Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

**«Технології захисту інформації»**

Лабораторна робота №4

Аудит конфігурацій та сканування вразливостей

Виконав:

студент 4-го курсу

групи KN1-B22

**Демченко Дмитро**

Кам’янець-Подільський – 2025

**Мета:** провести аудит ОС і базове сканування вразливостей.

**Опис середовища:**

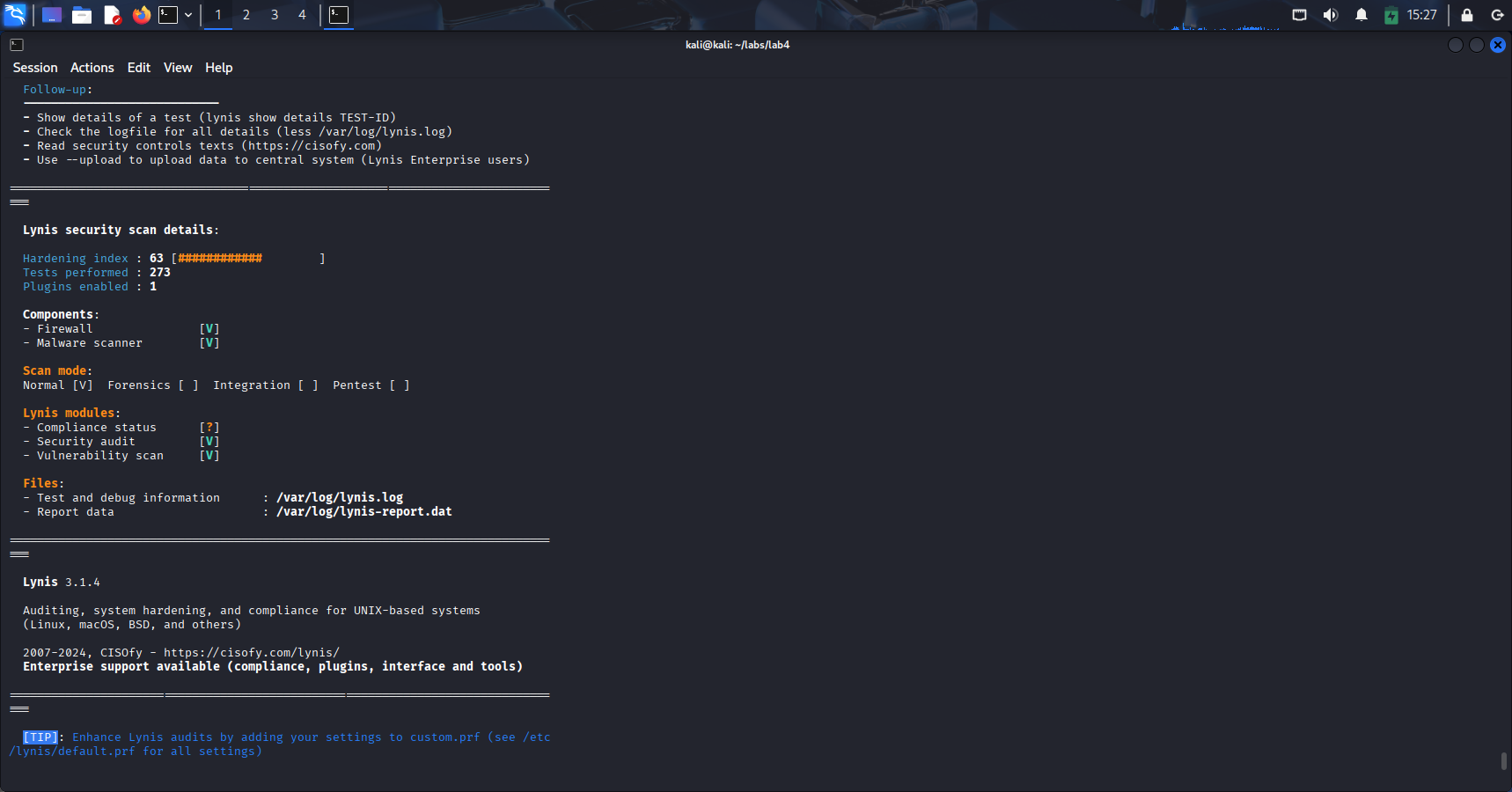
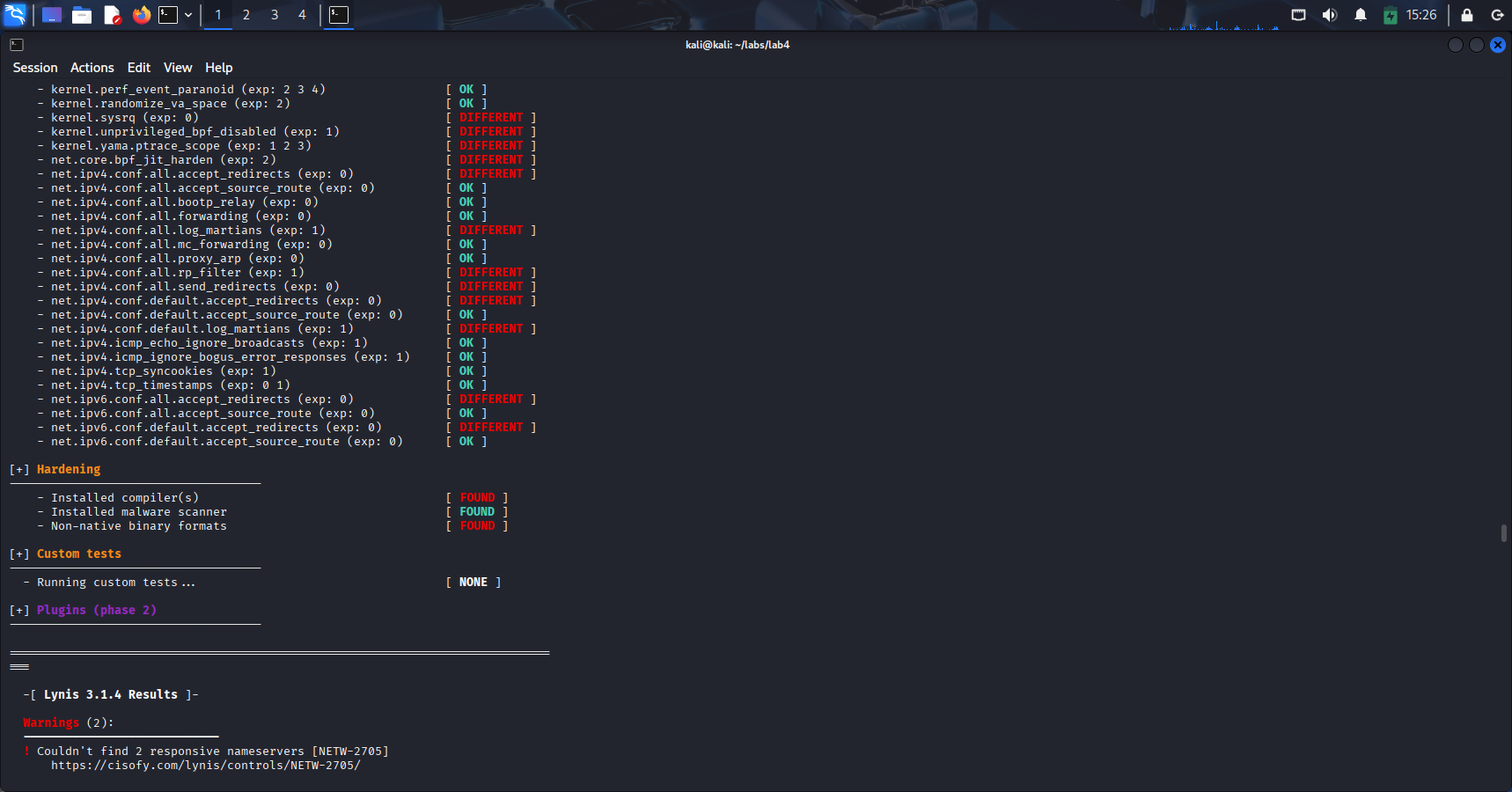
