

CHALLENGE NAME : CRACKING THE BAD VAULT

DEV : PRATIK PATIL

CATEGORY : DIGITAL FORENSICS

LEVEL : HARD

Challenge Description :

Hey there! I am stuck in a situation that could make me lose my job. NSA caught a hacker "Vera" who broke into our most secure SHA-512 Vault and stole very crucial data, but the data is now in his vault. Can you please help me crack and recover the data safely so that I don't lose my job?

Solution :

1)We Gave You Hint That This Partition Is Encrypted By Veracrypt .So Setup It For Your Host Machine Or VM.

2)To Crack Veracrypt Partition Firstly You Need To Extract Volume Header (Which Stores Hash Info) Is Located At 1st Sector(Usually 1 Sector = 512 byte).

3)Command To Extract Volume Header: **sudo dcfldd if=<image>.img of=<header>.tc bs=1 count=512**

4)After Extracting Hash You Need Crack This Using Hashcat And The Hash Algorithm Hint Is Give In The Description(SHA-512).Find Hash Mode On Hashcat Example Hash List Which Is 13721.

13721	VeraCrypt PBKDF2-HMAC-SHA512 + AES (legacy)
-------	---------------------------------------------

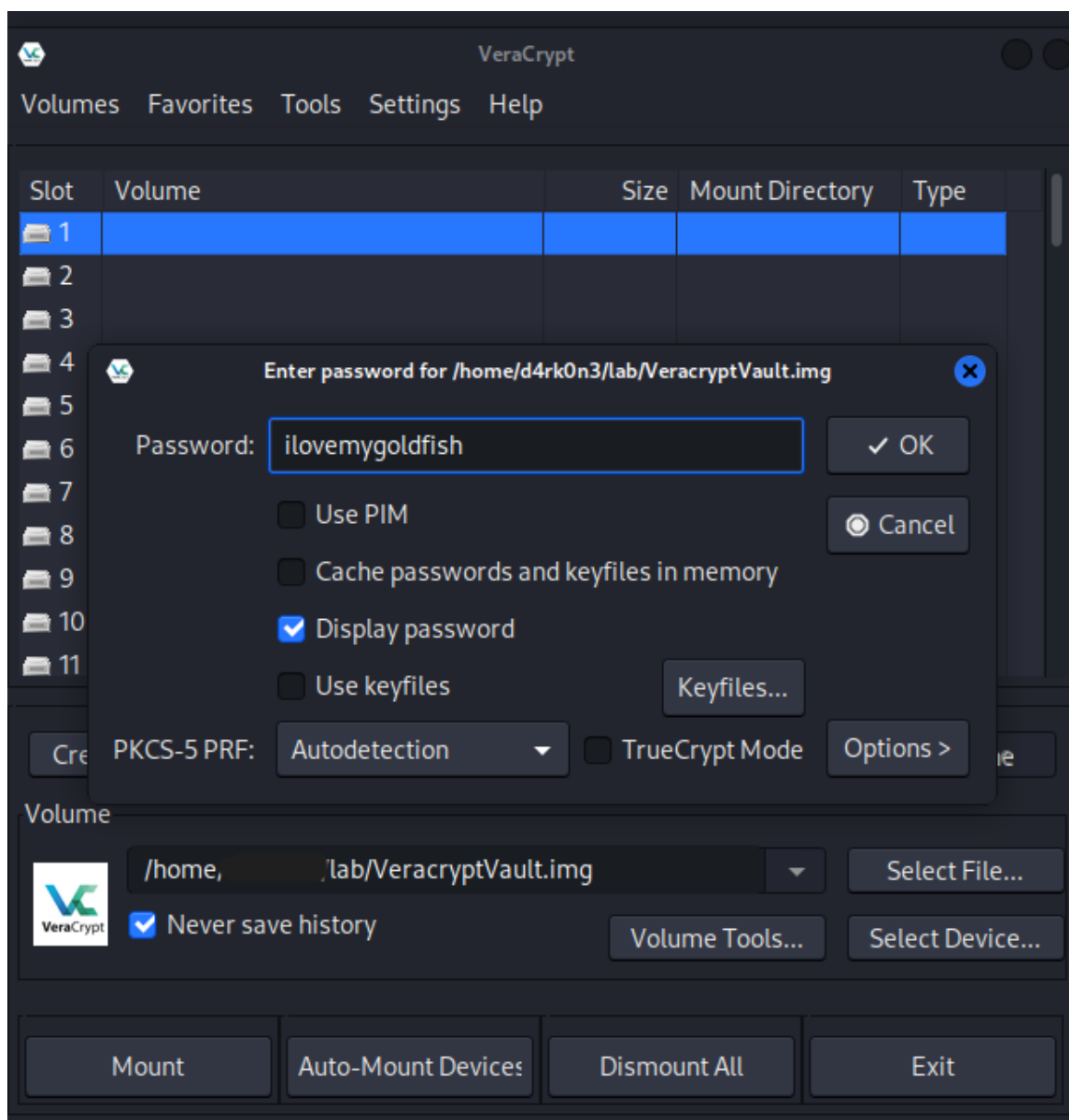
5)Hashcat Command To Crack Password Of Outer Volume : **sudo hashcat -a 3 -m 13721 <hash-path> <worldlist>**

