Anonymous_THM

Enuumuration

1- 4 Ports are open 21,22,139,225

2- ftp null session gave us 3 files

3- Smb has a share named pics which have 2 pictures and i couldnt crack them and they are password protected

4- That was a dead en

5 - We can edit the clean.sh file present in ftp because it s writable and executable

6- we can use the append fuction in ftp to add code in a file on ftp from out machine

Nmap

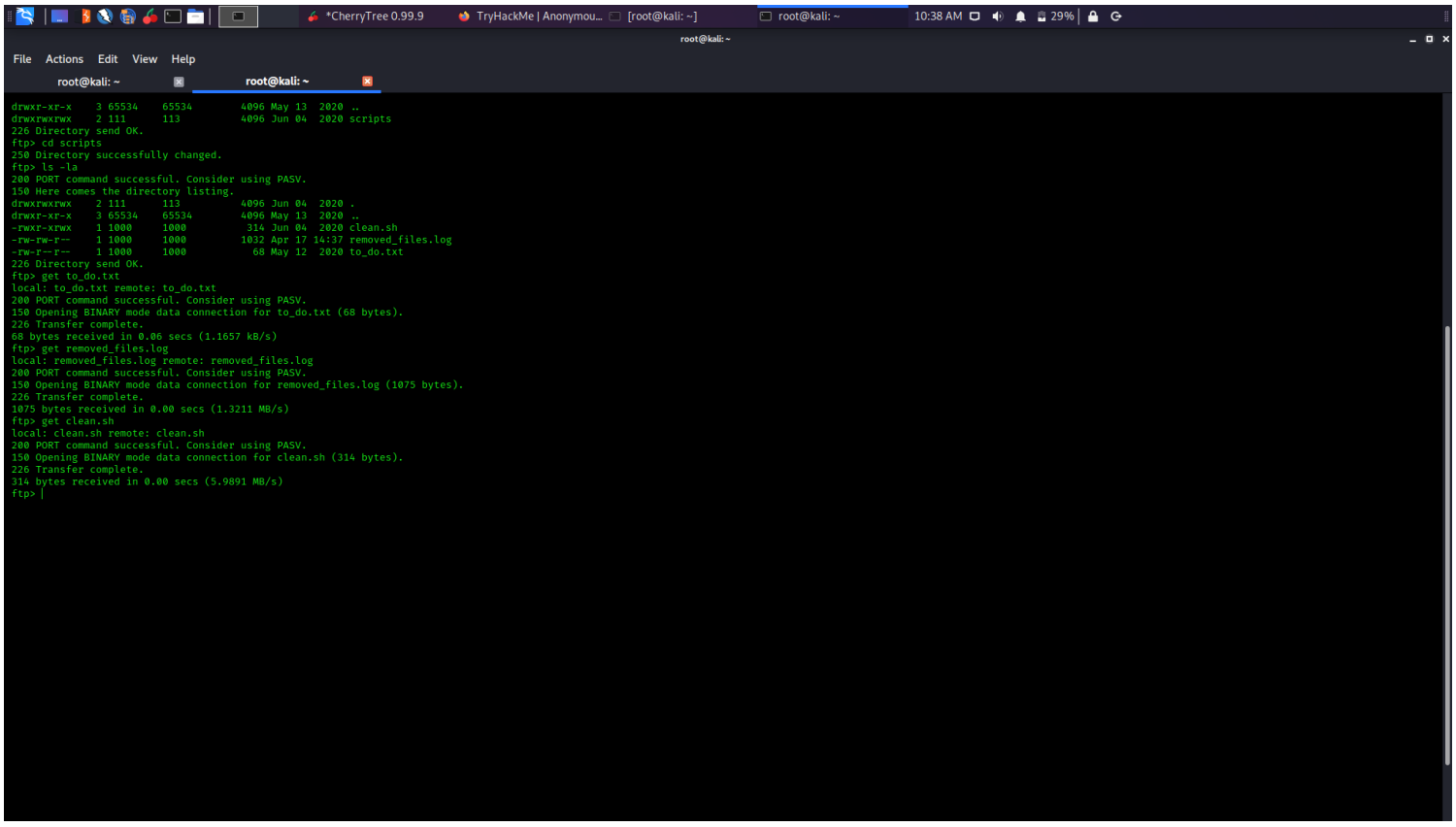
```
nmap -p21,22,139,445 10.10.134.52 -sS -sV -A -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-17 10:34 EDT
Nmap scan report for 10.10.134.52
Host is up (0.46s latency).

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:10.4.30.255
|      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
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)
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 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| 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: 2021-04-17T14:34:56+00:00
| smb-security-mode:
|   account_used: guest
```

```
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-04-17T14:34:56
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   203.00 ms 10.4.0.1
2   ... 3
4   457.99 ms 10.10.134.52

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 43.86 seconds
```

