ATTACK DEFENSE

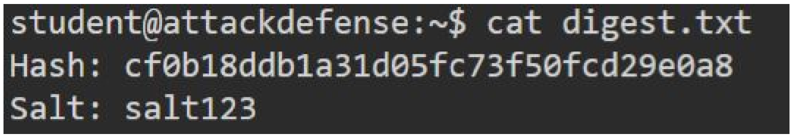
by PentesterAcademy

Name	Cracking Salted MD5 Hashes
URL	https://www.attackdefense.com/challengedetails?cid=52
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.

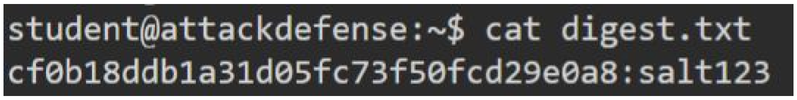
User should try dictionary attack using the provided dictionary file first. If the dictionary attack doesn't succeeds, then the user should go for mask based bruteforce approach according to given password policy.

Step 1: Check the given salted MD5 hash and salt.



```
student@attackdefense:~$ cat digest.txt
Hash: cf0b18ddb1a31d05fc73f50fcd29e0a8
Salt: salt123
```

This input format is not hashcat compliant, change it.



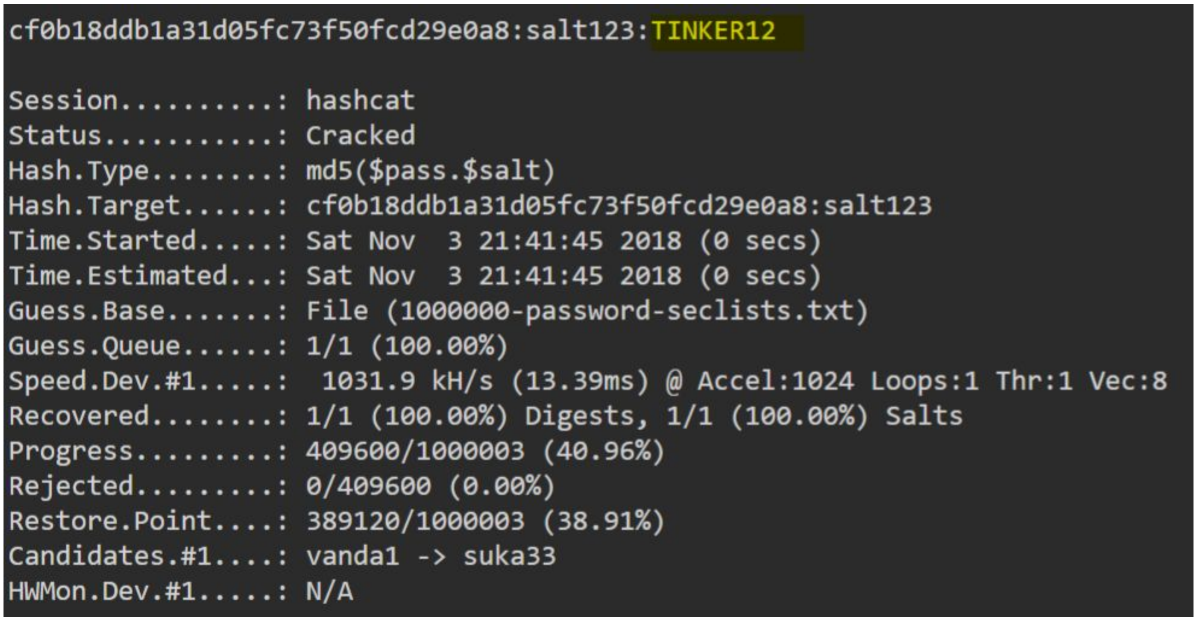
```
student@attackdefense:~$ cat digest.txt
cf0b18ddb1a31d05fc73f50fcd29e0a8:salt123
```

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

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

Explanation

-m 10	:	Salted MD5 hash mode
-a 0	:	Dictionary attack mode



```
cf0b18ddb1a31d05fc73f50fcd29e0a8:salt123:TINKER12

Session..........: hashcat
Status...........: Cracked
Hash.Type........: md5($pass.$salt)
Hash.Target......: cf0b18ddb1a31d05fc73f50fcd29e0a8:salt123
Time.Started.....: Sat Nov  3 21:41:45 2018 (0 secs)
Time.Estimated...: Sat Nov  3 21:41:45 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:  1031.9 kH/s (13.39ms) @ 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: TINKER12

References:

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