**NAME: SHRINATH**

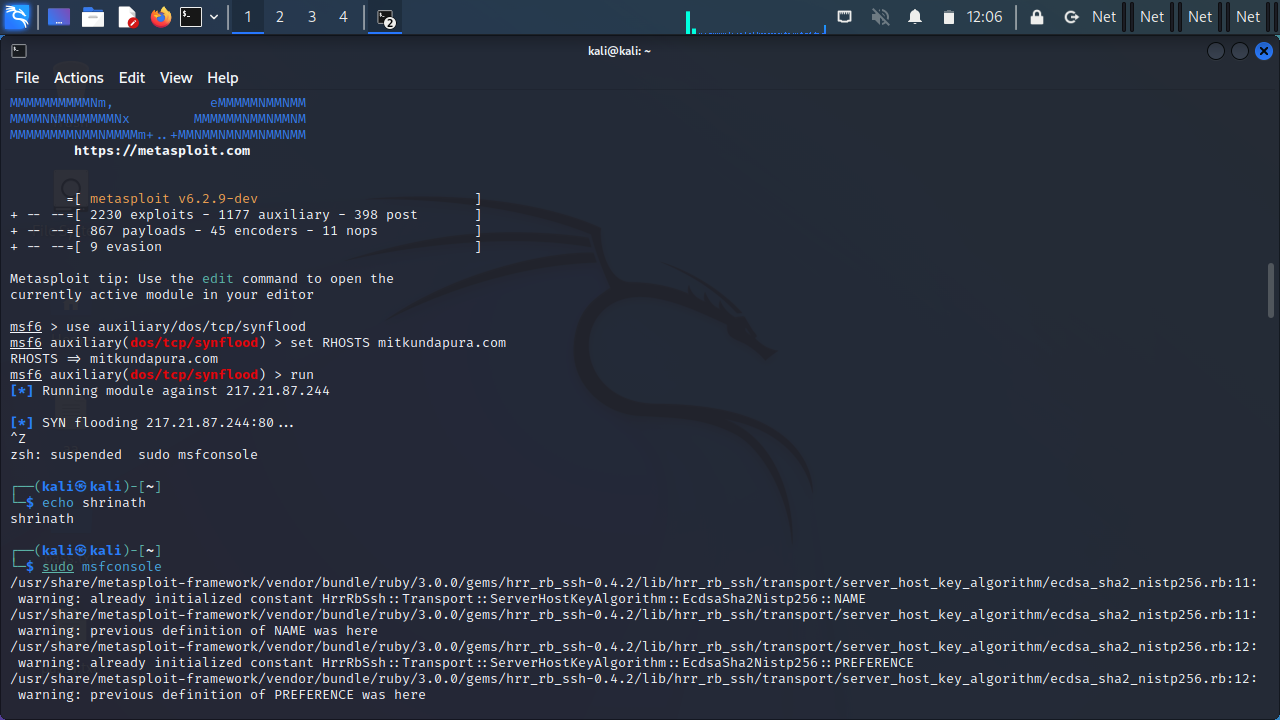
**DATE:28-02-2023**

1. **Dos attack using nmap:**

A denial-of-service (DoS) attack is a malicious attempt to overwhelm a web property with traffic in order to disrupt its normal operations.

