Penetration Test Report

Spice Hut — Web Server Assessment

Target: `10.130.180.94` / `startup.thm`
Test Type: Black Box
Methodology: PTES

Time Frame
March 28 – March 29, 2026

CONFIDENTIAL

Prepared by
Koussay Dhifi
March 29, 2026

Contents

1 Executive Summary

1.1 Objective of the Test

We are going to evaluate the security posture of Spice Hut, a startup that isn't sure about its security, to evaluate the quality of its developers and we need to access the server and escalate to root.

1.2 High-Level Findings

- Unauthorized access to the FTP server is allowed, and therefore we can upload a web shell that lets us access the whole server remotely.
- A pcap file that is lurking inside the machine that contains credentials of one of the accounts named Lennie.
- An old version of a software named pkexec (0.15) with some specific privileges lets us impersonate the root user, and with that we can take over the whole machine.

1.3 Overall Risk Level

Risk Level	Recommendation
HIGH / CRITICAL	Immediate remediation is recommended

1.4 Business Impact

All of this could allow attackers to access the server and deface the web application (change its content) and access sensitive information of potential clients and workers, which will cause financial, reputational and legal damage.

2 Scope & Engagement Details

Field	Details
Target	The website's server: `10.130.180.94` / website: `startup.thm`
Time Frame	March 28 – March 29, 2026
Rules of Engagement	No denial-of-service attacks. Basically we won't be attacking the availability of the website.
Testing Type	Black Box (We know nothing)

3 Methodology

For the methodology we used PTES (Penetration Testing Execution Standard).

- **Reconnaissance:** Performed passive reconnaissance but did not find much.
- **Scanning & Enumeration:** Nmap scans involved all ports to make sure there isn't any useful service lurking within some unknown port, to look for any outdated versions. We also did directory scanning using Gobuster to make sure there isn't any exposed resource, and we found `/files` that accesses the FTP server.

- **Exploitation:** Found unauthorized access in the FTP server, and with that we uploaded a PHP web shell using FTP and executed it with our browser in `/files`.
- **Post-Exploitation:** Found an interesting folder named `incident` that contains a `.pcapng` file. After analyzing it, we found that it is about a previous incident that happened. I checked what the hacker did and he inserted some credentials that he may have previously known. I also found that pkexec is SUID active, created by root, and has an old version of 0.15 which is vulnerable to PwnKit (CVE-2021-4034).
- **Privilege Escalation:** Used the credentials within the `.pcapng` file to escalate to the user named Lennie, and after that exploited CVE-2021-4034 to escalate to root.

4 Findings

4.1 Finding 1 — Exposed Web Directory `/files`

Severity	HIGH
Description	`/files` in the web app — it should be only authorized users that can access such a page.
Impact	Allows an attacker to access confidential files from the FTP server and can run some files.
Remediation	Disable normal access and add some kind of authorization using JWT or sessions.

4.2 Finding 2 — Unauthorized FTP Access

Severity	CRITICAL
Details	vsftpd 3.0.3 on Port 21 — FTP allows anonymous login, exposing directories and allowing us to write on them.
Impact	This allows an attacker to upload malicious content.

Remediation:

- Disable anonymous login ASAP.
- Enforce strong authentication.

4.3 Finding 3 — Left Artifact (`.pcapng` file) Containing Credentials

Severity	HIGH
Details	A `.pcapng` file lurking inside the `incident` folder on the server.
Impact	After analyzing the capture, we found credentials of the user Lennie that were inserted by a previous attacker, which allowed us to escalate to that user.
Remediation	Remove that `.pcapng` file or make it readable only by root.

4.4 Finding 4 — Vulnerable `pkexec` Binary (CVE-2021-4034 / PwnKit)

Severity CRITICAL
Details pkexec version 0.15, SUID active and created by root — vulnerable to PwnKit (CVE-2021-4034).
Impact This allows any user with a shell on the system to escalate to root.

Remediation:

- Update pkexec to the latest version.
- Remove the SUID bit from pkexec if it is not that important.

5 Attack Path / Kill Chain

Phase	Details
Initial Access Vector	Anonymous FTP login on `10.130.180.94`.
Steps to Gain Foothold	Uploaded web shell via FTP and executed it on the browser; executed commands remotely after setting up the listener.
Privilege Escalation Path	Leveraged a left artifact (`.pcapng` file) to take credentials of the user Lennie and escalate to it. Then leveraged CVE-2021-4034, which allowed us to escalate to root.
Final Impact	Full control over the server, access to all data within the server since we are root. We found the secret recipe of Spice Hut which is in a file called `recipe.txt`.

