אוניברסיטת
אריאל
בשומרון

idsiter

פלטפורמה לזיהוי מכניזם סייבר רשתי

הבעיה

- רשתות רבות אינן מחוברות לאינטרנט. דבר זה מקשה התוקף להגיע למידע מעניין ברשת. על מנת להתמודד עם עולם זה ההאקר תוקף את המחשבים שמחוברים לאינטרנט ועל ידי תפעול שלהם מגיע למחשבים שאינם רואים אינטרנט. דבר זה מבוצע לרוב ע"י מערכת תקיפה.
- מערכת התקיפה משתמשת באלגוריתם קבוע אשר לומד את מבנה הרשת, לאחר מכן מתפשט בצורה קבועה ברשת הפנימית ע"י חולשות רשת, מתקין עליהן עותק של מערכת תקיפה, לאחר מכן כלל מערכות התקיפה אוספות מידע ושולחות אותו ל"מערכת האב".

- **אין כיום מערכת שיעודה העיקרי היא התמודדות עם בעיה זו, המשלבת ידע רשתי וhost.**

שאלת המחקר

- שאלת החקר שלנו היא האם ישנן תקיפות שלא מזוהות ע"י ניטור היקפי ולא ע"י כלי ניטור מקומיים אך ניתנות לזיהוי ע"י איסוף מידע מכל התחנות (אנו מתמקדים בhids-ים) –מהם? ישנן התקפות אשר לא נמצאות ברמת הרשת בלבד או ברמת הhost בלבד, אך אנו סבורים שבהצלבת מידע מקבוצת hids-ים, מתקפות אלו עשויות להתגלות.

הפרויקט

- אנו מעוניינים ראשית לחקור האם ישנם סממנים המרמזים על מתקפות המתקיימות בצורה סיסטמטית (לדוגמא קשר מתמטי בין קבוצות זמנים של פאקטה שחוזרת על עצמה מכמה מערכות). בהמשך ליצור הוכחת נכונות למערכת שעשויה למצוא התקפות כאלו וכן מציעה הצעות לייעול החוקים שהhids-ים מעלים כדי למצוא את ההתקפות הללו.

abstract

Our research question is whether there are attacks which detected by neither local monitoring nor by network monitoring but can be identified by gathering information from all stations (we focus on hids-s) .

We believe that using cross-referencing hids-s outputs, these attacks may detected. we want to first investigate whether there are signs that suggest the attacks that take place in any systematic manner (eg mathematical correlation between the time of the packets repeated in several systems) . Next we will generate a proof of concept to the system and make it suggest rules in order to prevent these attacks.

As for the motivation for systematic network attacks, today many networks (except single computers) are not connected to the Internet, which makes it difficult for the attacker to attack it directly. To do this, the hacker attacks the computers that are connected to the Internet and by operating them to computers that do not see Internet. This is usually done by the attack system. The attack system uses a fixed algorithm that studies the network structure, then spreads continuously on the internal network by various network weaknesses, installs a copy of the attack system, then the attack systems collect information and send it to the parent system. The information collected is concentrated in the original attacker.

We will establish a company's network with some hids that report in two levels: 1. Silent alert - that will reach only us (to our algorithm) 2. noisy warning - will also report the real siem server of the company.

We describe our suggested algorithem in the attached github page.

המחקר

<u>תוצאות המחקר:</u>

במהלך הסריקה נקראו דוחות תקיפה רבים ואף התבצע ייעוץ עם אנשים מהתעשייה ומקהילת הבטחון. במחקר התגלו למעלה מ-10 מכניזמים יחודיים, בינהם:

