Name: Sanketh

Date:07-03-2023

Task:3

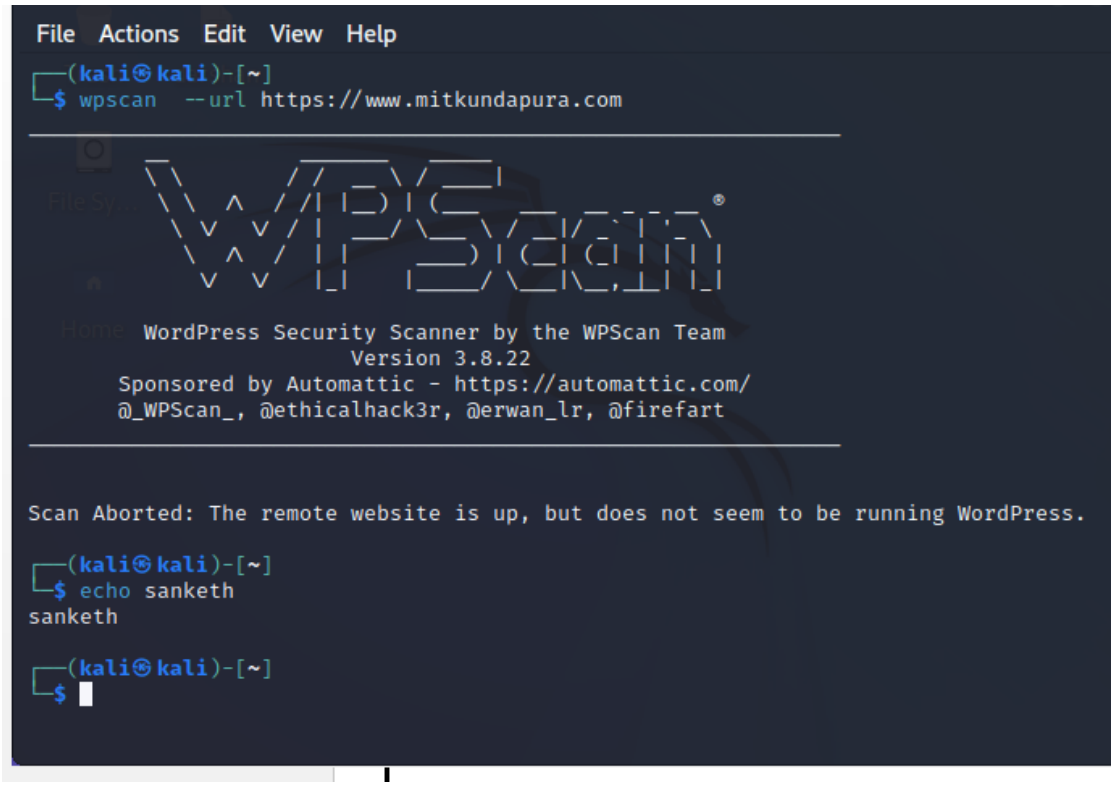
1.johntheripper:

John the Ripper (JtR) is a popular password-cracking tool. John supports many encryption technologies for Windows and Unix systems (Mac included).

One remarkable feature of John is that it can autodetect the encryption for common formats. This will save you a lot of time in researching the hash formats and finding the correct tool to crack them.

2.wpscan:

Wpscan is a vulnerability scanning tool, which comes pre-installed in Kali Linux. This scanner tool scans for vulnerabilities in websites that run WordPress web engines. The wpscan tool itself isn't a malicious tool, as it is only for reconnaissance against a particular site. However, a skilled hacker could use the information obtained from this tool to exploit your websites. Another feature of this tool is that it can, for instance, perform brute force attacks on the supplied URL thus, it is highly recommended to not use the tool (if you are trying to exploit a WordPress running website) on a site, you do not own or have authorization to pentesting.



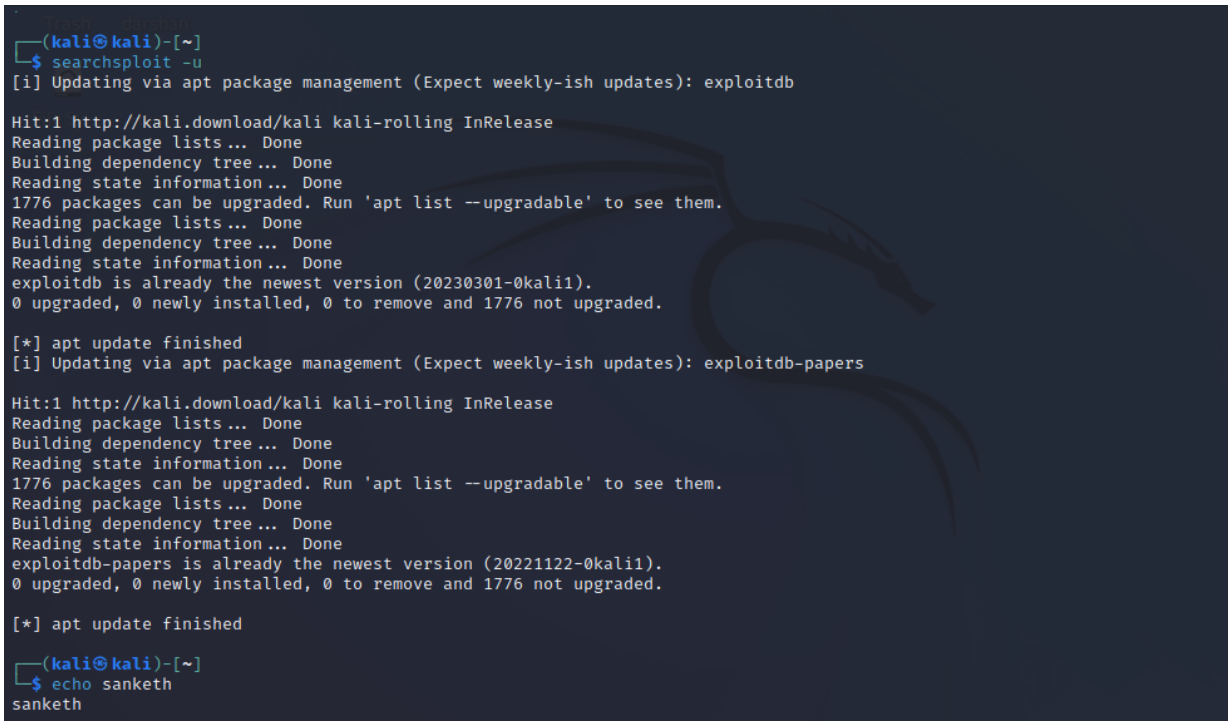
3.dirb:

DIRB is a command line based tool to brute force any directory based on wordlists. DIRB will make an HTTP request and see the HTTP response code of each request.

It internally has a wordlist file which has by default around 4000 words for brute force attack. There are a lot of updated wordlists available over the internet which can also be used. Dirb searches for the words in its wordlist in every directory or object of a website or a server. It might be an admin panel or a subdirectory that is vulnerable to attack. The key is to find the objects as they are generally hidden.

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. SearchSploit is very useful for security assessments when you don't have Internet access because it gives you the power to perform detailed offline searches for exploits in the saved Exploit-DB.



5.weevly:

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.