6 Post-Exploitation

Phase	Details
Starting Point	Low-privilege shell (`www-data`) on host `10.130.180.94` obtained via FTP web shell upload.
Lateral Movement	Leveraged from an artifact (`.pcapng` file) that captures the sequence of a previous attack that contains legitimate credentials of the user Lennie.
Privilege Escalation	Exploited CVE-2021-4034 to escalate to root because pkexec was SUID set, created by root, and is an old version of 0.15.
Persistence	No persistence was performed since the goal was to just access root, but it was possible to be persistent using some cron jobs and implementing a backdoor.
Data Access / Impact	Full access to everything and full management of everything within the business since we are root.

7 Conclusion

Overall Security Posture: The target website/server has potential high vulnerabilities that are catastrophic to the security posture — all of that because of the two findings mentioned within the report.

Key Risks:

- Unauthorized FTP access
- Exposed web directory without authorization
- Left artifacts with old software

Recommendations:

- Add authorization for FTP immediately.
- Add authorization for the `/files` resource.
- Remove the `.pcapng` file or make it readable only by root.
- Update pkexec to the latest version and remove SUID for root if not that important.

8 Appendix

8.1 Nmap Scan

Host	Port	Proto	Name	State	Info
10.130.180.94	21	tcp	ftp	open	vsftpd 3.0.3
10.130.180.94	22	tcp	ssh	open	OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 Ubuntu Linux; protocol 2.0
10.130.180.94	80	tcp	http	open	Apache httpd 2.4.18 (Ubuntu)

Metasploit Hosts:

Address	Name	OS Name	OS SP	Purpose
10.130.180.94	startup.thm	Linux	3.X	server

8.2 Gobuster Directory Listing Results

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.130.180.94
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/mohsen2/Downloads/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
```

```
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/files                (Status: 301) [Size: 314] [--> http
    ://10.130.180.94/files/]
/index.html           (Status: 200) [Size: 808]
/server-status        (Status: 403) [Size: 278]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```

8.3 Evidence Screenshots

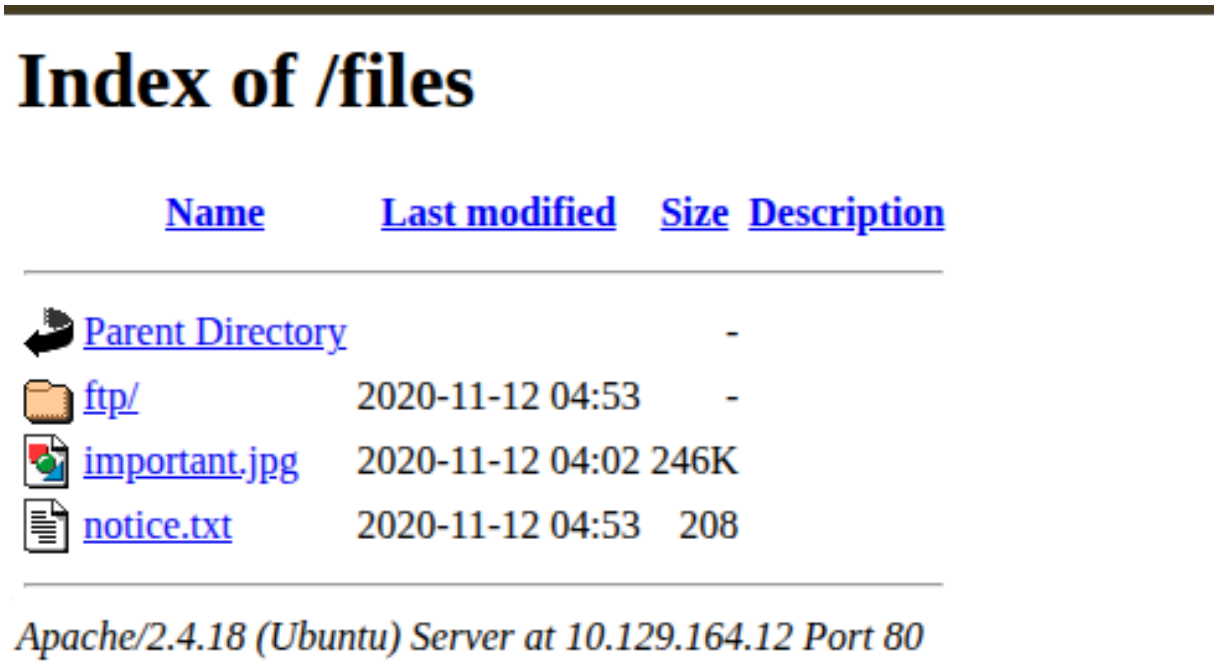

Figure 1: Screenshot that demonstrates the files directory is exposed within the browser.

