Team name Ping of Death



Penetration Testing Report

## Table of Contents

[General Information 2](#_Toc10038)

[Vulnerabilities Identified as a Result of the Penetration Test 2](#_Toc10039)

[Conclusion 9](#_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).

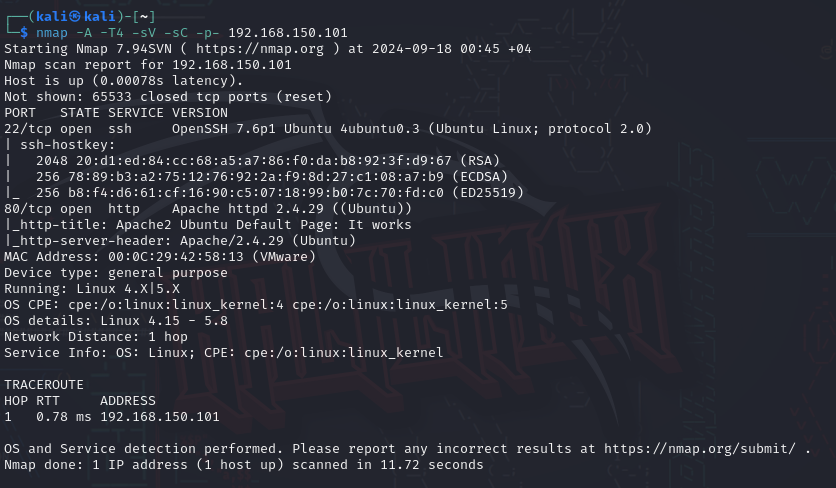


Photo 1

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 Exposure

**Description:**

The **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.

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).

