פרויקט בהנדסת תוכנה

תכנון ותכנות מערכות בהתמחות הגנת סייבר  
סמל מקצוע: 883589

**Eagle Eye**

מערכת לניטור ובקרת תקשורת

שם התלמיד: אופק ארז

מספר זהות: 214273393

שם בית ספר: קריית חינוך אמירים

עיר: ראשון לציון

שם המנחה: מוטי מתתיהו

מועד הגשת המסמך:

**יכלול:**

1. לוגו של האפליקציה/יישום/מערכת
2. נושא העבודה
3. שם התלמיד
4. ת"ז של התלמיד
5. שם בית הספר ועיר
6. שמות המנחים + המורים המלווים
7. מועד הגשת המסמך (חודש ושנה)

**תוכן עניינים וראשי פרקים**

# פרק א – Eagle - Eye Project - ייזום

1. תיאור ראשוני של המערכת

מבוא

בחרתי לפתח תוכנה לניטור תעבורת רשת מפני שכאשר השתמשתי בתוכנה הקיימת לניטור חבילות מידע – Wireshark, הרגשתי כי ניתן לעשות זאת בצורה נוחה ואינטואיטיבית יותר בשל עומס ועודף הנתונים אשר ברוב המקרים אינם רלוונטיים לבדיקות שגרתיות של תעבורת הרשת.

הפרויקט הוא מערכת אשר מטרתה לאפשר אבחון וניטור של תעבורת הרשת העוברת דרך המחשב.

כמו כן, מטרת הפרויקט הוא להוות כלי נוח ואינטואיטיבי לאנשי תקשורת על מנת לעבור על תעבורת הרשת בארגון, או אף במערכת הביתית שלהם, ולבודקי חוסן (penetration testers) לחקור את התעבורה במחשב מסוים אשר עליו הוא מבצע בדיקה והפורטים הפתוחים בו, על מנת לאבחן האם קיימות פגיעויות אפשריות הנובעות מהגדרת הרשת במחשב או בארגון.

**תקציר הפרויקט**

**רכיבי המערכת**

1. שרת((Server – השרת מאכסן לי את מסד הנתונים המכיל את נתוני המשתמשים ואת טבלת הבדיקות שכל משתמש עשה עד כה.
2. Controller – מחשב עליו נמצאת התוכנה, וממנו ניתן לבצע פעולות על כל המחשבים הנוספים בLAN המכילים את התוכנה. דרך מחשב זה בלבד מתחברים למשתמש/נרשמים כמשתמש.
3. לקוחות(Clients) – כל המחשבים עליהם מותקנת התוכנה מלבד הController ועליהם מתבצעות הבדיקות בהוראת הController-.

* תקציר כולל ורציונל הפרויקט
* מה המוצר המוגמר אמור לבצע
* למה בחרתי בפרויקט ומה האתגרים שאני צופה לי בפרויקט

1. הגדרת הלקוח

המערכת מכוונת לשני קהלי יעד עיקריים, כאשר שניהם טכנולוגיים בעיסוקם. קהל בודקי חוסן וחוקרי אבטחת מידע , קהל מנהלי הרשתות, אנשי system. הסיבה לכך, היא שהמערכת נועדה לסייע לאנשים בתפקידים אלו לבצע את עבודתם בצורה יעילה ומהירה יותר ובקלות ונוחות רבה יותר, באמצעות הכלים שפיתחתי כחלק מן המערכת.

1. הגדרת יעדים/מטרות

Eagle – Eye מאפשרת את הפעולות הבאות:

* מיפוי העמדות הפעילות ברשת והצגת כתובות הIP שלהן.
* ביצוע בדיקות תעבורה על מספר מחשבים.
* ראיית תוכן חבילות המידע שנקלטו.
* הצגה של המידע בצורה מסודרת על פי פרוטוקולים.
* סינון ומיון הפאקטות על פי זמן הקבלה, כתובת האיי פי ממנה התקבלו, הפורט וכו'..
* סריקת פורטים בכל המחשבים הנשלטים הן פורטי TCP והן פורטי UDP.
* בחינה של תוצאות בדיקות אשר נעשו בעבר דרך המשתמש.
* יצירת Reverse Shell בכל אחד מהמחשבים עליהם מותקנת התוכנה, מה שמאפשר השתלטות מרחוק כל זמן שהעמדה פעילה ומחוברת לController.

