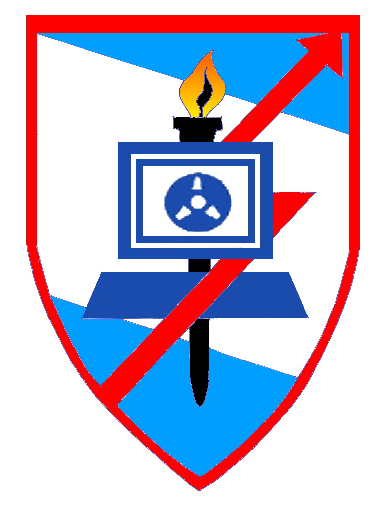
תיק עיצוב – פרויקט אישי





תוכן עניינים

1. יעדים 4

1.1. כללי 4

1.2. לקוח 4

1.3. בעיות 4

1.3.1. בעיות שהמערכת אמורה לפתור 4

1.3.2. בעיות שהמערכת איננה אמורה לפתור 4

2. יישום 5

2.1. אופי ומצב כללי של היישום 5

2.1.1. אופי המערכת 5

2.1.2. סוג המערכת 5

2.1.3. סוג הפעילויות הצפויה במערכת 5

2.1.4. אילוצים כלליים 7

2.2. משתמשים ומערכות משיקות - תיחום חיצוני 7

2.2.1. משתמשי פנים וחוץ 7

2.3. מודולים - תוכניות 9

2.4. מילון פריטי מידע 11

2.4.1. רשימת כל פריטי המידע 11

2.4.2. תיאור מפורט לכל פריט מידע 11

3. טכנולוגיה 13

4.1. חומרה מרכזית 13

4.2. מערכת הפעלה 13

4.3. בסיס נתונים 13

4. מימוש 14

5.1. גורם מבצע 14

5.2. פתרון נדרש 14

5.2.1. ספריות 15

5.3. תכנית עבודה מלאה 15

# יעדים

## Related imageכללי

כיום אנו נמצאים בתקופה בה משתמשים מבצעים מיליוני פעולות בשנייה במרכב הדיגיטלי.

רבות הפעמים שקשה לזהות את המשתמש מאחורי המסך אשר מבצע את הפעולה.

לעיתים קיים צורך לזהות את הבן אדם שעמד מאחורי המסך וביצע את הפעולה, כמו לדוגמה

במקרה של מבצע פשעי סייבר או כל פעולה אחרת שדורשת בדיקה על המבצע. נכון להיום קיימים

כלים שיכולים לעזור לאתר את המבצע של הפעולה מאחורי המסך אך כלים אלו אינם מקיפים ואינם מאפשרים איתור

משתמש על פי פרופיל חלקי או מלא.

DaitO מציעה פתרון מקיף לאיתור וזיהוי משתמשים מבוקשים על פי קלט מפרט פרופיל חלקי או מלא וקבלת

אופציות אפשריות לזהות ומיקום המשתמש המבוקש.

## C:\Users\u8558394\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CE35D676.tmpImage result for â«××¡× ×â¬âImage result for cia logoלקוח

לקוחות פוטנציאלים של המערכת הם גופים / ארגונים גדולים ואפילו

מדינות אשר זקוקים ליכולת מתקדמת של מעקב, איתור וזיהוי

משתמשים אשר זהותם אינה ידוע. לדוגמה : בסמ"ח, צה"ל, CIA וכוו.

## בעיות

### בעיות שהמערכת אמורה לפתור

|  |  |  |
| --- | --- | --- |
| תחום | תיאור הבעיה | חשיבות |
| איבוד עקבות משתמשים מבוקשים | במצב הקיים קשה מאוד לאתר ולזהות משתמשים מבוקשים אפילו אם קיים למחפש מידע שיכול לשמש לבניית פרופיל על המבוקש. במצב זה מבוקשים יכולים לברוח מעונש בקלות. | גבוהה |

### בעיות שהמערכת אינה אמורה לפתור

|  |  |  |
| --- | --- | --- |
| תחום | תיאור הבעיה | חשיבות |
| מניעת פעולות של משתמשים | המערכת אשר תהיה בצד הנבדק הינה אחראית על ניטור, האזנה ובניית פרופיל מלא לנבדק **ולא** אחראית על מניעת פעילותיו. | בינונית |
| יצירת פרופיל חלקי או מלא | המערכת אינה אחראית על יצירת פרופיל חיפוש למבוקש, מי שאחראי על יצירת פרופיל חיפוש למבוקש הוא המפעיל. | בינונית |

# יישום

## אופי ומצב כללי של היישום

### אופי המערכת

חדשה לגמרי, ללא כל זיקה למערכת קיימת (ידנית או ממוכנת).