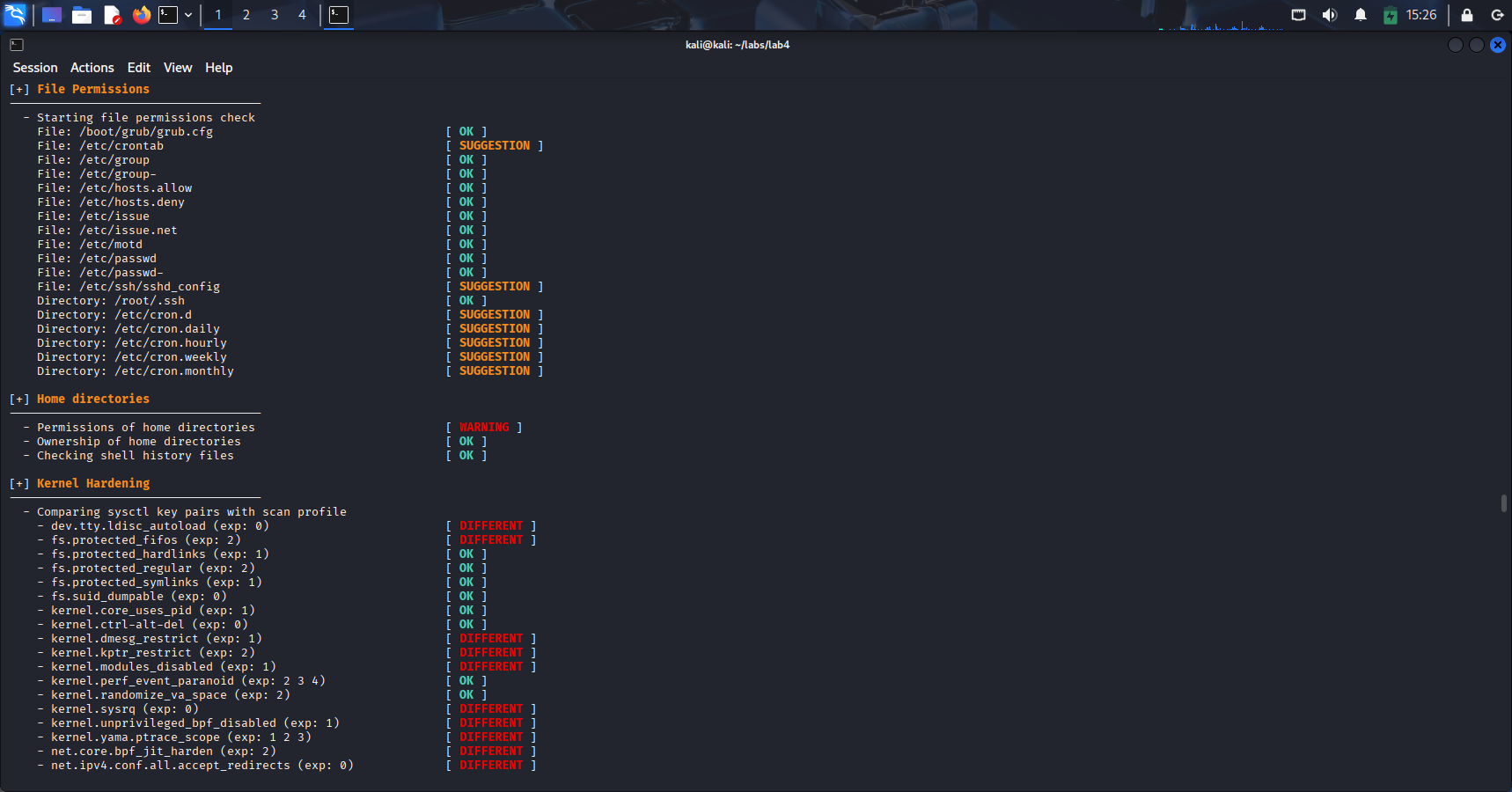
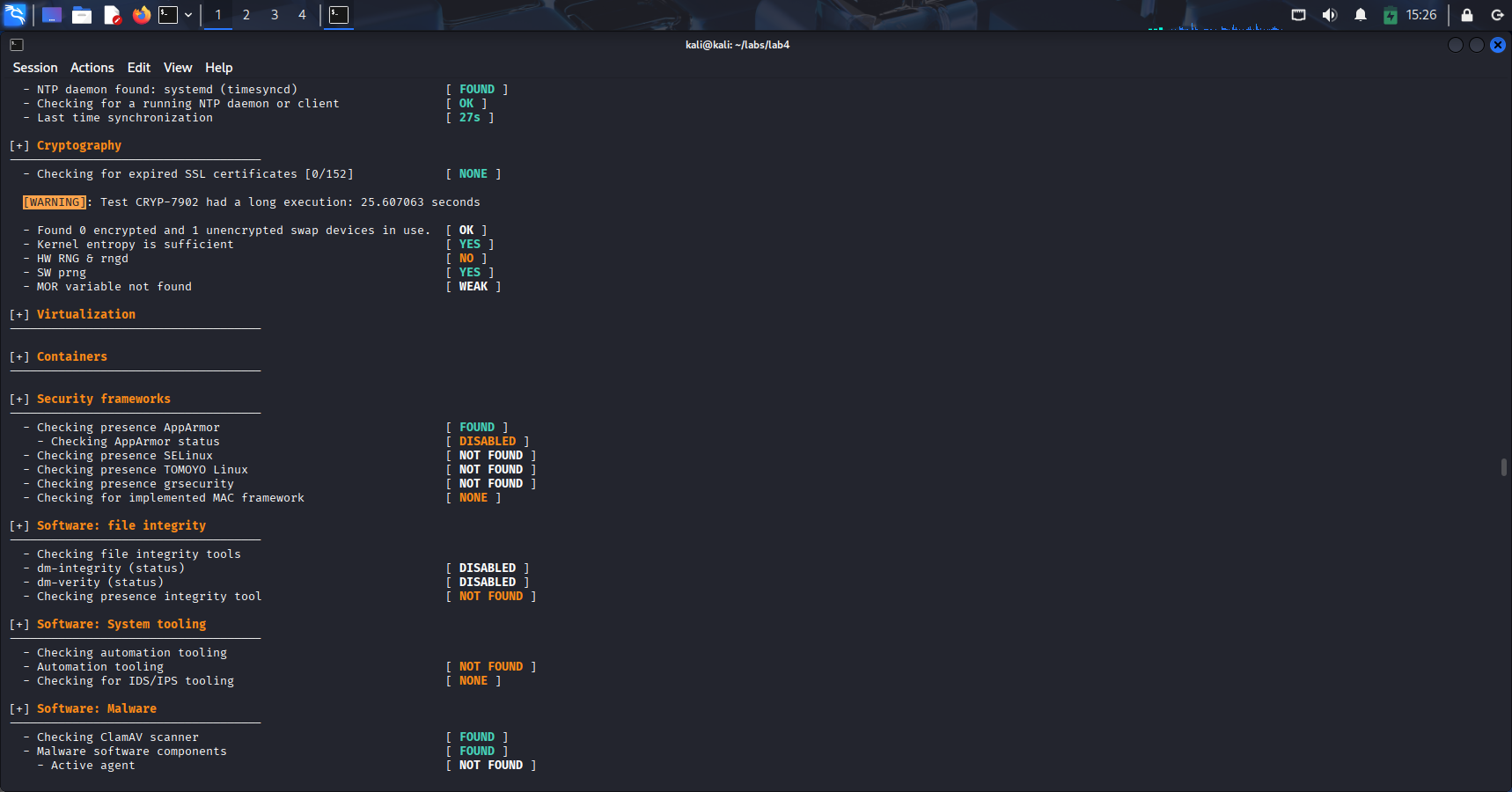
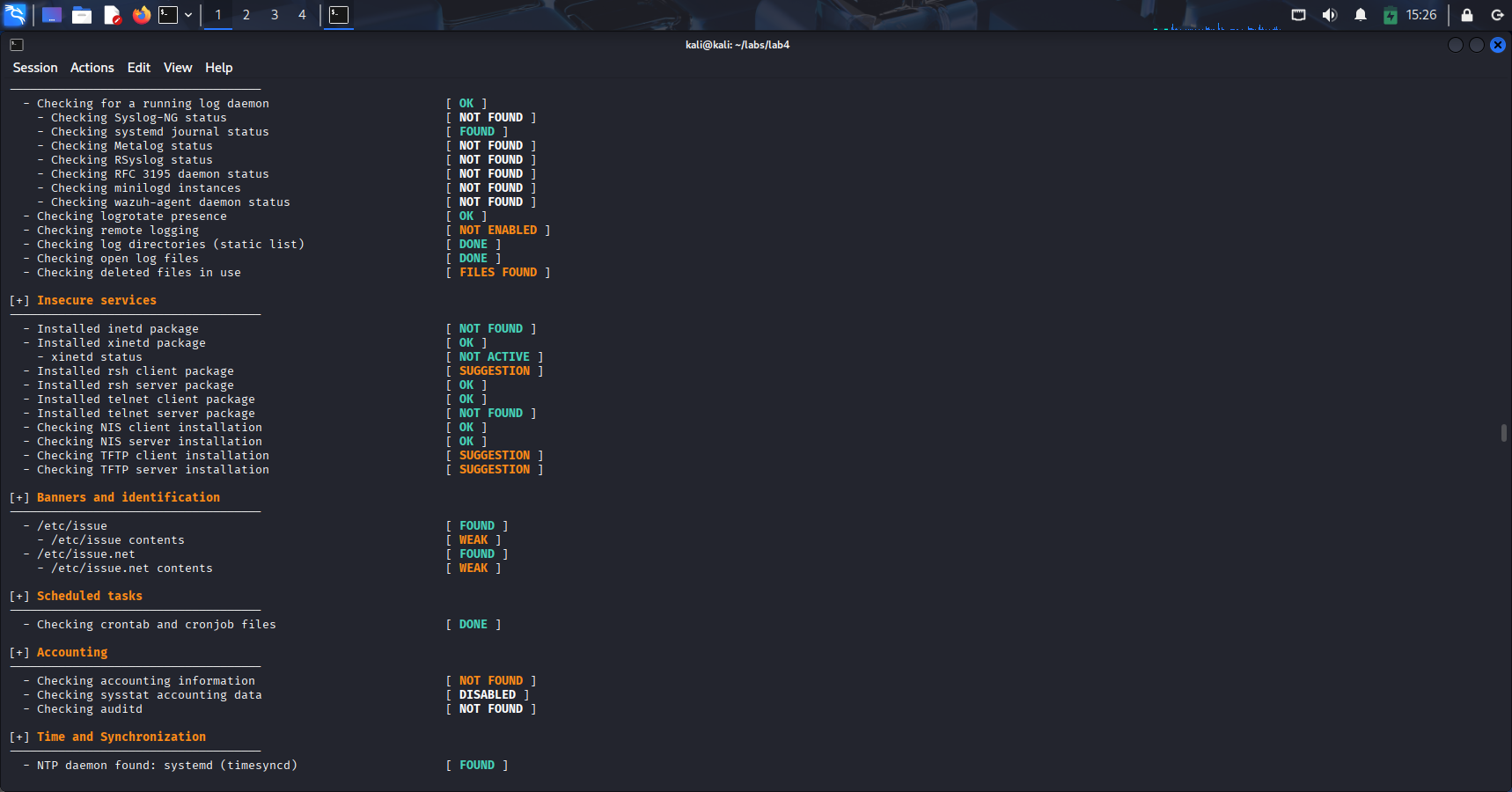