1. בעיות, תועלות וחסכונות

הבעיות אשר המערכת שלי פותרת היא סקירה של פגיעות רשת ארגונית מפני תקיפות זדוניות של אנשים המעוניינים בפגיעה בארגון/למען תועלת אישית. כמו כן, היא פותרת בעיה הקיימת בכלים הקיימים לצורך סקירות שכאלו כגון Nmap, Wireshark אשר אינם יעילים, נוחים ואינטואיטיביים עבור סקירה של רשת ארגונית ולא מחשב בודד מה שמקשה על אנשי המקצוע לבחון רשתות במהירות ובמקצועיות. כמו כן, לא מעט צצות בעיות של בלבול ושכחה בין היכולות הרבות והמסובכות/מסורבלות בכלים אלו אשר מעכבים את אנשי המקצוע להשיג את מטרתם במהירות. המערכת מנסה להציע פתרון נוח ופשוט לבעיות אלו באמצעות ממשק משתמש פשוט ואינטואיטיבי שיאפשר ללקוחות לבצע את עבודתם ללא צורך בפקודות מסובכות. המערכת מעניקה מספר שירותים ללקוחותיה, הראשון בהם הוא מסד נתונים המאפשר התחברות של הלקוח לאתר וקבלת תוצאות של סריקות שביצע על רשתות בעבר. כמו כן, המערכת מעניקה כלים להסנפת תעבורת רשת, סריקת פורטים, התחברות לממשק הפקודות של מחשבים וביצוע פעולות טכניות נוספות עליהם, כגון העברת קבצים ושליחת צילום מסך.

1. האם צפויים קשיים או מגבלות בהגדרת המערכת

ישנם מספר קשיים הצפויים במערכת. הראשון שבהם הוא מהירות הסריקה. מכיוון שמדובר במסניף תקשורת אשר נכתב בפייתון שהינה שפת High Level, זמן הפעולה של כל סריקת רשת יהיה איטי באופן יחסי לתוכנית מקבילה בשפת Low Level כגון C או ++C. בנוסף, ניתן יהיה לסרוק רק מחשב אחד בכל פעם מכיוון שאי אפשר להציג את תוצאות הסריקות ביחד באותו דף באתר.

בנוסף, יש צורך בשביל שהפרויקט יעבוד שעל כל המחשבים אותם אנו רוצים לסרוק יפעל השרת שבניתי ויהיה מותקן עליו הפרויקט שלי(לפחות קבצי הbackend).

כמו כן, יש מגבלה נוספת על הפרויקט שהוא עובד אך ורק על מחשבים הנמצאים בLAN, הרשת המקומית. זאת מכיוון שלא יישמתי port forwarding שינתב את כל התקשורת בפורטים בהם משתמש הפרויקט אל מחשב השרת.

* האם מדובר בטכנולוגיה חדשה ובלתי מוכרת?
* האם קיימים סייגים בהגדרת המערכת? (הגבלות שנובעות מבעיות/כשלים/צרכים/ציוד מיוחד... וכו')

1. תיחום הפרויקט

* יש לתאר את התחומים בהם הפרויקט עוסק (בדגש על רשתות ומערכות הפעלה)

הפרויקט עוסק ברשת רחבה של תחומים. הוא עוסק בתחום ה- Web בכך שממשק המשתמש שלי מבוסס על דפי HTML והשרת העיקרי בפרויקט הוא שרת Flask.

כמו כן, הפרויקט עוסק ונוגע בנושאים רבים בתחום אבטחת המידע, בכך שהוא משלב נושאים כגון: Reverse Shell, Encryptions, Hashes, Defense against SQLI, Port Scanning.

בנוסף, הפרויקט עוסק בצורה רחבה מאוד ברשתות. יש לי בפרויקט שלושה שרתים שונים, האחד שרת Flask, שהינו שרת TCP הפועל בפורט 80, הפורט המיועד לתקשורת בפרוטוקול HTTP, בה עובד עולם הWeb. שרת נוסף הינו שרת TCP הפועל בפורט 16549, הקיים על כל מחשבי הרשת, אשר מטרתו לקשר בין הfront end לback end. כל פעולה שנעשית באתר מובילה לפונקציה שנקראת בצד שרת הFlask וכאשר המשתמש מעוניין להפעיל סריקה כזו או אחרת על מחשב ברשת המקומית, ישלח הלקוח הנמצא על המחשב המחובר לאתר הודעה לשרת הנמצא על המחשב עליו המשתמש מעוניין לבצע בדיקה. בנוסף, ישנו גם שרת (מאזין) Reverse Shell, העובד בפרוטוקול TCP על פורט 9999 והינו בעל יכולות רבות: העברת קבצים, העברת צילום מסך, ביצוע פקודות shell והעברת התוצאות. נוסף לכל, הפרויקט מכיל מסניף תקשורת, אשר קולט את חבילות המידע הנשלחות ברשת המקומית ומציג למשתמש את התעבורה בפרוטוקולים הנמצאים בשימוש הרב ביותר והינם בסיכון הגבוה ביותר למתקפות רשת: SSH, ICMP, DNS, HTTP, DHCP, SMB וFTP.

