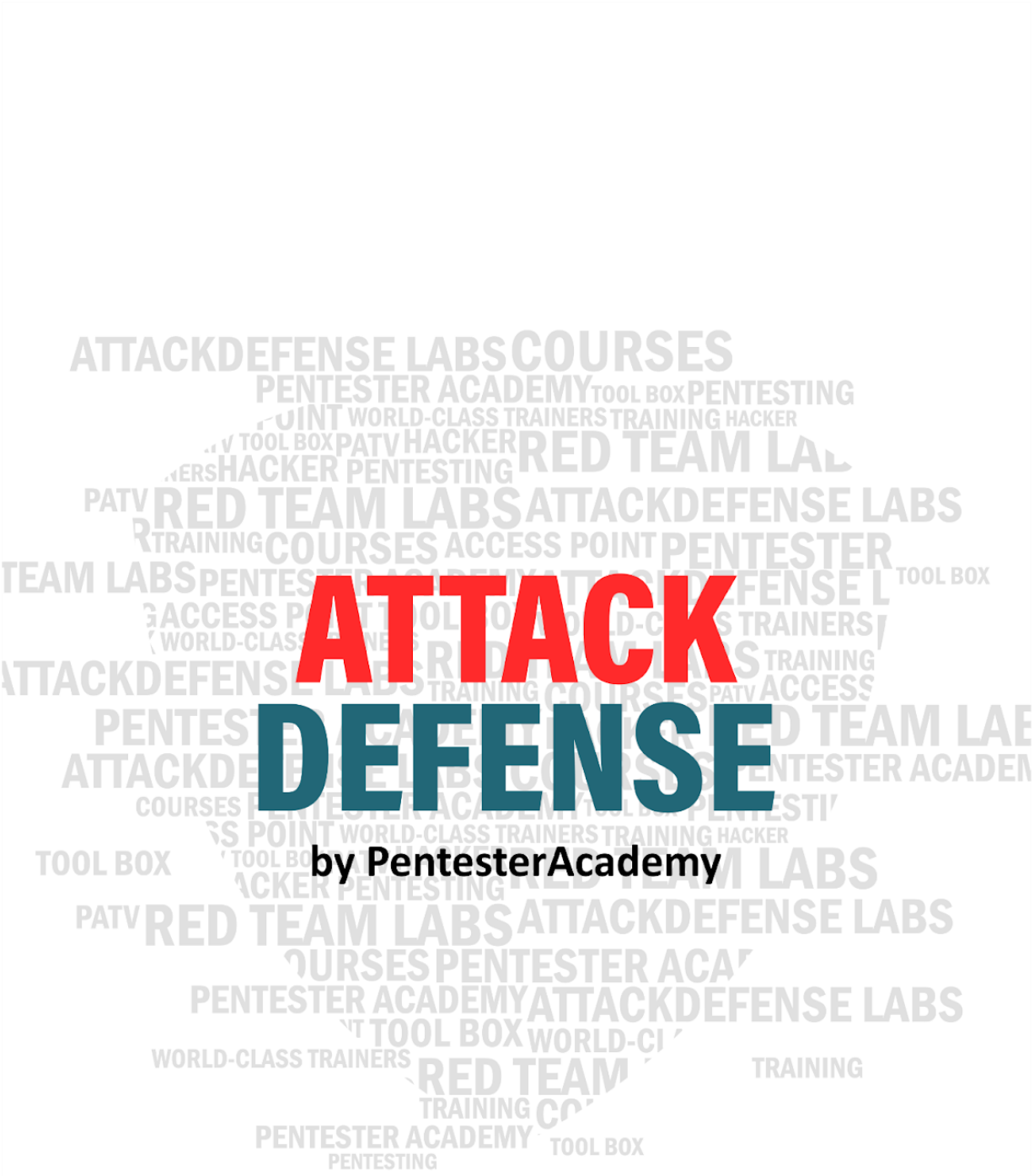
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking PDF (PDF 1.1-1.3)
URL	https://www.attackdefense.com/challengedetails?cid=716
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.

Note: Some snapshots are clipped to make them readable. So, screen content will not be an exact match. However, solutions will still match.

Step 1: An encrypted PDF (PDF 1.1-1.3) file is given. Extract the crackable information from the file using John the Ripper tools and check file contents

Command: tools/JohnTheRipper/pdf2john.pl secret.pdf > hash

```
root@attackdefense:~# tools/JohnTheRipper/pdf2john.pl secret.pdf > hash
root@attackdefense:~# cat hash
secret.pdf:$pdf$1*2*40*-64*1*16*b616d7f4fa31cae9a866bf776a0d1af1*32*74627f0e25f5972719fc3447c60201aeb40def3bb1
5cfabb35a316ec144e4fe1237fb7e7a657fcacd334445a224aef81ac7
root@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=/root/wordlists/1000000-password-seclists.txt hash

```
root@attackdefense:~#
root@attackdefense:~# john --wordlist=/root/wordlists/1000000-password-seclists.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Jamestow9        (secret.pdf)
1g 0:00:00:00 DONE (2018-12-06 16:11) 2.702g/s 810818p/s 810818c/s 810818C/s Jamestow9
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@attackdefense:~#
```

Password: Jamestow9

Hashcat (JTR)

We have to make edit the hash file to make it hashcat compatible. For this, remove the preceding file name i.e. “secret.pdf:”

Launch dictionary attack.

Command: hashcat -m 10400 hash -a 0 /root/wordlists/1000000-password-seclists.txt --force

Explanation

-m 10400	:	PDF (1.1.-1.3) format
-a 0	:	Dictionary mode

```
$pdf$1*2*40*-64*1*16*b616d7f4fa31cae9a866bf776a0d1af1*32*74627f0e25f5972719fc3447c60201aeb40def3bb1d4f9533f96fa6fc3090bc9*32*
6ec144e4fe1237fb7e7a657fcacd334445a224aef81ac7:Jamestow9

Session..........: hashcat
Status...........: Cracked
Hash.Type........: PDF 1.1 - 1.3 (Acrobat 2 - 4)
Hash.Target......: $pdf$1*2*40*-64*1*16*b616d7f4fa31cae9a866bf776a0d1a...f81ac7
Time.Started.....: Thu Dec  6 16:12:33 2018 (1 sec)
Time.Estimated...: Thu Dec  6 16:12:34 2018 (0 secs)
Guess.Base.......: File (wordlists/1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   369.0 kH/s (43.06ms) @ Accel:88 Loops:1 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 315392/1000003 (31.54%)
Rejected.........: 0/315392 (0.00%)
Restore.Point....: 270336/1000003 (27.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: robjack -> ds70726
```

Password: Jamestow9

Step 3: Decrypt the PDF and retrieve the flag.

Commands:
pdftotext -upw Jamestow9 secret.pdf
cat secret.txt

```
root@attackdefense:~# pdftotext -upw Jamestow9 secret.pdf
root@attackdefense:~# ls -l
total 48
-rw-r--r-- 1 root root   293 Nov 25 15:54 README
-rw-r--r-- 1 root root   190 Dec  7 06:03 hash
-rw-r--r-- 1 root root 24738 Dec  6 14:17 secret.pdf
-rw-r--r-- 1 root root    41 Dec  7 06:04 secret.txt
drwxr-xr-x 1 root root  4096 Dec  6 12:12 tools
drwxr-xr-x 1 root root  4096 Dec  6 14:23 wordlists
root@attackdefense:~# cat secret.txt
Flag: 7106eec34b6affc8975a8edc058c3521


root@attackdefense:~#
```

Flag: 7106eec34b6affc8975a8edc058c3521

References:

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