**Command**:

$nmap --script http-slowloris --max-parallelism 400 mitkundapura.com

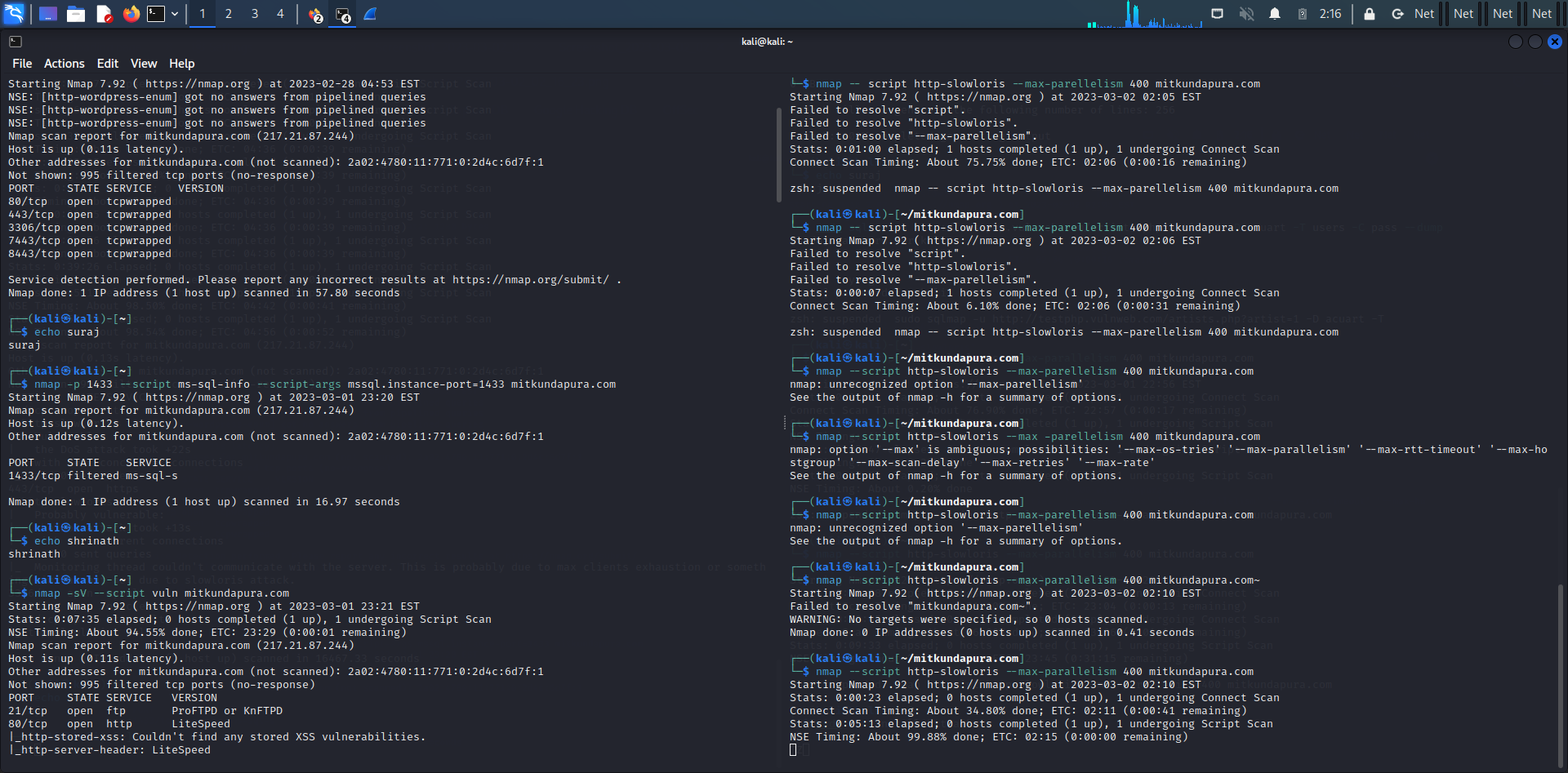


2**. sql empty password enumeration scanning using nmap:**

SQL empty password enumeration scanning using Nmap is a technique used to detect SQL servers that allow for authentication without the use of a password.