### סוג המערכת

DaitO מורכבת משלושה תת מערכות –

צד נבדק – מערכת מוסוות (Rootkit) אשר מתפשטת בצורה עצמאית ומוסוות (Worm) לכלל המחשבים ברשת

צד שרת – שרת לינוקס מרובה משתמשים

צד מפעיל – מערכת עם ממשק משתמש המאפשרת צפייה וסינון מידע המתקבל מהשרת

### סוג הפעילויות הצפויה במערכת

צד נבדק – אין פעילות משתמש, המשתמש אינו מודע לקיום המערכת.

צד שרת – מקבל נתונים מצד הנבדק, אוגר ומתחזק את נתונים המתקבלים וליצירת פרופיל עבור כל נבדק.

בצד המפעיל – Data Entry (הזנת נתונים) ופליטת מידע לאחר חישובים.

### מפרט פרופיל נבדק

כאמור, DaitO בצד הנבדק מנטרת מידע שיעזור לאיתור וזיהוי המבוקש. כל המידע שנאסף על כל נבדק מהווה פרופיל המורכב ממספר רב של קטגוריות. פירוט מפרט פרופיל מלא עבור נבדק יחיד :

* **רשת** :
  + **Ip** 
    - Ip פנימי או חלק ממנו "192.168.x.2"
    - Ip חיצוני או חלק ממנו "212. x.x.142"
  + **אתר בהם הנבדק ביקר**
    - www.evilsite.com
    - facebook.com/personname
    - ww.bankname.co.lk
* **התנהגות במחשב**
  + **זמנים בהם הנבדק היה פעיל במחשב**
    - 24.05.2019@12:52 — 24.05.2019@04:45
  + **אפליקציות בהן הנבדק השתמש**
    - Safari
    - Vim
    - Curl
    - Gitbash
  + **מילים בהם המבוקש השתמש**
    - Attack
    - Cyber
    - 317318
    - myemail@gmail.com
* **חומרה ותוכנות במחשב הנבדק**
  + **מערכת ההפעלה של מחשב הנבדק**
    - Windows
    - Linux
  + **גרסת מערכת ההפעלה של מחשב הנבדק**
    - 3.1.4
    - 9
  + **ארכיטקטורת המעבד של מחשב הנבדק**
    - Arm
    - ice lake
  + **שם המעבד של הנבדק**
    - i7
  + **יצרן המעבד של מחשב הנבדק**
    - Intel
    - Amd
    - Nvidia
  + **שם כרטיס הגרפי של מחשב הנבדק**
    - Nvidia Titan X
    - AMD Radeon HD
* **ניתוח תוכן קבצי המחשב - File forensics**
  + **קובץ המופיע במחשב בנבדק**
    - test.txt
    - virus.sh
  + **קובץ בעל md5 checksum מסוים**
    - 7ED0097D7E9EE73CF0952A1F0A07C07E
  + **ניתוח קובצי image שבאופן פוטנציאלי יכולים להיות מכונה וירטואליים בהם המבוקש השתמש על מחשב הנדבק**
* **פרטי המבוקש - במידה וכן ידועים פרטים על מבצע הפעולה והמפעיל מעוניין לדעת מאיזה מחשב התבצע הפעולה**
  + **שם ושם משפחה המבוקש**
  + **עיר**
  + **רחוב**
  + **ארץ**
  + **אימייל**
  + **גיל**

כאשר המפעיל במצע חיפוש של מבוקש על פי מודיעין שאסף על המבוקש ממקורות.

המפעיל יכול להכניס ל -DaitO את הנתונים שהוא יודע על המבוקש ובכך למלא את הפרופיל בצורה מלאה או חלקית.

מידה והפרופיל הנתון (מלא או חלקי) עונה על פרופיל הנמצא בממסד הנתונים

של DaitO יוצג למפעיל הפרופיל/ים הנמצאים.

