**NAME: SURAJ**

**DATE: 07/03/2023**

**TASK: 03**

**1)Johntheripper:**

John the Ripper is popular open source password cracking tool that combines several different cracking programs and runs in both brute force and dictionary attack modes.

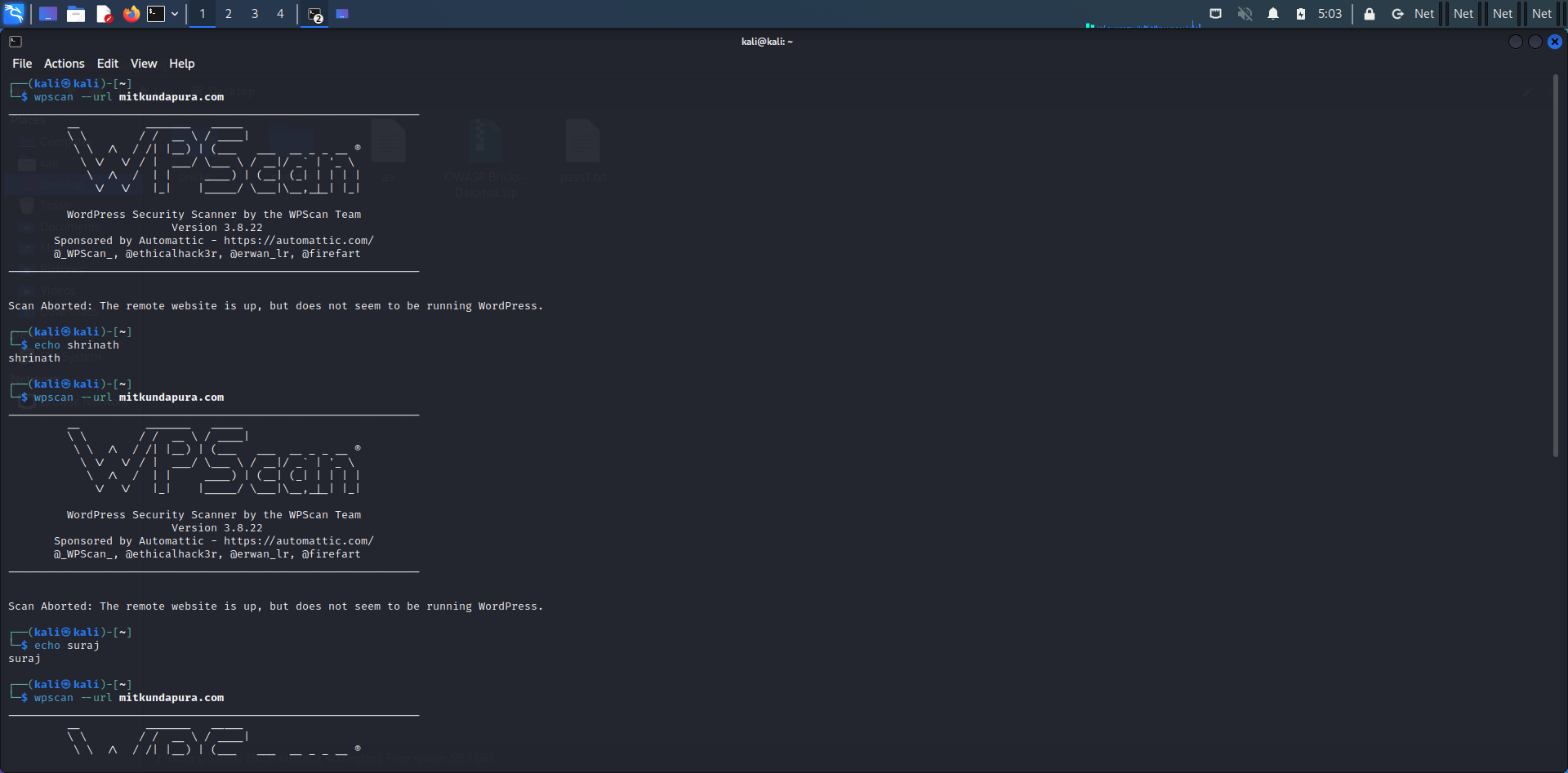
John the repair is often used the enterprises to detect where passwords that could put network security at risk as well as other administrative purposes The software can run a wide variety of password cracking techniques against the various user accounts on each operating system and can be scripted to run locally or remotely.

**2)wpscan:**

WPscan is a security scan a design for testing the security of websites built using wordpress. WPscan was developed using the Ruby programming language and then reduced in the first version in 2019. The WP scan security scanner is premierly intended to be used by worldpress administrators and security teams to assess the security status of their world press installation. It is used to scan worldpress websites for known vulnerabilities both in World Press and commonly used wordpress plugins.

