**NAME: SHASHIKALA**

**DATE:28-02-2023**

**1 . Dos attack using nmap:**

The nmap scripting engine(NSE) as a numerous scripts that can be used to perform dos attack

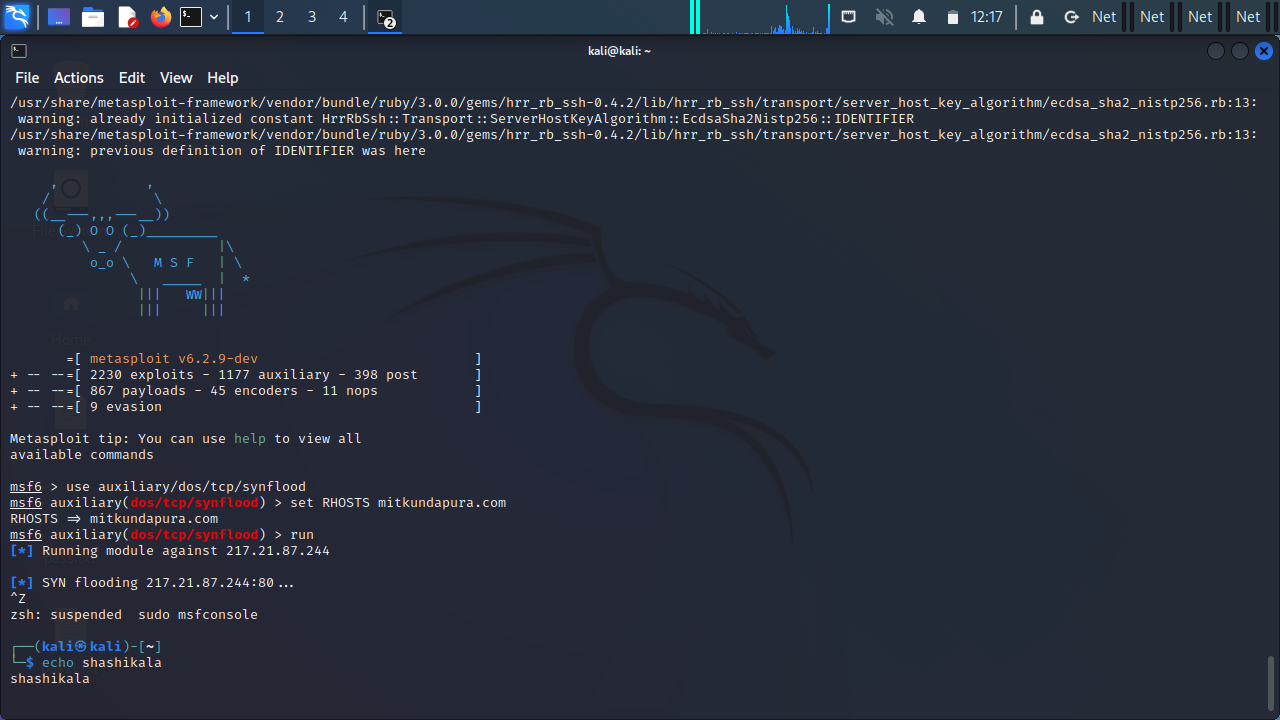
**Command:**

$ msfconsole

use auxiliary/dos/tcp/synflood

set RHOSTS mitkundapura.com

run

