Initiale Analyse

Wenn wir das Programm ausführen, fragt es uns nach einem "secret key", welchen wir eingeben sollen.

Nur haben wir diesen Schlüssel leider nicht. Wenn wir einen falschen Schlüssel eingeben, erhalten wir folgendes:

```
$ ./admin_login
Hello Admin!
Please input your secret key to prove your identity: test123456789
You are not the admin! Stop using the admin login!
```

Rie Challenge in der Kategorie **Reverse Engineering** und Reverse Engineering befasst sich damit, von einem fertigen Programm herauszufinden, wie es intern funktioniert.

Bei diesem kleinen Programm könnten wir uns fragen "Wie überprüft das Programm unser Passwort?", also wie erkennt das Programm, ob wir das korrekte Passwort eingegeben haben?

Die wohl einfachste Art, um solch eine Überprüfung zu implementieren, ist es einfach jedes Zeichen unserer Eingabe, mit jedem Zeichen des echten Passworts zu vergleichen und zu überprüfen, ob diese identisch sind. Genau so macht es auch das gegebene Programm.

Anmerkung: Wir könnten das Programm auch mithilfe des Tools **Ghidra** dekompilieren (also aus dem kompilierten Programm möglichst gut den Programmtext wiederherstellen), aber das wird hier nicht benötigt.

Lösung

Damit das Programm überprüfen kann, ob unsere Eingabe das echte Passwort ist, muss das Programm das echte Passwort kennen. Das bedeutet, dass der Schlüssel irgendwo in dem Programm drinstecken muss!

Der Hint der Challenge weist uns schon auf das Tool `strings` hin. Hiermit können wir unter Linux alle Zeichenketten in einer Datei anzeigen lassen. Mal schauen, ob wir eine Zeichenkette finden, die wie ein Schlüssel aussieht.

```
$ strings admin_login
      [...]
PTE1
VerySuperSecretKey_DontTellAnyone!!!
Hello Admin!
Please input your secret key to prove your identity:
I think you may need this:
You are not the admin! Stop using the admin login!
;*3$"
Z1TO~Cg
      [...]
```

`VerySuperSecretKey_DontTellAnyone` sieht doch verdächtig aus! Und wenn wir den String dem Programm als Schlüssel geben, erhalten wir die Flagge:

```
$ ./admin_login
Hello Admin!
Please input your secret key to prove your identity: VerySuperSecretKey_DontTellAnyone!!!
I think you may need this:
SSH{st0r1ng_pl41nt3xt_p455w0rd5_1n_b1n4r1es_15_1n53cure}
```