1.יציאה מונוטונית כל זמן קבוע לטווח הרשת לכתובות לא מוכרות

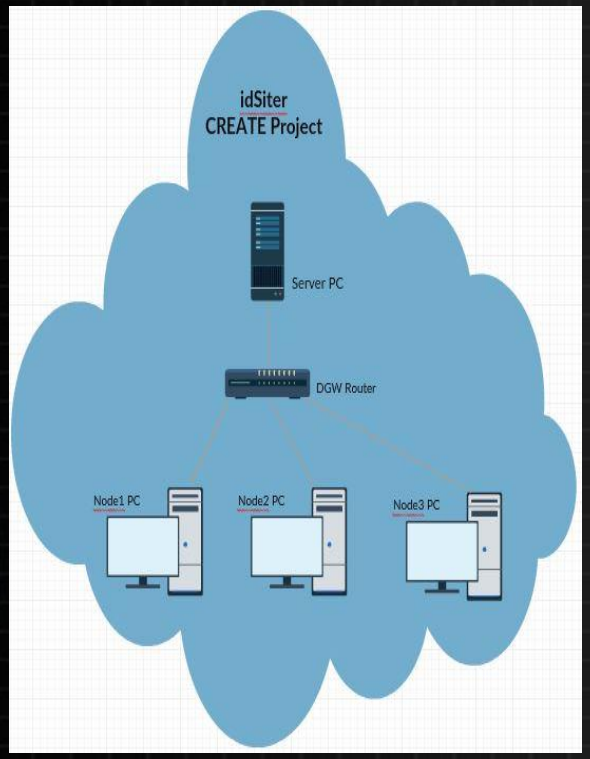
2.יציאה מהרשת בפרוטוקול Ssl בעל סטרטיפיקס לא חתום

3. יציאה מUser agent לא צפוי בצורה מונוטונית.

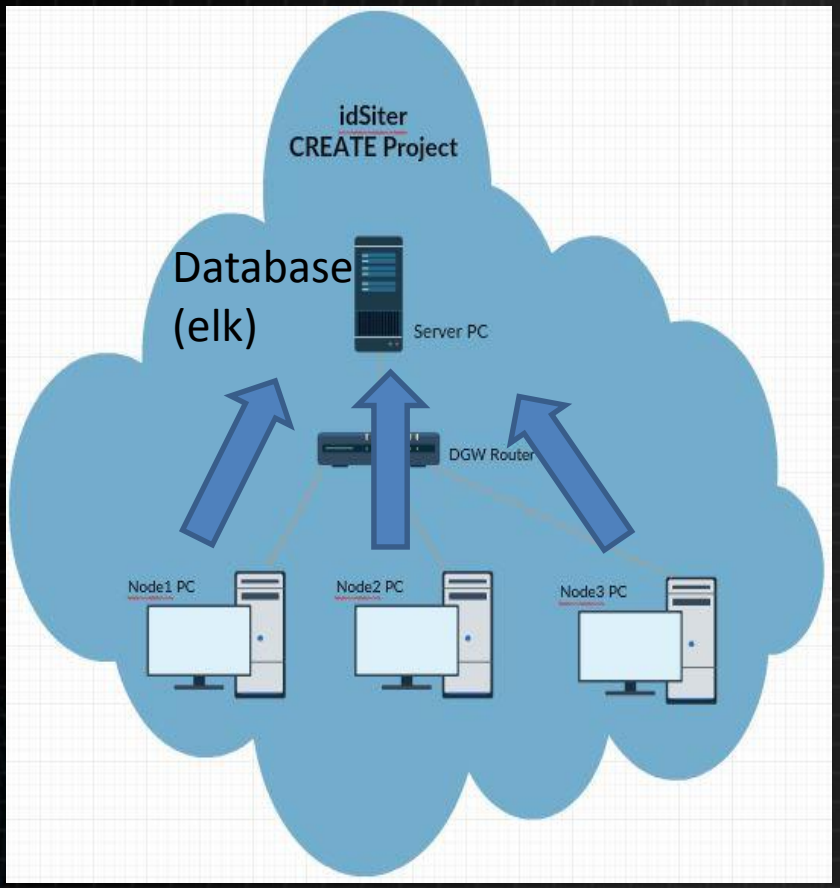
4.קריאת מידע משרת ברשת מכתובות מחו"ל

המערכת שלנו

- על כל מחשב יש hids.
- שימוש בפלטפורמה שנקראת create.