**Command**:

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

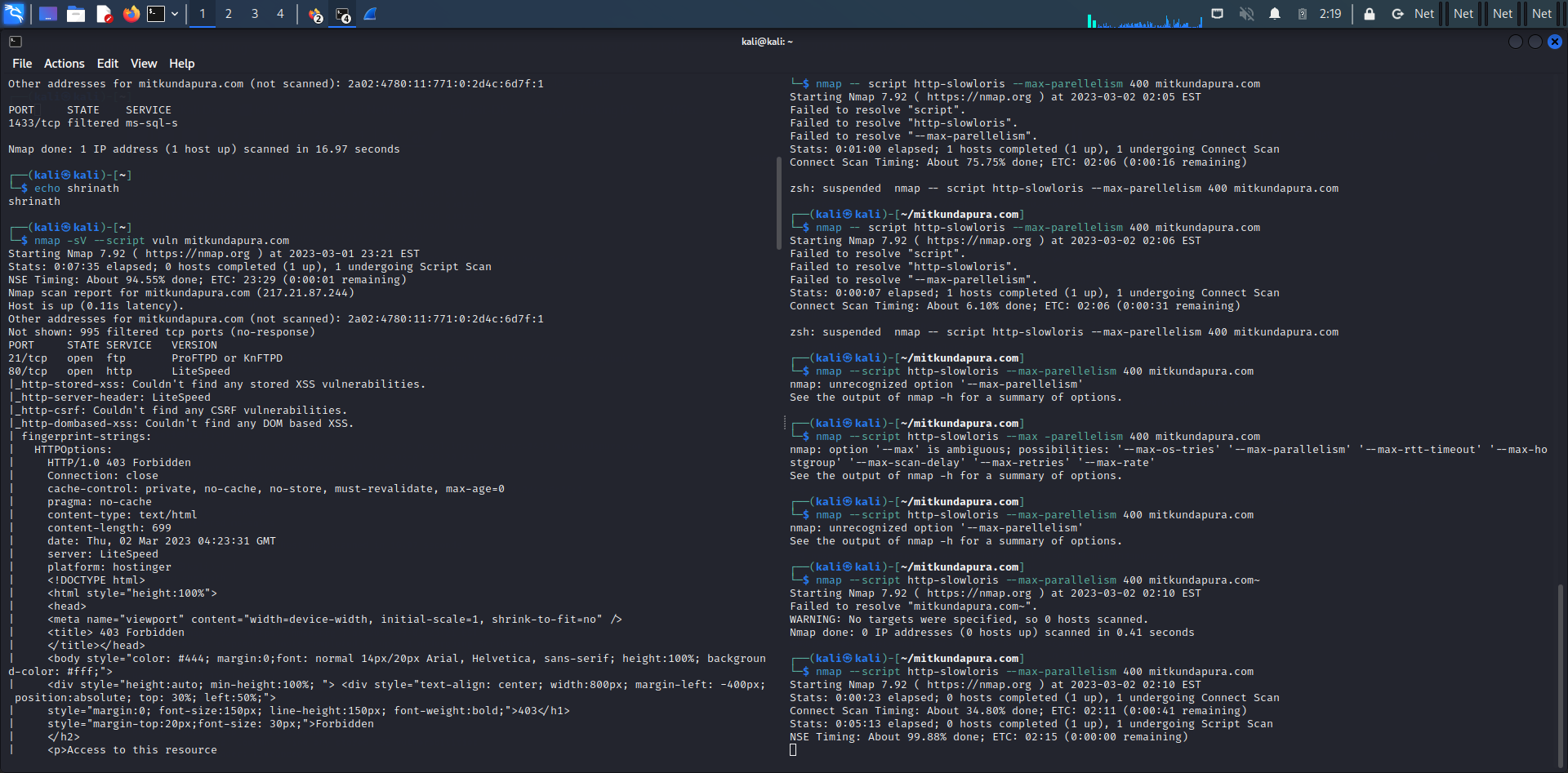


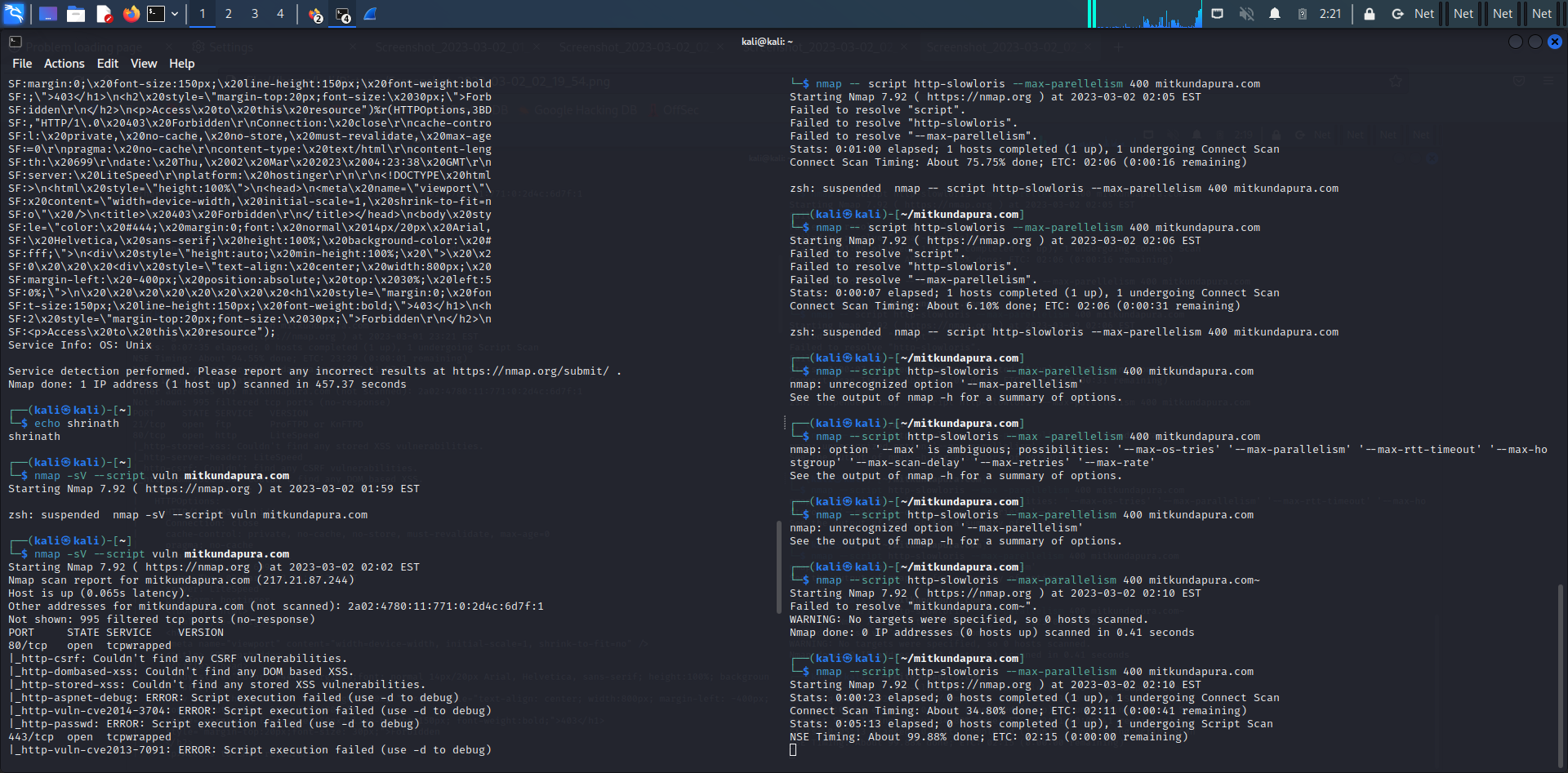
3. **vulnerability scan using nmap:**

A vulnerability scan using Nmap involves scanning a network or a specific target system for known vulnerabilities and weaknesses.