**פרק ב' - 'שם המערכת' – אפיון**

1. פרוט המערכת:

* שרטוט של המערכת (שרת/לקוחות/מצלמות/ אמצעים אחרים...) ארכיטקטורה (p2p או שרת לקוח)
* תיאור מפורט יותר של המערכת (להרחיב את הכתוב בייזום)
* מה היא אמורה לעשות (להרחיב את הכתוב בייזום)

**פונקציונליות המערכת**

1. הרשמה ראשונית למערכת.

2. התחברות משתמש קיים למערכת (Log In).

3. אימות משתמש דרך מייל.

4. אפשרות איפוס סיסמה.

5. אפשרות צפייה בסריקות קודמות.

6. אפשרות לסרוק את העמדות הפעילות ברשת המקומית.

7. אפשרות לבצע סריקת פורטים מסוג SYN TCP על כל אחד ממחשבי הרשת.

8.  אפשרות לבצע סריקת פורטים מסוג Stealth TCP על כל אחד ממחשבי הרשת.

9. אפשרות לבצע סריקת פורטי UDP על כל אחד ממחשבי הרשת.

10. אפשרות הפעלת הסנפת תקשורת על כל אחד ממחשבי הרשת.

11. אפשרות התחברות לממשק הפקודה של כל אחד מהמחשבים באמצעות Reverse Shell.

12. התנתקות מהמערכת( (Log out.

**דרישות פונקציונליות**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **דרישה** | **קלט** | **תהליך** | **פלט** | **טיפול בשגיאות** |
| **1** | הרשמה ראשונית למערכת – רישום של משתמש חדש | נתוני המשתמש החדש (שם פרטי, שם משפחה, אימייל, שם משתמש נבחר, סיסמה נבחרת). | העברת נתוני המשתמש המתקבלים לשרת ושמירתם בבסיס הנתונים( הסיסמה מגובבת). | דף HTML המודיע כי הלקוח נרשם בהצלחה למערכת. | תוחזר הודעת שגיאה במקרה של:  - אימייל לא תקין/תפוס.  - שם משתמש תפוס.  - סיסמה קצרה מידי.  - אימות סיסמה שגוי. |
| **2** | התחברות משתמש קיים למערכת | נתוני המשתמש הקיים (שם משתמש, סיסמה). | העברת נתוני המשתמש המתקבלים לשרת ובדיקתם בבסיס הנתונים. | הודעה המודיעה כי הלקוח התחבר בהצלחה למערכת, ומעבר למסך אימות. | תוחזר הודעת שגיאה אם:  - לפחות מהנתונים שהתקבלו לא מתאים לנתונים הקיימים מראש במסד הנתונים. |
| **3** | איפוס סיסמה | אימייל | ביצוע בדיקת התאמה בין ה ושם המשתמש הנקלטים. אם קיים מייל זה במערכת, ישלח לאימייל קוד אימות לשחזור סיסמה. המשתמש יתבקש להקליד קוד זה, ובמידה והקוד נכון תינתן אפשרות לשינוי סיסמה. | מסך המאפשר איפוס ושינוי סיסמה. | תוחזר הודעת שגיאה במקרה וכתובת האימייל שהתקבלה לא תקינה.  תוחזר הודעה מתאימה במקרה שלא קיים מייל כזה במערכת. |
|  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **דרישה** | **קלט** | **תהליך** | **פלט** | **טיפול בשגיאות** |
| **4.1** | הפעלת הסנפה | מספר הפאקטות להסנפה(ברירת מחדל 1000). | הסנפת תקשורת | הפאקטות שהוסנפו ושייכות לפרוטוקולים הבאים: SSH, ICMP, DNS, HTTP, DHCP, SMB וFTP | אין |
| **4.2** | הפעלת סריקת פורטים SYN | טווח הפורטים לבדיקה | סריקת פורטים | הפורטים הפתוחים | אין |
| **4.3** | הפעלת סריקת פורטים Stealth | טווח הפורטים לבדיקה | סריקת פורטים | הפורטים הפתוחים | אין |
| **4.4** | הפעלת סריקת פורטים UDP | טווח הפורטים לבדיקה | סריקת פורטים | הפורטים הפתוחים | אין |
| **4.5** | התחברות בReverse Shell | פקודה לביצוע | הרצת הפקודה על המחשב המרוחק | תוצאות הפקודה | פקודה לא תקינה, שגיאות חיבור. |
| **5** | התנתקות מהמערכת | בקשת התנתקות מהמערכת של המשתמש. | ניתוק המשתמש מהמערכת. | סגירת הSession של המשתמש והעברה לדף HTML האומר כי התנתק בהצלחה. | אין |