6)You will Get Password : **ilovemygoldfish**

```
header.tc:ilovemygoldfish
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13721 (VeraCrypt SHA512 + XTS 512 bit (legacy))
Hash.Target.....: header.tc
Time.Started.....: Tue Mar 28 17:55:59 2023 (6 secs)
Time.Estimated...: Tue Mar 28 17:56:05 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ilovemygoldfish [15]
Guess.Queue.....: 3/79 (3.80%)
Speed.#1.....: 0 H/s (0.49ms) @ Accel:128 Loops:500 Thr:1 Vec:2
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1/1 (100.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:499500-499999
Candidate.Engine.: Device Generator
Candidates.#1....: ilovemygoldfish → ilovemygoldfish
Hardware.Mon.#1..: Util: 27%

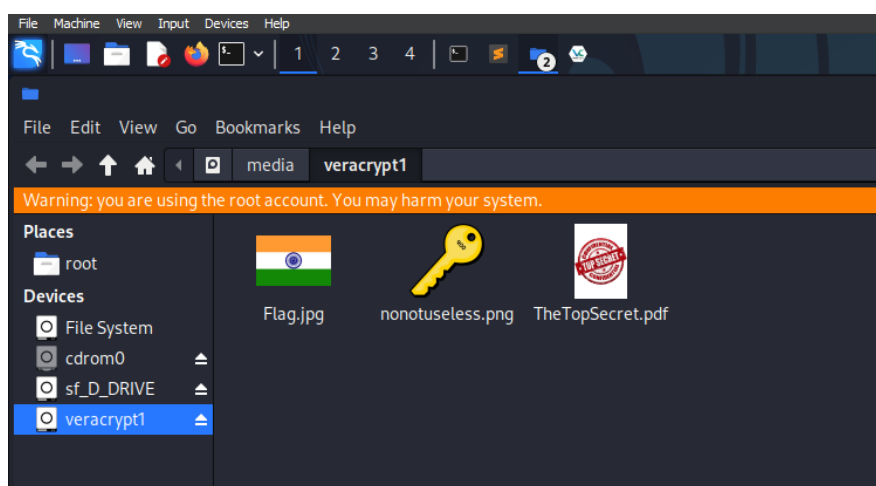
Started: Tue Mar 28 17:50:44 2023
Stopped: Tue Mar 28 17:56:06 2023
```

7) Now Mount This Partition Using This Password.

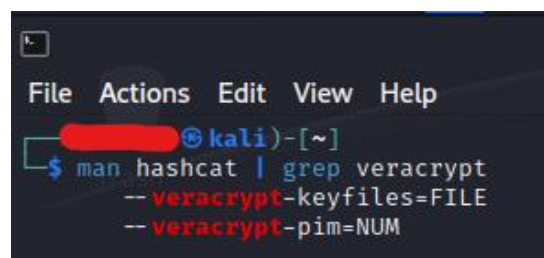


8) You Will See That There Are 3 files Inside It.

9) 1st flag.png and 2nd TheTopSecret.pdf These Both Are Distraction For You. There Was Nothing Inside It.