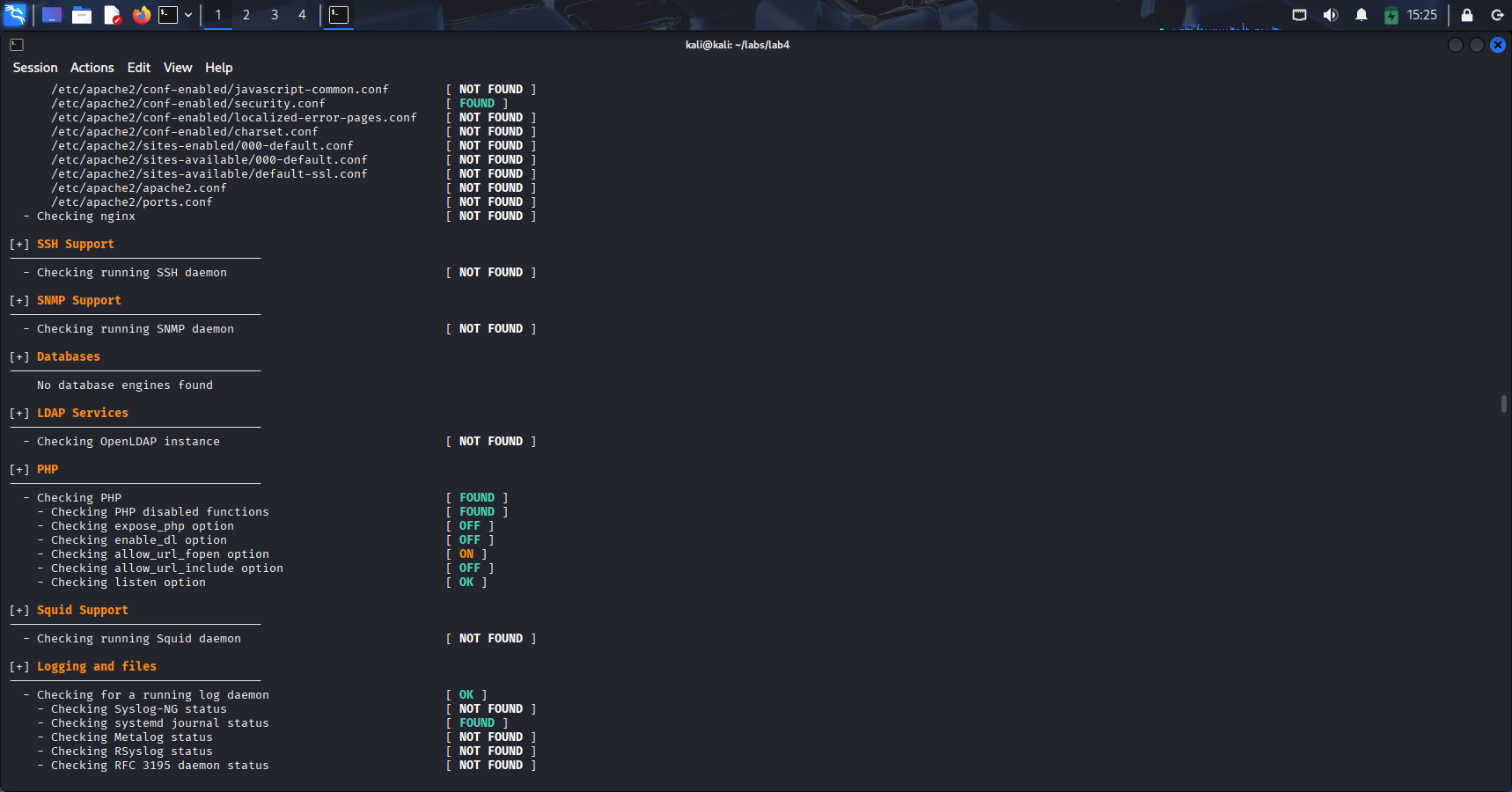
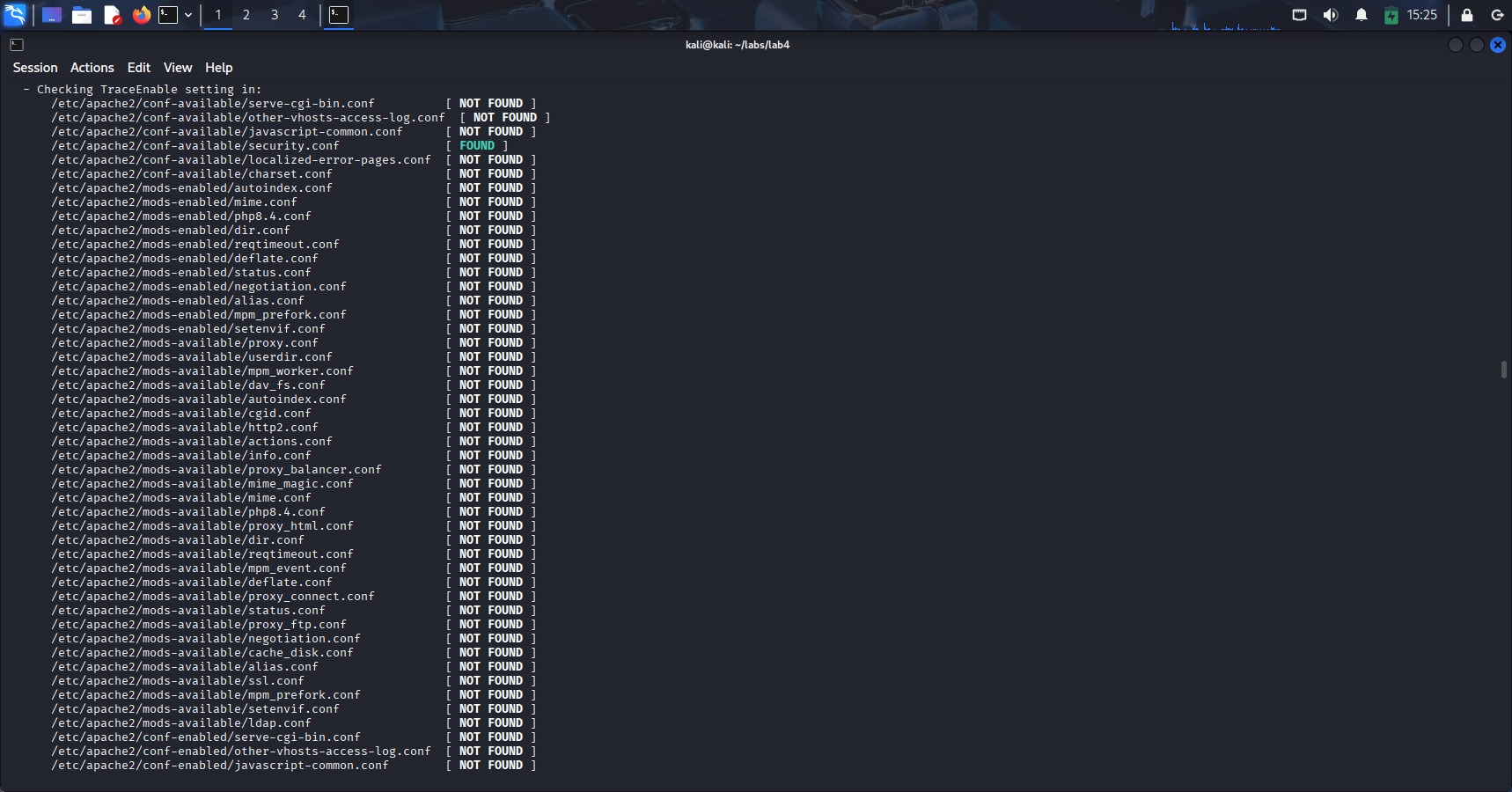
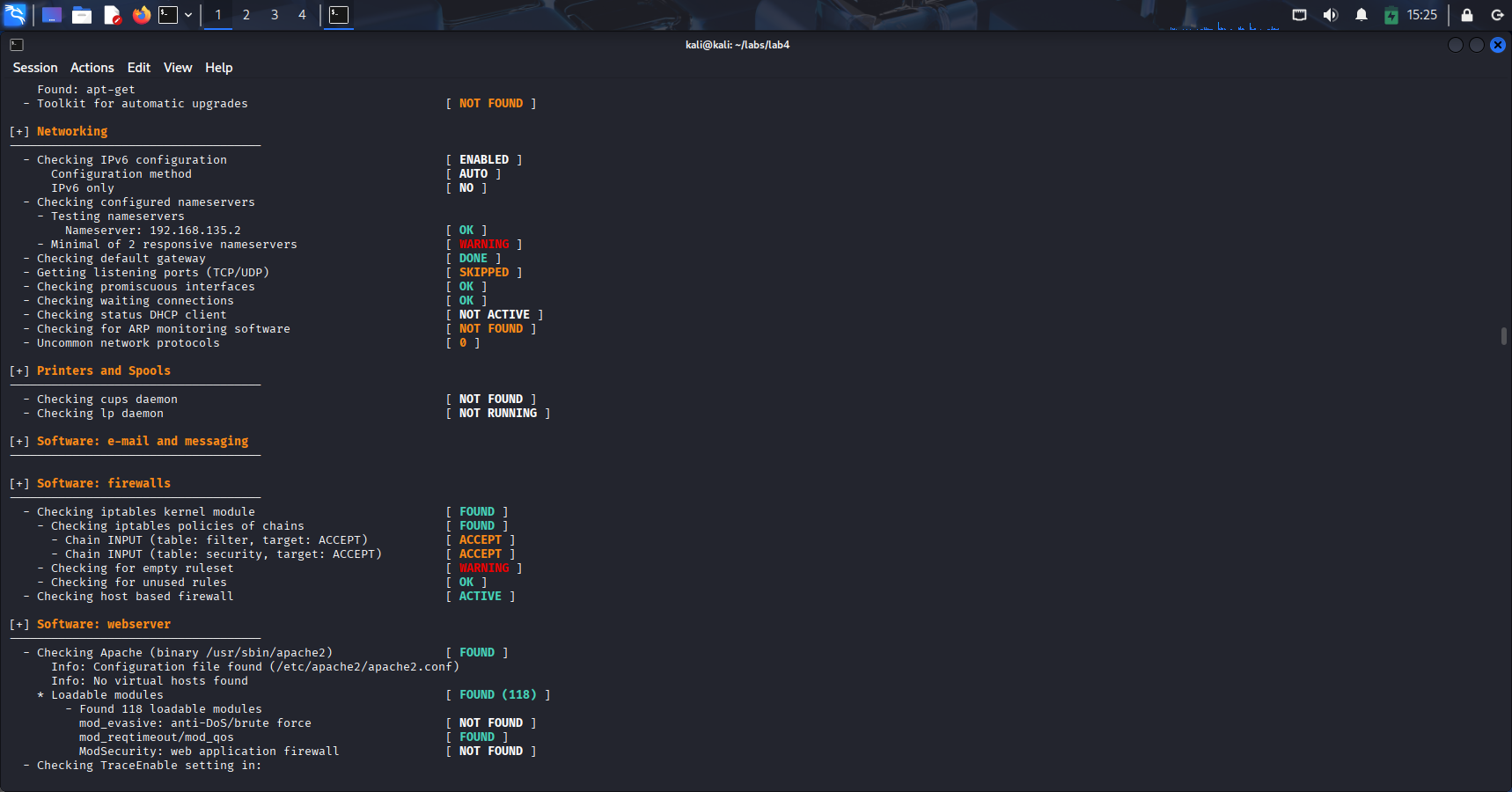
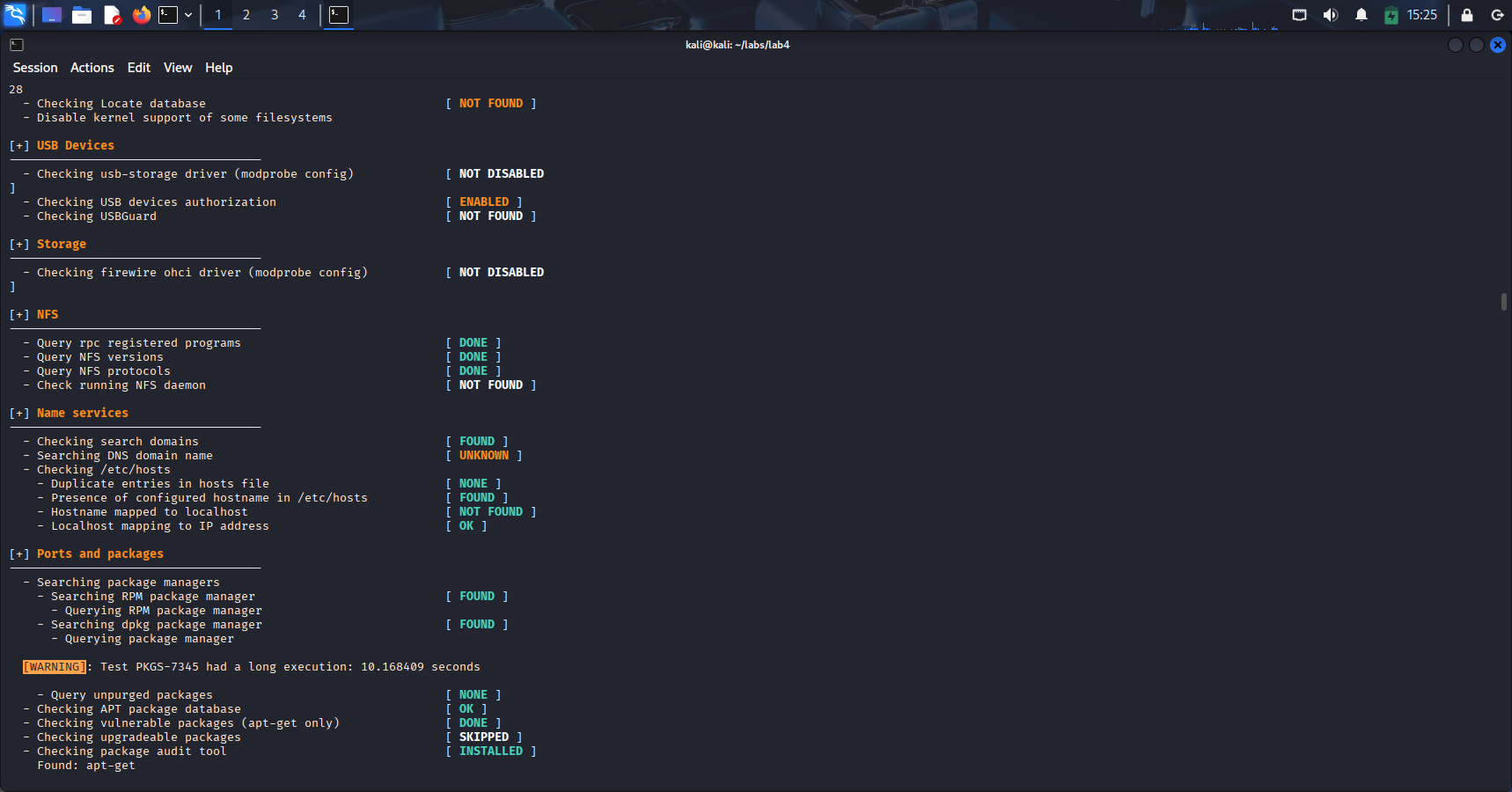
