# **Week One Lab: Footprint and Reconnaissance**

In this lab assignment, you will perform the tasks you have been taught in the Guided Practices (iLabs content form EC-Council). You may review your prior labs to supplement your understanding of the material. This lab reinforces your learning and knowledge and increases material retention through hands-on application.

# How does this practical lab apply in the real world?

During the reconnaissance phase, an ethical hacker collects as much information as possible about a target. This phase should be allotted significant time since it provides the starting point for all later phases.

Passive Reconnaissance is used to gather information without directly interacting with the target system. This process can include techniques such as looking through discarded documents, getting information from discarded devices, wardriving, and collecting Open-Source Intelligence (OSINT) information. An ethical hacker is less likely to be detected in this phase since they are not interacting with the target.

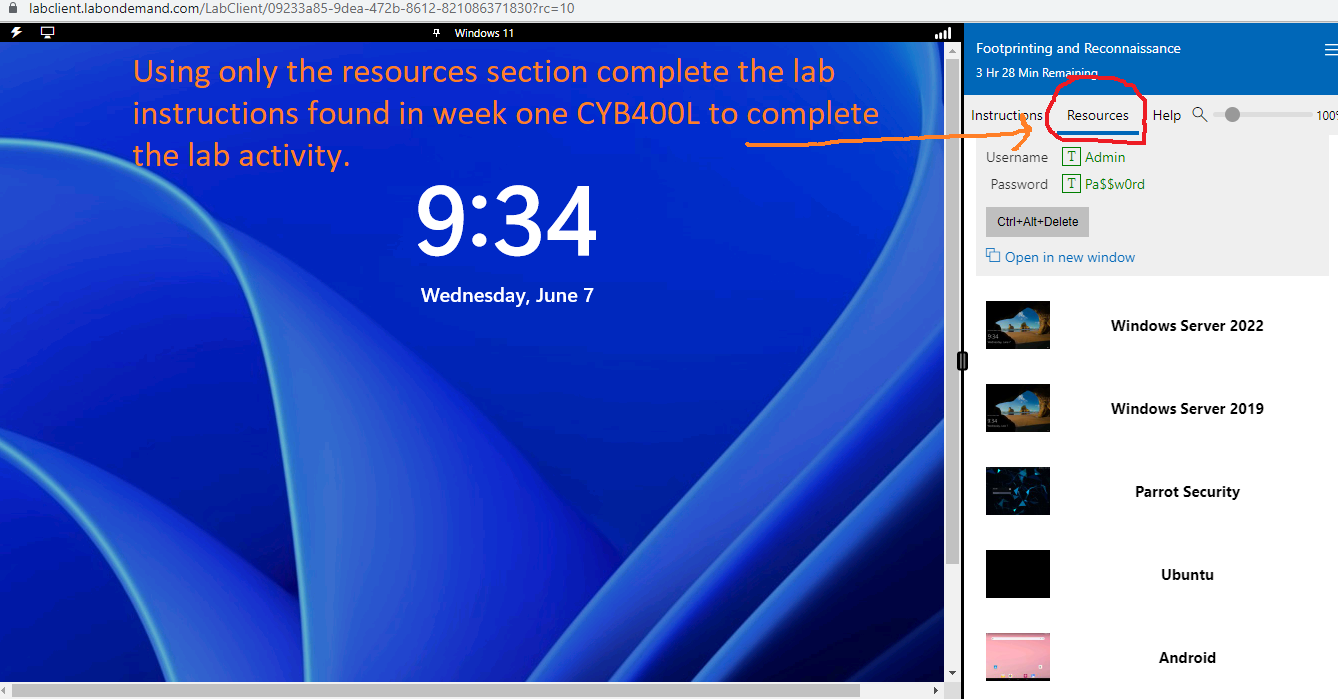
Active Reconnaissance involves interacting with the target directly, so it is more likely that the ethical hacker will be discovered and that the system admins will take action to prevent further reconnaissance steps.

