מחוון לבדיקת תרגיל SYN Flood

שימו לב- בתרגיל זה נתונות לפניכם כל הבדיקות שהבודקים יעשו, כולל התוצאות הצפויות וקובץ עם התוצאות שאתן צריכות לקבל.

|  |  |  |
| --- | --- | --- |
| **הבדיקה** | **תוצאה רצויה** | **ניקוד** |
| תוכנה רצה תקין | התוכנה לא נתקעת או קורסת | 0 |
| איכות כתובות IP | נמצאות כל 51 כתובות ה-IP החשודות שבקובץ המצורף למחוון filteredAttackersList | מינוס 2 נקודות על כל כתובת חסרה |
| כמות כתובות IP חשודות | בין 50-150 | מינוס 2 נקודות על כל חריגה מהטווח |
| אתרעות שווא. לרשת המותקפת יש טווח כתובות IP, נבדוק שאף אחת מהן לא מזוהה כתוקף | לא מזוהות כתובות IP מתוך הרשת המותקפת | מינוס 20 נקודות |
| אלגוריתם האיתור מתבסס על לפחות שלוש פרמטרים מתוך הפרמטרים הבאים:   1. שימוש בדגל SYN 2. שימוש בדגל ACK 3. קצב שליחת פקטות 4. טווח כתובות IP יעד 5. טווח כתובות IP מקור 6. רעיון יצירתי אחר שנמצא פועל | האלגוריתם כולל לפחות שלושה פרמטרים מתוך הרשימה | מינוס 20 (אם האלגוריתם לא מתועד, יירדו נקודות), אין הגשה מחדש |