DC-2 Machine :-

🔐 DC-2 CTF Challenge Overview

- 🖥️ **Platform:** VulnHub
- 🎯 **Objective:** Gain root access and capture the `flag.txt` file
- 📄 **Challenge Type:** Boot-to-Root, Beginner to Intermediate Level
- 🔍 **Focus Areas:** Web application enumeration, file upload vulnerability, privilege escalation.

Step 1:-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

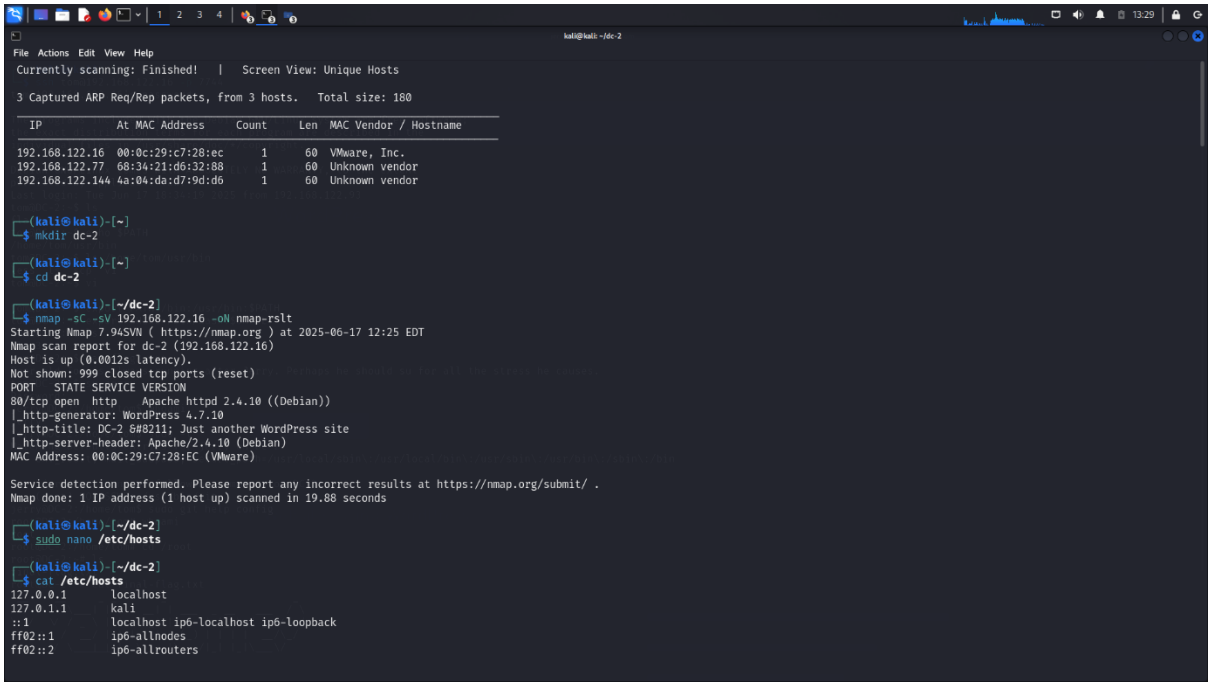
ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.

Step 2:-

Nmap is a powerful, open-source tool used for network discovery and security auditing.It is widely used by

