# Assignment Description

Network Penetration Testing Lab

Pentesting Lab Administration

2026

**Abstract**

This assignment simulates a real-world penetration test against a hybrid infrastructure. The objective is to identify, exploit, and document vulnerabilities within a **Windows Active Directory (AD) Environment** and a standalone **Linux server**.

## Contents

# 1 Deliverables

Students must submit a comprehensive report detailing their methodology and findings, in accordance with professional penetration testing standards.

**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.

**Reporting Tool**
We recommend using SysReptor. It provides a structured format that aligns with industry expectations (Executive Summary, Vulnerability Rating, Remediation).

**Oral Exam**
Your report is your primary defense. 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.

# 2 Rules of Engagement (RoE)

## 2.1 Strictly Prohibited Actions

Failure to comply with these rules may lead to disqualification or disciplinary measures.

- **Denial of Service (DoS):** Any attack that disrupts service availability or infrastructure stability.
- **Credential Modification:** Do **not** change passwords on any system.
- **Inter-team Interference:** Do not target, block, or interfere with other teams' environments.
- **Unauthorized Deletion:** Do not delete files you did not create. Do not remove or modify system flags.
- **Password Cracking Policy:** All crackable hashes in this lab are solvable using the rockyou.txt wordlist.
- **Tool Awareness:** Ensure you understand the impact of your tools (e.g., account lockout, password modification, etc.).

## 2.2 Environment Integrity & Cleanup

You are responsible for leaving the lab as you found it.

- **Reversibility:** Instead of deleting critical files, **rename them temporarily** (e.g., `file.bak`).
- **Post-Exploitation Cleanup:** After successfully documenting a finding, you must remove all artifacts, including created files, web shells, and temporary user accounts.

# 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.

### 4.4 Enumeration Check

Perform an initial sweep to ensure targets are reachable:

```
nmap -sn 192.168.X.0/24
```

Report any connectivity issues immediately via the lab communication channel.