Assignment Description

2026

Contents

1 Task description

FuzzyCorp is a startup that just launched their first product, a web based password manager. It was designed with security in mind, but it's still in beta. You were tasked to test the security of their server.

`10.0.2.8`

The password manager, which is their flag-ship product, is running on this server as well.

The **ansible**-user on this server is **out-of-scope**, it is being used by us to build the environment. On the linux-server, the bash-history is disabled.

Everything can be solved with this wordlist: privesc_wordlist.txt

2 Deliverables

We expect a comprehensive report detailing your methodology and findings.

Deadline

The final report must be submitted by **May 31th, 2026, 23:59** via CTFd.

- **Filename:** `pentesting_report_LastName1_LastName2.pdf`
- **Format:** Strictly PDF format only.

Oral Exam

You will be expected to explain and justify your reported vulnerabilities, their rating, mitigation steps, attack vectors, lateral movement steps, privilege escalation techniques, and post-exploitation steps during the oral examination.

Infrastructure Access

Dedicated Student Kali VMs are allocated per team and accessible via Web SSH. You are encouraged to install custom tools and maintain your working environment here.

3 CTFd & Flag Policy

Flags are hosted on CTFd to track technical progress.

- **Submission:** Only **one** team member needs to submit the flag. However, **both** members must be prepared to explain the exploitation path in detail.
- **Grading:** Flags prove task completion but are not your final grade.
- **Reporting:** Flags should not be the focus of the report. If included, they belong strictly in an **Appendix**.

4 Connection Tutorial

4.1 Provisioned Materials

You should have received an email containing the following:

- A **WireGuard configuration file** for every member of the team.
- Credentials for your **Kali VM** on `https://webssh.vuln.at`.
- A pre-deployed **SSH Key** for your Kali VM.
- An **SSH configuration** (`ssh-config`) to facilitate direct connection.

4.2 VPN Access

1. Copy your VPN config (`firstname_lastname.conf`) to `/etc/wireguard/`.
2. Open the connection using WireGuard:

```
wg-quick up firstname_lastname
```

4.3 Kali VM Access

- **Web SSH:** Access your instance directly via webssh.vuln.at.
- **Direct SSH:** Connect to the VPN first. Place the provided `ssh-config` content inside your `.ssh/config` file. Then connect via:

```
ssh ptl_kali
```

Kali VM Behavior

Your Kali VM boots automatically upon your first connection via Web SSH.

- **Boot Time:** Expect a 1–2 minute delay for the initial boot.
- **Auto-Shutdown:** The VM shuts down **5 minutes** after the last session is closed.
- **Inactivity:** Connections are terminated and the VM is shut down after **3 hours** of inactivity.
- **Note:** If the VM is already running (via Web SSH), you can connect to it via standard SSH over the VPN.