In this activity, you will focus on collecting information about a target using OSINT. Document your findings thoroughly, using screenshots and well-written paragraphs that describe the purpose of the tools you used, the options you set, and the interpretation of the results.

|  |
| --- |
| Please check with your instructor what organizations you can choose to do reconnaissance on. Please note that all techniques that you will be using in this exercise are to be used for learning purposes only, and all information that results from this exercise is to be included in the report without any further action to be taken against the “target”.  Also note that, due to the risk of unjustifiably increasing interest for collecting information on ECPI University, instructors, etc., you are not permitted to use ECPI University, current or past instructors, current or past employees, current or past students as potential targets for this exercise. |

# Resources Needed (PLEASE READ FIRST)

This lab assessment covers Modules 01 and 02 from your EC Council lab content. Thus, all resources you will need will be from your iLabs, your textbook, and your notes. Please remember that you will only use the iLabs resources for the lab.



# Level of Difficulty

Moderate

# \*\*Important\*\*

**Please note the following guidance for success**:

1. This Assessment should be performed using any browser.
2. All screenshots should reflect your own work and should have the date, time and user information (name, student ID) clearly displayed in the screenshot.
3. All takeaways/inferences you can make about your target based on the reconnaissance should be clearly expressed (using complete sentences and without excessive use of bullet points) and should be in your own words and result from you doing the work.
4. Please remember that you will also complete a summary of the lab when completed this will be in paragraph format of 3-5 complete sentences if you submit a summary that is less than a complete paragraph, points will be deducted. Please remember to include screenshot for each Task.

# Instructions

Complete the following lab tasks in the **Footprinting and** **Reconnaissance** iLab Module:

***Tasks:***

1. Perform footprinting through search engines
   * Gather information from FTP search engines
   * Gather information from IoT search engines
2. Perform footprinting through web services
   * Gather personal information using PeekYou online people search service
   * Gather information using deep and dark web searching
3. Perform website footprinting
   * Gather information about a target website using Photon
   * Gather information about a target website using Central Ops
   * Extract a company’s data using Web Data Extractor
   * Mirror a target website using HTTrack Web Site Copier
   * Gather information about a target website using GRecon
4. Perform email footprinting
   * Gather information about a target by tracing emails using eMailTrackerPro
5. Perform DNS footprinting
   * Gather information of subdomain and DNS records using SecurityTrails
6. Perform footprinting using various footprinting tools
   * Footprinting a target using Maltego
   * Footprinting a target using FOCA
   * Footprinting a target using BillCipher

**Example for Deliverables**

**This is an example only and does not reflect the requirements of this assignment. Use this as a template for how to format and complete deliverables one through six.**

**Task 1 (EXAMPLE):** Perform DNS footprinting using a tool of your choice.

A screenshot of a computer

Description automatically generated

**Deliverable for Task One (EXAMPLE)**

Task 1:

* The implementation of tools such as DNS dumpster allows for finding organizational resources to contribute to an effective mapping strategy for creating a map to use to pen test an organization.
* **Threat:** DNS Dumpster identified a Microsoft server using HTTPAPI/2.0, which has an IP address of 121.171.142.220 and is located in South Korea. The exploits available for this protocol include Banner Disclose vulnerable on WAP servers.
* **Mitigation** The Microsoft-HTTPAPI/2.0 vulnerability can be mitigated by disabling the server Header in the registry key via HKEY\_LOCAL\_MACHINE.
* **Summary:** This site has various potential vulnerabilities that need to be remediated and then verified. The use of DNS dumpster provided a DNS snapshot at a moment in time that indicated possible potential threats that the United Nations could possibly face. It is important to understand each threat and make recommendations to prevent such threats. There are more vulnerabilities within this organization that should be mitigated and then reverified as corrected.

#### Deliverables Footprinting and Recon: Complete this section using the example above as a template for each answer.

Task 1:

Task 2:

Task3:

Task4:

Task5:

Task6: