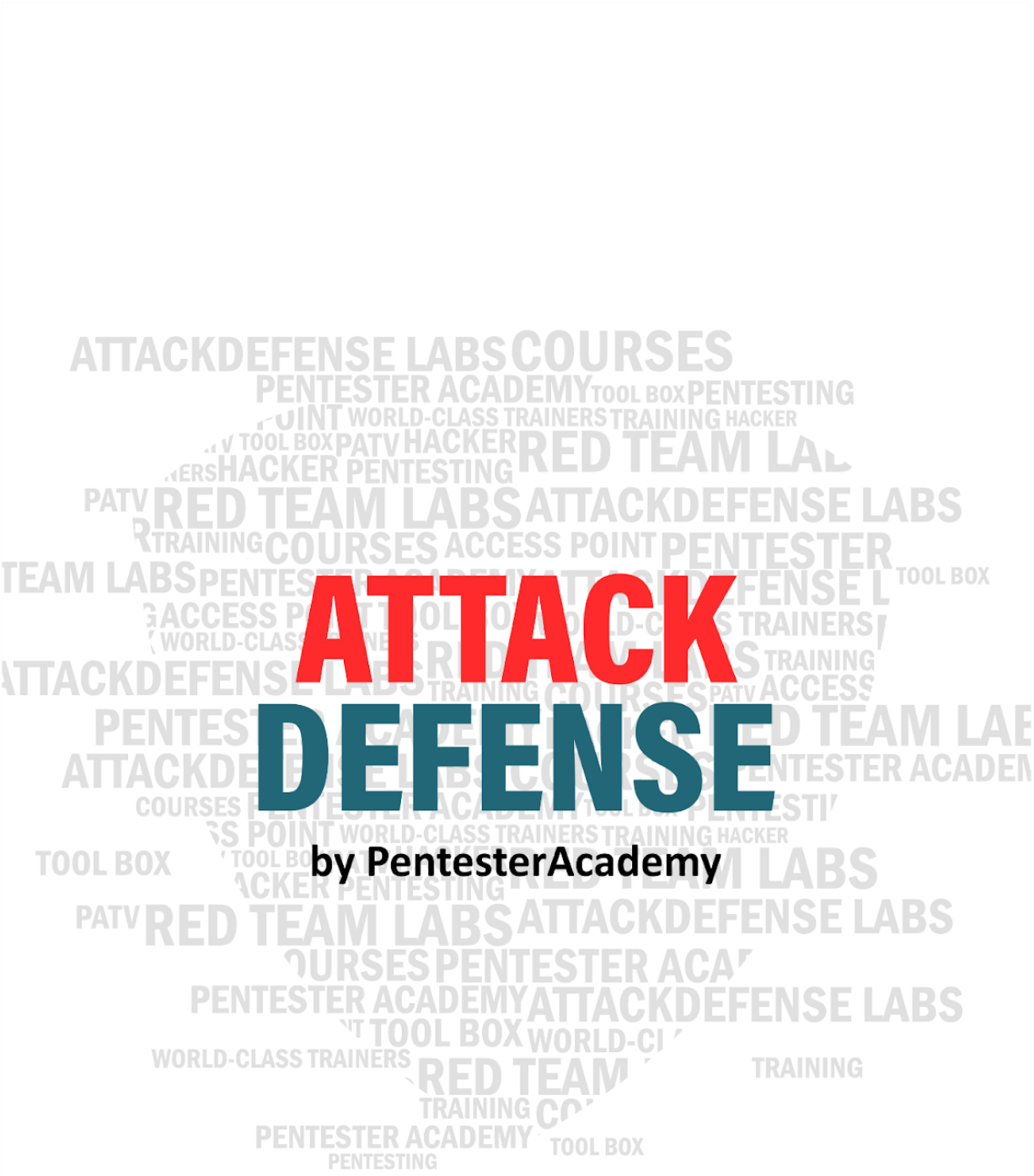
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking PDF (PDF 1.4-1.6)
URL	https://www.attackdefense.com/challengedetails?cid=717
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 1.4-1.6) 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$2*3*128*-3904*1*16*400fe7ec4c2ecbba360a1e4707085fd5*32*924ea8d9badcbd235a750efb0891
ec3846be71e419c10ae059c0b3507a21440ae0cf17189c92755918e90561
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:~# john --wordlist=/root/wordlists/1000000-password-seclists.txt hash
Created directory: /root/.john
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
sopranos         (secret.pdf)
1g 0:00:00:00 DONE (2018-12-06 16:19) 3.846g/s 44415p/s 44415c/s 44415C/s sopranos
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@attackdefense:~#
```

Password: sopranos

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:”

```
root@attackdefense:~# vim hash
root@attackdefense:~# cat hash
$pdf$2*3*128*-3904*1*16*400fe7ec4c2ecbba360a1e4707085fd5*32*924ea8d9badcbd235a750efb0891f4830000000000000000000000000000
419c10ae059c0b3507a21440ae0cf17189c92755918e90561
root@attackdefense:~#
```

Launch dictionary attack.

Command: hashcat -m 10500 hash -a 0 /root/wordlists/1000000-password-seclists.txt --force

Explanation

-m 10500	:	PDF (1.4.-1.6) format
-a 0	:	Dictionary mode

```
$pdf$2*3*128*-3904*1*16*400fe7ec4c2ecbba360a1e4707085fd5*32*924ea8d9badcbd235a750efb0891f48300000000000
419c10ae059c0b3507a21440ae0cf17189c92755918e90561:sopranos

Session..........: hashcat
Status...........: Cracked
Hash.Type........: PDF 1.4 - 1.6 (Acrobat 5 - 8)
Hash.Target......: $pdf$2*3*128*-3904*1*16*400fe7ec4c2ecbba360a1e47070...e90561
Time.Started.....: Thu Dec  6 16:20:22 2018 (1 sec)
Time.Estimated...: Thu Dec  6 16:20:23 2018 (0 secs)
Guess.Base.......: File (wordlists/1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    35352 H/s (121.43ms) @ Accel:80 Loops:8 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 40960/1000003 (4.10%)
Rejected.........: 0/40960 (0.00%)
Restore.Point....: 0/1000003 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:64-70
Candidates.#1....: 123456 -> taint
```

Password: sopranos

Step 3: Decrypt the PDF and retrieve the flag.

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

```
root@attackdefense:~# pdftotext -upw sopranos secret.pdf
root@attackdefense:~# ls -l
total 44
-rw-r--r-- 1 root root   293 Nov 25 15:54 README
-rw-r--r-- 1 root root   193 Dec  7 06:22 hash
-rw-r--r-- 1 root root 24319 Dec  6 12:14 secret.pdf
-rw-r--r-- 1 root root    41 Dec  7 06:23 secret.txt
drwxr-xr-x 1 root root  4096 Dec  6 12:12 tools
drwxr-xr-x 1 root root  4096 Dec  6 12:34 wordlists
root@attackdefense:~# cat secret.txt
Flag: 49cdf40206c7c06c49f8284f83dfd7a3


root@attackdefense:~#
```

Flag: 49cdf40206c7c06c49f8284f83dfd7a3

References:

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