האלגוריתם


idSiter
CREATE Project
Database
(elk)
Server PC
DGW Router
Node1 PC
Node2 PC
Node3 PC

Elk

- Logstash, ElasticSearch ו Kibana

איסוף, פרסור ושליחה של נתונים, בעיקר לוגים

מנוע לאינדוקס וחיפוש בטקסט המאפשר גם יכולות אנליטיות רבות

מפלטרת לפי בקשתינו ומציגה וויזואליזציות שונות בהתבסס על הנתונים

נוסחת האינטרפולציה של ניוטון

$$P_n(x) = a_0 + a_1(x - x_0) + a_2(x - x_0)(x - x_1) + a_3(x - x_0)(x - x_1)(x - x_2) + \ldots\ldots + a_n(x - x_0)(x - x_1)\ldots(x - x_{n-1}).$$

$$a_0 = f_0 = f[x_0]$$

$$a_1 = \frac{f_1 - f_0}{x_1 - x_0} = f[x_0, x_1]$$

$$a_2 = \frac{\frac{f_2 - f_1}{x_2 - x_1} - \frac{f_1 - f_0}{x_1 - x_0}}{x_2 - x_0} = \frac{f[x_1, x_2] - f[x_0, x_1]}{x_2 - x_0}$$

$$= f[x_0, x_1, x_2]$$

$$a_n = f[x_0, x_1 \ldots x_n]$$

$$f[x_k, x_{k+1}] = \frac{f[x_{k+1}] - f[x_k]}{x_{k+1} - x_k}$$

$$f[x_k, x_{k+1}, x_{k+2}] = \frac{f[x_{k+1}, x_{k+2}] - f[x_k, x_{k+1}]}{x_{k+2} - x_k}$$

$$f[x_k, x_{k+1} \ldots x_i, x_{i+1}] = \frac{f[x_{k+1} \ldots x_{i+1}] - f[x_k \ldots x_i]}{x_{i+1} - x_k}$$

נוסחת האינטרפולציה המשך

הנוסחה משמשת למציאת, או לפחות לקירוב פונקציה בהתבסס על מספר נקודות הנמצאות בה.

```
('point after 1270 is ', 2550.0, ' in ', '30+2*(X-10)')
('f(x)=', '30+2*(X-10)', ' from ', [10, 30, 70])
```

קשייה

בעיה- הנוסחא דורשת נקודות (x,y) וברשותנו רק מערך זמנים, כלומר סדרה.
איטואיציה- ניקח כשיעורי האיקסים את הנקודות עצמן וכנקודות הy ניקח את המספרים שעוקבים אחריהם.

כלומר:
עבור הסדרה [10,20,30,40] ניצור את הנקודות (10,20), (20,30), (30,40)

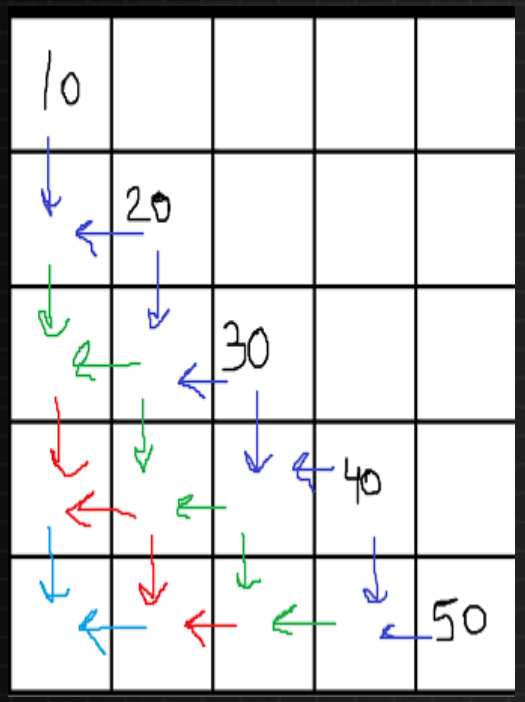
הדגמה

עבור הסדרה
[0,10,20,30,40,50]