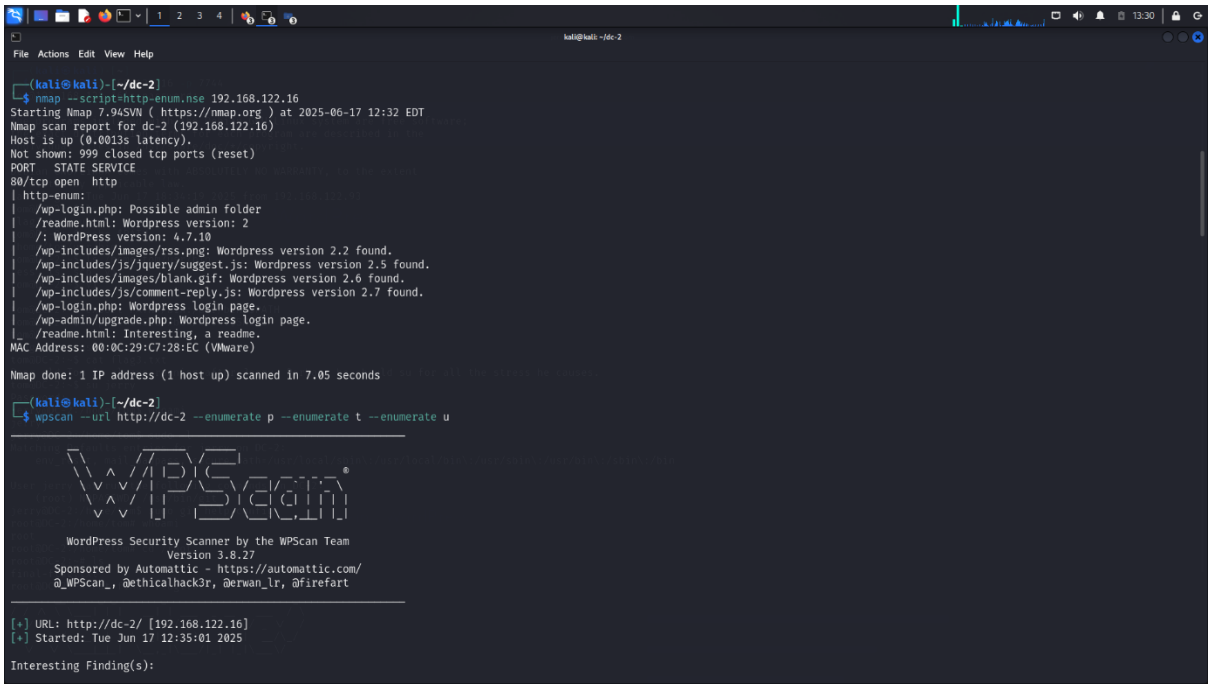
network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.

Cat /etc/host



Step-3 :-

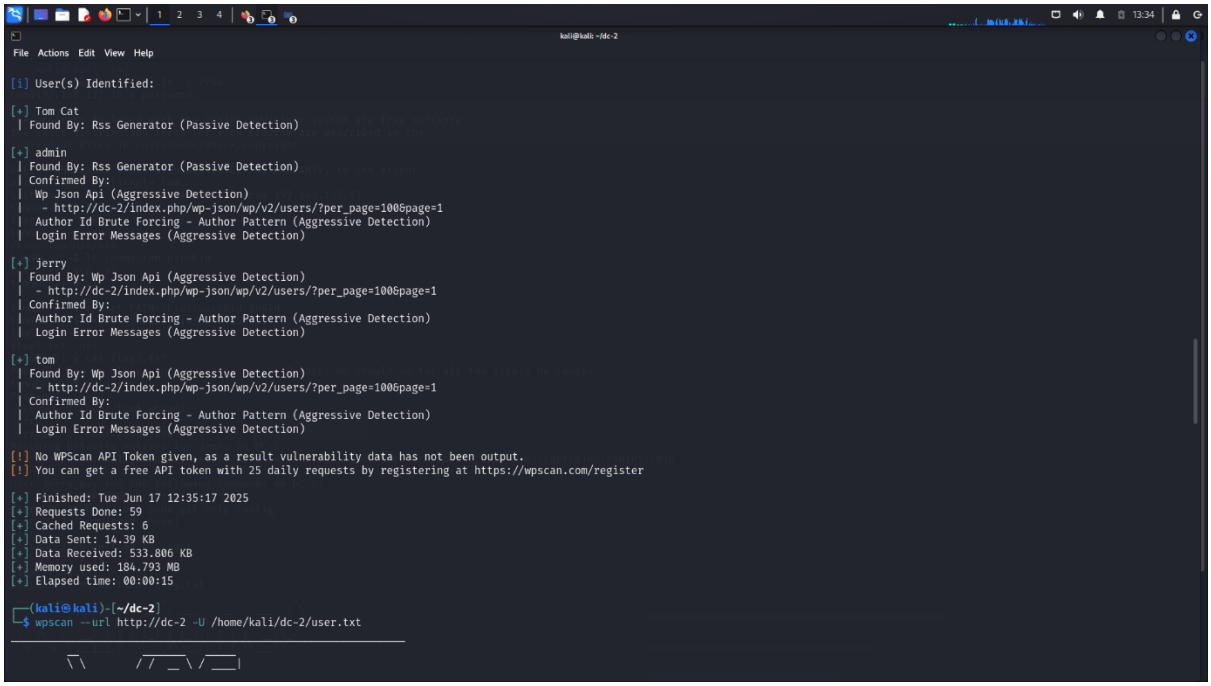
The `http-enum.nse` script attempts to enumerate directories used by **popular web applications** and **services**.