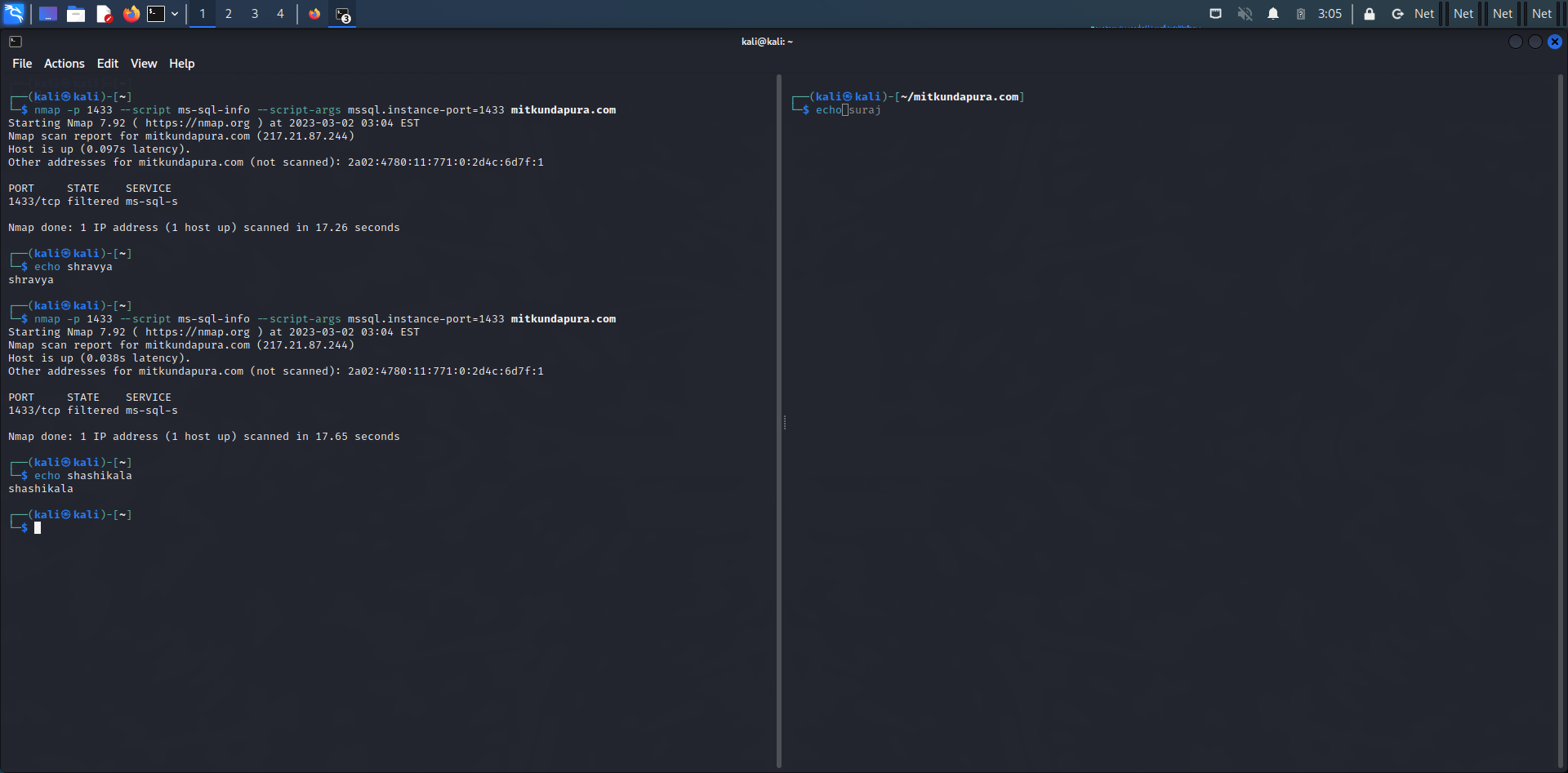


2**. sql empty password enumeration scanning using nmap**

The ms-sql-empty-password.nse script attempts to authenticate to Microsoft SQL servers using an empty password for the sysadmin account

**Command:**

$nmap -p 1433 --script ms-sql-info --script -args mssql.instance-port=1433 mitkundapura.com