נשים באלכסון את נקודות ה y

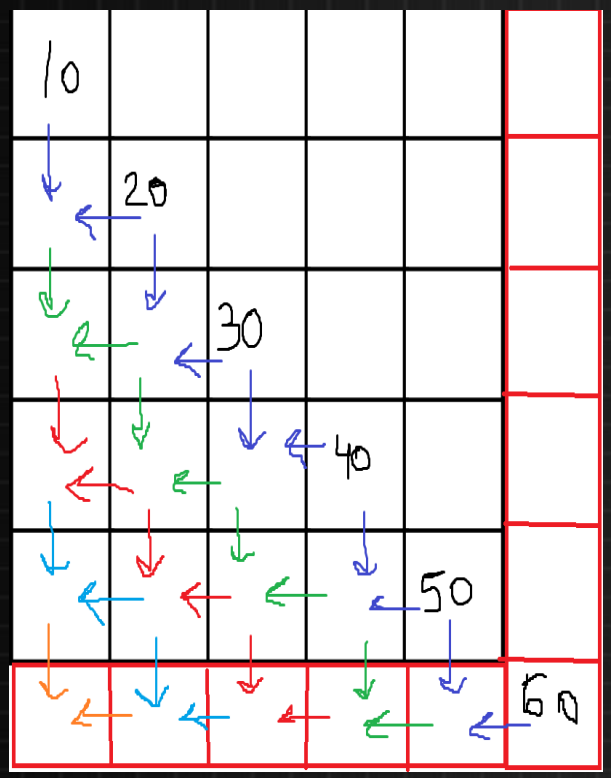
10				
	20			
		30		
			40	
				50

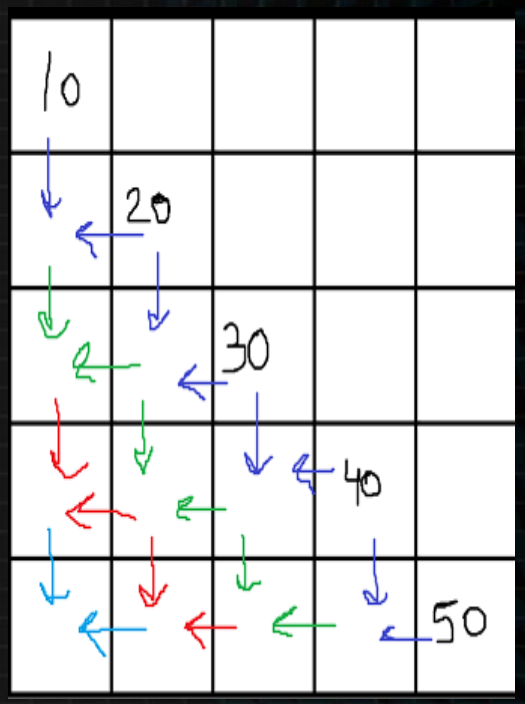
עבור כל משבצת במשולש התחתון, נחשב את ה- divided differences משכניו העליון והימני.



ומה קורה אם בהמשך הגיעו עוד נקודות?

נרחיב את המטריצה מצד ימין ומלמטה

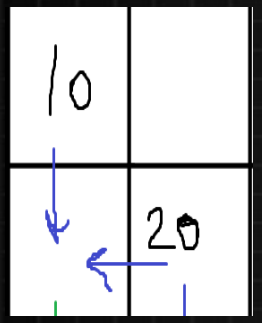


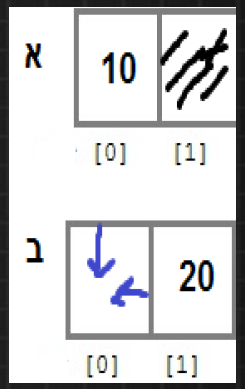


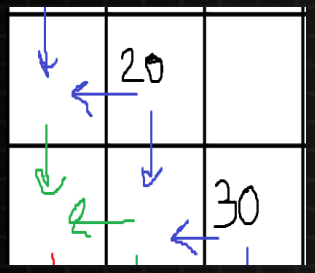
על בסיס רעיון זה, אנו שידרגנו את האלגוריתם

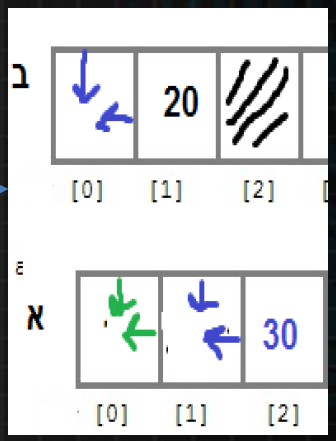
למה במקום להשתמש במטריצה לא נשתמש בשתי רשימות?