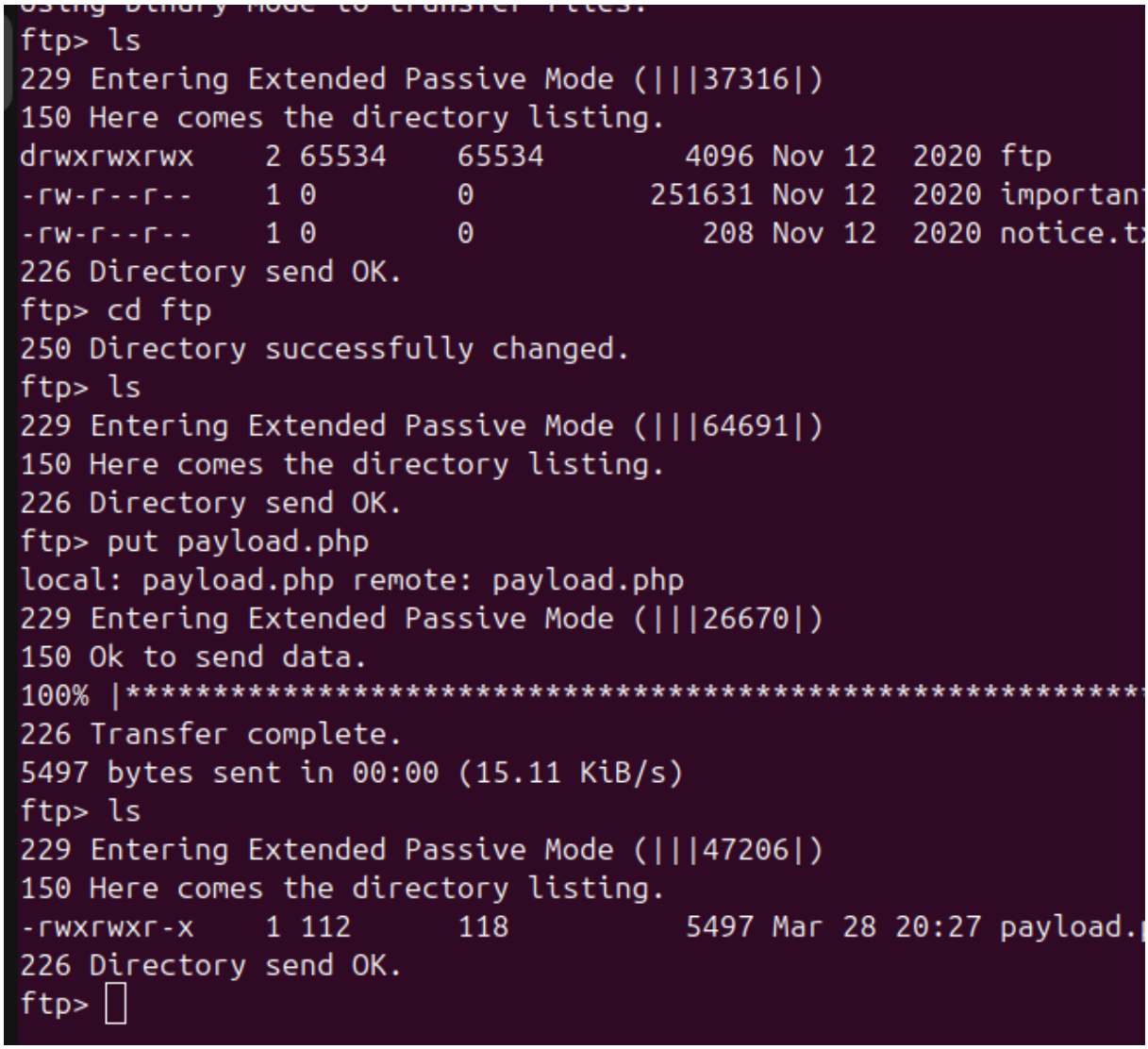

Figure 2: Screenshot that demonstrates unauthorized access to the FTP server.

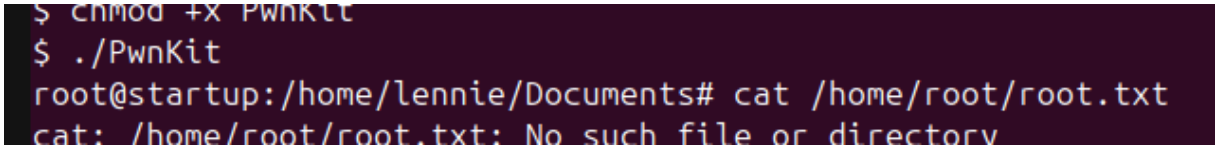

Figure 3: Screenshot that demonstrates root access after exploiting PwnKit.