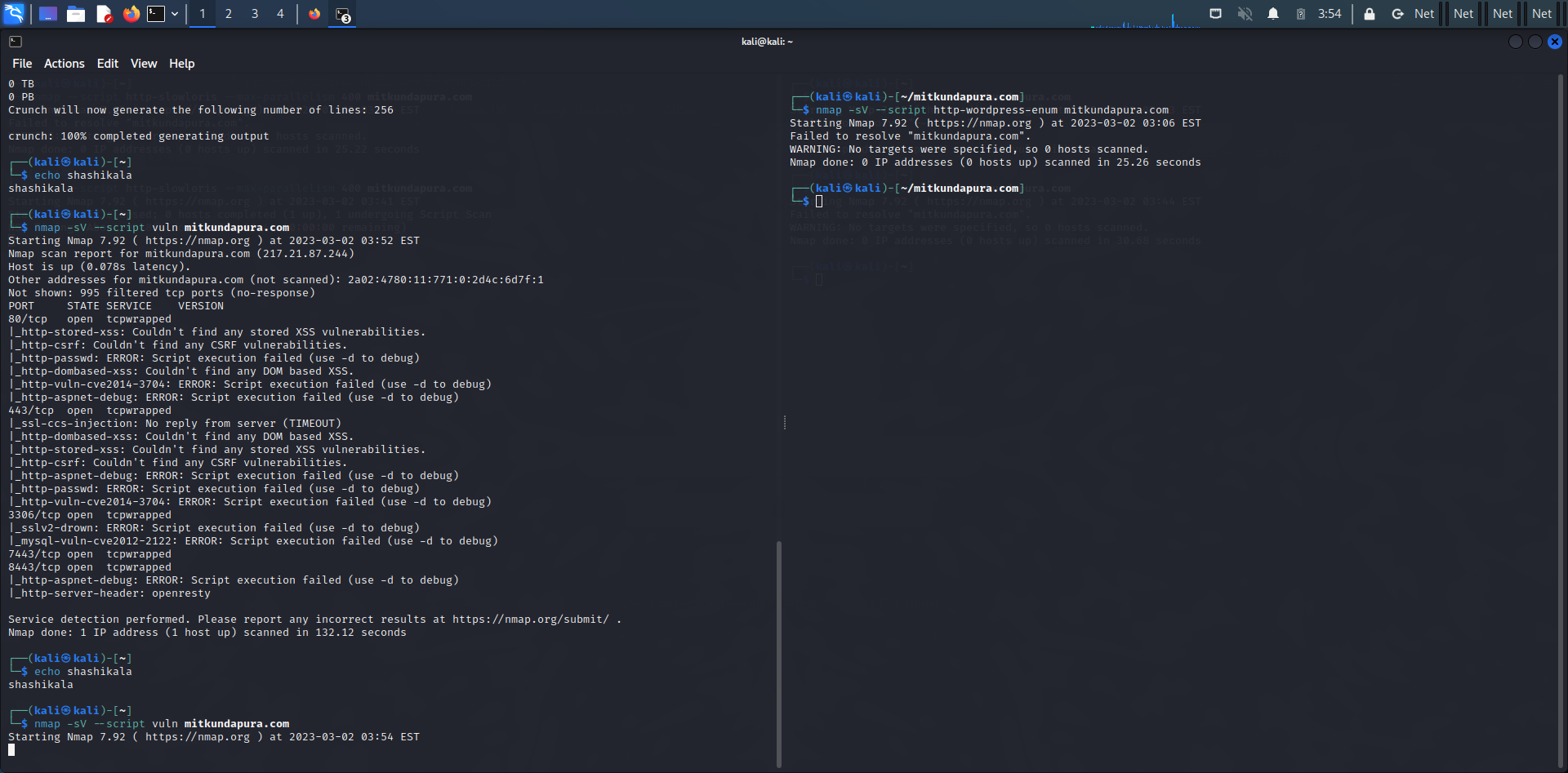


3. **vulnerability scan using nmap:**

Vulscan is an NSE script that assists nmap in detecting vulnerabilities on targets based on services and version detection. Vulscan is like a module for nmap that transforms it into a vulnerability scanner. The nmap option -sV allows per-service version detection,which is used to identifiy potential exploits for the detected vulnerabilities in system.

