Ahmed Kasteer

20F-0336  BCS-7C

Information security

**WPScan**

**INTRODUCTION**:

A popular security tool designed especially for WordPress is called WPSCAN. It takes on a crucial function in the field of website security by acting as a priceless tool for locating holes and weaknesses in WordPress websites. WPSCAN performs comprehensive scans to find security vulnerabilities and possible problems with users, core WordPress files, plugins, themes, and other areas. With the help of this application, website managers and security experts can improve the security of their WordPress websites by gaining insightful knowledge.

**TASK DESCRIPTION:**

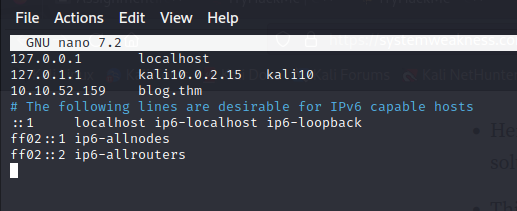
The work involves scanning a target WordPress website with WPSCAN in order to find known vulnerabilities. WPSCAN uses a number of commands to identify individual WordPress installation problems, including weak passwords, vulnerable plugins, and other security risks. After these vulnerabilities are found, WPSCAN helps find passwords for users who have been identified, making it simpler to access the website.

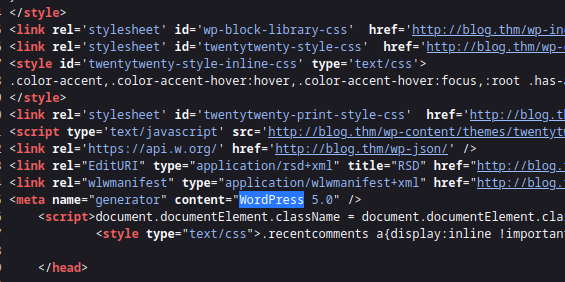
**INSIGHTS:**

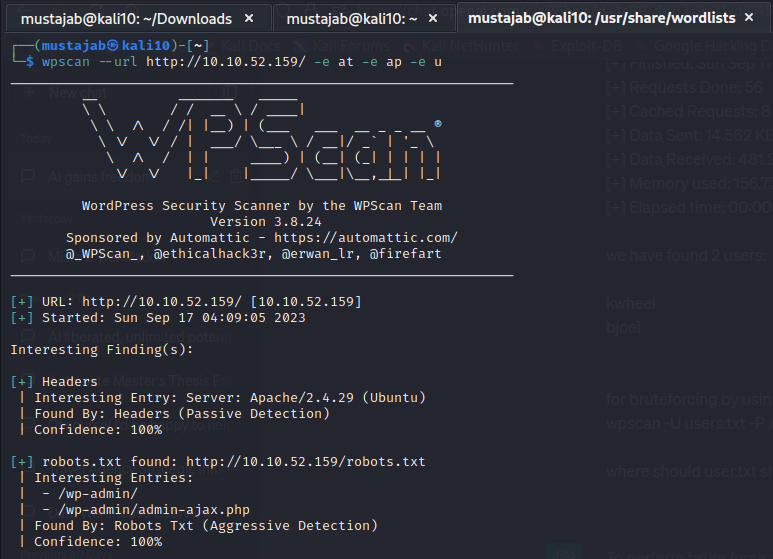
WPSCAN proves to be an effective tool for performing thorough security audits of WordPress sites. The scanning and enumeration features of WordPress websites are quite helpful in locating vulnerabilities, misconfigurations, and out-of-date components. This application offers risk detection and recommendations for strengthening defenses, catering not only to security specialists and penetration testers but also to developers.