1. מה היכולות שהיא תעניק למשתמש , פירוט היכולות   
   במידה ויש משתמשים שונים, לפרט לפי כל משתמש:

* אפשרות צפייה בסריקות קודמות.
* אפשרות לסרוק את העמדות הפעילות ברשת המקומית.
* אפשרות לבצע סריקת פורטים מסוג SYN TCP על כל אחד ממחשבי הרשת.
* אפשרות לבצע סריקת פורטים מסוג Stealth TCP על כל אחד ממחשבי הרשת.
* אפשרות לבצע סריקת פורטי UDP על כל אחד ממחשבי הרשת.
* אפשרות הפעלת הסנפת תקשורת על כל אחד ממחשבי הרשת.
* אפשרות התחברות לממשק הפקודה של כל אחד מהמחשבים באמצעות Reverse Shell.

1. פירוט הבדיקות ('קופסא שחורה')

(בדיקות לביצוע אך ורק עם קובץ ההרצה, ללא הקוד, בדגש על כך שכל אחד לפי הכתוב בטבלה יצליח לבצע את הבדיקה)

|  |  |  |  |
| --- | --- | --- | --- |
| **מספר** | **שם הבדיקה (שם שיעיד על תוכן הבדיקה)** | **מה אמורה לבדוק** | **איך מתכננים לבדוק**  **(לתאר בפירוט את שלבי הבדיקה)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. תכנון לוח זמנים לפרויקט

* תכנון לוח זמנים ראשוני
* עבור כל פעילות בלוח: זמן התחלה מתוכנן, זמן סיום מתוכנן , זמן התחלה בפועל, זמן סיום בפועל והערות. יש לכלול את התאריכים שניתנו לכם עבור כל פרק כ'זמן סיום מתוכנן' ואת החודש של הקידוד לפרק לאבנים גדולות ולתת להן זמנים

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **פעילות** | **זמן התחלה מתוכנן** | **זמן סיום מתוכנן** | **זמן התחלה בפועל** | **זמן סיום בפועל** | **הערות** |
| יזום |  |  |  |  |  |
| אפיון |  |  |  |  |  |
| ניתוח |  |  |  |  |  |
| עיצוב |  |  |  |  |  |
| קוד (לפרוט לאבנים גדולות) |  |  |  |  |  |
| גרסה ראשונית |  |  |  |  |  |
| מסמך בדיקות |  |  |  |  |  |
| מדריך למשתמש |  |  |  |  |  |
| גרסה סופית |  |  |  |  |  |
| סגירת תיק פרויקט |  |  |  |  |  |
| מצגת הסבר |  |  |  |  |  |

* **לוח הזמנים – הינו מסמך חי ויש לעדכנו לאורך כל הפרויקט**

1. ניהול סיכונים בפרויקט

* זיהוי סיכוני הפרויקט, ניתוחם ומענה עליהם, הטבלה תמוין מסיכון גבוה לנמוך (הגבוהים באדום, בינוני –כתום , קל – צהוב) סיכון שיוסר יצבע בירוק ויעבור לתחתית המסמך

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **הסיכון** | **פירוט הסיכון** | **רמת הסיכון**  **(קל/בינוני/קשה)** | **תיאור דרכים (לפחות 2 ) להתמודדות עם הסיכון ולהקטין אותו** | **מה בוצע בפועל** | **תאריך** |
| אי עמידה בזמנים | פרויקט לא יושלם | קשה | * הקדמת לו"זים משימות * ארגון הזמן בצורה יעילה * להתחיל בדברים היותר קשים |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

* **ניהול סיכונים – הינו מסמך חי ויש לעדכנו לאורך כל הפרויקט**

**פרק ג' - 'שם המערכת' - מסמך ניתוח**

פרוט יכולות המערכת

**יכולות בצד שרת: רנדור דפי HTML ושליחתם ללקוח(שרת הFlask- ), שליחת פקודות לכל אחד מהמחשבים לביצוע אחת מפעולות הבאות: סריקת פורטים, הפעלת לקוח לReverse Shell, הפעלת הסנפה, שמירת תוצאות ההסנפה בקובץ PCAP, יצירת קשר עם מסד הנתונים לצורך שינוי ואחזור נתונים.**