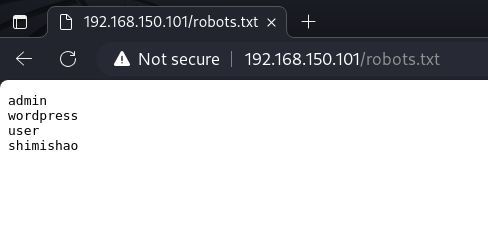
****

Photo 2

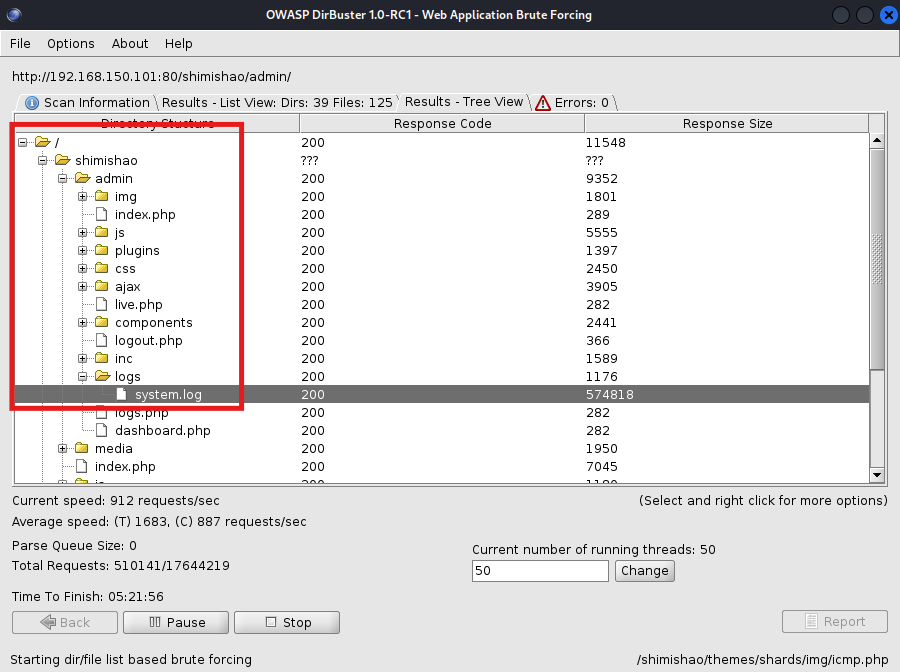


Photo 3

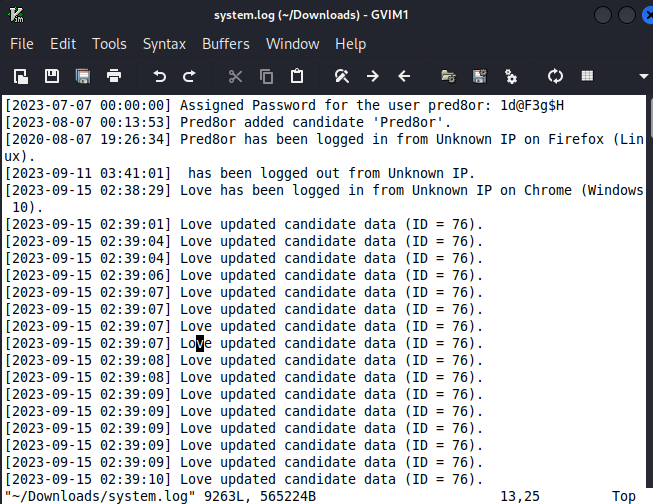


Photo 4

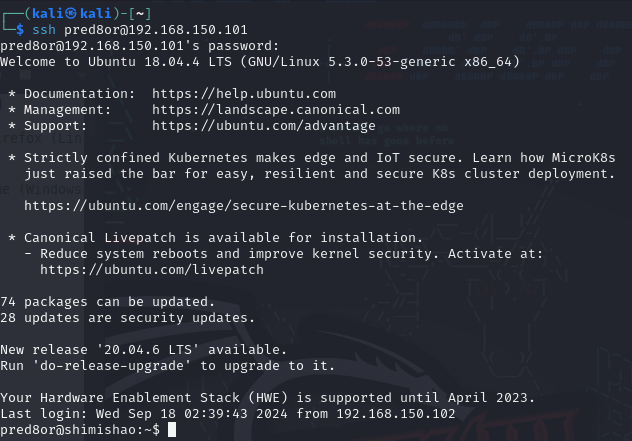


Photo 5

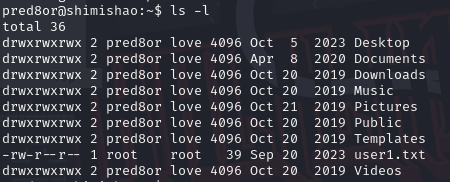


Photo 6

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

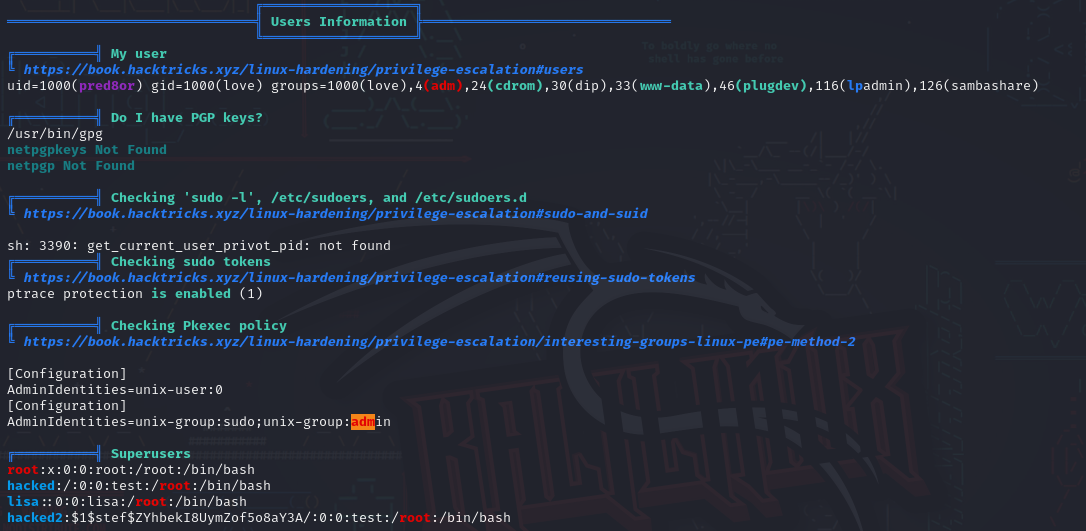


Photo 9

IMG_256

Photo 10

Local Privelege Escalation Vulnerability

**Vulnerability ID: 1**

|  |  |
| --- | --- |
| Vulnerability name | Local Privelege Escalation Vulnerability |
| CVSS | **Base Score**: 9.5 (Critical Risk) |
| CWE | CWE-276 |
| Severity | Critical |
| Risk level | Critical |

CWE-276: Incorrect Default Permissions  
**Description:**  
CWE-276 refers to the vulnerability where default permissions in systems and applications are not properly configured. Incorrect default permissions arise when the system fails to ensure security upon initial deployment.

Key Aspects of the Vulnerability:

1. **Incorrect Permission Assignment**: Systems or applications may allow unauthorized access and modifications due to improper permission settings during deployment.
2. **Unauthorized Access**: Default permissions can grant users or systems access to critical files or functions without proper authorization.
3. **Weak Configuration**: Misconfiguration of default permissions weakens network and system security.

Risks:

* **Data Loss**: Incorrect default permissions may allow unauthorized individuals to access sensitive information.
* **Unauthorized Operations**: Attackers may exploit incorrect permissions to perform malicious operations on the system.
* **Security Breaches**: Improper permissions can compromise system security, putting the organization's integrity at risk.

Mitigation Measures:

* **Proper Permission Configuration**: It is essential to correctly assign default permissions for systems and applications.
* **Access Control**: Implement role-based access control (RBAC) and ensure each user has specific permissions.
* **Security Audits**: Regularly review and audit permissions to identify potential vulnerabilities.

Access to the “root” user and discovery of the second flag:

By exploiting the vulnerability in the "pkexec policy", we escalated privileges to the root user and discovered the second flag in the "root.txt" file (Photo 11).

IMG_256

Photo 11

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 |

|  |  |
| --- | --- |
| **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. |