Step -4 :-

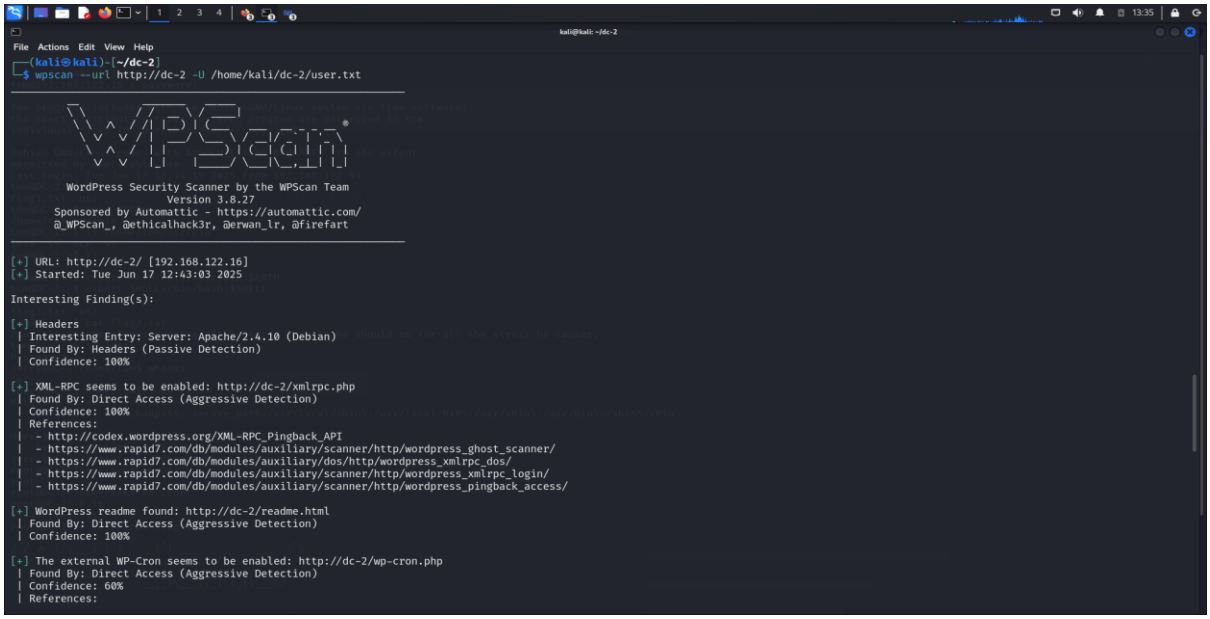
This command uses **WPScan**, a WordPress security scanner, to scan a WordPress site hosted at `http://dc-2` and **enumerate**:

- `p`: Plugins
- `t`: Themes
- `u`: Users



Step-5 :-

This command runs **WPScan** against a WordPress site at `http://dc-2` and attempts to **brute-force WordPress logins** using a **list of usernames** provided in the file `/home/kali/dc-2_user.txt`.



Step-6:-

SSH (Secure Shell) is a **network protocol** used to **securely connect** to a **remote system** over an **unencrypted or public network**. It provides a **secure channel** for managing servers, transferring files, and executing commands remotely.