

Date:07-03-2023

1.johntheripper:

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.

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.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url https://www.mitkundapura.com

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

(kali㉿kali)-[~]
$ echo sanketh
sanketh

(kali㉿kali)-[~]
$
```

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.

```
(kali㉿kali)-[~]
$ dirb https://www.mitkundapura.com

DIRB v2.22
By The Dark Raver

START_TIME: Wed Mar  8 22:34:47 2023
URL_BASE: https://www.mitkundapura.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: https://www.mitkundapura.com/ —
=> DIRECTORY: https://www.mitkundapura.com/~adm/
=> DIRECTORY: https://www.mitkundapura.com/~admin/
=> DIRECTORY: https://www.mitkundapura.com/~administrator/
=> DIRECTORY: https://www.mitkundapura.com/~amanda/
=> DIRECTORY: https://www.mitkundapura.com/~apache/
=> DIRECTORY: https://www.mitkundapura.com/~bin/
=> DIRECTORY: https://www.mitkundapura.com/~ftp/
=> DIRECTORY: https://www.mitkundapura.com/~guest/
=> DIRECTORY: https://www.mitkundapura.com/~http/
=> DIRECTORY: https://www.mitkundapura.com/~httpd/
=> DIRECTORY: https://www.mitkundapura.com/~log/
^Z
zsh: suspended  dirb https://www.mitkundapura.com

(kali㉿kali)-[~]
$ echo sanketh
sanketh
```

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.

```
(kali㉿kali)-[~]
$ searchsploit -u
[i] Updating via apt package management (Expect weekly-ish updates): exploitdb

Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1776 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
exploitdb is already the newest version (20230301-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 1776 not upgraded.

[*] apt update finished
[i] Updating via apt package management (Expect weekly-ish updates): exploitdb-papers

Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1776 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
exploitdb-papers is already the newest version (20221122-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 1776 not upgraded.

[*] apt update finished

(kali㉿kali)-[~]
$ echo sanketh
sanketh
```

5.weevly:

Weevly 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.

```
(kali㉿kali)-[~]  
$ weevly  
[+] weevly 4.0.1  
[!] Error: the following arguments are required: url, password  
  
[+] Run terminal or command on the target  
weevly <URL> <password> [cmd]  
  
[+] Recover an existing session  
weevly session <path> [cmd]  
  
[+] Generate new agent  
weevly generate <password> <path>  
  
(kali㉿kali)-[~]  
$ sudo weevly generate 12345 /root/404.php  
Generated '/root/404.php' with password '12345' of 754 byte size.  
  
(kali㉿kali)-[~]  
$ echo sanketh  
sanketh
```