ATTACK DEFENSE

by PentesterAcademy

Name	Cracking SSH known_hosts File
URL	https://www.attackdefense.com/challengedetails?cid=104
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.

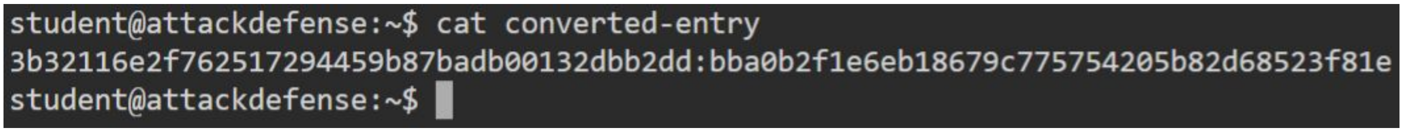
User should try dictionary attack using the provided dictionary file first. If the dictionary attack doesn't succeeds, then the user should go for mask based bruteforce approach according to given password policy.

Step 1: The python script (kh-converter.py) needed to convert the SSH host entry into a hashcat compatible format and mask file for IPv4 addresses (ipv4_hcmask.txt) is given in tools directory.

Use kh-converter.py to convert the information

Command: python tools/known_hosts-hashcat/kh-converter.py known_hosts > converted-entry

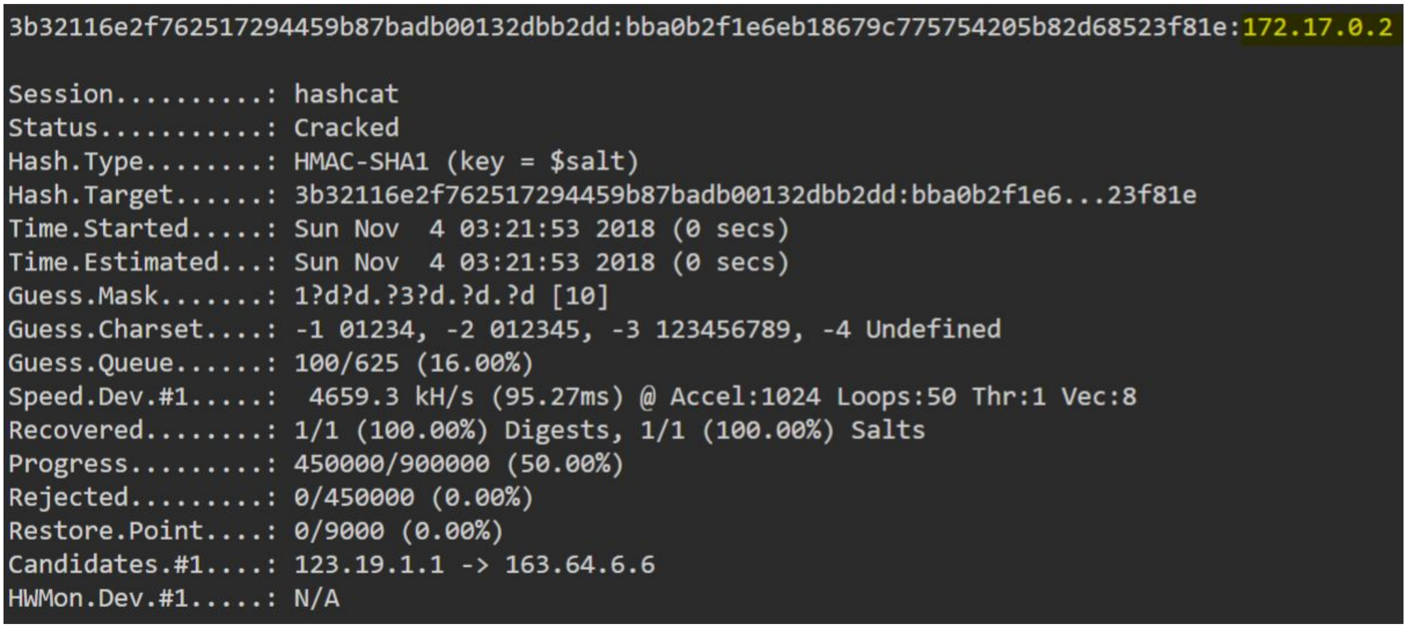
Check the contents of this file.



```
student@attackdefense:~$ cat converted-entry
3b32116e2f762517294459b87badb00132dbb2dd:bba0b2f1e6eb18679c775754205b82d68523f81e
student@attackdefense:~$ 
```

Step 2: Use hashcat to bruteforce the converted entry

Command: hashcat -m 160 --hex-salt converted-entry -a 3 tools/known_hosts-hashcat/ipv4_hcmask.txt



```
3b32116e2f762517294459b87badb00132dbb2dd:bba0b2f1e6eb18679c775754205b82d68523f81e:172.17.0.2

Session..........: hashcat
Status...........: Cracked
Hash.Type........: HMAC-SHA1 (key = $salt)
Hash.Target......: 3b32116e2f762517294459b87badb00132dbb2dd:bba0b2f1e6...23f81e
Time.Started.....: Sun Nov  4 03:21:53 2018 (0 secs)
Time.Estimated...: Sun Nov  4 03:21:53 2018 (0 secs)
Guess.Mask.......: 1?d?d.?3?d.?d.?d [10]
Guess.Charset....: -1 01234, -2 012345, -3 123456789, -4 Undefined
Guess.Queue......: 100/625 (16.00%)
Speed.Dev.#1.....:  4659.3 kH/s (95.27ms) @ Accel:1024 Loops:50 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 450000/900000 (50.00%)
Rejected.........: 0/450000 (0.00%)
Restore.Point....: 0/9000 (0.00%)
Candidates.#1....: 123.19.1.1 -> 163.64.6.6
HWMon.Dev.#1.....: N/A
```

Flag: 172.17.0.2

References:

1. Hashcat (https://hashcat.net)
2. Hashcat Wiki (https://hashcat.net/wiki/)
3. John the ripper jumbo (https://www.openwall.com/john/)
4. Known hosts file cracking (https://github.com/chris408/known_hosts-hashcat)