**Command:**

$Nmap -sV –script vuln mitkundapura

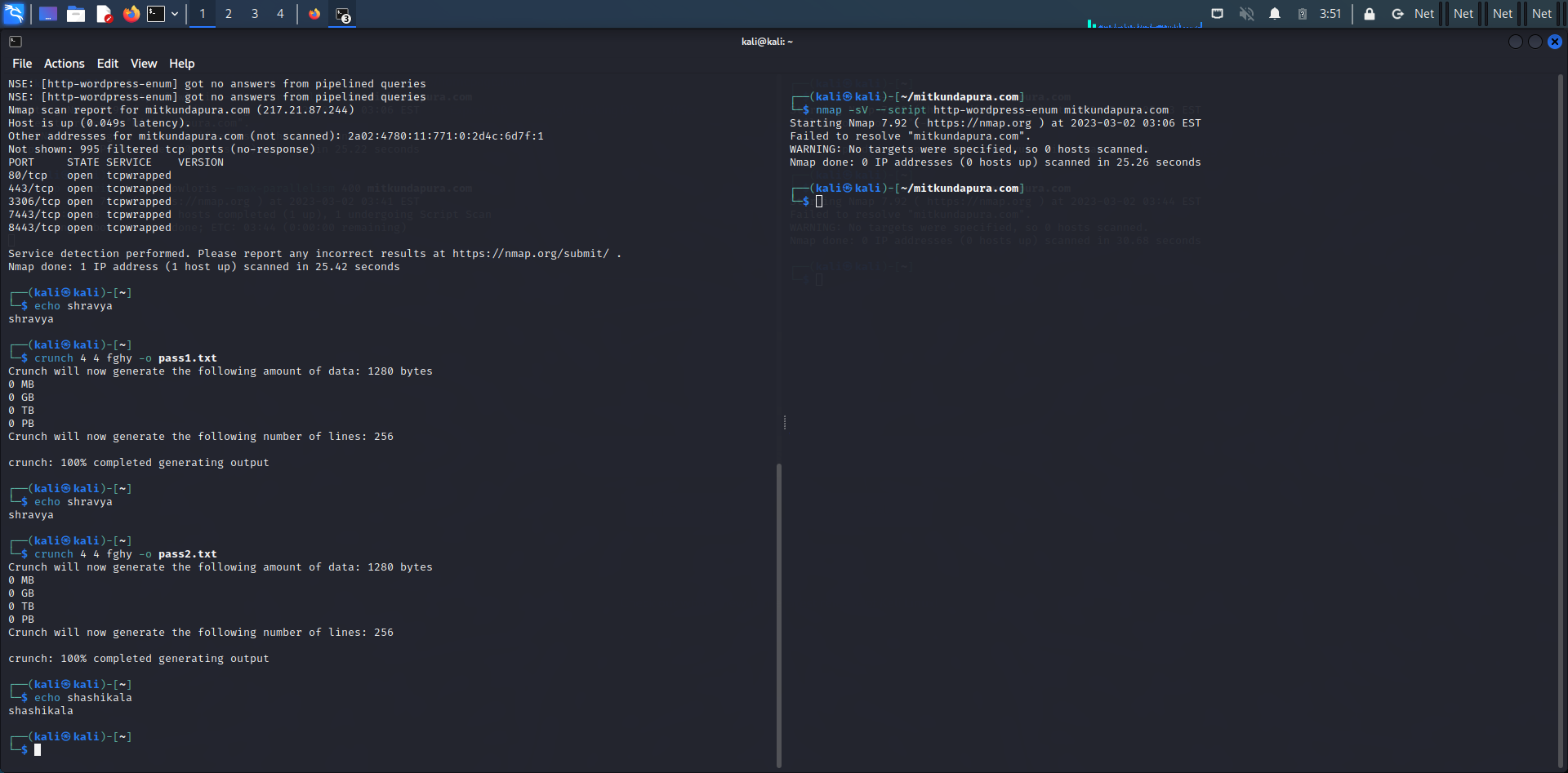


4.**create a password list using characters “fghy” the password should be minimum and maximum length 4 letters using tool crunch:**

Crunch is an easy to use tool for generating a custom made password list used for brute force password cracking. Crunch comes as a standerd tool In kali linux