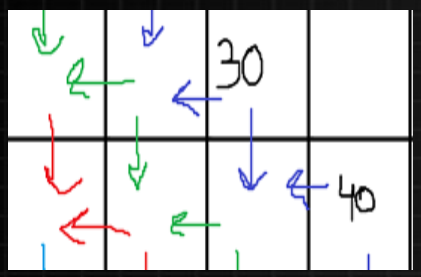
למה? כי זה שקול: נחלק את המטריצה מהשקופית הקודמת לשלבים

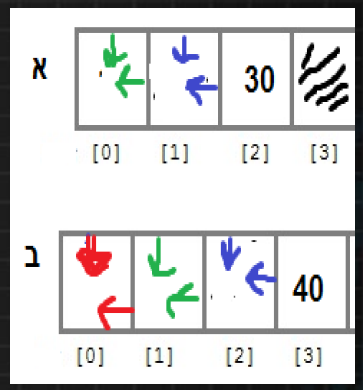


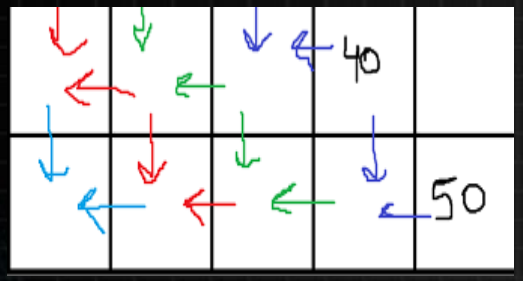


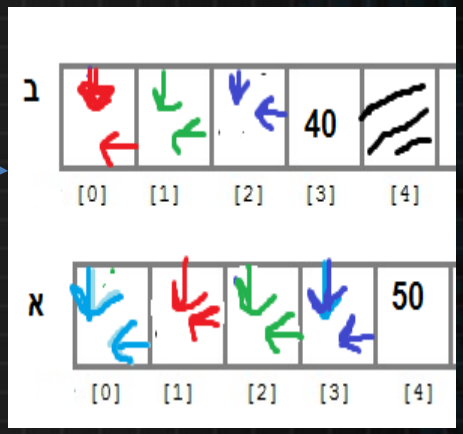





30
40


א
30
[0] [1] [2] [3]
ב
40
[0] [1] [2] [3]


40
50


ב
40
[0] [1] [2] [3] [4]
א
50
[0] [1] [2] [3] [4]

איך נמצא את הנקודה הבאה?

נציב את הנקודה האחרונה בסדרה בנוסחא שלנו.

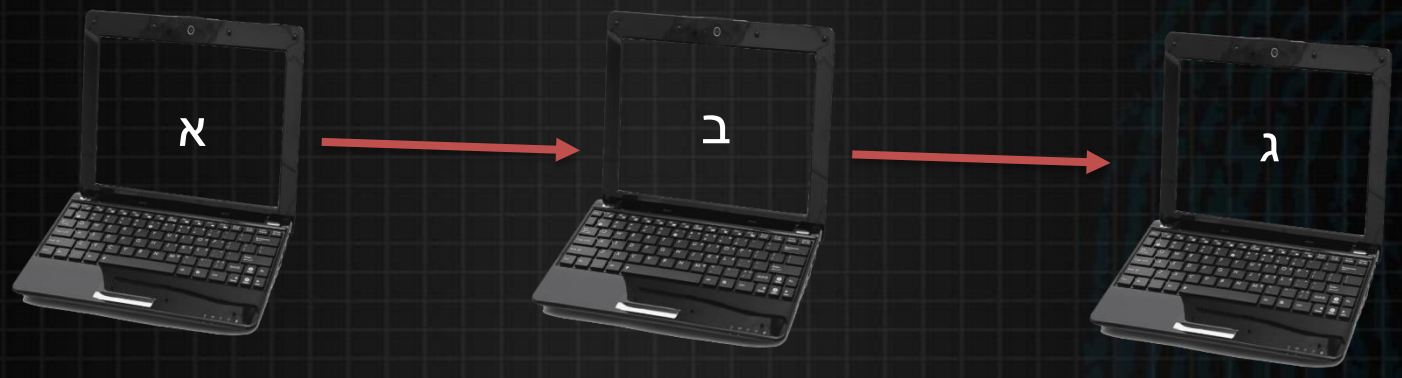
ולבסוף?

נשלח את הנוסחא והנקודות למכשירי הניטור המלצות לחוקים החדשים.

