**Reconnaissance & Scanning Lab**

**Author: Kalyan sai Ch  
Environment: Kali (attacker) + Metasploitable2 (target) — host-only / isolated network (authorized lab)  
Date: [DD-MM-YYYY]**

**Project overview**

**This repository contains a complete lab exercise for reconnaissance, port/service scanning and basic vulnerability assessment performed on an isolated Metasploitable2 virtual machine. All work is performed in a controlled host-only network and is strictly educational.**

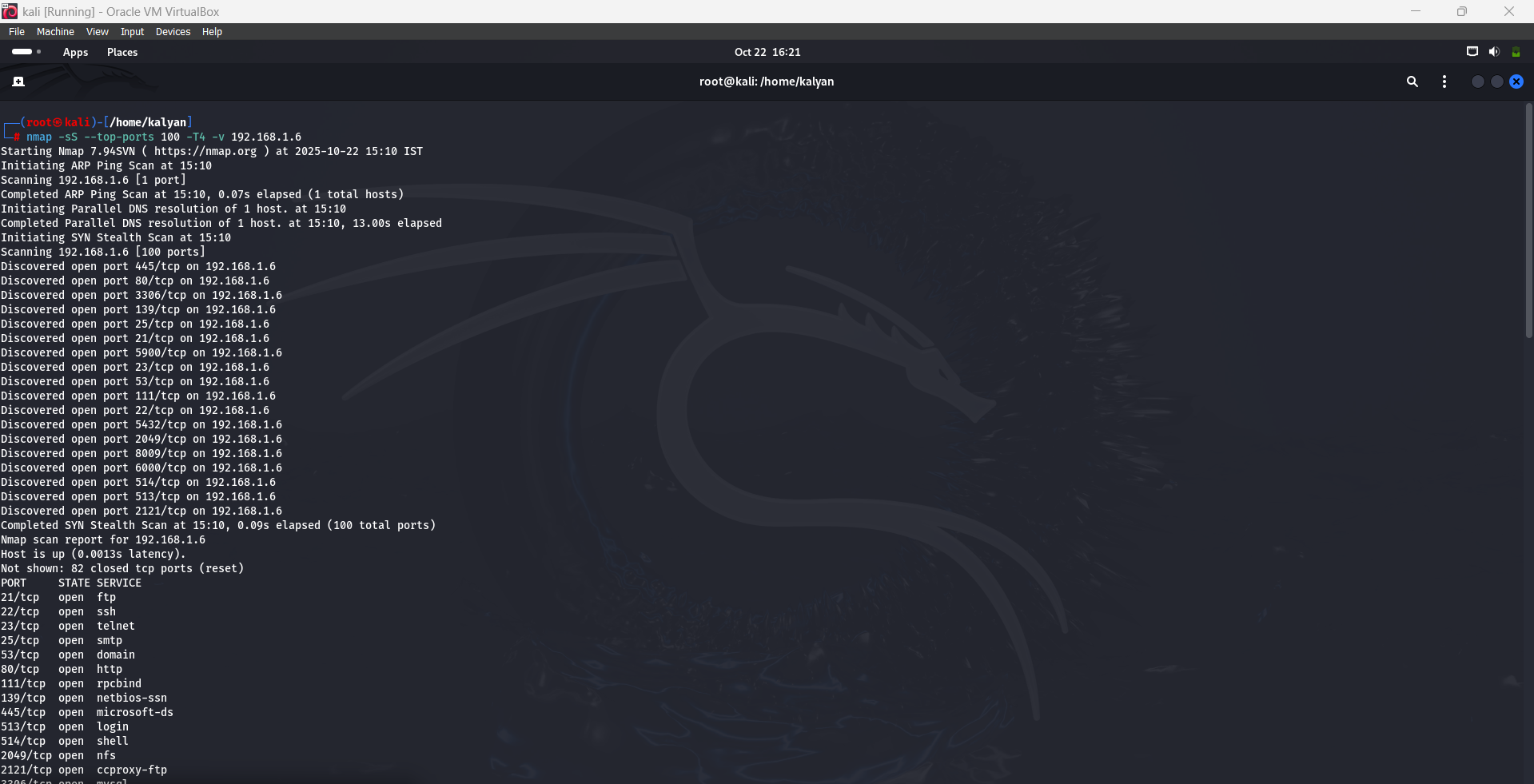
**I performed three Nmap scans to discover ports and services and one OpenVAS vulnerability scan. I recorded every step (terminal, scanner UI, and packet captures) and included the raw outputs, parsed summaries, evidence screenshots, PCAP(s) and a 5-minute demo video.**