### אילוצים כלליים

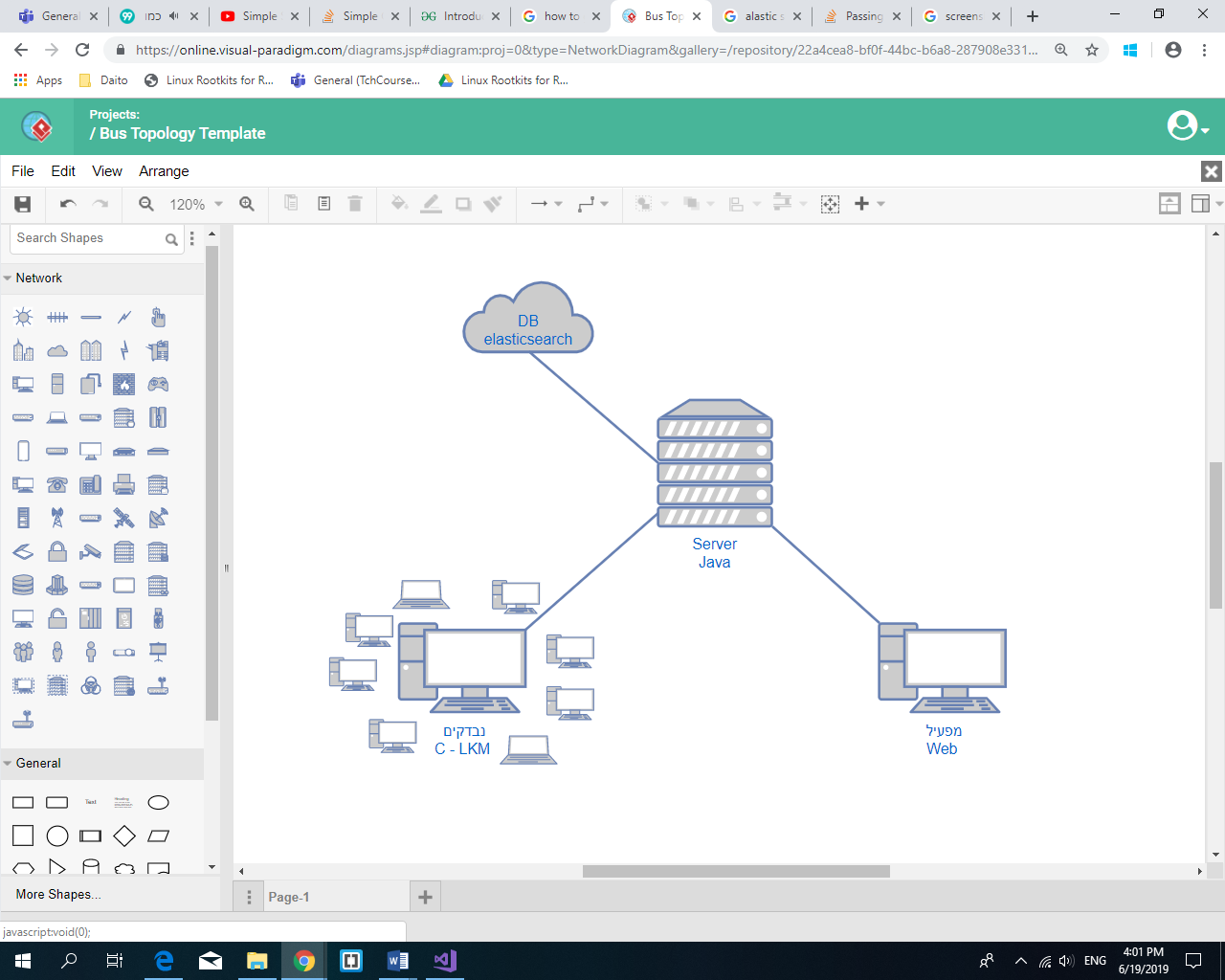
1. מערכות קיימות בארגון ומחוצה לו: ככל הנראה מערכות דומות או חופפות מפותחות כרגע או כבר נמצאות בשימוש, אולם אין להן השפעה על מערכת זו.
2. סביבה טכנית קיימת או מתוכננת: בזמן פיתוח המערכת, מחשב PC בעל מערכת הפעלה **Linux**.
3. על המערכת להישמר בסודיות מוחלטת, המערכת תופץ לכל המחשבים בארגון / גוף / מדינה כך שכל מחשב יוכל להיבדק על ידי המפעיל, בשביל שמשתמשים לא יחבלו בתקינות הניטור או הנתונים חשוב שהמערכת מצד הנבדק ובכלל תשמר בסודיות מוחלטת.