WP scan is avoided press black box scanner.The goal for using WP scan is to execute the activities of real threat actor. WPS scan doesn’t require access to the source code or the world press dashboard. WP scan uses the wpvlnbd.com vulnerability database which is comprehensive list of world press core plugin and team vulnerabilities frequently running WP scan is important to make sure that plug insurance and teams have no exposed vulnerabilities.

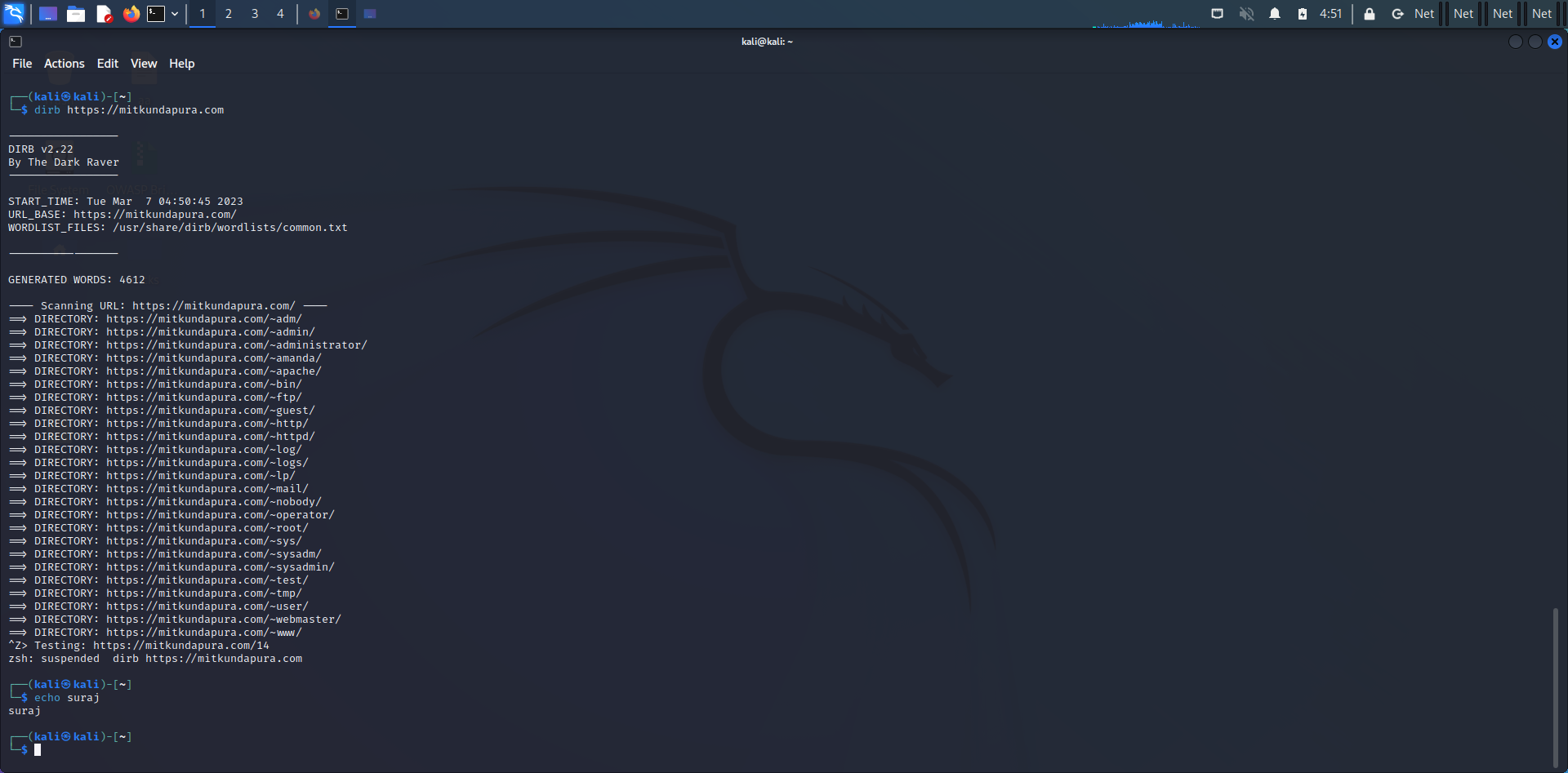
$ wpscan –url mitkundapura.com



**3)dirb command:**

dirb is a web content scanner It looks for existing web objects it basically works by launching a dictionary based attack against Avib Server and analyzing the responses dirbhu comes with a set of preconfigured attack world lists for easy usage But you can use your custom world list

