SMB:

1. What is the OS ?
   Your response: **OS: Unix (Samba 3.0.20-Debian)**

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap --script smb-os-discovery 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-16 06:05 EDT
Nmap scan report for 10.13.1.36
```

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
```

2. What is the version of samba on the box?
   Your response:
   Samba 3.0.20-Debian

3. How many group names are there? (use nbtstat)
   Your response: 4

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap --script nbstat.nse 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-16 06:12 EDT
```

```
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
```

4. What is the FQDN ?
   Your response: **Metasploitable.localdomain**

```
|   FQDN: metasploitable.localdomain
```

5. What is the Netbios computer name?
   Your response: **METASPLOITABLE:**

```
┌──(kali㉿ntsapi)-[~]
└─$ nbtscan 10.13.1.36
Doing NBT name scan for addresses from 10.13.1.36

IP address       NetBIOS Name     Server    User             MAC address
──────────────────────────────────────────────────────────────────────────
10.13.1.36       METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

6. How many disks are shared?
   Your response: 3

```
┌──(kali㉿ntsapi)-[~]
└─$ smbclient -L 10.13.1.36
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ─────────       ────      ───────
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
```

7. Which one is available for reading and writing?
   Your response:
   tmp Disk oh noes!

```
┌──(kali㉿ntsapi)-[~]
└─$ crackmapexec smb 10.13.1.36 -u '' -p '' --shares
SMB         10.13.1.36      445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdoma
SMB         10.13.1.36      445    METASPLOITABLE   [+] localdomain\:
SMB         10.13.1.36      445    METASPLOITABLE   [+] Enumerated shares
SMB         10.13.1.36      445    METASPLOITABLE   Share           Permissions     Remark
SMB         10.13.1.36      445    METASPLOITABLE   -----           -----------     ------
SMB         10.13.1.36      445    METASPLOITABLE   print$                          Printer Drivers
SMB         10.13.1.36      445    METASPLOITABLE   tmp             READ,WRITE      oh noes!
SMB         10.13.1.36      445    METASPLOITABLE   opt
SMB         10.13.1.36      445    METASPLOITABLE   IPC$                            IPC Service (met
SMB         10.13.1.36      445    METASPLOITABLE   ADMIN$                          IPC Service (met
```

8. What flag did you find when you logged in?
   Your response:

9. What is the path that begins with `c:\` in this file?
   Your response:

```
path:   C:\var\lib\samba\printers
```

10. How many users can you find ?
    Your response: 5 or 49

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" -N 10.13.1.36
rpcclient $> netshareenumall
netname: print$
        remark: Printer Drivers
        path:   C:\var\lib\samba\printers
        password:
netname: tmp
        remark: oh noes!
        path:   C:\tmp
        password:
netname: opt
        remark:
        path:   C:\tmp
        password:
netname: IPC$
        remark: IPC Service (metasploitable server (Samba 3.0.20-Debian))
        path:   C:\tmp
        password:
netname: ADMIN$
        remark: IPC Service (metasploitable server (Samba 3.0.20-Debian))
        path:   C:\tmp
        password:
rpcclient $>
```

Another possibility

```
┌──(kali㉿ntsapi)-[~]
└─$ enum4linux 10.13.1.36
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on
Sun Jun 16 14:44:14 2024
```

```
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
```