

**מסמך פרויקט מגן שרת - תשפ"ד**

**צוות:** מאור קבלו, איתי ריפ זיידיס

**כיתה:** חיפה 14

**ראש צוות:** ניב קוצר

**מנטור:** שם המנטור

פרק 1: יזום

תיאור כללי

**הפרויקט הוא ids reverse proxy שמגן על שרת מפני התקפות שונות.**

מטרת הפרויקט

מטרת הפרויקט היא להעמיק את הידע שלנו בעולם הסיקיוריטי ואבטחת רשתות***, עם ניסיון במערכת הפעלה שונה מזו של ווינדוס (לינוקס). החלטנו לעשות את פרוייקט זה מכיוון שאנו מתעניינים בנושאים הנוגעים לפרויקט, הפרויקט מממש ומרחיב את יכולתינו כמתכנתים.***

***ליבה טכנולוגית***

***הליבה הטכנולוגית של הפרויקט היא זיהוי והגנה נגד התקפות על ידי ניתוח התעבורה דרך* reverse proxy**

טכנולוגיות עיקריות ושיקולים עיקריים

**כדי לממש את הפרויקט נצטרך ללמוד לעבוד עם cpp לינוקס.**

**בחרנו ב cpp בגלל שזו שפת התכנות המועדפת על שנינו בנוסף להיותה השפה המוכרת ביותר לשנינו.**

**בחרנו לעבוד לינוקס כדי שנוכל להשתמש בebpf.**

**נצטרך גם ללמוד איך לעבוד עם ebpf ואיך להמיר קוד לbytecode.**

**אתגרים טכנולוגיים ומקורות**

**האתגרים הטכנולוגיים הצפויים לנו בתחום הלימודי הם ללמוד לעבוד עם ebpf.**

**בתחום המעשי יהיו לנו כנראה כמות יפה של בגים בהתחלה נפתור את זה באמצעות דיבור עם המנטור ודיבור בננו בנוסף להשקעת זמן בדיבגין ובדיקת הקוד אחד של השני.**

* [**google.com**](https://www.google.com/)
* [**https://chat.openai.com**](https://chat.openai.com)
* [**https://ebpf.io/what-is-ebpf/#documentation**](https://ebpf.io/what-is-ebpf/#documentation)
* [**https://stackoverflow.com**](https://stackoverflow.com)

***סוגי משתמשים / קהל היעד***

**הכלי נועד לכל שרת, באמצעות המערכת שניצור יהיה לשרתים שכבת הגנה נוספת שתפחית את כמות הבקשות הלא לגיטימיות שיגעו לשרת**

***דרישות חומרה***

**בשלב הראשוני אין דרישות חומרה מיוחדות כי נבנה את הפרויקט במכונה וירטואלית. בשלב מסוים נצטרך לבנות שרת בסיסי בשביל לבדוק שהסינון באמת עובד.**

***פתרונות קיימים***

**קיימים מלא סוגים של IPS/IDS יכולים להגן על התעבורה למחשב לדוגמה Snort או Suricata.**

פרק 2: אפיון

***מסומן*** *– נתון לדיון*

פיצ'רים ותהליכים עיקריים

רשימת פיצ'רים

* חסימת כתובות IP זדוניות:

1. **קלט:** IP המזוהה כזדוני
2. **פלט:** חסימת IP
3. **תיאור:** חסימת IP ביעילות ובמהירות רבה באמעות eBPF החוסם את התעבורות הבאות מאותו כתובת ביעילות מרבית מתוך Kernal המערכת.

* בדיקה ראשונית, בדיקת אם IP זדוני ממאגרי מידע:

1. **קלט:** IP חדש הנכנס לשרת
2. **פלט:** חסימת ה-IP אם זדוני או השמה ב-Whitelist אם לא
3. **תיאור:** שימוש במאגרי מידע חיצוניים כמו AbuseIPDB או IPinfo כדי לעשות בדיקה ראשונית אם ה-IP זדוני או לא, אם כן חוסמים ישירות את ה-IP, אם לא ממשכים לפקח על התנהגות הלקוח באמצעות הפיצ'רים הבאים.

