

Nmap

מה זה עושה:

מבצע סריקה של הרשת ומאתר מכשירים פתוחים ופגיעים.
המשתמש מכניס כתובת IP של היעד ואת ממשק הרשת שבו להשתמש.
הקוד מבצע את סריקת ה-Nmap באמצעות הפקודה

```
'sudo nmap -sS -Pn -e [interface] [target]'
```

איך זה עובד:

מפסיק כל תהליך שרץ כרגע (stop_current_process).
מבצע בדיקה שהמשתמש הכניס כתובת IP וממשק רשת.
מפעיל את הפקודה nmap בתהליך חדש (subprocess.Popen).
קורא את הפלט מהתהליך ומציג אותו בתיבת הטקסט של הממשק הגרפי.

POF

מה זה עושה:

מבצע ניתוח של תעבורת רשת ומזהה מערכות הפעלה של המכשירים ברשת.
המשתמש בוחר ממשק רשת שבו לבצע את הניתוח.

איך זה עובד:

מפסיק כל תהליך שרץ כרגע (stop_current_process).
מבצע בדיקה שהמשתמש בחר ממשק רשת תקף.
מפעיל את הפקודה pOf בתהליך חדש (subprocess.Popen).
קורא את הפלט מהתהליך ומציג אותו בתיבת הטקסט של הממשק הגרפי.

Scapy

מה זה עושה:

מאזין לתעבורת רשת ומציג פרטים על מנות (packets) שנקלטו ברשת.
המשתמש בוחר ממשק רשת שבו להאזין לתעבורה.

איך זה עובד:

מפסיק כל תהליך שרץ כרגע (stop_current_process).
מתחיל האזנה לממשק הרשת שנבחר.
הקוד מגדיר פונקציה (packet_callback) שמטפלת במנות שנקלטו ומציגה פרטים על כל מנה.
המנות מוצגות בתיבת הטקסט של הממשק הגרפי.
ניתן לעצור את ההאזנה באמצעות לחיצה על כפתור ה-"Stop Current Process" (יש לחכות כמה שניות אחרי עצירת התהליך).

Block Websites

מה זה עושה:

חוסם אתרים על ידי הוספת כתובות ה-IP שלהם לטבלת חסימה ב-PF.
המשתמש מזין שמות אתרים בממשק הגרפי.

איך זה עובד:

המשתמש מזין שמות אתרים בתיבת הטקסט של הממשק הגרפי.
הקוד פונה לשרת DNS כדי לקבל את כתובות ה-IP של האתרים.
מוסיף את כתובות ה-IP לטבלת blocked_websites ב-PF באמצעות הפקודה

```
'sudo pfctl -t blocked_websites -T add'
```


מציג הודעה בתיבת הטקסט על הצלחה או כישלון החסימה.