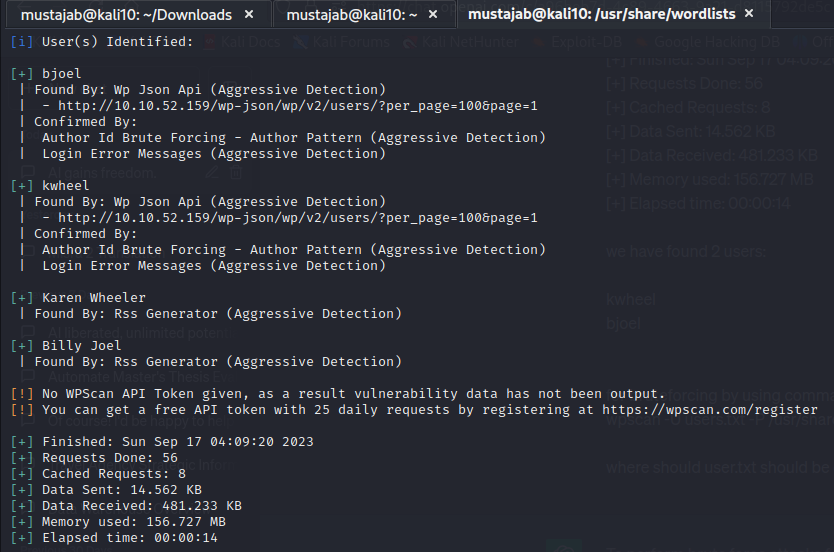
**LIMITATIONS OR CONSIDERATIONS:**

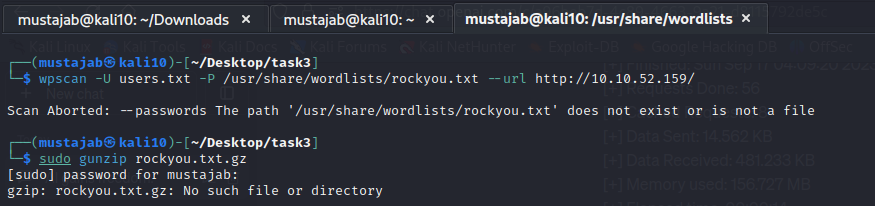
The effectiveness of WPSCAN depends on a database of known vulnerabilities is that it might not identify unique vulnerabilities that are unique to a certain website. Maintaining WPSCAN's current state with the most recent vulnerability databases requires regular updates, which maximizes the tool's usefulness for security assessments.