**Scans performed**

**Quick port discovery (SYN + top ports)**

**Purpose: fast discovery of commonly used services to get an initial asset list and reduce scan time.  
Command used:**

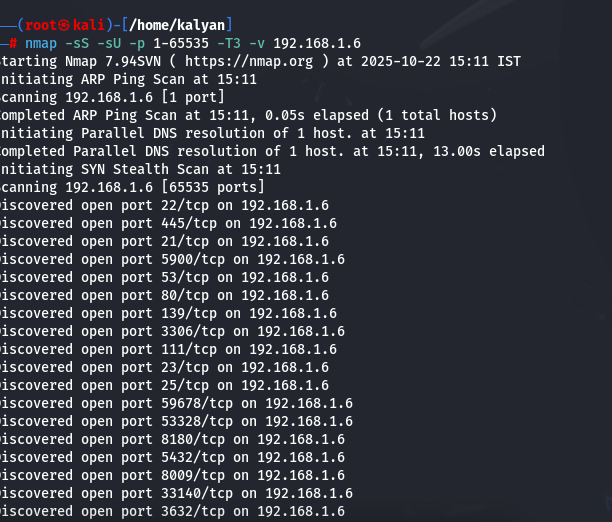
**nmap -sS --top-ports 100 -T4 -v 192.168.1.6**

****

**Full TCP & UDP sweep (SYN, all ports)**

**Purpose: comprehensive discovery of all TCP ports to find non-standard or hidden services. discover UDP services (UDP scanning is slower and may need verification due to timeouts and retransmissions).  
Command used:**

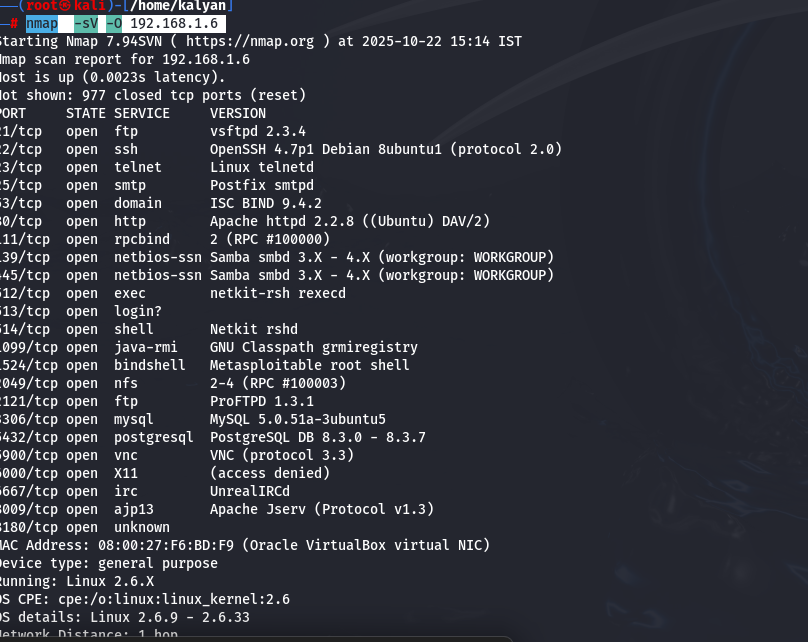
**nmap -sS -sU -p 1-65535 -T3 -v 192.168.1.6**