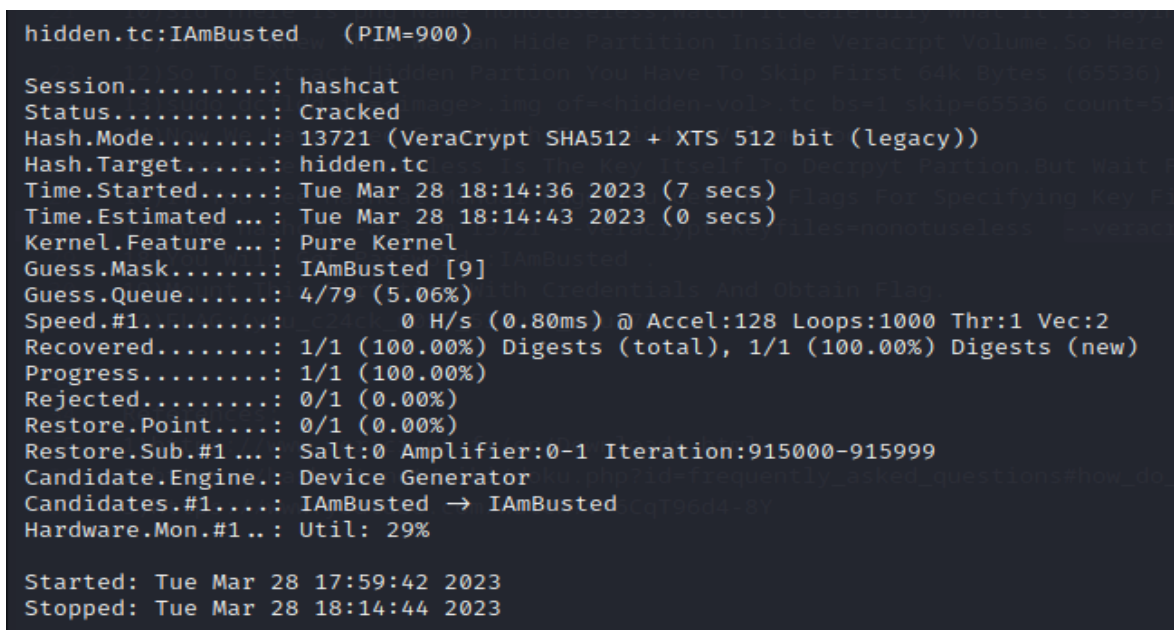


- 10)3rd There Is Png Name nonotuseless ,Watch It Carefully What It Is Saying.
- 11)If You Knew This We Can Hide Partition Inside Veracrypt Volume. So There Is One More Partition Hidden Inside This
- 12)So To Extract Hidden Partition You Have To Skip First 64k Bytes (65536)And Extract The Next 512 Bytes.
- 13)Command To Extract Volume Header Of Hidden Partition : **sudo dcfldd if=<image>.img of=<hidden-vol>.tc bs=1 skip=65536 count=512**
- 14)Now We Have Used Same Hash For Hidden Volume Too.
- 15)Here File nonotuseless.png Is The Key Itself To Decrypt Partition.But Wait For Twist Here We Are Using PIM(Personal Iteration Number) Too.If You See Carefully On That Png There Is Number Written On It 900.
- 16)If You See Hashcat Manual Page You Get The Flags For Specifying Key File As (--veracrypt-keyfiles=FILE) And PIM As (--veracrypt-pim=NUM).Time To Brute Force Again.



```
File Actions Edit View Help
kali)-[~]
$ man hashcat | grep veracrypt
--veracrypt-keyfiles=FILE
--veracrypt-pim=NUM
```

- 17)Hashcat Command To Crack Password Of Inner Volume : **sudo hashcat -a 3 -m 13721 --veracrypt-keyfiles=nonotuseless.png --veracrypt-pim-start=900 --veracrypt-pim-stop=901 <hidden-vol>.tc <wordlist>**
- 18)You Will Get Password : **IAmBusted .**



