Lab 7: The Inside Job

1 Introduction

Welcome to the fold, Detective.

You successfully navigated the silent stakeout and proved you have the eyes to see what others miss. You are no longer an applicant; you are a fully badged member of **The Baker Street Society**. But eyes alone cannot secure the city. Sometimes, we need hands.

We have a new assignment. We have placed you inside the perimeter of a client's internal network. The client believes their digital vault is impenetrable. We believe they are arrogant.

Your mission is a classic **Internal Audit**. You have access to a machine on the local network. Your task is to map the room, identify the active machines listening in the silence, and find the open doors they forgot to lock.

Intelligence suggests their internal hygiene is poor. We suspect multiple services have been left unsecured or misconfigured. You must treat every open port as a potential entry point.

Find the machines. Interrogate the services. Steal the Flag.

2 The PI Code (Active Measures)

In your last assignment, you were strictly forbidden from touching the glass. That restriction has been lifted, **for this network only**.

Authorized Aggression. You are authorized to use active scanning tools against the targets within the designated IP range. You may knock on every door (port scanning) and rattle every handle (service enumeration). The goal is to be thorough.

Scope of Engagement. Do not mistake this authorization for a blank check. You remain confined to the specific internal network provided for this operation. Attacking any external infrastructure or fellow Agents' machines will result in immediate disavowal and expulsion from **The Baker Street Society**.

3 The Setup

The Society has established a secure foothold inside the perimeter—a "Jump Host" that sits on the edge of the target network. You must connect to this machine to launch your internal audit.

3.1 Establishing the Connection

You will access the Jump Host using the SSH protocol. Use the following credentials to authenticate your session:

- **Jump Host IP:** `130.208.246.239`
- **Username:** Your RU username (e.g., if your email is `student23@ru.is`, use `student23`).
- **Password:** `icyb2025lab7!#?`
  (Note: This is a shared agency key used by all operatives for this mission.)

3.2 The Target

Once you have successfully breached the Jump Host, your sights must turn to the internal network. Intelligence indicates the vulnerable machine—the vault containing the flag—is located at:

`130.208.246.241`

All scanning, enumeration, and exploitation attempts must be directed at this specific target IP from the Jump Host.

4 The Toolkit

An operative is only as good as their tools. For this job, **The Baker Street Society** has unlocked the armory.

The Mapper (Nmap). This is your sonar. You will use it to ping the darkness and see what replies. Use it to identify live hosts on the network and determine which ports are open and listening. A skilled agent knows that a simple scan is loud; a precise scan is deadly.

The Master Keys (Enumeration Tools). Finding an open port is useless if you don't know what is running behind it. You must inspect the protocols. You will need tools (like `smbclient`, `nc`, or `curl`) to query the services directly. You are looking for the careless mistakes: default settings, anonymous access, or unprotected directories.

5 The Job

You start on the Jump Box. From there, the network is a black void. You must illuminate it.

First, perform a **Network Sweep**. Identify every active IP address on the local subnet. Once the targets are revealed, launch a detailed **Port Scan** against them. Do not assume anything; you must identify *every* service running.

Next, shift to **Full Enumeration**. Do not focus on a single protocol. Interrogate every listening service to determine its version and configuration. Is it a Web Server? A Database? A File Share? Check for access. Deep within one of these services lies the sensitive data: **The Flag**. Retrieve it.

6 The Dossier

The Baker Street Society pays for results, but we reward intelligence. To close this contract, you must submit a Field Report containing the following:

The Map: A detailed list of the hosts you found, the open ports associated with them, and a brief description of the service running on each port.

The Breach: Documentation of exactly which vulnerability you exploited to access the Flag, including the specific commands used.

The Bounty (Bonus): The Baker Street Society suspects there is more than one way to breach this network. A standard operative finds one door; a master operative finds them all. If you can document **multiple distinct vectors** or methods to access the target or find the flag, your compensation (grade) will be increased.

Get in. Map the room. Get the data.