### **Lab 2- Nmap**

**What Was Learned:**This lab introduced the use of Nmap (Network Mapper) for scanning a target system or network, with a focus on discovering key information such as open ports, running services, and system details. Participants learned how to perform both basic and advanced scans, analyze the results, and explore the functionality of different Nmap flags.

**Key Learnings:**

1. **Basic Scans:**
   * Performed a simple scan using nmap scanme.nmap.org.
   * Identified open ports and the basic services running on them.
   * Learned that basic scans are limited to the top 1000 ports.
2. **Advanced Scans:**
   * Conducted an advanced scan using sudo nmap -v -sT -sV -O scanme.nmap.org to gather detailed information:
     + Service versions running on each port.
     + The operating system of the target system.
   * Understood that advanced scans may not work as effectively if the target has a firewall in place.
3. **Using Flags for Customized Scans:**
   * Explored the -A flag to perform a comprehensive scan, combining service, version, and OS detection.
   * Learned to experiment with various Nmap flags to customize scans for specific objectives, referencing the Nmap documentation for guidance.

**Takeaways:**

* **Nmap as a Versatile Tool:** Nmap is invaluable for discovering network and system details, making it a critical tool for both system administrators and ethical hackers.
* **Permission is Essential:** Always obtain explicit permission before scanning systems to avoid legal and ethical issues.
* **Flag Customization:** Familiarity with Nmap flags allows users to tailor scans to their specific needs, enhancing effectiveness and efficiency.

This lab reinforced the importance of understanding scanning tools and techniques to strengthen network security and identify vulnerabilities.