**Command:**

$Crunch 4 4 fghy -o pass.txt

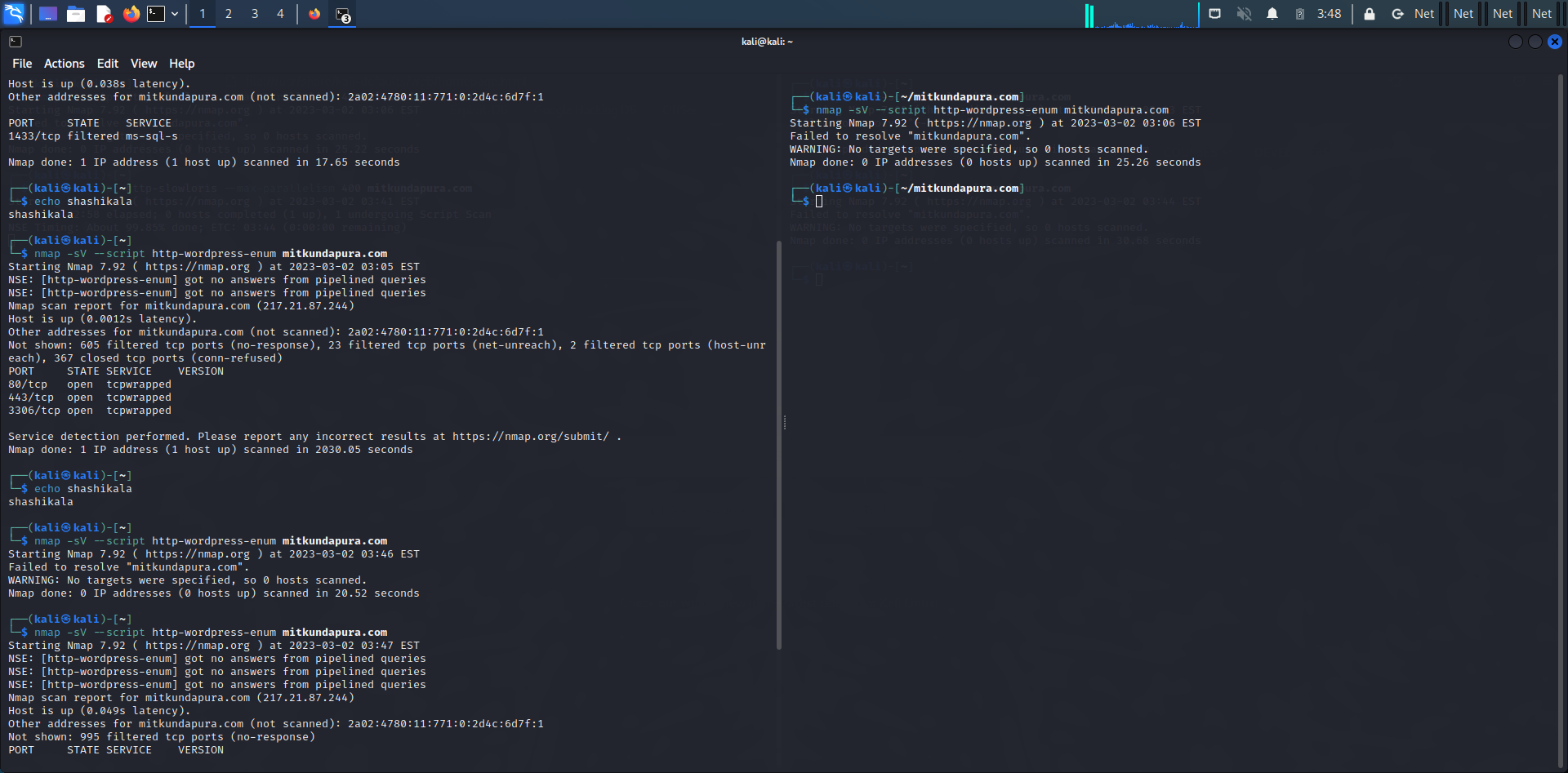


**5.Wordpress scan using nmap:**

WPscan is a security scanner designed for testing the security of websites built using wordpress . wordpress security scanner to test vulnerabilities of wordpress installation.

**Command:**

$nmap -sV --script http-wordpress-enum mitkundapura.com



**6.what is the use of HTTRACKS?**

HTTrack is a free and open-source web crawler and offline browser. HTTrack allows user to download world wide web site from the internet to a local computer

**Command:**

httrack <https://www.mitkundapura.com/>

