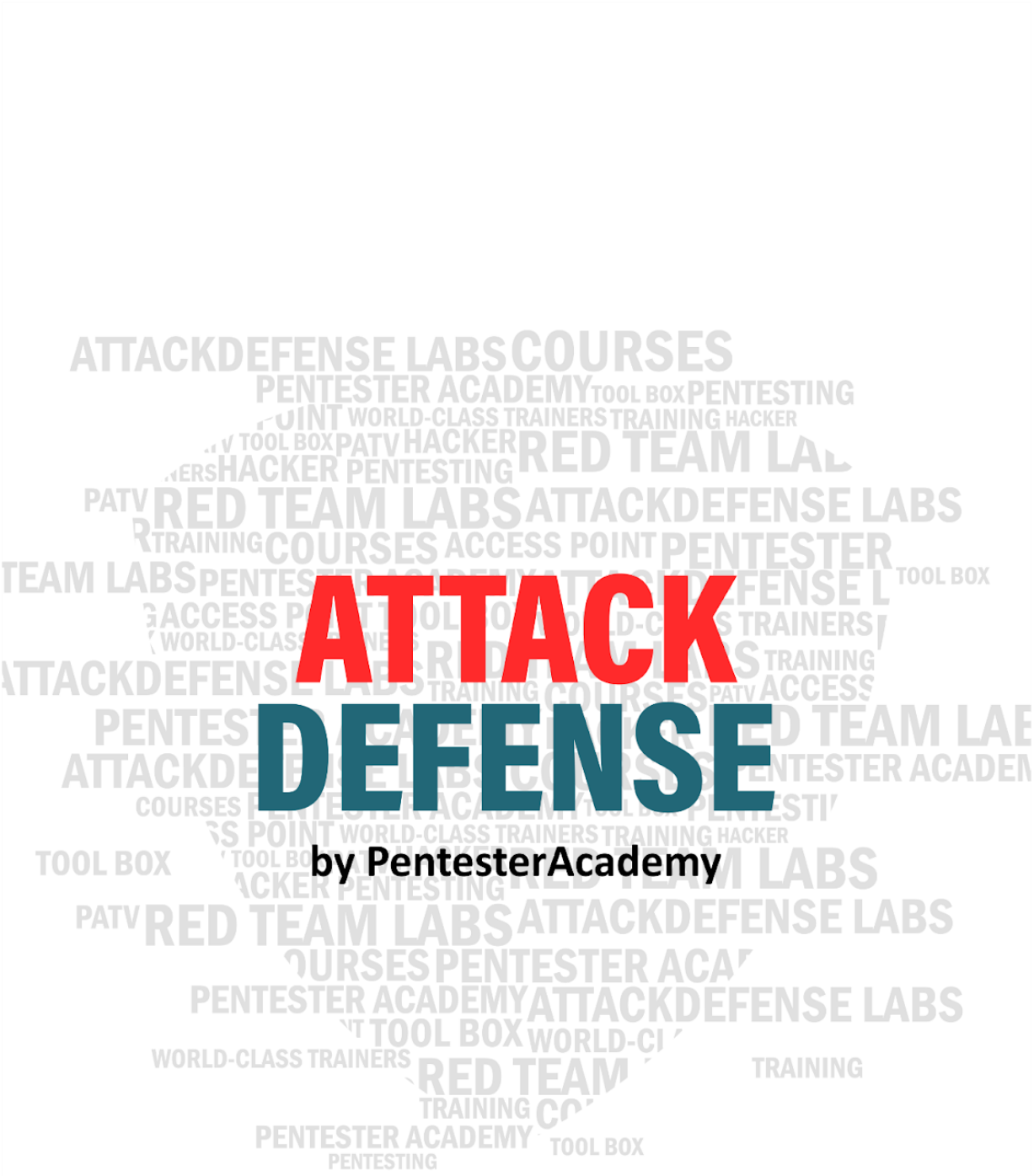
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking MS Word .doc
URL	https://www.attackdefense.com/challengedetails?cid=109
Type	Cracking : Protected Files

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

User should try dictionary attack using the provided dictionary file first. If the dictionary attack doesn't succeeds, then the user should go for mask based bruteforce approach according to given password policy.

Step 1: An encrypted MS Word .doc file is given. Extract the crackable information from the file using John the Ripper tools and check file contents

Command: office2john MS_Word_Document_97_2003.doc > hash

```
student@attackdefense:~$ cat hash
MS_Word_Document_97_2003.doc:$oldoffice$4*f1efb1c529cff63cb08cf439df074c5d*9256d6abe832
ff6ea:::::MS_Word_Document_97_2003.doc
student@attackdefense:~$
```

Step 2: We can use either of two tools

John The Ripper (JTR)

Launch dictionary attack using given dictionary file 1000000-password-seclists.txt

Command: john --wordlist=1000000-password-seclists.txt hash

```
student@attackdefense:~$  john --wordlist=1000000-password-seclists.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (oldoffice, MS Office <= 2003 [MD5/SHA1 RC4 32/64])
Cost 1 (hash type) is 4 for all loaded hashes
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
AMORTEAM         (MS_Word_Document_97_2003.doc)
1g 0:00:00:02 DONE (2018-11-04 04:08) 0.4016g/s 259084p/s 259084c/s 259084C/s ashrba02..akbayan
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Flag: AMORTEAM

Hashcat

Make extracted crackable information hashcat compatible.

```
student@attackdefense:~$ cat hash
$oldoffice$4*f1efb1c529cff63cb08cf439df074c5d*9256d6abe8325534e7dae97f9f5967d9*8f015d41
student@attackdefense:~$
```

Launch mask based attack on the extracted information.

Command: hashcat -m 9800 hash -a 0 1000000-password-seclists.txt

Explanation

-m 9600	:	MS Office 2003 format
-a 0	:	Dictionary mode

```
$oldoffice$4*f1efb1c529cff63cb08cf439df074c5d*9256d6abe8325534e7dae97f9f5967d9*8f015d410f45812c5e554ab7a147f1d9285ff6ea:AMORTEAM

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MS Office <= 2003 $3/$4, SHA1 + RC4
Hash.Target......: $oldoffice$4*f1efb1c529cff63cb08cf439df074c5d*9256d...5ff6ea
Time.Started.....: Sun Nov  4 04:19:12 2018 (2 secs)
Time.Estimated...: Sun Nov  4 04:19:14 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:   385.7 kH/s (139.53ms) @ Accel:80 Loops:1 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 717850/1000003 (71.78%)
Rejected.........: 1050/717850 (0.15%)
Restore.Point....: 615268/1000003 (61.53%)
Candidates.#1....: broadsta -> 1sucker
HWMon.Dev.#1.....: N/A
```

Flag: AMORTEAM

References:

1. Hashcat (https://hashcat.net)
2. Hashcat Wiki (https://hashcat.net/wiki/)
3. John the ripper jumbo (https://www.openwall.com/john/)