דוד ורטנטייל

Python Interpreter: WinPython-64bit-3.6.2.0Qt5

הסבר:

את הפורט מצאתי באמצעות תוכנת nmap כך: הרצתי אותה לפני ואחרי שהפעלתי את התכנית שאליה אנו צריכים לפרוץ וכך ראיתי איזה פורט חדש מאזין במחשב.

הסבר על מציאת הסיסמא: מאתחל מערך בסימני / כי זה ב ASCII נמצא לפני המספר 0 ואז שולח לתוכנית ומקבל הערכת זמן ראשונית לכמה זמן לוקח למערכת לבדוק. מוסיף לזמן הזה מרווח טעות של 0.05 (כי יש תנודות קטנות בזמן) ומתקדם לאות הבא ב ASCII (באמצעות המרה ל int ואז +=1 ואז המרה חזרה ל char). כאשר אני מקבל זמן גדול מהזמן המקסימלי שהיה אני מבין שעליתי על אות נכונה ולכן אני מוסיף אותה לpassword ומתקדם לתא הבא במערך ההתחלתי. כאשר התכנית מחזירה משהוא שהוא לא Bad Password! אני מבין שמצאתי את הדגל, מדפיס את הדגל וסיסמא ומסיים לרוץ.