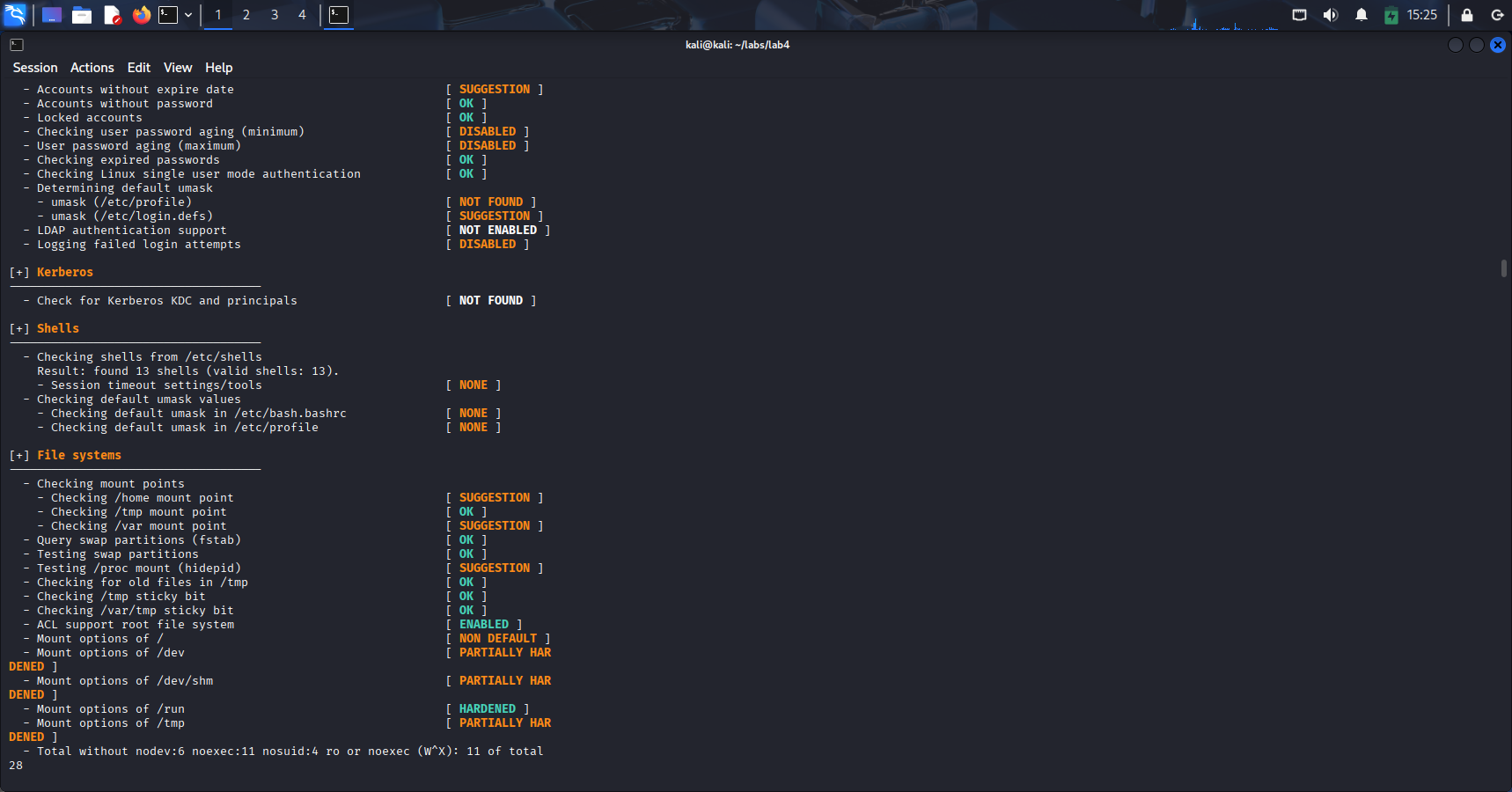
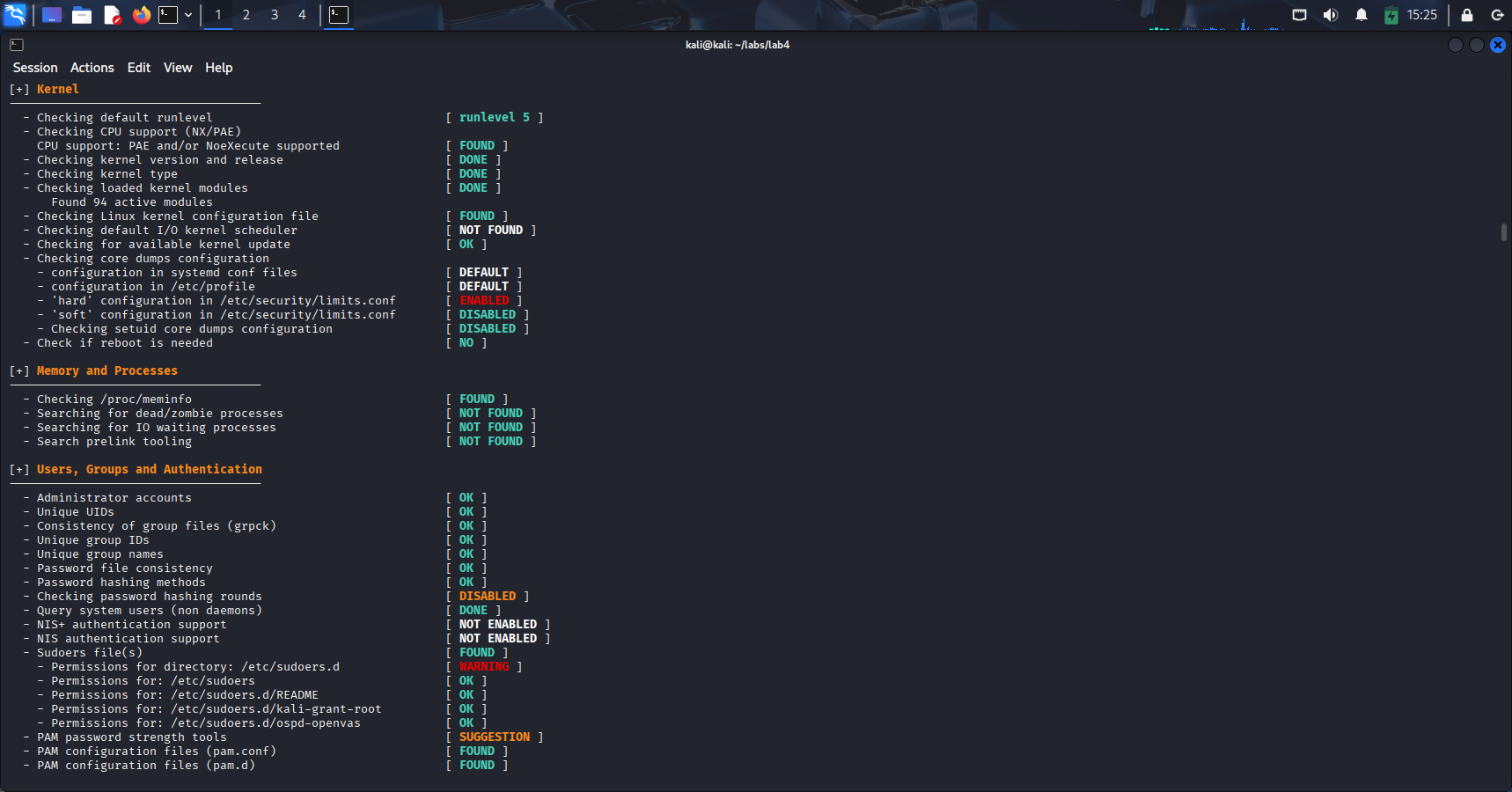
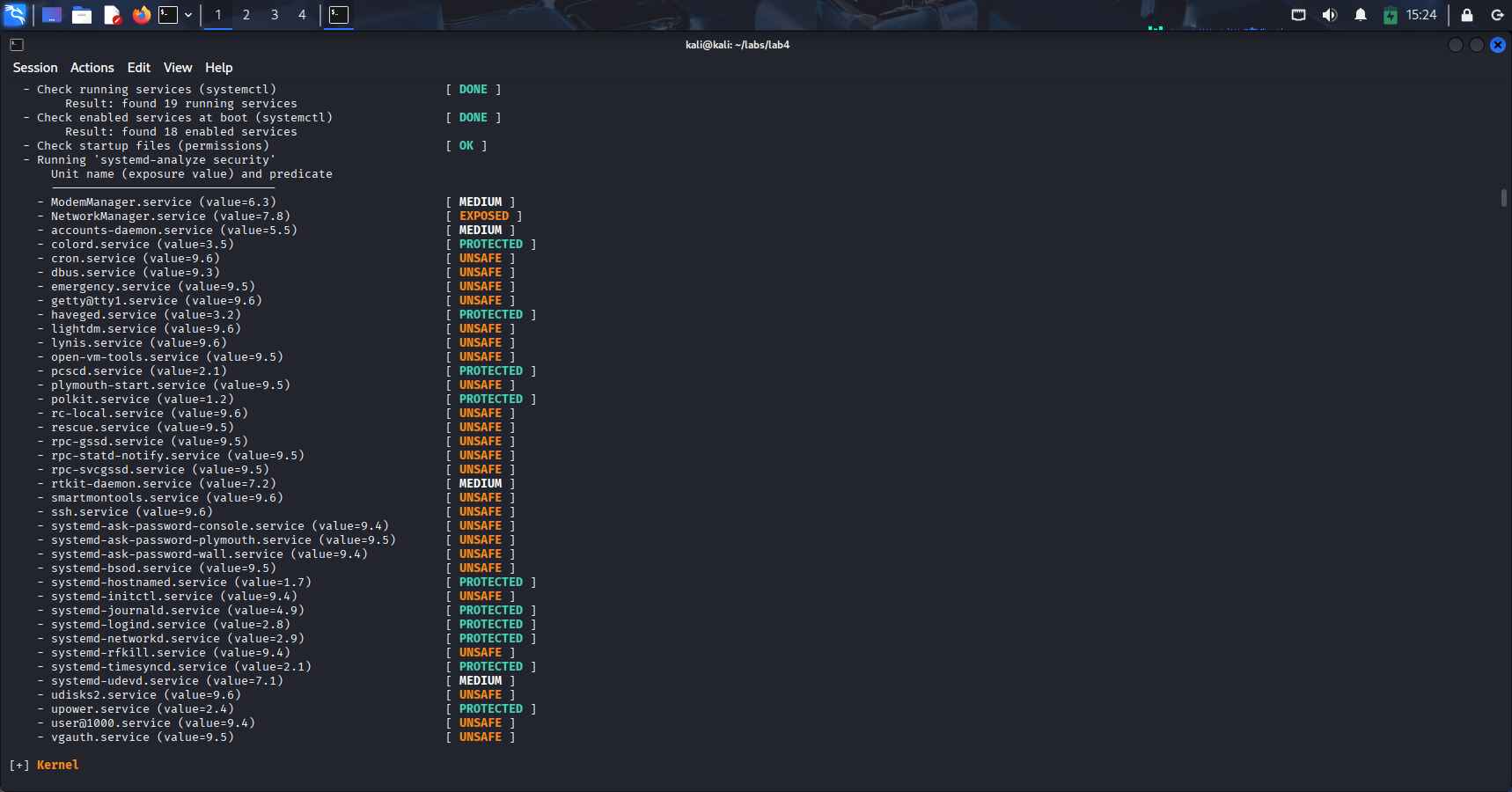
