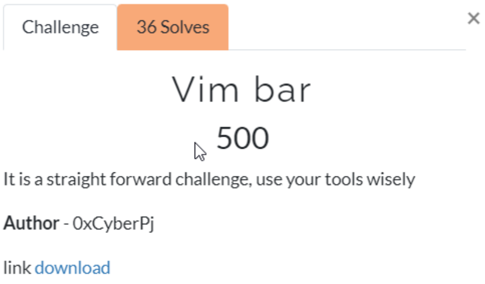
TamilCTF Vim_bar Writeup

Author : Paul Jeremiah

Category: Forensics.

Level: Medium+

Flag: `TamilCTF{vi_vii_viiim_lol}`



Challenge 36 Solves ×

Vim bar

500

It is a straight forward challenge, use your tools wisely

Author - 0xCyberPj

link download

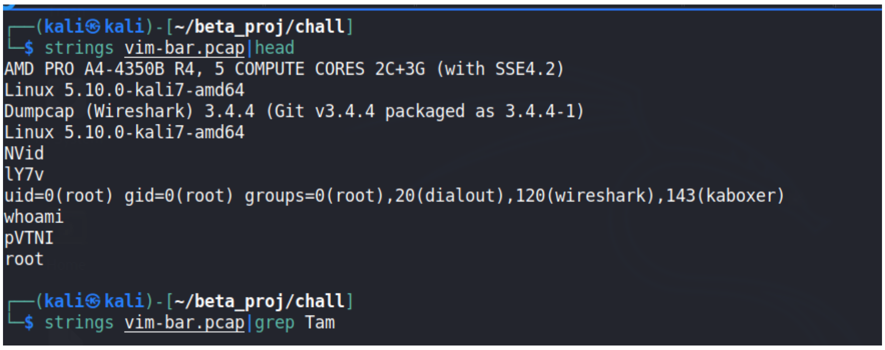
Given :

```
┌──(kali㉿kali)-[~/nope]
└─$ file vim-bar.pcap
vim-bar.pcap: pcapng capture file - version 1.0
```

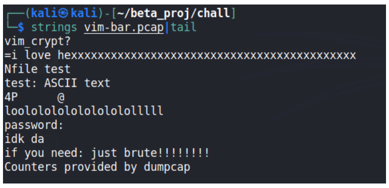
Description: its a simple straight forward challenge, use tools wisely, hope you know the power of vim dish wash bar!..... :/

Writeup:

- *As basics Lets starts with* $strings



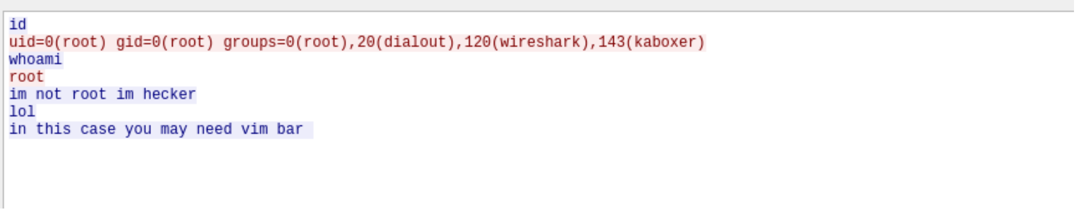
```
┌──(kali㉿kali)-[~/beta_proj/chall]
└─$ strings vim-bar.pcap|head
AMD PRO A4-4350B R4, 5 COMPUTE CORES 2C+3G (with SSE4.2)
Linux 5.10.0-kali7-amd64
Dumpcap (Wireshark) 3.4.4 (Git v3.4.4 packaged as 3.4.4-1)
Linux 5.10.0-kali7-amd64
NVid
lY7v
uid=0(root) gid=0(root) groups=0(root),20(dialout),120(wireshark),143(kaboxer)
whoami
pVTNI
root

┌──(kali㉿kali)-[~/beta_proj/chall]
└─$ strings vim-bar.pcap|grep Tam
```



```
┌──(kali㉿kali)-[~/beta_proj/chall]
└─$ strings vim-bar.pcap|tail
vim_crypt?
=i love hexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Nfile test
test: ASCII text
4P      @
loololololololololollll
password:
idk da
if you need: just brute!!!!!!!!
Counters provided by dumpcap
```