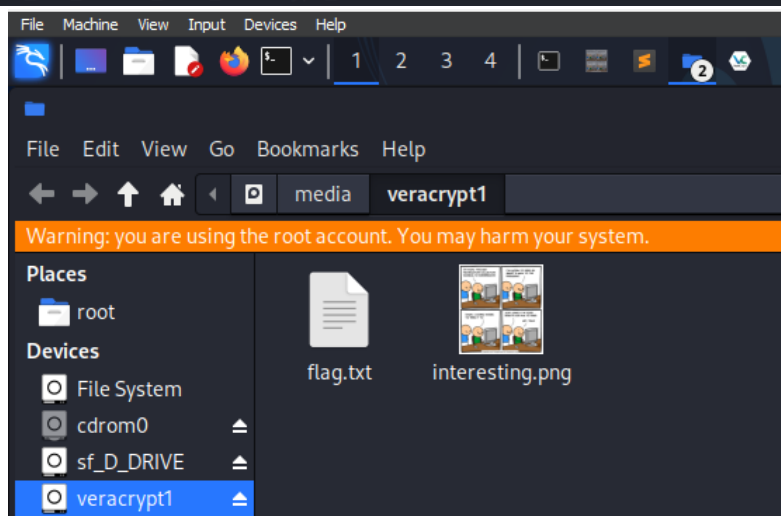
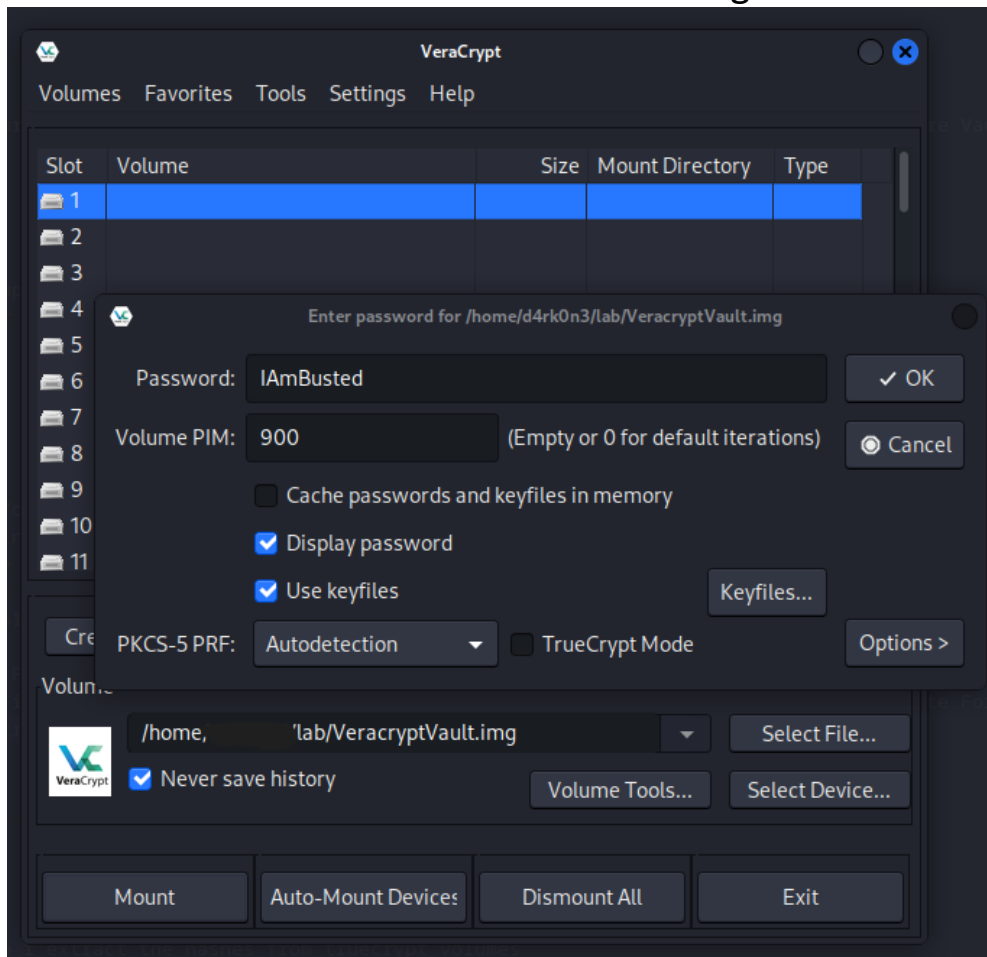
```
hidden.tc:IAmBusted (PIM=900)

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13721 (VeraCrypt SHA512 + XTS 512 bit (legacy))
Hash.Target.....: hidden.tc
Time.Started....: Tue Mar 28 18:14:36 2023 (7 secs)
Time.Estimated...: Tue Mar 28 18:14:43 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: IAmBusted [9]
Guess.Queue.....: 4/79 (5.06%)
Speed.#1.....: 0 H/s (0.80ms) @ Accel:128 Loops:1000 Thr:1 Vec:2
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1/1 (100.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:915000-915999
Candidate.Engine.: Device Generator
Candidates.#1....: IAmBusted -> IAmBusted
Hardware.Mon.#1..: Util: 29%

Started: Tue Mar 28 17:59:42 2023
Stopped: Tue Mar 28 18:14:44 2023
```

- 19) Password : IAmBusted PIM : 900 Key: nonotuseless.png

20)Mount This Partition With Credentials And Get Flag.



21)FLAG : VishwaCTF{y0u_c24ck_m057_53cu23_v4u17}

References:

- 1)<https://www.veracrypt.fr/en/Downloads.html>
- 2)https://hashcat.net/wiki/doku.php?id=frequently_asked_questions#how_do_i_extract_the_hashes_from_truecrypt_volumes
- 3)<https://www.youtube.com/watch?v=6CqT96d4-8Y>