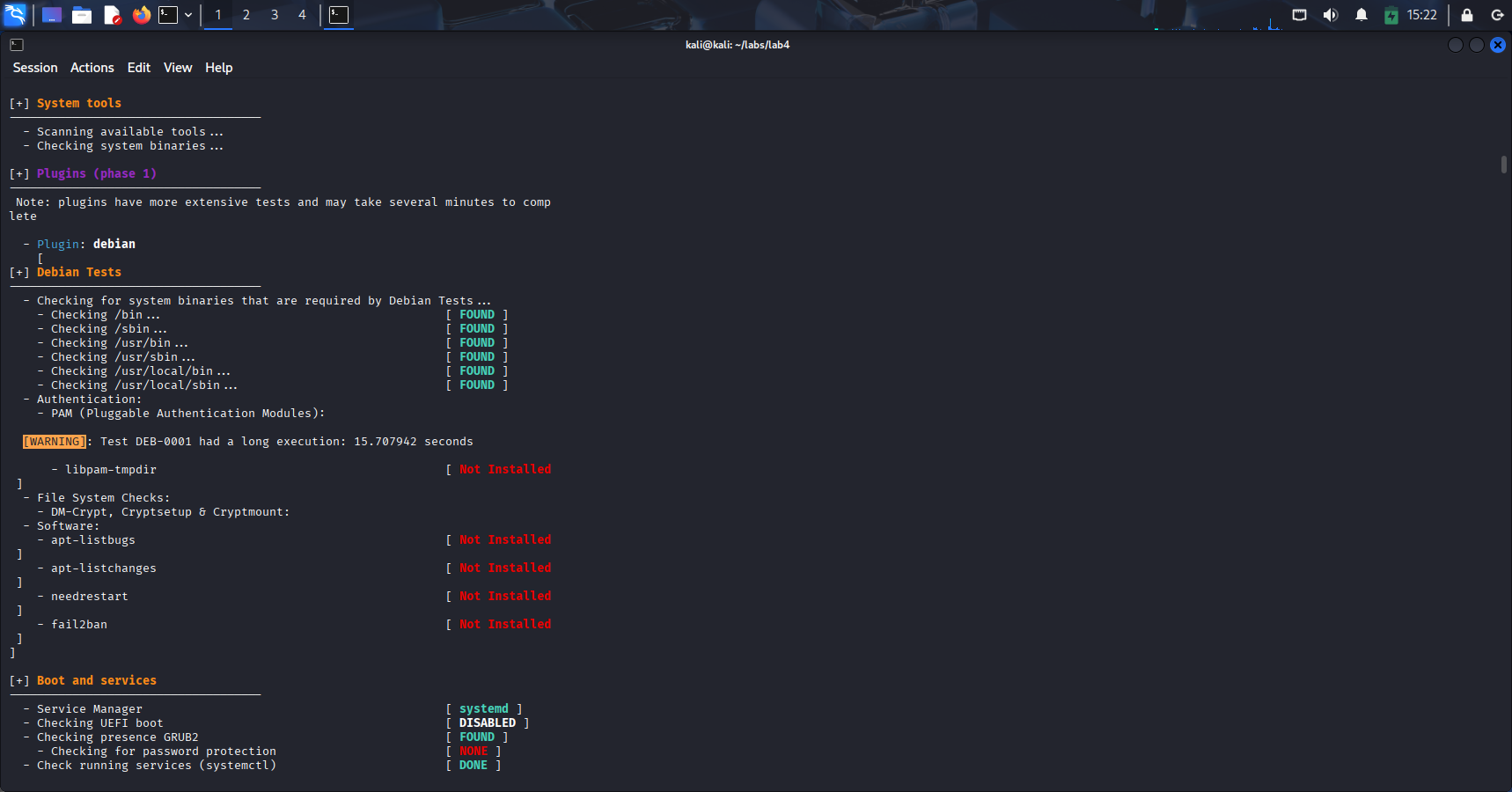
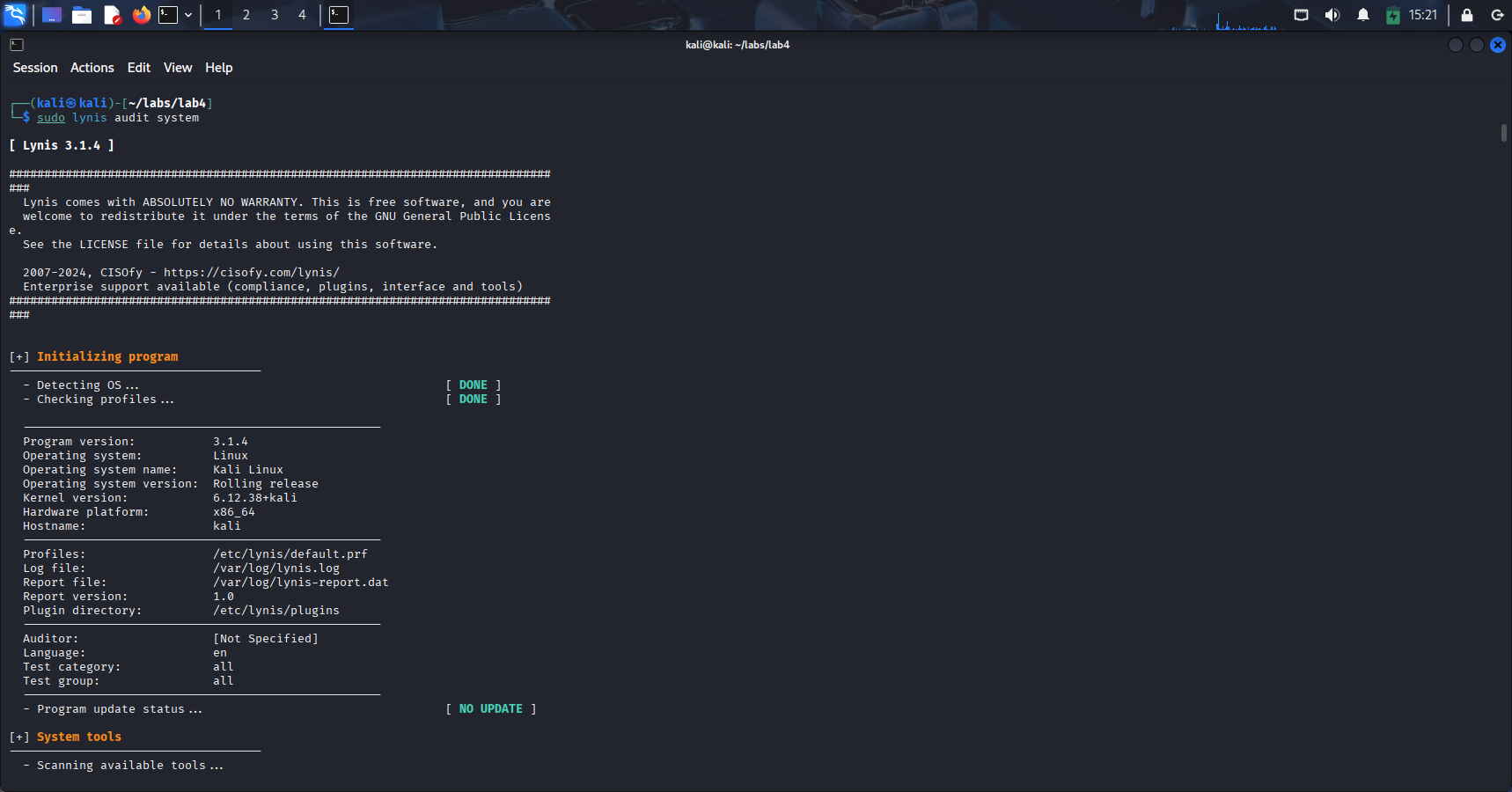
ПЗ для віртуальної машини: VMware® Workstation 17 Pro 17.6.4 build-24832109