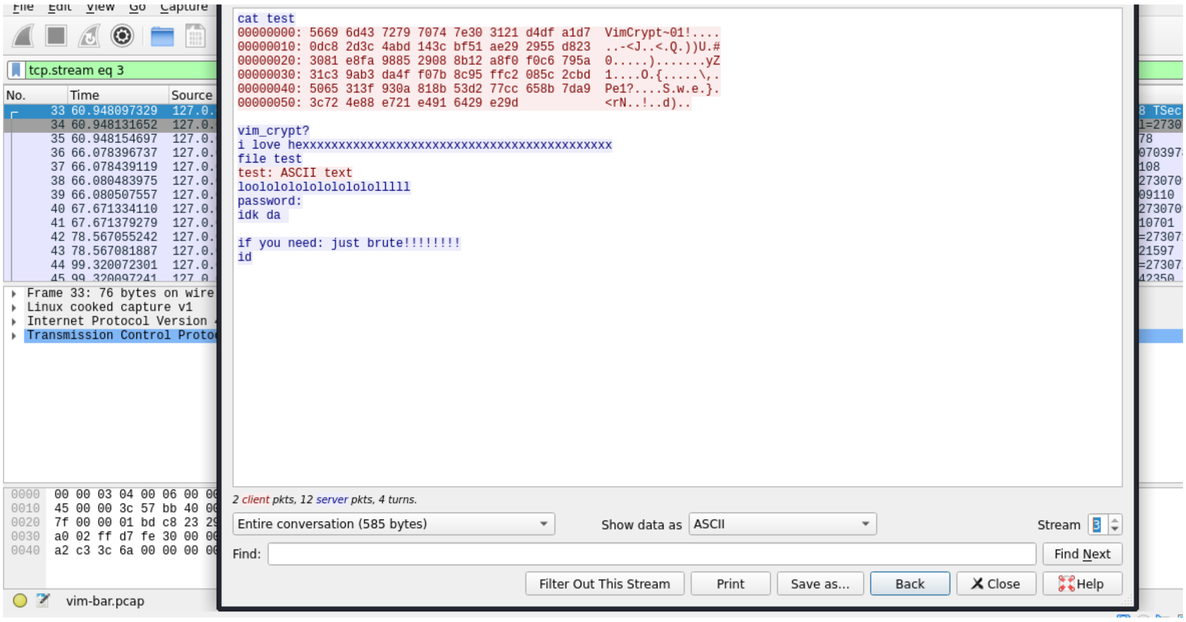
something is related to vim..?

1.Lets open with wireshark and Analyse it

- Follow TCP stream
- 

```
id
uid=0(root) gid=0(root) groups=0(root),20(dialout),120(wireshark),143(kaboxer)
whoami
root
im not root im hecker
lol
in this case you may need vim bar
```

Check other Streams

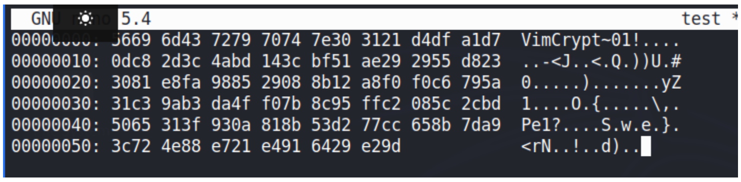


```
cat test
00000000: 5669 6d43 7279 7074 7e30 3121 d4df a1d7  VimCrypt~01!....
00000010: 0dc8 2d3c 4abd 143c bf51 ae29 2955 d823  ..-<J..<.Q.))U.#
00000020: 3081 e8fa 9885 2908 8b12 a8f0 f0c6 795a  0.....).......yZ
00000030: 31c3 9ab3 da4f f07b 8c95 ffc2 085c 2cbd  1....O.{.....\,.
00000040: 5065 313f 930a 818b 53d2 77cc 658b 7da9  Pe1?....S.w.e.}.
00000050: 3c72 4e88 e721 e491 6429 e29d            <rN..!..d)..

vim_crypt?
i love hexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
file test
test: ASCII text
loololololololololollll
password:
idk da

if you need: just brute!!!!!!!!
id
```

File Edit View Go Capture
tcp.stream eq 3
No. Time Source
Frame 33: 76 bytes on wire
Linux cooked capture v1
Internet Protocol Version
Transmission Control Proto
vim-bar.pcap
2 client pkts, 12 server pkts, 4 turns.
Entire conversation (585 bytes)
Show data as ASCII
Stream 3
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

so you can notice some hex dump value their

- copy it in text file first



```
00000000: 5669 6d43 7279 7074 7e30 3121 d4df a1d7  VimCrypt~01!....
00000010: 0dc8 2d3c 4abd 143c bf51 ae29 2955 d823  ..-<J..<.Q.))U.#
00000020: 3081 e8fa 9885 2908 8b12 a8f0 f0c6 795a  0.....).......yZ
00000030: 31c3 9ab3 da4f f07b 8c95 ffc2 085c 2cbd  1....O.{.....\,.
00000040: 5065 313f 930a 818b 53d2 77cc 658b 7da9  Pe1?....S.w.e.}.
00000050: 3c72 4e88 e721 e491 6429 e29d            <rN..!..d)..
```

```
$ file test
test: ASCII text
```

