

**Name: PRAMAL POOJARY**

**REG NO : 145CS20011**

**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.

```
(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

Contact Us

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

(kali@kali)-[~]
$ echo PRAMAL
PRAMAL
```

### 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: Tue Mar 7 05:03:41 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/~admin/
=> 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/
=> DIRECTORY: https://www.mitkundapura.com/~logs/
=> DIRECTORY: https://www.mitkundapura.com/~lp/
=> DIRECTORY: https://www.mitkundapura.com/~mail/
=> DIRECTORY: https://www.mitkundapura.com/~nobody/
=> DIRECTORY: https://www.mitkundapura.com/~operator/
```

```
=> 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/
=> DIRECTORY: https://www.mitkundapura.com/~logs/
=> DIRECTORY: https://www.mitkundapura.com/~lp/
=> DIRECTORY: https://www.mitkundapura.com/~mail/
=> DIRECTORY: https://www.mitkundapura.com/~nobody/
=> DIRECTORY: https://www.mitkundapura.com/~operator/
=> DIRECTORY: https://www.mitkundapura.com/~root/
=> DIRECTORY: https://www.mitkundapura.com/~sys/
=> DIRECTORY: https://www.mitkundapura.com/~sysadm/
=> DIRECTORY: https://www.mitkundapura.com/~sysadmin/
=> DIRECTORY: https://www.mitkundapura.com/~test/
=> DIRECTORY: https://www.mitkundapura.com/~tmp/
=> DIRECTORY: https://www.mitkundapura.com/~user/
=> DIRECTORY: https://www.mitkundapura.com/~webmaster/
=> DIRECTORY: https://www.mitkundapura.com/~www/
^Z Testing: https://www.mitkundapura.com/10
zsh: suspended dirb https://www.mitkundapura.com

(kali@kali)-[~]
└─$ echo PRAMAL
PRAMAL
```

## 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: ~  
File Actions Edit View Help  
[kali@kali]~  
$ searchsploit -u  
[i] Updating via apt package management (Expect weekly-ish updates): exploitdb  
  
[sudo] password for kali:  
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  
  
Reading package lists... Done  
E: Could not get lock /var/lib/apt/lists/lock. It is held by process 2183 (apt)  
N: Be aware that removing the lock file is not a solution and may break your system.  
E: Unable to lock directory /var/lib/apt/lists/  
  
[-] Issue with apt update (Please check network connectivity & apt SourcesList values)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  exploitdb-papers  
0 upgraded, 1 newly installed, 0 to remove and 1776 not upgraded.  
Need to get 2561 MB of archives.  
After this operation, 2952 MB of additional disk space will be used.  
Get:1 http://kali.download/kali kali-rolling/main amd64 exploitdb-papers all 20221122-0kali1 [2561 MB]  
Fetched 2561 MB in 3min 59s (10.7 MB/s)  
  
File Actions Edit View Help  
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  
  
Reading package lists... Done  
E: Could not get lock /var/lib/apt/lists/lock. It is held by process 2183 (apt)  
N: Be aware that removing the lock file is not a solution and may break your system.  
E: Unable to lock directory /var/lib/apt/lists/  
  
[-] Issue with apt update (Please check network connectivity & apt SourcesList values)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  exploitdb-papers  
0 upgraded, 1 newly installed, 0 to remove and 1776 not upgraded.  
Need to get 2561 MB of archives.  
After this operation, 2952 MB of additional disk space will be used.  
Get:1 http://kali.download/kali kali-rolling/main amd64 exploitdb-papers all 20221122-0kali1 [2561 MB]  
Fetched 2561 MB in 3min 59s (10.7 MB/s)  
Selecting previously unselected package exploitdb-papers.  
(Reading database ... 338571 files and directories currently installed.)  
Preparing to unpack .../exploitdb-papers_20221122-0kali1_all.deb ...  
Unpacking exploitdb-papers (20221122-0kali1) ...  
  
zsh: suspended searchsploit -u  
  
[kali@kali]~  
$ echo PRAMAL  
PRAMAL
```

## 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.

```
(root@kali)-[~]  
# weevly generate 12345 404.php  
Generated '404.php' with password '12345' of 677 byte size.  
  
(root@kali)-[~]  
# echo PRAMAL  
PRAMAL  
  
(root@kali)-[~]  
#
```