הגנה ממתקפות DDOS

מסמך אפיון

טום לב

גרסה 1

23.1.23

הקדמה:

מטרת המסמך של הפרויקט היא לעזור למשתמשים להבין מה הפרויקט עושה ולמי הוא מיועד.

הקהל שפרויקט זה מיועד לו זה כל אחד שיש בבעלותו אתר אינטרנט.

קצת על המוצר:

מוצר זה דומה מאד ל WAF – WEB APPLICATION FIREWALL.

תפקידו או מטרתו של המוצר זה להגן ממתקפות DDOS כגון SYN FLOOD וPING על אתרי אינטרנט או על סוקטים.

המוצר מגן על יישומי האינטרנט שלך על ידי סינון, ניטור וחסימת כל תעבורת HTTP/S זדונית העוברת לאתר האינטרנט, ומונע מכל מידע לא מורשה לצאת מהאפליקציה. הוא עושה זאת על ידי הקפדה על מערכת מדיניות שעוזרת לקבוע איזו תנועה היא זדונית ואיזו תנועה בטוחה.

יתרונותיו של המוצר: חינמי ,פשוט לתפעול ,מממש הגנה נגד מתקפות בצורה יעילה.

הגדרות:

**WAF**- WEB APPLICATION FIREWALL

-**PING** הוא יישום השולח [חבילת נתונים](https://he.wikipedia.org/wiki/%D7%97%D7%91%D7%99%D7%9C%D7%AA_%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D) [בפרוטוקול](https://he.wikipedia.org/wiki/%D7%A4%D7%A8%D7%95%D7%98%D7%95%D7%A7%D7%95%D7%9C_%D7%AA%D7%A7%D7%A9%D7%95%D7%A8%D7%AA) [ICMP](https://he.wikipedia.org/wiki/ICMP) ממקור מסוים ליעד מסוים [ברשת](https://he.wikipedia.org/wiki/%D7%A8%D7%A9%D7%AA_%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D) לפי כתובתו. המטרה העיקרית לה היא משמשת היא בחינת תקינות התקשורת בין נקודת המקור לנקודת היעד.

**SYN FLOOD** - היא סוג של [התקפת מניעת שירות](https://he.wikipedia.org/wiki/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA_%D7%9E%D7%A0%D7%99%D7%A2%D7%AA_%D7%A9%D7%99%D7%A8%D7%95%D7%AA) המנצלת [פרצת אבטחה](https://he.wikipedia.org/wiki/%D7%A4%D7%A8%D7%A6%D7%AA_%D7%90%D7%91%D7%98%D7%97%D7%94) במנגנון הקמת הקשר של ה-[TCP](https://he.wikipedia.org/wiki/TCP). במסגרת ההתקפה התוקף שולח רצף של חבילות [SYN](https://he.wikipedia.org/wiki/SYN) ל[מחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91) המותקף ובכך מאלץ אותו לפתוח במקביל חיבורים רבים עד שלא נותרים לו משאבים לקבלת חיבורים חדשים. בכך התוקף מונע מהמחשב המותקף להעניק שירות למשתמשים אחרים ומשיג את מבוקשו.

תקציר:

הקדמה-

תיאור כללי-

דרישות מפורטות-

תיאור כללי:

פונקציונליות:

תעשה סינון וניטור של כל תעבורת הHTTP שעוברת לאתר או לסוקט.

חוסמת תעבורה זדונית שהפונקציה הקודמת מצאה כזדונית.

חוסמת משתמשים, שנמצאו כזדוניים בעבר ושומרת אותם.

אפשרות בממשק המשתמש למחוק משתמש חסום במידה וחלה טעות.

הגנה בזמן אמת ממתקפות.

קהל היעד:

מנהלי רשת או אנשי אבטחת רשת.

אילוצים עיקריים:

המערכת דורשת חיבור לאינטרנט.

המערכת צריכה לתמוך במספר משתמשים רב.

הנחות ותלויות:

המערכת תקבל הודעות Http,כל תקיפה שתתקיים תהיה במילון עם מדיניות שתעזור לקבוע איזה תעבורה הינה זדונית.

סיקור מצב השוק:

פרויקטים דומים- , AWS WAF, Wallarm API Security Platform,Azure Web Application Firewall ועוד.

מה ההבדל בין מוצרים אלו לבין הפרויקט שלי:

תוכנות אלו כוללות הגנה מיותר סוגי התקפות, התוכנות האלו בתשלום, בחלקן יש משוב עם נציג במידה ויש באג בתוכנה.

דרישות מפורטות:

מתוך פונקציונליות:

תעשה סינון וניטור של כל תעבורת הHTTP שעוברת לאתר.

מקבלת את תעבורת הHTTP ברשת.

עוברת על כל התעבורה ומסננת לפי סט של חוקים שנקבעו מראש.

מחזירה את כתובות המקור של התעבורה הזדונית.

מוסיפה אותם למאגר מידע של משתמשים לא מורשים (חסומים).

חוסמת משתמש על ידי זיהוי כתובת המקור ובדיקה האם הוא מורשה או חסום, ורק אז מסננת לפי סט החוקים שנקבעו.

המשתמש שמעוניין לגשת לסוקט או לאתר מתקשר תחילה עם מחשב שבין המשתמש לשרת.

המחשב הזה קובע אם לתת למשתמש לעבור ולנתב אותו לשרת או לא.

הGUI של המשתמש יהיה מסודר לפי הגדרות, רשימה שחורה (משתמשים חסומים), ומצב הרשת.

כמובן שתהיה אפשרות להפעיל ולכבות את חומת האש.