**Nmap Network Scanning Project Report**

**Introduction**

The objective of this project is to utilize the Nmap tool to perform a detailed assessment of the network at https://indrive.com/. The project includes the identification of live hosts, open ports, running services, operating systems, and potential vulnerabilities. The findings are compiled into this professional report with appropriate screenshots, diagrams, and recommendations.

**Project Setup**

**Environment Configuration**

1. **Nmap Installation:**
   * Verified the installation of Nmap.
   * Command used to check installation: nmap --version
   * Output: *Nmap version 7.93 (example output)*

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Target Network:**
   * The network scanned: https://indrive.com/.
   * Permissions confirmed for scanning.

**Task 1: Basic Scans**

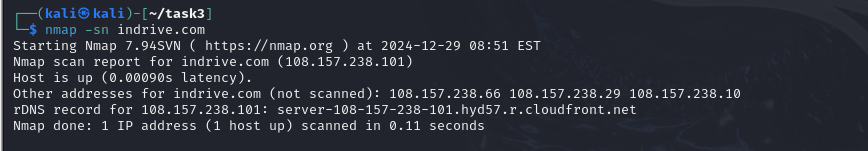
**1.1 Ping Scan**

* **Command Used:**

A screenshot of a computer

Description automatically generated

* **Output:**

****

**1.2 TCP SYN Scan**

* **Command Used:**

**A screenshot of a computer

Description automatically generated**

**Output:**

**A screenshot of a computer

Description automatically generated**

Purpose: Discover open TCP ports.

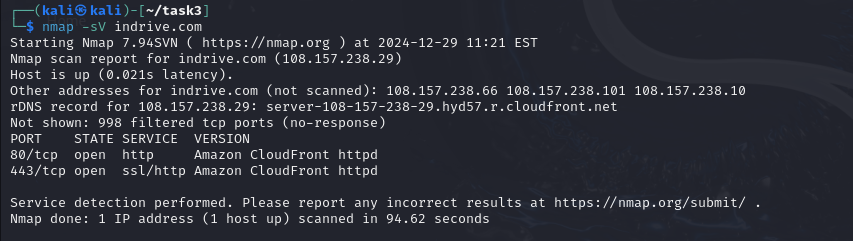
**Task 2: Detailed Scanning**

**2.1 Service Version Scan (-sV)**

* **Command Used:**

A computer screen with white and blue text

Description automatically generated

Output:  


**Purpose:** Identify services running on open ports.

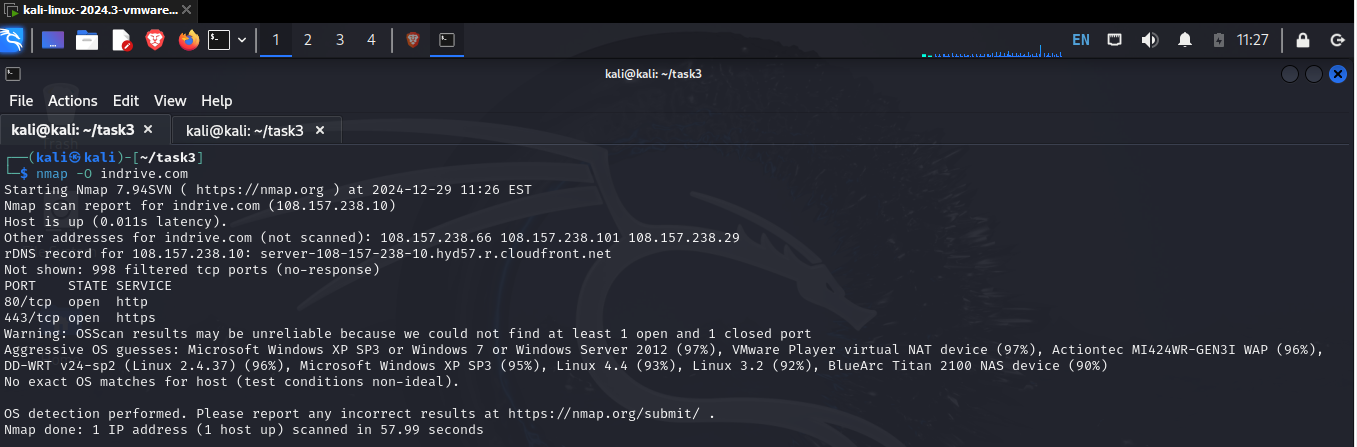
**2.2 OS Detection (-O)**

* **Command Used:**

**A screenshot of a computer

Description automatically generated**

**Output:**

****

**Purpose: Determine the operating system of the live host.**

**Task 3: NSE Scans**

**3.1 Vulnerability Scripts**

* **Command Used:**

**A screen shot of a computer

Description automatically generated**

**Output:**

**A screenshot of a computer

Description automatically generated**

**Purpose: Identify vulnerabilities.**

**Key Observations:**

* Target: indrive.com (IP: 108.157.238.101)
* Host: Up and reachable (Latency: 0.0047 seconds)

**Open Ports Identified:**

* + **Port 80 (HTTP):**
    - No stored XSS vulnerabilities detected.
    - No CSRF vulnerabilities identified.
    - No DOM-based XSS vulnerabilities identified.
  + **Port 443 (HTTPS):**
    - No stored XSS vulnerabilities detected.
    - No CSRF vulnerabilities identified.
    - No DOM-based XSS vulnerabilities identified.
* **File Type Exploiter Results:**
  + No exploitable file types were detected on either port

**Findings and Recommendations**

**Summary of Findings**

* **Live Hosts:**
  + Host: scanme.nmap.org (IP: 45.33.32.156)
  + Host: indrive.com (IP: 108.157.238.101)
* **Open Ports:**
  + For scanme.nmap.org:
    - Port 22 (SSH) running OpenSSH 6.6.1
    - Port 80 (HTTP) running Apache HTTPD 2.4.7
  + For indrive.com:
    - Port 80 (HTTP) and Port 443 (HTTPS) detected as open with no critical vulnerabilities.
* **Operating System:** Linux Kernel 3.x for scanme.nmap.org (98% accuracy).

**Recommendations**

1. **SSH Security:**
   * Update OpenSSH to the latest version to mitigate potential vulnerabilities.
   * Use strong SSH key-based authentication.
2. **HTTP and HTTPS Security:**
   * Ensure Apache HTTPD and HTTPS configurations are up-to-date.
   * Implement secure headers and disable unnecessary features.
3. **General Network Security:**
   * Enable firewall rules to restrict access to critical services.
   * Regularly monitor and audit network traffic.
   * Use vulnerability management tools for ongoing assessments.