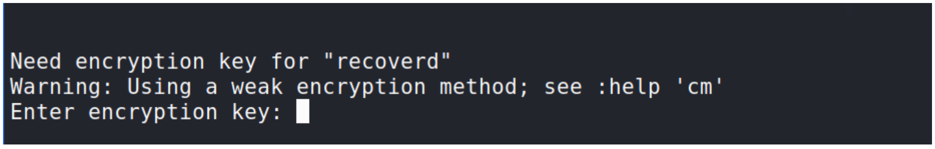
convert into binary

```
xxd -h : -r          reverse operation: convert (or patch) hexdump into binary.
```

```
┌──(kali㉿kali)-[~/nopel]
└─$ xxd -r test > recoverd

┌─(kali㉿kali)-[~/nope]
└─$ file recoverd
recoverd: Vim encrypted file data
```

(let's check strings)

```
└─$ strings recoverd
VimCrypt~01!
Pe1?
```

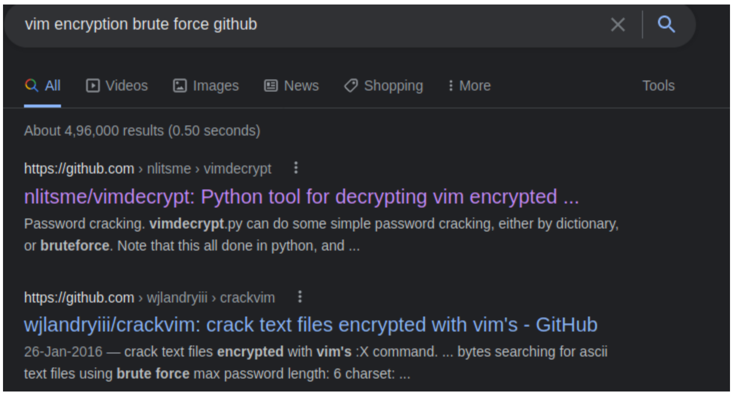
1. open it in vim! as they said
2. 

```
Need encryption key for "recoverd"
Warning: Using a weak encryption method; see :help 'cm'
Enter encryption key: █
```

Wait for What? **vim encryption? , Key: where should I got for key ..?**

```
Vim can encrypt your documents. :X prompts for an encryption key, which is
stored in the key option. The file will remain unchanged until you write it. ...
When the text has been decrypted, this also means that the key can be revealed,
and other files encrypted with the same key can be decrypted
```

Let's check



About 4,96,000 results (0.50 seconds)

https://github.com › nlitsme › vimdecrypt

nlitsme/vimdecrypt: Python tool for decrypting vim encrypted ...

Password cracking. **vimdecrypt**.py can do some simple password cracking, either by dictionary, or **bruteforce**. Note that this all done in python, and ...

https://github.com › wjlandryiii › crackvim

wjlandryiii/crackvim: crack text files encrypted with vim's - GitHub

26-Jan-2016 — crack text files **encrypted** with **vim's** :X command. ... bytes searching for ascii text files using **brute force** max password length: 6 charset: ...

Boom, i'm gonna use the first one

[Tool for decrypting VIM encrypted files]

```
└─# python3 /opt/vimdecrypt/vimdecrypt.py -h                                130
usage: vimdecrypt.py [-h] [--test] [--verbose] [--debug] [--password PASSWORD]
                     [--encoding ENCODING] [--writezip] [--dictionary
DICTIONARY]
                     [--bruteforce]
                     [files ...]
vimdecrypt
optional arguments:
  --debug               abort on exceptions.
  --password PASSWORD, -p PASSWORD
  --dictionary DICTIONARY, -d DICTIONARY
                        Dictionary attack, pass filename or - for STDIN
  --bruteforce, -b      Bruteforce attack
```

Here I'm going to use Rockyou.txt

Final One :

```
┌──(root💀kali)-[/nope]
└─# python3 /opt/vimdecrypt/vimdecrypt.py -d /usr/share/wordlists/rockyou.txt
recoverd
probable password: samantha
---------
Hello Friend, Vanakam Nanba
so Here You Go .....XD

TamilCTF{vi_vii_viiim_lol}
---------
```

Btw The Key is "samantha" 😆

Flag : TamilCTF{vi_vii_viiim_lol}
