PENTEST REPORT

FACTS

Penetration Test Report

Target:	10.129.17.220 (facts.htb)
Date:	February 1, 2026
Author:	Pentester

Confidential Document

Contents

1 Executive Summary

1.1 1.1 Overview

This report documents the findings of a penetration test conducted against the host **Facts** (10.129.17.220). The objective was to identify exploitable vulnerabilities and assess the risk level of the target system.

The assessment resulted in a complete compromise of the system, achieving **Root** level access. The critical vulnerabilities identified included a Local File Inclusion (LFI) vulnerability within the Content Management System (Camaleon CMS). This flaw allowed for the exfiltration of sensitive SSH keys, providing initial system access. Furthermore, a misconfigured `sudo` permission on the `facter` utility facilitated privilege escalation to Root.

1.2 1.2 Scope

- **IP Address:** 10.129.17.220
- **Hostname:** facts.htb
- **Services:** SSH (22), HTTP (80), MinIO (54321)

1.3 1.3 Assessment Recommendations

The following high-level recommendations are proposed to secure the environment:

- **Patch Management:** Update Camaleon CMS to the latest version immediately to resolve the Path Traversal vulnerability (CVE-2024-46987).
- **Configuration Hardening:** Remove the `NOPASSWD` sudo permission for `/usr/bin/facter` or ensure it cannot load custom facts from writable directories.
- **Credential Hygiene:** Enforce strong passphrase policies for SSH keys to prevent offline cracking.

2 Network Penetration Test Assessment Summary

2.1 2.1 Summary of Findings

The following table summarizes the vulnerabilities identified during the engagement.

ID	Title	Severity	CVSS	Status
FIND-01	Local File Inclusion (CVE-2024-46987)	**High**	7.5	Exploited
FIND-02	PrivEsc via Sudo Misconfiguration	**Critical**	8.8	Exploited
FIND-03	Weak SSH Key Passphrase	**Medium**	4.0	Exploited

3 Internal Network Compromise Walkthrough

3.1 3.1 Reconnaissance

The engagement began with a TCP port scan using Nmap, which identified three open ports: SSH (22), HTTP (80), and MinIO (54321). Upon accessing `http://facts.htb`, the application was identified as **Camaleon CMS** version **2.9.0**.

3.2 3.2 Web Exploitation (Local File Inclusion)

During enumeration of the CMS, a Path Traversal vulnerability (CVE-2024-46987) was identified in the `download_private_file` action. This vulnerability allows an authenticated user to traverse the file system and read arbitrary files.

Exploit Vector: The vulnerability was leveraged to access the SSH private keys stored in user home directories. The following request was used to retrieve the key for the user `trivia`:

```
http://facts.htb/admin/media/download_private_file?file=../../../../../../home/
    trivia/.ssh/id_ed25519
```

The downloaded key was encrypted. Using `john` (John the Ripper), the passphrase was successfully cracked:

- **Key:** id_ed25519
- **Passphrase:** dragonballz

With the cracked key, SSH access was established as the user `trivia@facts.htb`.

3.3 3.3 Privilege Escalation (Root)

Enumeration of sudo privileges (`sudo -l`) revealed that the user `trivia` could execute `/usr/bin/facter` as root without a password.

```
(ALL) NOPASSWD: /usr/bin/facter
```

The `facter` utility allows loading custom "facts" (Ruby scripts) from a specified directory. A malicious fact was created to spawn a privileged shell:

```
echo ’exec("/bin/bash")’ > /tmp/root.rb
sudo /usr/bin/facter --custom-dir /tmp
```

Listing 1: Root Exploitation

This command executed the Ruby script as root, resulting in a full system compromise.

4 Technical Findings Details

4.1 FIND-01: Local File Inclusion (CVE-2024-46987)

Description:
The `download_private_file` action in the `Admin::MediaController` of Camaleon CMS 2.9.0 is vulnerable to path traversal. The application takes the user-supplied `file` parameter and concatenates it to a base directory path without sufficient sanitization. This allows an attacker to navigate outside the intended directory using `../` sequences and read sensitive system files.

Remediation:
Upgrade Camaleon CMS to version 2.9.1 or later. Alternatively, implement strict input validation on the file parameter to ensure it does not contain traversal characters or reference files outside the allowed storage directory.

4.2 FIND-02: Privilege Escalation via Facter

Description:
The `facter` utility was configured in `/etc/sudoers` to run without a password. Facter supports the `-custom-dir` flag, which loads and executes all Ruby scripts found in a user-controlled directory. This allows for trivial arbitrary code execution as root.

Remediation:
Remove the sudoers entry for `/usr/bin/facter`. If the functionality is required, wrap the command in a script that hardcodes specific arguments and prevents the use of `-custom-dir` or `-external-dir`.

A Appendix

A.1 A.1 Exploited Hosts

Host	Scope	Notes
10.129.17.220	facts.htb	Full Root Compromise

A.2 A.2 Compromised Users

Username	Type	Method
trivia	System User	SSH Key Theft (LFI)
root	System Admin	Sudo / Facter Injection

A.3 A.3 Loot / Flags

Item	Location
User Flag	`/home/trivia/user.txt`
Root Flag	`/root/root.txt`