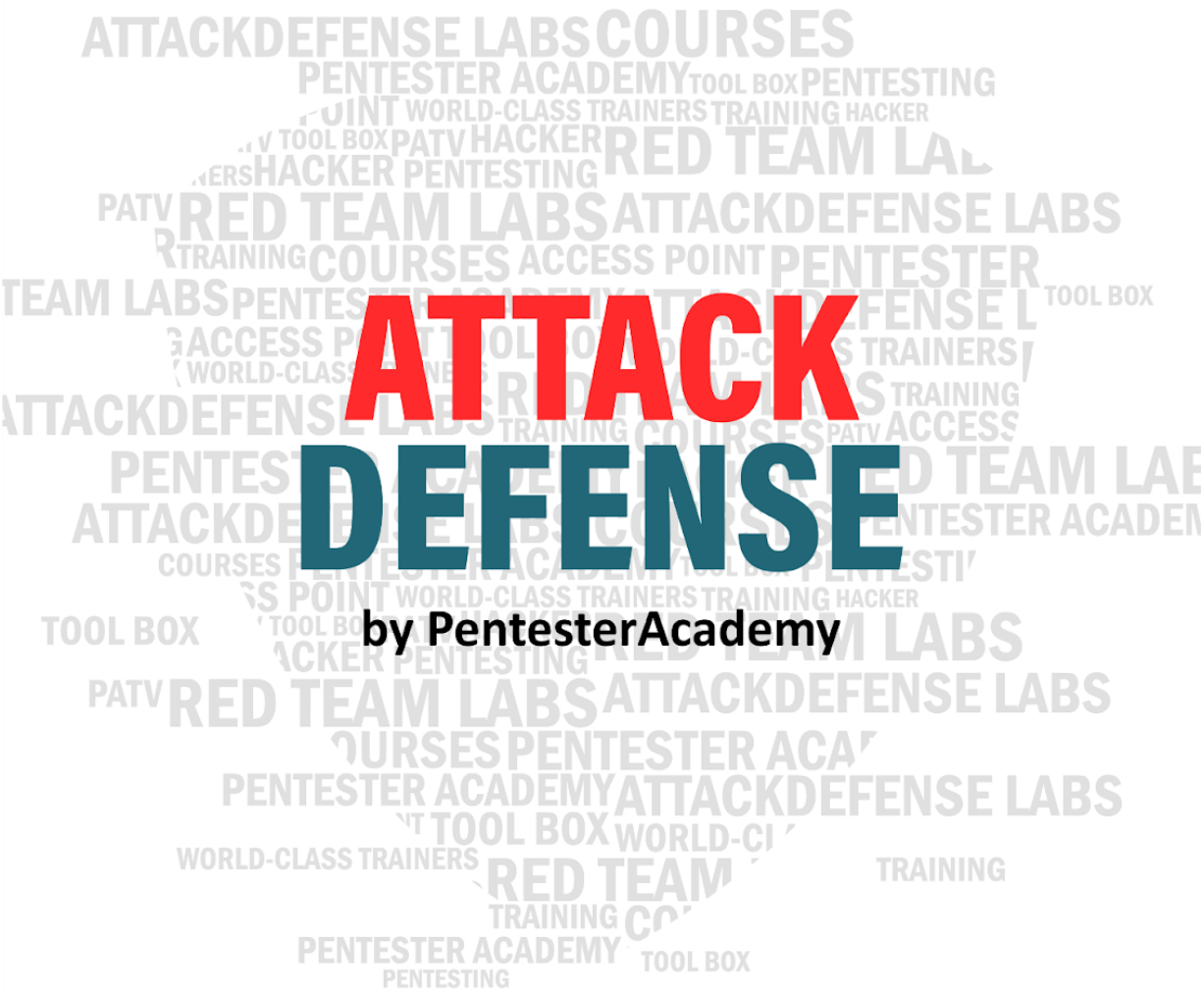
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking HMAC-SHA1 key
URL	https://www.attackdefense.com/challengedetails?cid=53
Type	Cracking : Hashcat All

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: A plain-text string and corresponding HMAC-SHA1 digest is provided in digest.txt file. Check the file contents.

```
student@attackdefense:~$ cat digest.txt
Input : tinkerbell97
HMAC Digest: 69f7e54d484620ed6e9d731ca51780a000463fc2
student@attackdefense:~$
```

This format is not hashcat compliant, change it.

```
student@attackdefense:~$ cat digest.txt
69f7e54d484620ed6e9d731ca51780a000463fc2:tinkerbell97
student@attackdefense:~$
```

Step 2: Launch dictionary attack using given dictionary file 1000000-password-seclists.txt

Command: hashcat -m 150 -a 0 digest.txt 1000000-password-seclists.txt

Explanation

-m 150 : HMAC-SHA1 digest mode
-a 0 : Dictionary attack mode

```
69f7e54d484620ed6e9d731ca51780a000463fc2:tinkerbell97:tinhouse

Session..........: hashcat
Status...........: Cracked
Hash.Type........: HMAC-SHA1 (key = $pass)
Hash.Target......: 69f7e54d484620ed6e9d731ca51780a000463fc2:tinkerbell97
Time.Started.....: Sun Nov  4 00:41:09 2018 (0 secs)
Time.Estimated...: Sun Nov  4 00:41:09 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:   821.9 kH/s (18.51ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 409600/1000003 (40.96%)
Rejected.........: 0/409600 (0.00%)
Restore.Point....: 389120/1000003 (38.91%)
Candidates.#1....: vanda1 -> suka33
HWMon.Dev.#1.....: N/A
```

Flag: tinhouse

References:

1. Hashcat (https://hashcat.net)
2. Hashcat Wiki (https://hashcat.net/wiki/)