* הטמעת גבולות מוגדרים מראש בפרוקסי:
  + הגבלת בקשות לפרק זמן מסוים מצד הלקוח

1. **קלט:** IP של לקוח מסוים השולח בקשה, חלון זמן (שניות), מקסימום בקשות לחלון זמן (כנראה יהיו קבועים)
2. **פלט:** החזרת תשובה לבקשה, עם קוד סטטוס הבודק אם הלקוח עומד בדרישות (200 – OK, 429 – To Many Requests, תלוי פרטוקול), במקרים קיצוניים חסימת IP של הלקוח.
3. **תיאור:** באמצעות הפיצ'ר יהיה פיקוח על מספר הבקשות של כל לקוח ולפעול בהתאם כאשר הבקשות גדולות מן הרצוי, **כנראה ירוץ על טריידים נפרדים וינתר את כמות הבקשות של כל לקוח**
   * הגבלת מספר לקוחות המחוברים לשרת במקביל, ליצור "תור" של לקוחות הנכנסים לשרת
   * הגבלת מספר **ההתחברויות** לשרת ברצף
   * הגבלת רוחב הפס המותרת בשרת, כדי למנוע העברת נתונים מוגזמת. לדוגמה, 10 MB/s.
   * הגבלה בשימוש המשאבים בשרת, מעבד, זיכרון ואחסון
4. **קלט:** לציין באיזה משאב להשתמש, מה גבול השימוש בו (באחוזים), מה לעשות כאשר הגבול עבר, תוך כמה זמן לבדוק אם הגבול עבר
5. **פלט: *תלוי מקרה***
6. **תיאור:** הגבלה בשימוש המשאבים בשרת מבטיחה שהשרתמוגן מפני ניצול משאבים. מנהלי מערכת מגדירים איזה משאב לנטר במערכת (לדוגמה, מעבד, זיכרון, שטח דיסק) ומגדירים גבול הרצוי עבור כל משאב. המערכת מנטרת באופן רציף את המשאבים שצוינו בזמן אמת, תוך דגימת ניצול שלהם במרווחי זמן קבועים. כאשר המערכת מזהה כי הגבול חורג, אפשר להקצות עוד משאבים באופן אוטומטי ***או לפעול באופן קיצוני יותר ולחסום את הכתובת ממנה שימוש המשאבים עולה מן הרצוי*.**

* זיהוי והגנה מהמתקפות עצמן:
  + Port Scanning

1. **קלט:** ניסיונות חיבור לשרת, Source IP, Dest Port
2. **פלט:** ***חסימה/הרשאה/הגבלת בקשות*** של כתובת ה-IP של הלקוח
3. **תיאור:** הכלי יזהה מתקפת Port Scanning ויעצור אותה באמצעות כמה דרכים:
   * + - **ניתוח קצב חיבורים לשרת:** כאשר מתבצעות באופן חוזר ניסיונית להתחבר לשרת מפורטים שונים בזמן קצר יחסית מ-IP מסוים, הדבר יכול להעיד על מתקפה.
       - הכלי יזהה כתובת IP שמנסה להתחבר לפורטים בסדר רציף מסוים, שהיא טכניקה נפוצה המשומשת ב-Port Scanning
       - באמצעות הפיצ'ר "הגבלת מספר ההתחברויות לשרת ברצף" יהיה אפשר להגביל את כמות ההתחברויות לפורטים ברצף.
       - הכלי יזהה כאשר לקוח מסוים מנסה להתחבר לפורטים שאינם בשימוש בדרך כלל על ידי שירותים נפוצים או אפילו סגורים, סורקים עשויים לחקור פורטים פחות נפוצות כדי למצוא נקודות תורפה אפשריות.

* סריקת התעבורה והרשת (ביעילות) - ...