FTP

Anonymous login allowed

We have 3 files in ftp



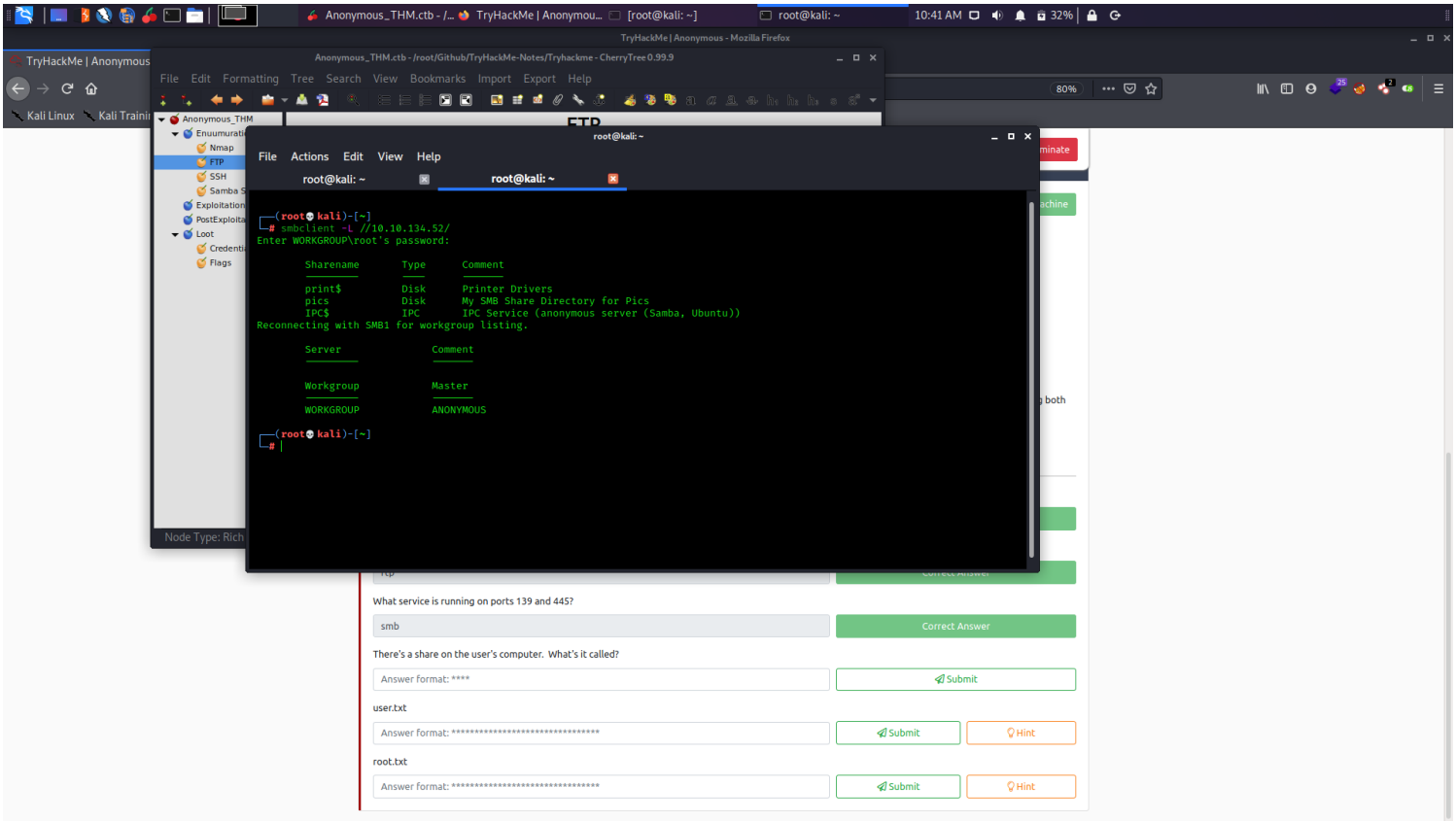
Nothing interesting here

#

SSH

Samba Shares

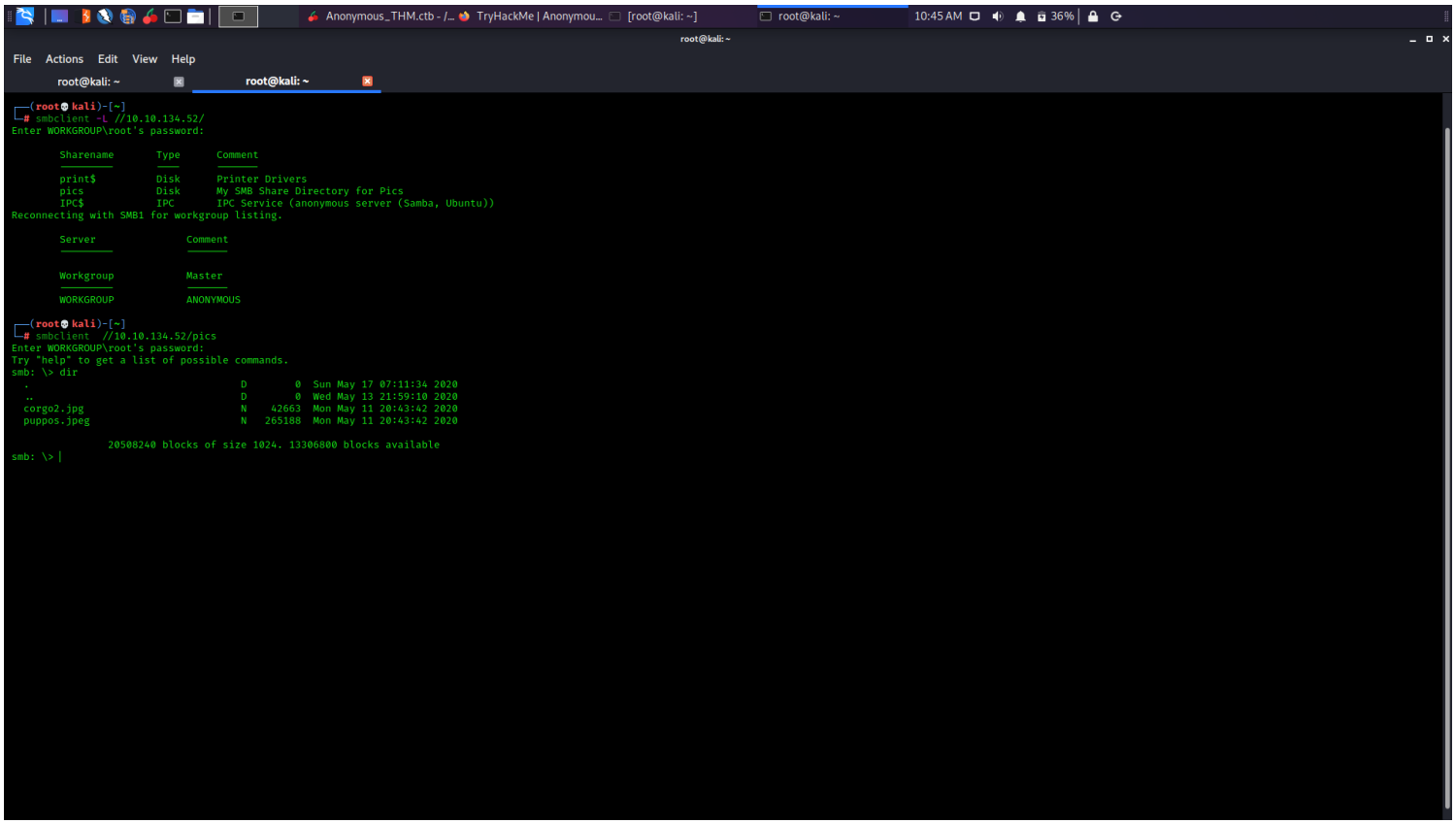
Null Session allowed



We got a samba share named pics

pics (Samba Share)

we can access a share named pics and it has 2 pictures



#

Exploitation

PostExploitation

We got as namelessone user and got the user flag

CHecked for sudo priveleges but we require password which we dont have

There were many suid binaries set and we got root by /usr/bin/env from gtfo bins

got the root

Loot

Credentials

Flags

User Flag

90d6f992585815ff991e68748c414740

Root Flag

4d930091c31a622a7ed10f27999af363