****

**Service/version & OS detection**

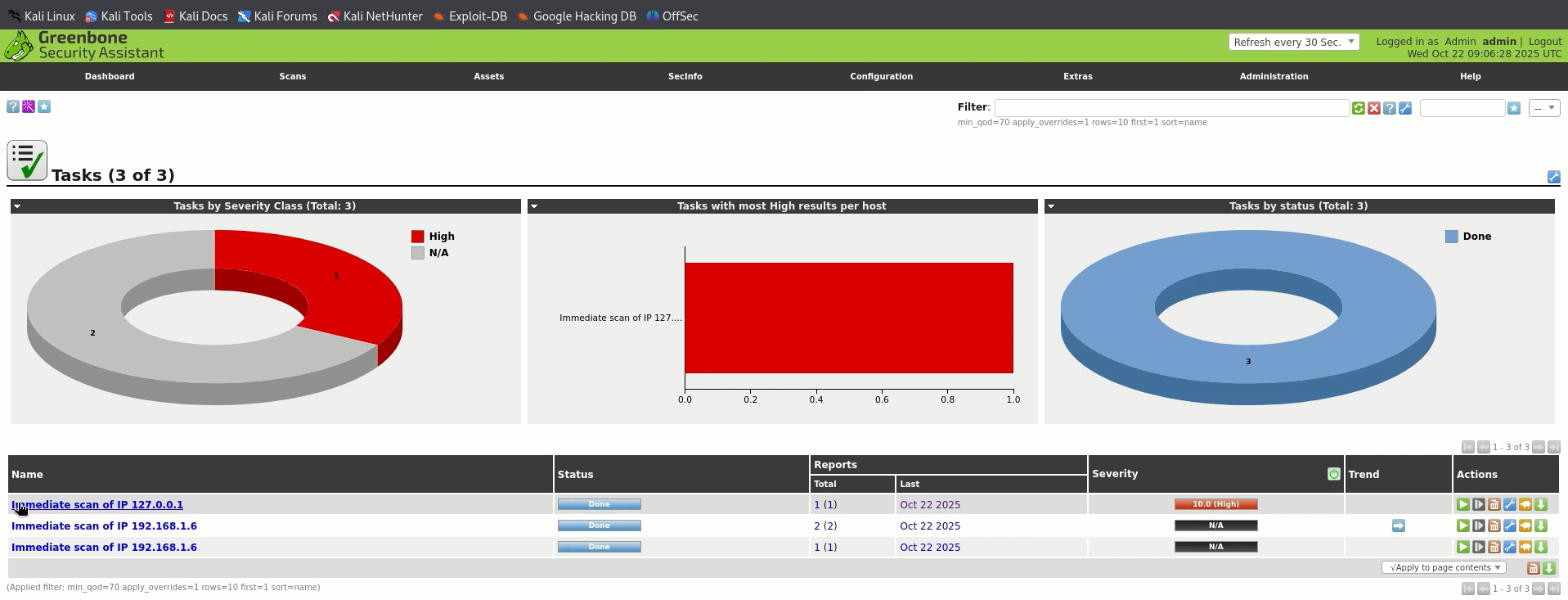
**Purpose: identify service versions and attempt OS fingerprinting to map vulnerabilities.  
Command used:**

**nmap -sV -O 192.168.1.6**

****

**OpenVAS vulnerability scan**

**Purpose: automated vulnerability discovery and risk rating for discovered services.  
Notes: exported full HTML report and saved key findings (Critical/High/Medium) with remediation suggestions.**

****

**Deliverables included**

* **Raw Nmap outputs and parsed summaries (/nmap-reports/)**
* **OpenVAS full HTML report (/openvas-reports/)**
* **Demo video (5 minutes) showing the scan and findings (/demo/demo\_video.mp4)**
* **Evidence screenshots: Nmap, OpenVAS, submission confirmation (/evidence/)**
* **A concise findings & remediation summary (prioritized by severity) (scan\_report\_summary.md)**

**to reproduce (exact steps)**