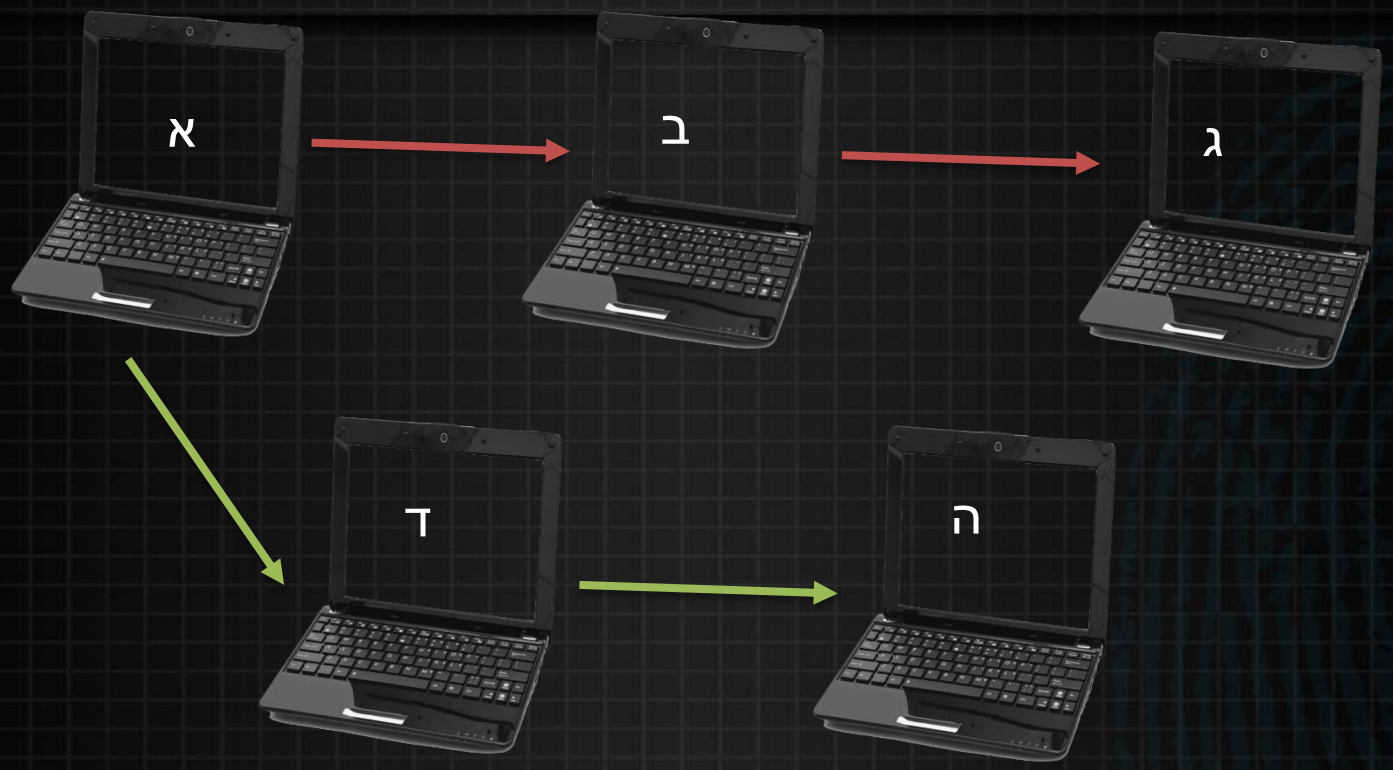
ניקח סדרות חדשות בכל נקודת זמן קבועה.

עד כאן?

הדרך פותרת מקרים בהם התולעת מתפשטת רק פעם אחת כל פעם:



בדר"כ התולעת מתפשטת לכמה מקומות ויוצרת כמה מסלולים:



בהינתן רשימת זמנים, נבדוק עבור כל תת קבוצה (שמתחילה מהאיבר הראשון בהכרח) אם היא מבחינה הגיונית יוצרת מסלול רציף, אם כן, ניצור לה פונקציה. יש לנו כמה פונקציות עכשיו, בהינתן נקודות עתידיות נבדוק איזה פונקציות לא מתאימות עד שנגיע לפונקציה אחת נכונה בלבד.