, lynis 3.1.4, Nmap version 7.95, Nikto 2.5.0 (LW 2.5), Linux kali 6.12.38+kali-amd64, Metasploitable 2, Local Kali ip: 192.168.135.128, Metasploitable ip: 192.168.135.129

**Команди:**

1) Lynis аудит:

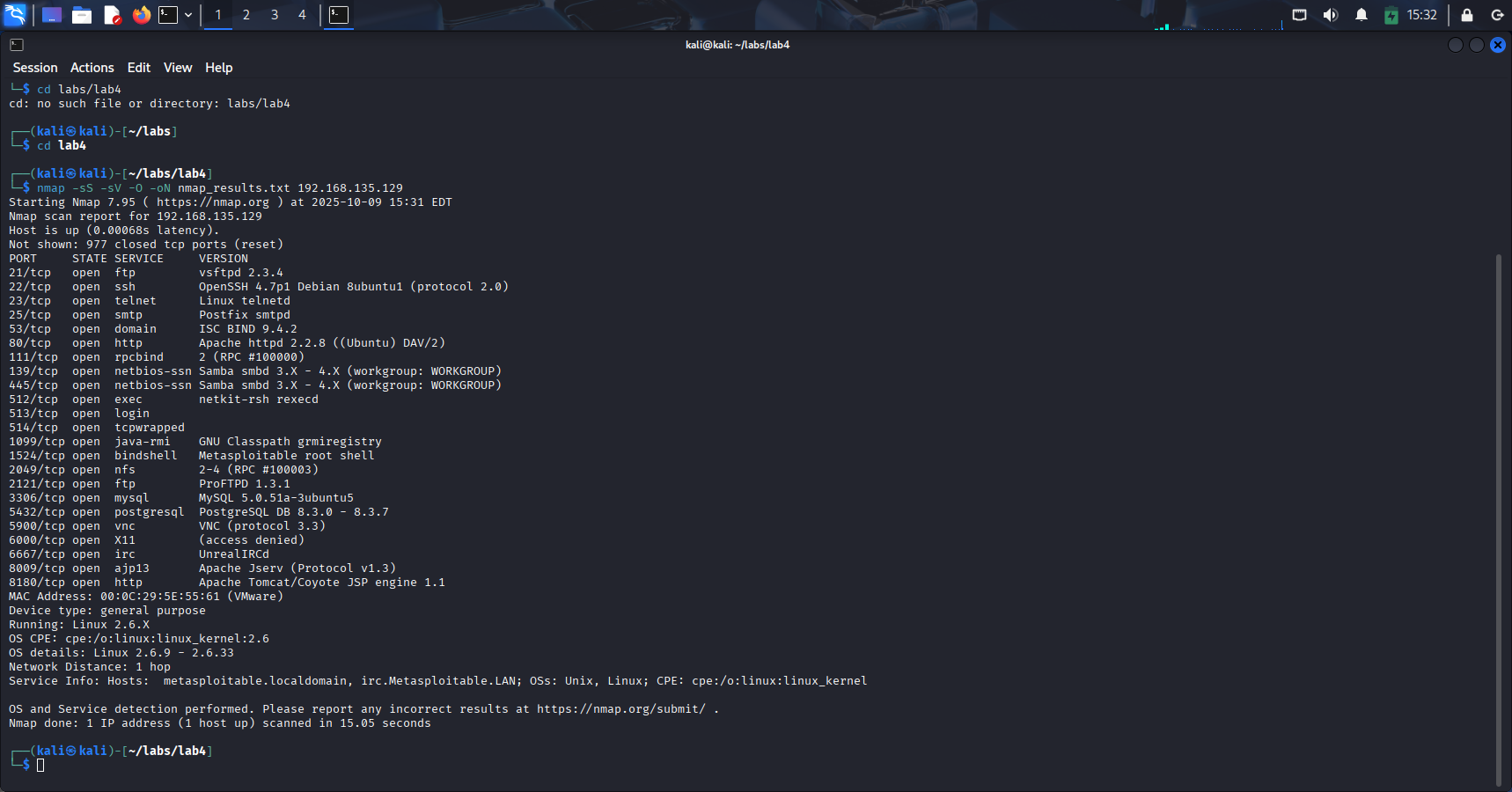
sudo lynis audit system



2) Nmap сканування:

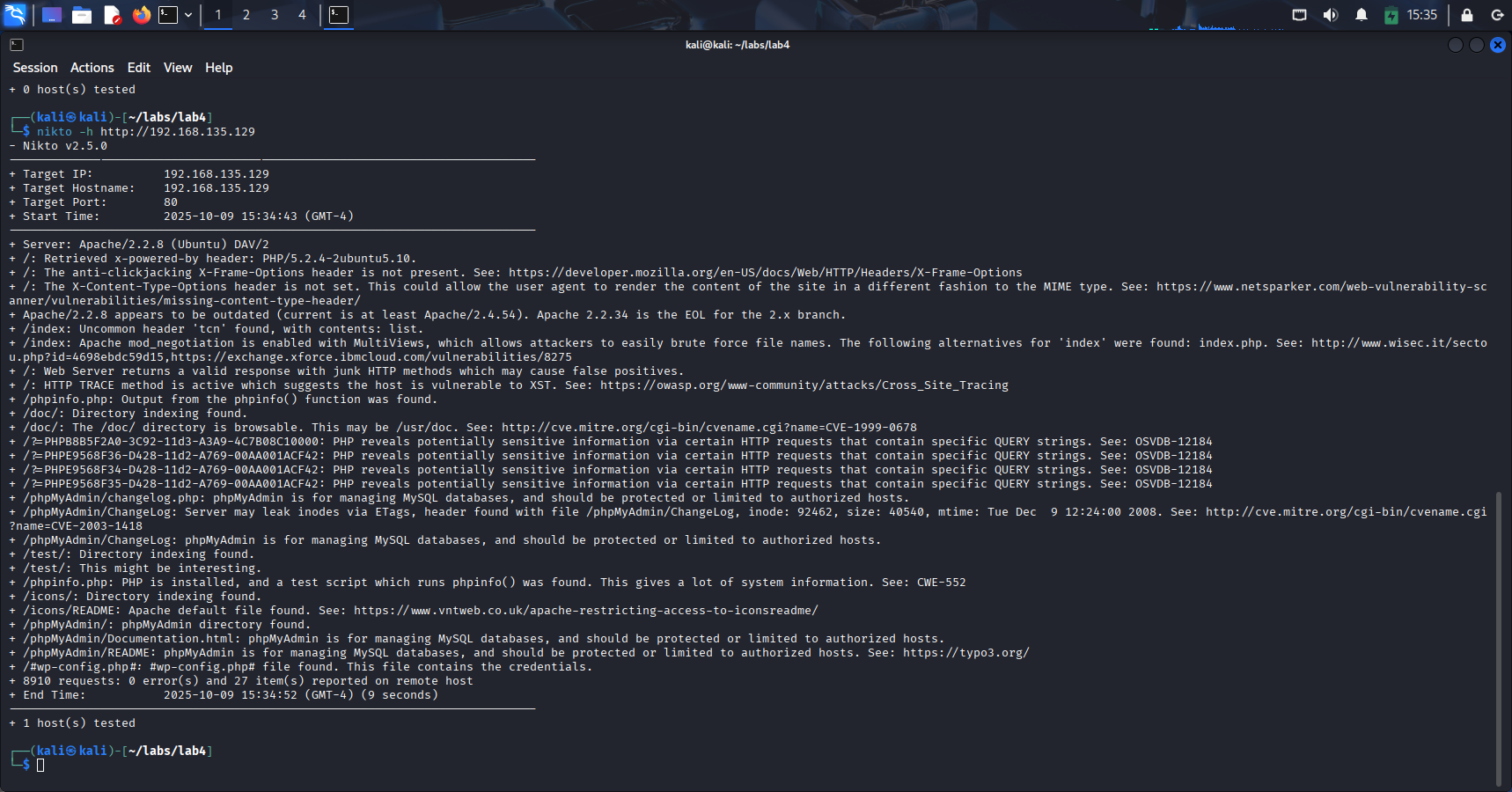
nmap -sS -sV -O -oN nmap\_results.txt 192.168.135.129

Веб-сервер: Metasploitable 2 – 192.168.135.129



3) Nikto для веб:

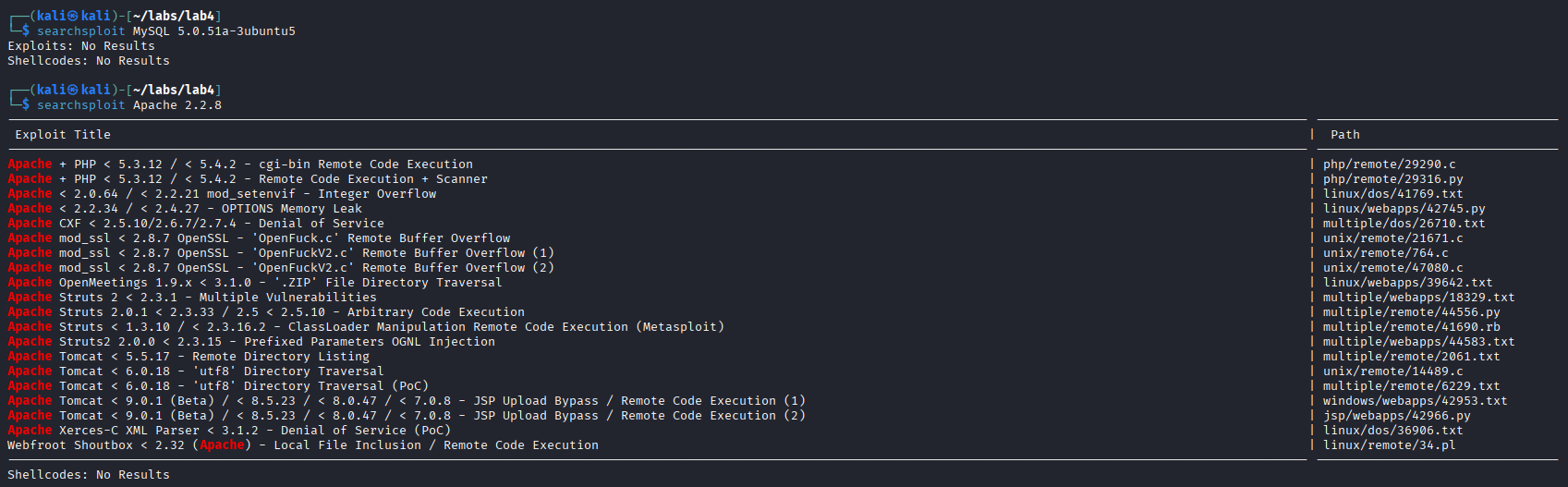
nikto -h http://192.168.135.129



4) Використати searchsploit для пошуку експлойтів:

searchsploit Apache 2.2.8

searchsploit MySQL 5.0.51a-3ubuntu5



**Висновки:** Під час виконання лабораторної роботи було проведено аудит ОС Kali Linux, а також базове сканування вразливостей за допомогою різних утиліт.