### **Lab 3- Recon-ng Lab**

**What Was Learned:**This lab demonstrated the use of Recon-ng, a reconnaissance framework, to automate the collection of WHOIS information and discover subdomains of a target domain. Participants learned how to install and use modules within Recon-ng to gather information systematically and effectively.

**Key Learnings:**

1. **Setting Up Recon-ng Workspaces:**
   * Created a project-specific workspace using the workspaces create command.
   * Organized and saved data automatically within the workspace for efficient analysis.
2. **Gathering WHOIS Information:**
   * Installed and used the recon/domains-contacts/whois\_pocs module from the marketplace.
   * Retrieved detailed WHOIS information about a target domain (e.g., facebook.com), including location, registration details, and contact information.
3. **Discovering Subdomains:**
   * Installed and utilized the recon/domains-hosts/hackertarget module.
   * Found subdomains and their associated IPv4 addresses using HackerTarget.com’s API.
   * Recognized the importance of subdomain discovery for identifying potentially weaker entry points in a system.
4. **Module Usage:**
   * Learned to search for, install, load, and configure modules from the Recon-ng marketplace.
   * Used the options set command to define the target domain and info to understand module details.
   * Executed scans with the run command and analyzed the generated output.

**Takeaways:**

* **Recon-ng as a Powerful Reconnaissance Tool:** Recon-ng simplifies data collection through its modular framework, enabling efficient and organized reconnaissance efforts.
* **WHOIS Data Significance:** WHOIS information provides critical insights into domain ownership and administration, useful for both ethical and malicious purposes.
* **Subdomain Enumeration:** Identifying subdomains and IPs is valuable for pinpointing vulnerabilities in a system’s security.
* **Ethical Boundaries:** Emphasized the importance of using such tools responsibly, with permission, to avoid unethical behavior or legal repercussions.

This lab highlighted Recon-ng’s capabilities for automating reconnaissance and gathering actionable data about a target domain.