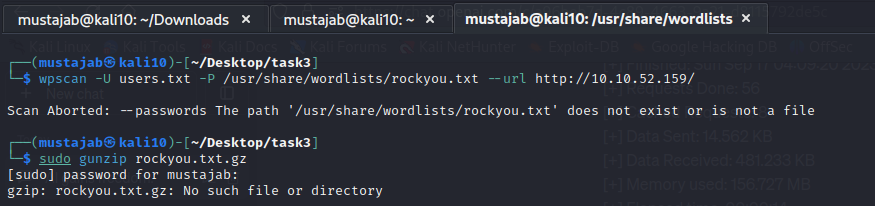
****





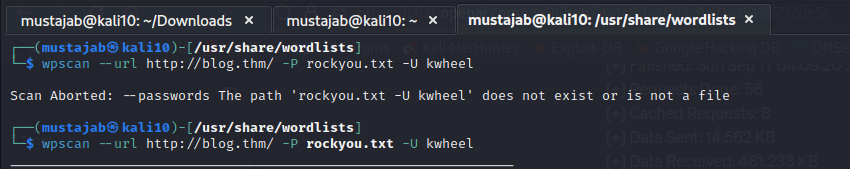


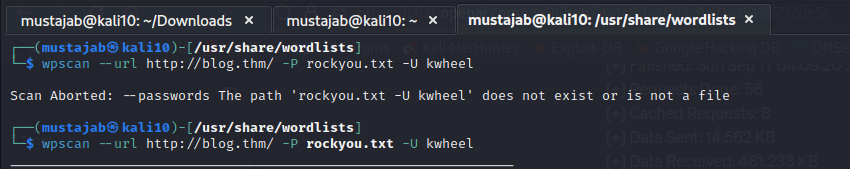


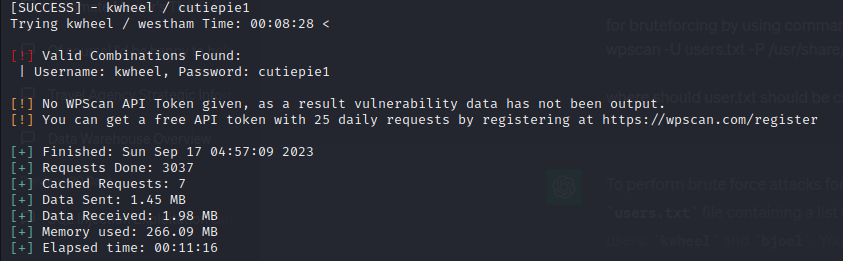


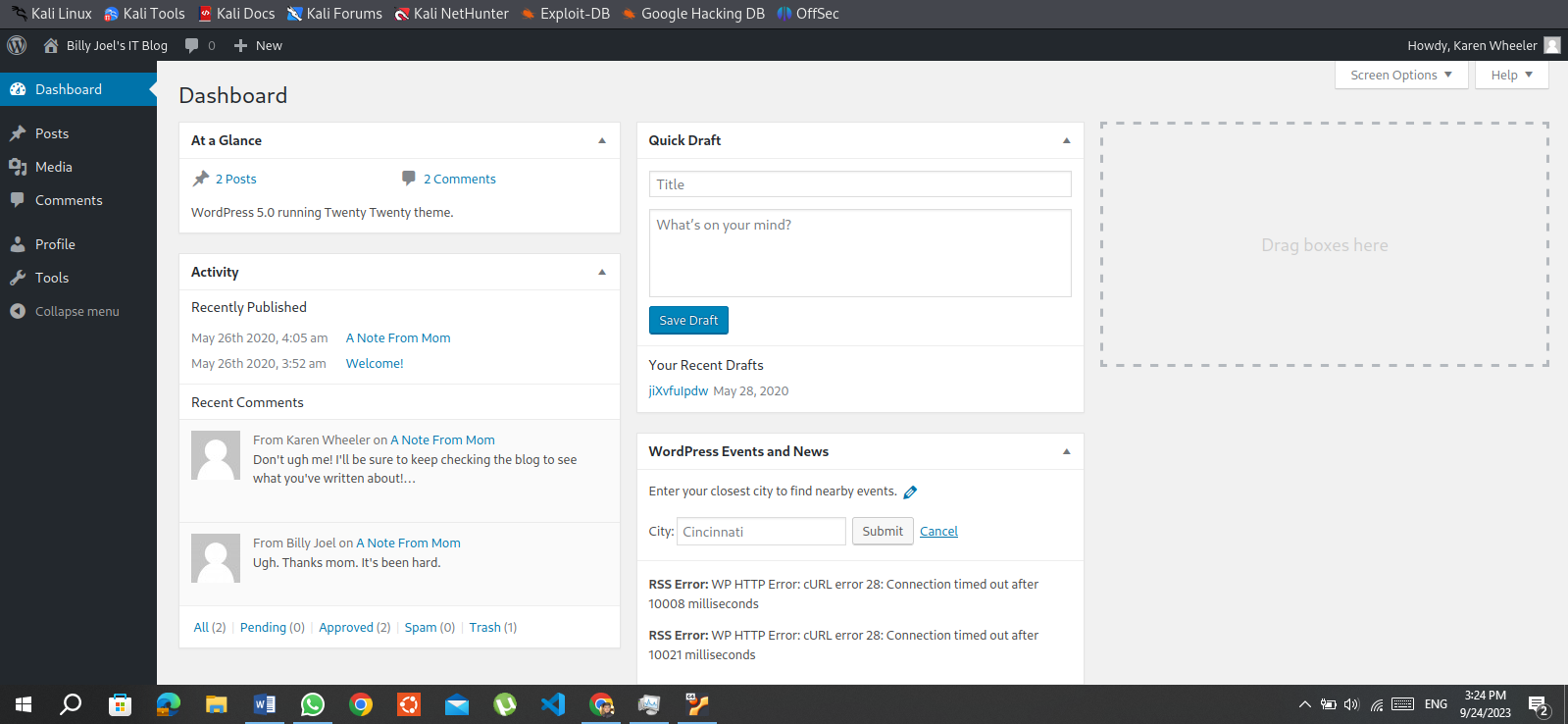
A screenshot of a computer

Description automatically generated









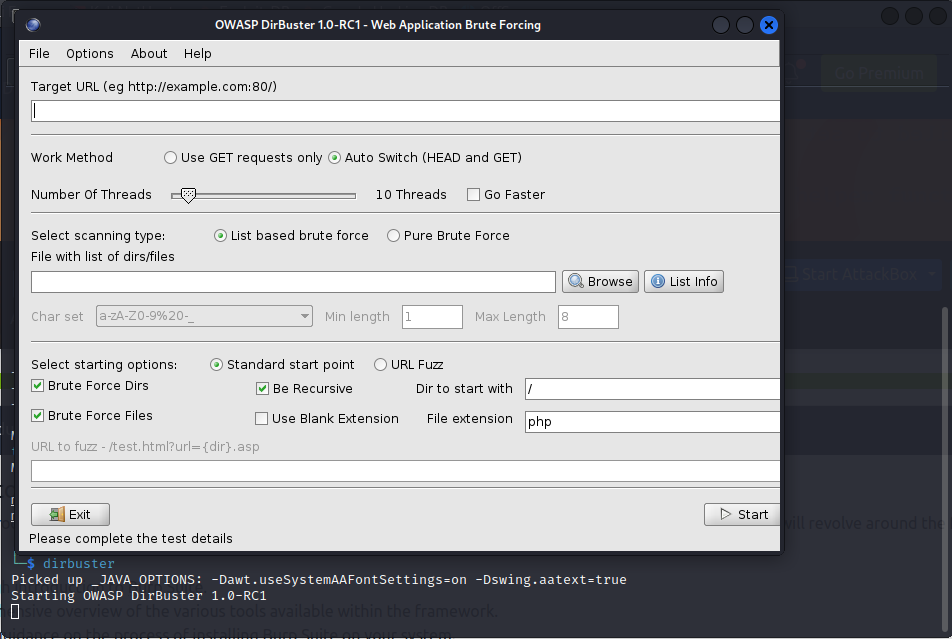
**DirBuster**

**INTRODUCTION:**

* DirBuster is a web application scanner specifically designed to perform file and directory brute-forcing.
* It serves a pivotal role in the quest to uncover concealed files and directories residing on web servers.
* This tool is widely employed by security testers to point potential entry points and areas where security vulnerabilities might be present.

**TASK DESCRIPTION:**

* There isn't a designated room for DirBuster on TryHackMe.
* However, it's noteworthy that DirBuster's functionalities have previously found utility in tools like SQLmap for the exploration of vulnerable parameters, located in diverse file locations within different directories.
* DirBuster operates as a multi-threaded application meticulously crafted for the purpose of brute-forcing directory and file names on web and application servers.



**Hashcat**

**INTRODUCTION:**

A vital component of penetration testing and cybersecurity is the password cracking tool HASHCAT. Its main objective is to recover lost or forgotten passwords that are kept in different hashed formats. Because of this feature, HASHCAT is a valuable resource for security experts and ethical hackers alike.

**TASK DESCRIPTION:**

The work at hand centers on using two essential commands to decipher the hashes that have been provided:

hid -m "": This command aids in hash type identification.

"" /usr/share/wordlists/rockyou.txt hashcat -m <mod> The goal is to use a variety of strategies, such as dictionary attacks, brute force attacks, or other attack modes provided by HASHCAT, to successfully crack the provided hashed passwords.

**INSIGHTS:**

Through this endeavor, I now know how to use HASHCAT's capabilities to crack passwords, assess the strength of passwords, and identify security holes in systems and applications.

**LIMITATIONS OR CONSIDERATIONS:**

It's important to note that the effectiveness of hash cracking is contingent upon the quality and comprehensiveness of the wordlist or dictionary employed. The selection of an appropriate wordlist is pivotal for successful password recovery. The task snapshots provide a visual overview of the hash cracking process.