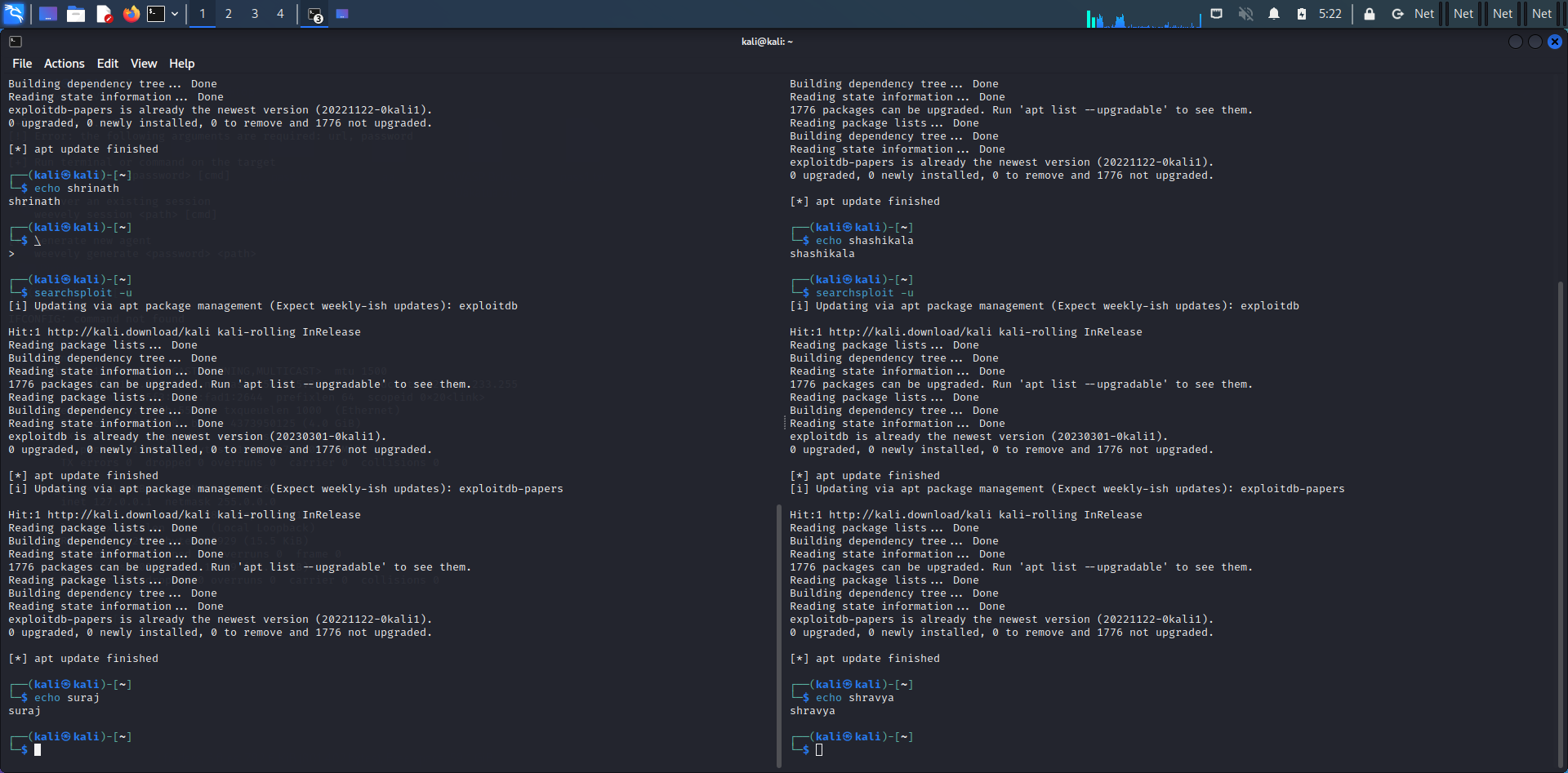
$dirb <https://mitkundapura.com>



**4)searchsploit command:**

Searchsploit is a command-line tool used for searching and exploiting known vulnerabilities in software applications. It is part of the Exploit Database (EDB), which is a popular online repository of exploits and vulnerable software.

$searchsploit -u



**5)weevely command:**

Weevely is a command-line tool used for web application security testing and exploitation. It provides a shell-like interface to interact with a web server, allowing an attacker to execute commands on the server and perform various tasks, including reconnaissance, privilege escalation, data exfiltration, and more.

**$ weevely generate 12345 /root/downloads/pass.php**

**$ weevely** [**http://192.168.233.130/404.php**](http://192.168.233.130/404.php) **12345**