## משתמשים ומערכות משיקות - תיחום חיצוני

### משתמשי פנים וחוץ

|  |  |  |  |
| --- | --- | --- | --- |
| משתמש | ספק/צרכן מידע | חיוניות המערכת | תיאור הפעילות |
| מפעיל | ספק וצרכן מידע | גבוהה | מכין פרופיל חלקי או מלא של המשתמש המבוקש בפורמט נתון. מקבל רשימה של כל המשתמשים העונים על הפרופיל הנתון. |
| נבדק | ספק מידע | גבוהה | תוכנת צד הנבדק מאזינה ומנטרת נתונים רלוונטיים לאפיון פרופיל המשתמש, את נתונים אלה שולחת לשרת להמשך העיבוד ואחסון. |

## ארכיטקטורת תוכנה

שכבות

Data

Data access layer

Business logic layer

Gui

## <https://www.youtube.com/watch?v=89k3llI51fU> קילוגרמודולים - תכניות

### צד הנבדק

מאפיינים דרושים

1. מערכת צריכה להיות עמידה בפני הפעלה מחדש של המחשב
2. המערכת תוכל לשנות התנהגות של מערכת הפעלה
3. המערכת תוכל להחביא קבצים, תיקיות, תהליכים, תעבורת רשת, משתמשים ותכונות מערכת נוספות.
4. המערכת צריכה להיות עמידה בפני איתור, יצירת לוגיים ושינוי דגלים
5. המערכת צריכה לאפשר הרצת קוד מוגדר מראש

כללי

### צד המפעיל

### צד השרת

* **מובטח:**
  + הספרה השמאלית ביותר בקוד אינה 0.
  + אורך הקוד לא יעלה על 9 ספרות.

**דגשים חשובים:**

קלטים

|  |  |
| --- | --- |
| שם המקור | תיאור הקלט |
| מספר מחלקות | מספר המחלקות שיש בטייסת של מפקד הטייסת |
| כמות הדלק המלאי | כמות הדלק שיש לטייסת באותו יום במלאי |
| קוד מטוס | מספר המייצג את מהירותו הממוצעת של המטוס וזמן הטיסה שלו. |

פלטים

|  |  |
| --- | --- |
| שם היעד | תיאור הפלט |
| כמות הדלק שיש להזמין | * במידה ולא צריך להזמין דלק התוכנית תדפיס שיש מספיק דלק לטייסת, בכמה ליטרים תכנית הטיסה השתמשה וכמה יישאר לה בסוף היום. * במידה וצריך להזמין דלק, יש להדפיס כי יש להזמין דלק וכמה דלק צריך להזמין. |

**הקלט והפלט יכתבו בצורה ברורה וקריאה (הודעת קלט למשתמש, ירידת שורה, עימוד מסודר וכו')**

מפרט בדיקות

**בדיקת קומפילציה** - התוכנית תעבור קומפילציה ללא שגיאות ברמת חומרה כלשהי.

**בדיקות קבלה** - יש לבדוק את התוכנית ע"פ המפרט הבא (כמובן שבדיקות נוספות שלכם תתקבלנה בברכה):

* **הקלט נעשה משמאל לימין**
* כל פסיק ( , ) מסמן קלט חדש

|  |  |  |
| --- | --- | --- |
| מהות בדיקה (מה רוצים לבדוק) | קלט / מצב שנגרם בעקבות קובץ הקלט | פלט רצוי/ תגובה רצויה |
| צריך להזמין עוד דלק לאותו יום | 1, 1000, 666555, 2233, 134526, -999 | אין מספיק דלק בטייסת, צריך להזמין 18468 ליטר דלק |
| יש מספיק דלק לאותו היום. | 1, 14356, 13245, 5263, 63547, -999 | יש מספיק דלק לטייסת, היא תשתמש ב1116 ליטר ויישאר לה 13240 ליטר בסוף היום |
| יש כמות דלק מדויקת לאותו היום | 1, 503, 13425, 9843, 333, -999 | יש מספיק דלק לטייסת, היא תשתמש ב503 ליטר ויישאר לה 0 ליטר בסוף היום |

## מילון פריטי מידע

### רשימת כל פריטי המידע

|  |  |
| --- | --- |
| שם פריט המידע | תיאור |
| מפעיל |  |
| פרופיל חלקי |  |
| פרופיל מלא |  |
| נבדק |  |

### תיאור מפורט לכל פריט מידע

|  |  |  |
| --- | --- | --- |
| שם פריט המידע | מבנה פנימי | מרחב ערכים ובדיקות סבירות |
| מספר מחלקות | מספרי | מובטח שתקין. |
| כמות דלק | מספרי | מובטח שתקין. |
| קוד מטוס | מורכב משני מספרים: מהירותו הממוצעת וזמן טיסתו של מטוס (על פי ההסבר בסעיף 2.3.1.) | מובטח שהספרה השמאלית ביותר בקוד לא תהיה 0.  מובטח שאורך הקוד לא יעלה על 9 ספרות.  **קוד תקין:**  חייב להיות חיובי.  לא יכול להיות שהמהירות תהיה 0, או שזמן הטיסה יהיה 0. |

# טכנולוגיה

## חומרה מרכזית

המערכת מצריכה מחשב PC 586 ומעלה, MB 8 זיכרון לפחות, המסוגל להריץ Windows7.

