# CYBR430, Penetration Testing and Incident Response Week 2 Lab – Open-Source Collection

Using passive collection techniques as discussed in your readings and listed under the resources for the week see what information you can find out about Happy Accident Labs. You will complete this lab from any internet connected computer. There are some questions below for you to answer but there may also be other information you find which could also be useful in this penetration test. Be sure and take good notes.

Happy Hunting…

Answer each question using research you conduct on the web and using various information gathering tools. Remember, this is passive collection, you will only need an internet connected computer to answer the below. **Provide both the answer, a description of your process to find the information, and any applicable screen shots.** Don’t know where to start, hmmm – what would be a good guess for a domain name?

What is the domain name for Happy Accident Labs?

The domain name is http://happyaccidentlabs.com

Who is the domain name provider?

GoDaddy.com

Graphical user interface, text, application

Description automatically generated

Do they have an email provider or do they provide this service internally? If external who is the provider?

This service is provided internally.

Who might be a good technical point of contact?

Domains by Proxy

What might be the address of their company? Phone number(s)?

2155 E Warner Rd, Tempe, Arizona, 85284, US  
+1.480-624-2599

What type of building are they in?

They’re in an office building with a property size of 150,000 SF and a Lot size of 17.02 Acre.

What is the area like around their offices? Can you think of any opportunities for Social Engineering encounters?

Around the office building is a recreational area that consists of a basketball court, a volleyball court and multiple sitting areas that is more conducive for kick off social engineering.

Are there any email addresses you found?

russells@happyaccidentlabs.com

Do you know anything about their network or potential access to their network?

Their job openings for a System Administrator does list what type of Operating Systems the company is running on. It also shows the type of firewall they’re running which seems to have some XSS Security Vulnerabilities.

Did you find any other potentially useful information?

The Happy Accident Labs website is not secure. It is using the http instead of https.