**Command**:

$nmap -sV –script vuln mitkundapura.com



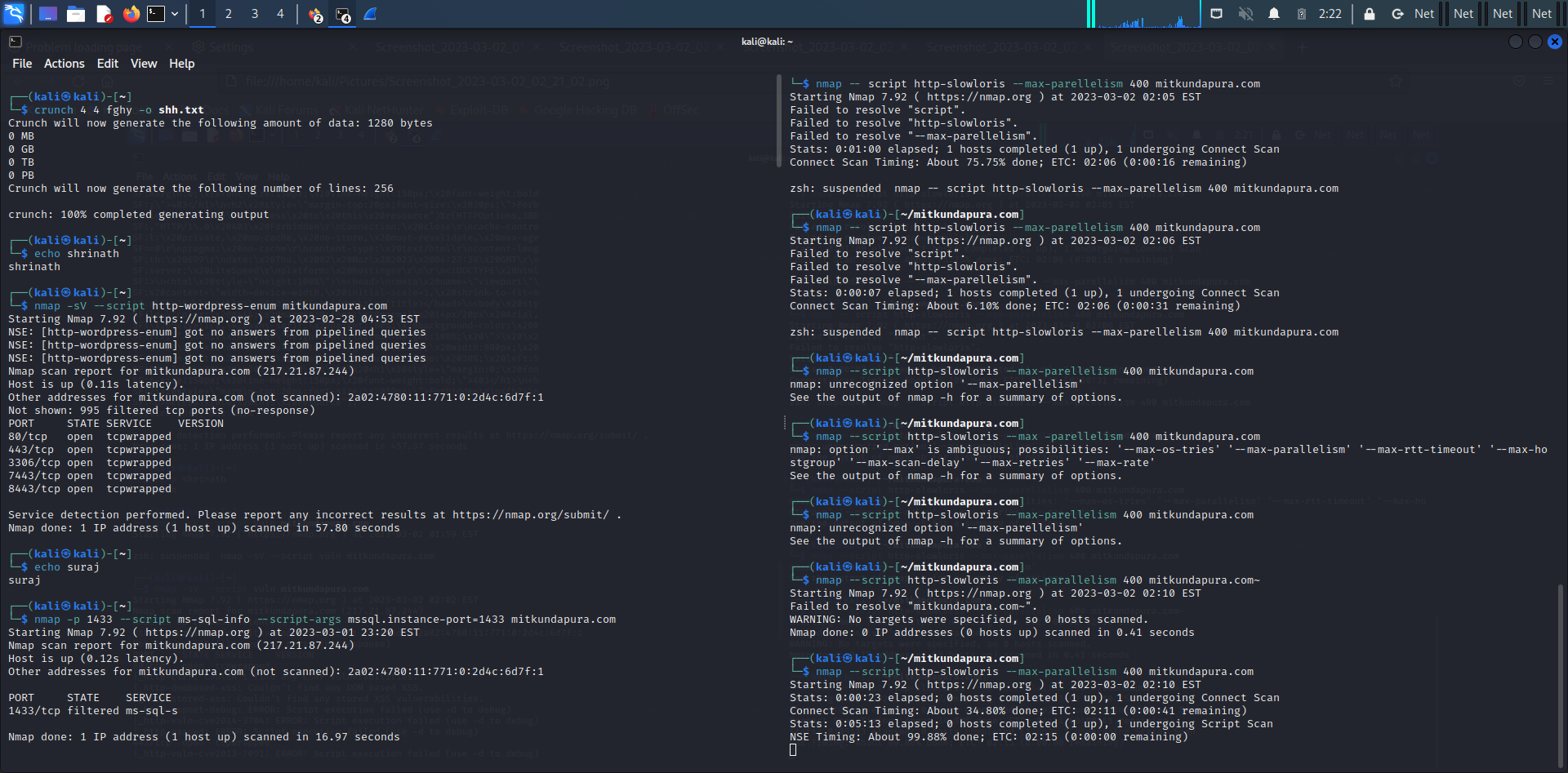


**4.** **create a password list using characters “fghy” the password should be minimum and maximum length 4 letters using tool crunch:**

Crunch is a command-line tool used for generating custom wordlists or password lists. It allows users to define various parameters such as character sets, minimum and maximum length, and other constraints to create a wordlist tailored for specific purposes such as brute force attacks or password cracking.

