

Name: Shilpa

Reg.No:145CS20016

Date: 07-03-2023

### Task-3

#### 1.John the ripper:

John the ripper is a popular open source password cracking tool that combines several different cracking programs and runs in both brute force and dictionary attack modes.

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, at 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.

```
(kali㉿kali)-[~/Downloads]
$ wpscan --url http://example.com

WPScan
WordPress Security Scanner by the WPScan Team
Version 3.8.22
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.

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

(kali㉿kali)-[~/Downloads]
$ echo shilpa
shilpa
```

### 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 to each request.

It internally has a wordlist file which has by default around 4000 words for brute force attack. There are a lot of updates wordlists available over the internet which can also be used. Dirb searches for the words in its wordlist in every directory or object of 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)-[~/Downloads]
$ dirb http://www.mitkundapura.com

DIRB v2.22
By The Dark Raver

File System: /usr/share/dirb/wordlists/common.txt
START_TIME: Wed Mar  8 03:55:56 2023
URL_BASE: http://www.mitkundapura.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://www.mitkundapura.com/ —
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
(Try using FineTunning: '-f')

END_TIME: Wed Mar  8 03:55:57 2023
DOWNLOADED: 0 - FOUND: 0

(kali㉿kali)-[~/Downloads]
$ echo shilpa
shilpa
```

### 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 in 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.

```
(root㉿kali)-[/home/kali]
# searchsploit openssh 7.2

Exploit Title | Path
-----|-----
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (P | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Comma | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Dis | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Li | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration | linux/remote/40113.txt

Shellcodes: No Results

(kali㉿kali)-[/home/kali]
# echo shilpa
shilpa
```

## 5.weevely:

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 has stealth backdoor or as a web shell to manage legit web accounts, even free hosted once.

```
(kali㉿kali)-[~]
$ weevely generate 12345 404.php
Generated '404.php' with password '12345' of 754 byte size.

(kali㉿kali)-[~]
$ weevely http://192.168.31.129/404.php 12345

[+] weevely 4.0.1
[+] Target:      192.168.31.129
[+] Session:     /home/kali/.weevely/sessions/192.168.31.129/404_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
zsh: suspended  weevely http://192.168.31.129/404.php 12345

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