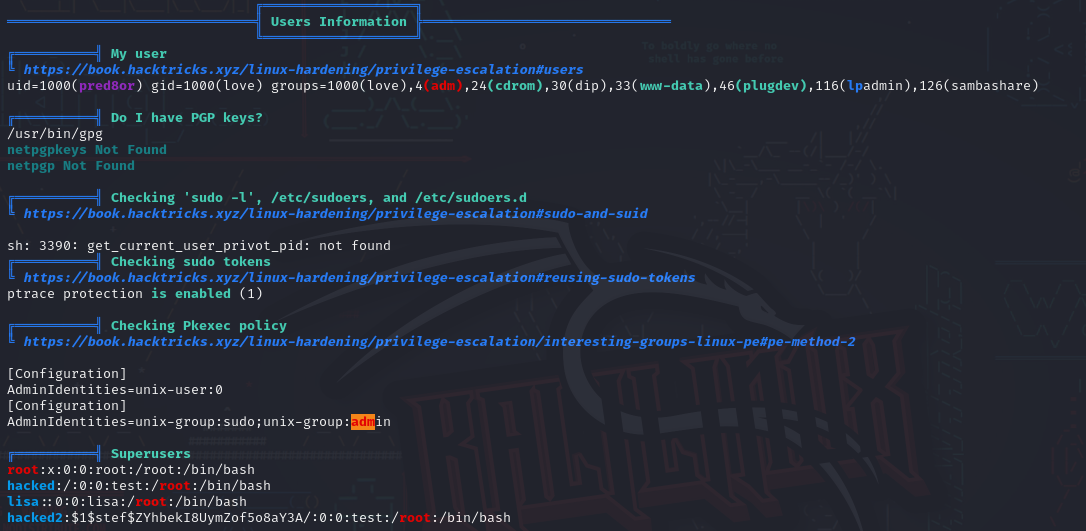


Photo 9

IMG_256

Photo 10

Conclusion

As a result of the penetration test, two vulnerabilities were identified: Exposure of Sensitive Information to an Unauthorized Actor and Local Privilege Escalation Vulnerability. One of these vulnerabilities (Local Privilege Escalation Vulnerability) poses a critical risk, while the other (Exposure of Sensitive Information to an Unauthorized Actor) carries a high-risk level.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Target** | **Low** | **Medium** | **High** | **Critical** |
| callobes | 0 | 0 | 1 | 1 |

6

|  |  |
| --- | --- |
| **Risk level** | **Risk Description** |
| **Critical** | Vulnerabilities at the critical level pose a serious threat to the organization's security and must be addressed as soon as possible. The required time frame for remediation is 7-14 days. |
| **High** | High-risk vulnerabilities present a real threat to the organization and must be resolved in a short time. Such issues directly impact the organization's security. The required time frame for remediation is 15-30 days. |
| **Medium** | Medium-level risks pose relatively lower threats but should still be addressed through specific actions. It is more appropriate to resolve these after handling critical and high risks. The required time frame for remediation is 1 to 3 months. |
| **Low** | Low-level risks pose very small or minimal threats, so their resolution is a lower priority compared to other issues. The required time frame for remediation is 3 to 6 months. |

7