

Name:SWATHI

Date:07-03-2023

Task:3

1.johntheripper:

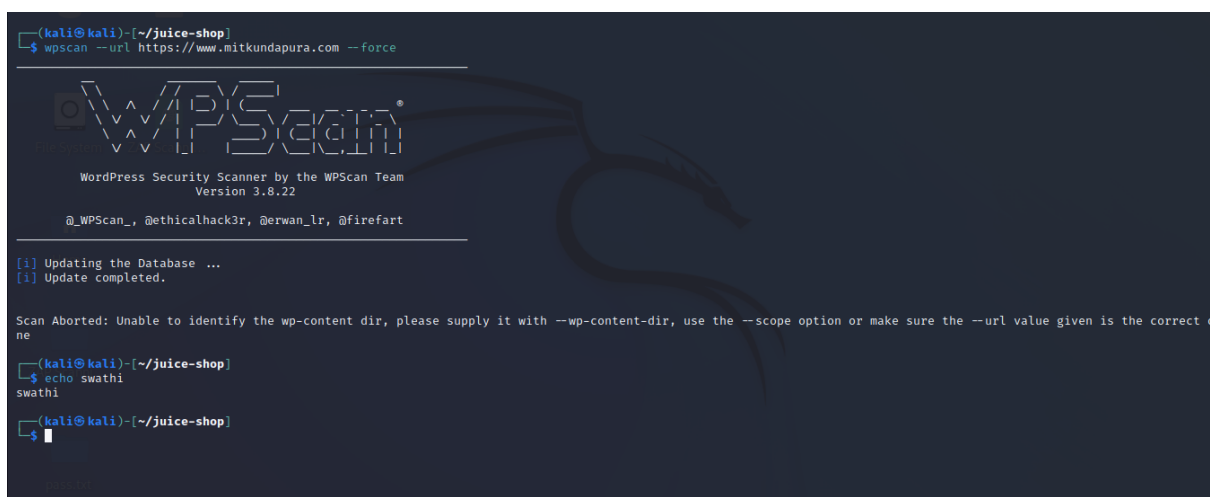
John the Ripper (JtR) is a popular password-cracking tool. John supports many encryption technologies for Windows and Unix systems (Mac included).

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.

`$ wpscan --url http://www.example.com`

A screenshot of a terminal window with a dark background. At the top, the prompt is `(kali@kali)-[~/juice-shop]`. The command `$ wpscan --url https://www.mitkundapura.com --force` has been entered. Below the command, a large, stylized logo for 'WPSecm' is displayed, with the text 'WordPress Security Scanner by the WPSecm Team' and 'Version 3.8.22' underneath it. Below the logo, there are social media handles: '@_WPScan_', '@ethicalhack3r', '@erwan_lr', and '@Firefart'. The terminal shows two status messages: `[i] Updating the Database ...` and `[i] Update completed.`. Below these, a message reads: 'Scan Aborted: Unable to identify the wp-content dir, please supply it with --wp-content-dir, use the --scope option or make sure the --url value given is the correct one'. The prompt returns to `(kali@kali)-[~/juice-shop]`. The command `$ echo swathi` is entered, and the output 'swathi' is shown. The prompt returns to `(kali@kali)-[~/juice-shop]` with a cursor at the end.

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.

```
$ dirb http://www.mitkundapura.com
```

```
(root@kali)-[~]
└─$ dirb https://www.mitkundapura.com

DIRB v2.22
By The Dark Raver

START_TIME: Tue Mar 7 04:51:52 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/
^Z
zsh: suspended  dirb https://www.mitkundapura.com

(root@kali)-[~]
└─$ echo swathi
swathi

(root@kali)-[~]
└─$
```

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.

\$ searchsploit -u

```
(root@kali)-[~]
└─$ searchsploit -u
[*] 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
1773 packages can be upgraded. Run 'apt list --upgradable' to see them.
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontent. It is held by process 72519 (apt)
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 1773 not upgraded.

[*] apt update finished
[*] 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
1773 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 1773 not upgraded.

[*] apt update finished

[*] apt update finished
[*] 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
1773 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 1773 not upgraded.

[*] apt update finished
(root@kali)-[~]
└─$ echo swathi
swathi
```

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.

```
$ weevly generate 1234 404.php
```

```
$ weevly http://192.168.209.130/404.php 1234
```

```
(root@kali)~# weevly generate 12345 /root/downloads/404.php
Generated '/root/downloads/404.php' with password '12345' of 697 byte size.
^[[A
Not Found
(root@kali)~# weevly http://192.168.209.130/404.php 12345
404.php was not found on this server.
[+] weevly 4.0.1
[+] Target: 0 (192.168.209.130) server at 192.168.209.130 Port 80
[+] Session: /root/.weevly/sessions/192.168.209.130/404_0.session
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.
weevly>
zsh: suspended weevly http://192.168.209.130/404.php 12345
(root@kali)~# echo swathi
swathi
(root@kali)~#
```