Lab 6: The Silent Stakeout

1 Introduction

You want the badge? You have to earn it. You have applied for membership in **The Baker Street Society**, the city's most exclusive league of Private Investigators. We don't hire muscle; we hire eyes. We hire minds that can see the invisible threads connecting people, money, and data.

Your final initiation test is simple: **The Silent Stakeout.**

In the digital age, everyone lives in a glass house, yet they believe their blinds are drawn. Your task is to select a target, a real world corporate entity, and build a complete profile on them using only **Open Source Intelligence (OSINT)**.

We are not assigning you a specific list of evidence to find. Real detective work is not a checklist. Instead, we demand **breadth and variety**. You must scour the public archives of the internet, social forums, and digital footprints to uncover as many different types of intelligence as possible. The more varied your findings are, the higher your standing will be.

Prove to us that you can identify the pressure points. Prove that you are worthy of **The Baker Street Society**.

2 The PI Code

Every PI has a code. Cross the line, and you don't just lose the job; you go to jail.

Passive Reconnaissance Only. You are an observer, not an intruder. You must **NOT** perform any active scanning (such as Nmap or Nessus), password guessing, or social engineering. Ideally, you should not even send a packet directly to the target's servers if it can be avoided. Stick to public repositories, search engines, and third-party data sources.

Do Not Disturb. Silence is your greatest asset. You must not disrupt the company's operations, harass employees, or interact with their systems in any way that leaves a log entry. If you leave a footprint, you have already failed the assignment.

Legal Compliance. We operate in the shadows, but we stay within the law. Do not access data that requires breaking a lock (such as cracking a password) to view. If it is public, it is fair game. If it is private, walk away.

3 The Subject

The Baker Street Society grants you the freedom to choose your own mark, but requires you to operate locally. You must select a real-world corporate entity based here in **Iceland**.

This choice is critical; do not pick a target at random. You require a target with a visible digital footprint. Avoid small, local operations with no online presence, as they will not yield enough data for a proper dossier. Instead, seek out an Icelandic company that interacts with the world. A target with a heavy footprint will always leave tracks; your job is simply to find them. Once you have acquired your target, proceed to the stakeout.

4 The Stakeout

Your goal is to paint a complete picture of the target. While we reward creativity over checklists, The Society specifically requests that you map out the **Infrastructure and Technical Details** of the company.

Look beyond the surface. We want to know how their digital house is constructed. Identify their hosting providers and map their digital real estate. Check DNS records for clues about their email providers and verification systems. Attempt to identify the **Technology Stack** they utilize. The more technical depth you can provide regarding their infrastructure, the higher your standing will be.

5 The Sting

Information is useless without application. Now that you know their secrets, you must determine how they can be used against them.

Based on the intelligence you gathered, you must draft a hypothetical **Plan of Attack**. This is a theoretical exercise only. Describe how a motivated competitor could disrupt this company's activities using entirely legal means.

Your plan must be actionable. Detail the **Method** you would use, the **Timing** of the strike, and the estimated **Budget** required to pull it off.

6 The Dossier

To close this case, you must submit a professional dossier to **The Baker Street Society**.

This report should include the **Intel Report**, a structured collection of all the information you found, categorized clearly. It must also include your **Attack Plan** detailing the hypothetical disruption strategy. Finally, include a brief **Reflection** on the investigation: how easy was it to find this information, and what does it reveal about the target's privacy?