**PAHSE ONE RECONAISSANCE**

Step 1: Search for the Website Using an OSINT Tool

1. Choose an OSINT Tool: You can use tools like [whois.com](https://www.whois.com/) to gather information about the domain "Learn About Security."
2. Perform a WHOIS Lookup:
   * Go to the WHOIS website.
   * Enter the domain name (e.g., learnaboutsecurity.com) in the search bar.
   * Take a screenshot of the results, which typically includes information like the domain registrar, registration dates, and contact information.

Step 2: Discover DNS Information

1. Use DNS Lookup Tools: You can use tools like nslookup or online DNS lookup services (e.g., MXToolbox).
2. Perform DNS Lookup:
   * Open a terminal or command prompt.
   * Run the command: nslookup learnaboutsecurity.com or use the DNS lookup tool.
   * Collect the DNS records, including A records (IP addresses), MX records (mail servers), and any other relevant information.
   * Take a screenshot of the results.

Step 3: Identify Web Technologies

1. Use Web Technology Scanners: Tools like [BuiltWith](https://builtwith.com/) or [Wappalyzer](https://www.wappalyzer.com/) can help identify the technologies used on the website.
2. Scan the Website:
   * Go to the chosen tool and enter the domain name.
   * Review the results to see the technologies (e.g., CMS, frameworks, hosting providers).
   * Take a screenshot of the identification results.

Step 4: Documentation and Reporting

* As you perform each step, make sure to document your findings. Include:
  + The commands you used (e.g., WHOIS, nslookup).
  + Screenshots of the results.
  + Any observations or notes about the information you gathered.

Helpful Tips

* Stay Organized: Create a folder for your project and save all screenshots and documents in it.
* Report as You Go: This will help you keep track of your progress and ensure you meet the project requirements.
* Be Thorough: Even if you don’t find much information, document what you did and the results.

Finalizing Your Report

Once you have completed all the steps, compile your findings into a report format that includes:

* An introduction to the reconnaissance phase.
* The results of your WHOIS lookup.
* The DNS information you discovered.
* The web technologies identified.
* Screenshots and documentation supporting your findings.