Hilfe für Challenge PWN-1

Hinweis:

> Wenn ihr einen Windows-Rechner nutzt, könnt ihr die Datei nicht ausführen, da es sich um eine sogenannte ELF-Binärdatei handelt. ELF steht hierbei für `Executable and Linking Format`, was so viel bedeutet wie: `Ausführbares und verknüpfbares Format`.
> Damit wir die Datei also ausführen können, wechseln wir im Linux-Subsystem mit dem Befehl `cd` (change directory) den aktuellen Arbeitspfad zu der heruntergeladenen Datei.
> Wenn die Datei in Windows unter `Downloads` liegt, dann findet ihr sie im Subsystem unter `/mnt/c/Users/<nutzername>/Downloads/`, wobei `<nutzername>` natürlich durch euren Windows-Nutzernamen ersetzt wird. Ihr führt also folgenden Befehl aus:
> `cd /mnt/c/Users/<nutzername>/Downloads/`.

Um diese Challenge meistern zu können, benötigen wir Wissen über die Datei, die ihr heruntergeladen habt. Wir können sie einfach mal mit folgendem Befehl im Linux-Subsystem ausführen: `./pwn1`.
Wie ihr seht, fordert uns das Programm auf ein Passwort anzugeben. Wir kennen es aber leider nicht. Da es sich jedoch um ein lokales Programm handelt, welches nicht mit dem Internet kommuniziert, muss das Passwort in dem Programm selbst stecken. Daher untersuchen wir das Programm nun auf enthaltene Zeichenketten.
Das Ganze erreichen wir mit folgendem Befehl: `strings pwn1`. Untersuche nun die Ausgabe nach einem möglichen Passwort und teste es gegen das Programm. Hast du das richtige Passwort gefunden, spuckt das Programm eine Beispielflag aus. Du weißt nun, wie du das lokale Programm ausgetrickst hast und kannst das Kennwort auch gegen unseren Server testen.

Viel Erfolg!