## מערכת הפעלה

התוכנית תרוץ על מערכת ההפעלה Windows 7.

## בסיס נתונים

אין בסיס נתונים.

הנתונים מוזנים ידנית למערכת.

# מימוש

## גורם מבצע

|  |  |  |  |
| --- | --- | --- | --- |
| שלב | תאריך התחלה | תאריך סיום | המבצע |
| ניתוח | מאי 2014 | מאי 2014 | י.מ |
| עיצוב | מאי 2014 | מאי 2014 | י.מ |
| התחלת הקידוד | ‏ אוג 2017 | אוג 2017 | חניכי קורס תכנות |

## פתרון נדרש

**שם הפרויקט: BlackGold**

**שם הקובץ: BlackGold.cpp**

### ספריות

|  |  |  |
| --- | --- | --- |
| סביבה | מיקום | תאור |
| תכנון | Subjects\Algo\Tars\01 - BlackGold\Algo | קובץ תכנון האלגוריתם |
| פיתוח | Subjects\ Algo \Tars\01 - BlackGold | ספריית הפיתוח של המערכת |
| ייצור (סביבה מבצעית) | Subjects\ Algo \Tars\01 - BlackGold\Prod\Src | מיקום קבצי ה-Source של המערכת בסיום המערכת (קבצי cpp) |
|  | Subjects\ Algo \Tars\01 - BlackGold\Prod\Bin | מיקום קובץ ה-EXE של המערכת בסיום המערכת |
|  | Subjects\Algo\Tars\01 - BlackGold\Prod\Test | מיקום קובץ ה Testing שכתבתם |

## תכנית עבודה מלאה

|  |  |  |
| --- | --- | --- |
| שלב | תיאור | משך |
| א | קריאת הנוסח | 40 דקות |
| ב | מימוש התוכנית ע"ג המחשב | 155 דקות |
| ג | בדיקות קבלה וביצוע תיקונים | 60 דקות |
| ד | העברה לסביבת ייצור | --- |

# נספח – פעולת חלוקה ופעולת שארית ב- ++C

### פעולת חלוקה

**עד עכשיו כאשר חילקנו בין 2 מספרים היינו משתמשים באופרטור /**

**האופרטור / מחזיר לנו כמו פעמים נכנס מספר אחד בתוך מספר אחר.**

**דוגמה : 9 / 2 = 4.**

### שארית חלוקה (מודולוס)

**האופרטור % מחזיר לנו את שארית החלוקה של מספר ממספר אחר.**

**דוגמה: 11 % 3 = 2**

**כלומר 3 נכנס ב-11 3 פעמים (3 \* 3 = 9), וכדי להגיע ל11 נצטרך להוסיף עוד 2.**



Abi ron

כיום אנו נמצאים בתקופה בה משתמשים מבצעים מיליוני פעולות בשנייה במרכב הדיגיטלי.

רבות הפעמים שקשה לזהות את המשתמש מאחורי המסך אשר מבצע את הפעולה.

לעיתים קיים צורך לזהות את הבן אדם שעמד מאחורי המסך וביצע את הפעולה, כמו לדוגמה

במקרה של מבצע פשעי סייבר או כל פעולה אחרת שדורשת בדיקה על המבצע. נכון להיות קיימים

כלים שיכולים לעזור לאתר את המבצע של הפעולה מאחורי המסך אך כלים אלו אינם מקיפים ואינם מאפשרים איתור

משתמש על פי פרופיל חלקי או מלא.

DaitO מציעה פתרון מקיף ומלא לאיתור וזיהוי משתמשים מבוקשים על פי קלט מפרט פרופיל חלקי או מלא וקבלת אופציות אפשריות לזהות ומיקום המשתמש מבוקש.

## CE35D676Image result for â«××¡× ×â¬âImage result for cia logoלקוח

לקוחות פוטנציאלים של המערכת הם גופים / ארגונים גדולים ואפילו

מדינות אשר זקוקים ליכולת מתקדמת של מעקב, איתור וזיהוי

משתמשים אשר זהותם אינה ידוע. לדוגמה : בסמ"ח, צה"ל, CIA וכוו

English description:

Now days we live in a time that users perform millions of actions per second in the digital area. Many times its hard or even impossible to **detect** and **identify** the user behind the computer that perform the action