**Command**:

$Crunch 4 4 fghy -o pass.txt

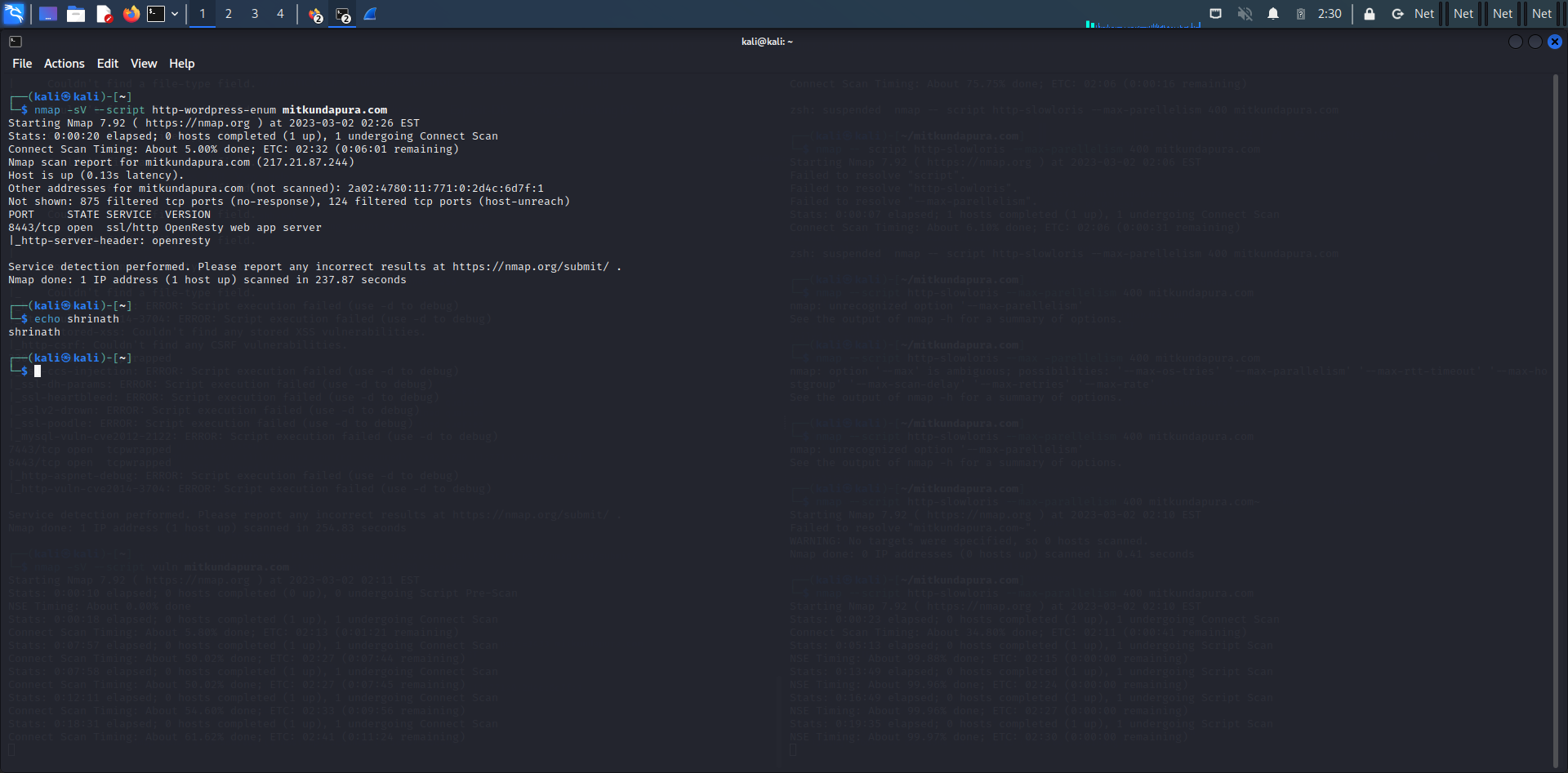


**5.Wordpress scan using nmap:**

WordPress is used to create websites and blogs. As with any popular software, WordPress sites can be targeted by hackers and security vulnerabilities can be exploited.

**Command:**

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



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

Used to download and save a copy of an entire website, including all pages, images, and other files.

Once a website has been downloaded with HTTrack, users can browse the website offline without an internet connection.

**Command:**

httrack https://www.mitkundapura.com/