**צד שרת((Flask:**

שם היכולת: הרשמה למערכת

מהות היכולת: רישום משתמש חדש במערכת

אוסף יכולות:

* קבלת נתונים מהלקוח
* בדיקה מול בסיס הנתונים
* גיבוב סיסמא
* הוספה לבסיס נתונים
* החזרת דף תשובה

שם היכולת: התחברות למערכת

מהות היכולת: התחברות משתמש למערכת

אוסף יכולות:

* קבלת נתונים מהלקוח
* בדיקה מול בסיס הנתונים
* החזרת דף תשובה

שם היכולת: איפוס סיסמה

מהות היכולת: איפוס סיסמה של משתמש לפי מייל

אוסף יכולות:

* קבלת נתונים מהלקוח - מייל
* בדיקה מול בסיס הנתונים
* שליחת מייל עם קוד אימות.
* החזרת דף לאיפוס
* קבלת נתוני סיסמה חדשה
* בדיקת האימות.
* שינוי הסיסמה במסד הנתונים.

שם היכולת: אפשרות צפייה בסריקות קודמות

מהות היכולת: הצגת דף עם תוצאות של סריקות שבוצעו בעבר.

אוסף יכולות:

* הצגת סריקות שבוצעו בעבר.
* הצגת תוצאות הסריקה שנבחרה על ידי טעינה מקובץ PCAP.

**צד שרת(שרת 2) :**

שם היכולת: התחלת סריקת פורטי TCP

מהות היכולת: השרת יקבל הודעה מלקוח להתחיל לבצע סריקת פורטי TCP מסוג מסוים על המחשב עליו הוא נמצא ויפעיל את הפעולה המתאימה.

אוסף יכולות:

* קבלת הודעה מלקוח ובהתאם הפעלת סריקת פורטים, החזרת המידע לשרת הFlask.

שם היכולת: התחלת סריקת פורטי UDP

מהות היכולת: השרת יקבל הודעה מלקוח להתחיל לבצע סריקת פורטי UDP על המחשב עליו הוא נמצא ויפעיל את הפעולה המתאימה.

אוסף יכולות:

* קבלת הודעה מלקוח ובהתאם הפעלת סריקת פורטים, החזרת המידע לשרת הFlask.

שם היכולת: התחלת הסנפה

מהות היכולת: השרת יקבל הודעה מלקוח להתחיל לבצע הסנפה של התקשורת שתפעל על המחשב עליו הוא נמצא, יתחיל בהסנפה ויחזיר את תוצאותיה לשרת הFlask אשר יציג אותן על גבי האתר.

אוסף יכולות:

* קבלת הודעה מלקוח ובהתאם התחלת הסנפה.
* החזרת מחרוזת המכילה את המידע הרלוונטי מהפאקטות שהוסנפו ושייכות לפרוטוקולים הבאים: SMB, FTP, DHCP, SSH, DNS, HTTP, ICMP לשרת הFlask.

שם היכולת: הפעלת לקוח Reverse Shell.

מהות היכולת: השרת יקבל הודעה מלקוח להדליק את לקוח הReverse Shell על המחשב עליו הוא נמצא ויפעיל את הפעולה המתאימה.

אוסף יכולות:

* הדלקת לקוח הReverse Shell-.

**צד שרת(שרת 3) :**

שם היכולת: התחברות ב- Reverse Shell למחשב ברשת המקומית.

מהות היכולת: השרת יבקש להתחבר לאחד מהמחשבים ברשת(אחד מהלקוחות) וישלח ללקוח הודעה בהתאם לפקודה שהכניס המשתמש באתר ויקבל את תוצאות הפקודה מן הלקוח ויעבירן לשרת הFlask אשר ירנדר את המידע שהתקבל אל תוך דפי הHTML ויציג אותו למשתמש או יעביר את הקובץ המבוקש ללקוח/ יקבל קובץ מן הלקוח.

אוסף יכולות:

* שליחת הודעה ללקוח עם פקודה להפעלה על מחשב הלקוח.
* קבלת תוצאות הפקודה/ קבלת הקובץ/ שליחת הקובץ.

**יכולות בצד לקוח:**

(להתחיל לבנות לפי הרשימה של היכולות שציינתם באפיון, שימו לב שכאן תצטרכו לפרט עד הרמה הבסיסית הנדרשת למימוש כל יכולת , שימו לב מדברים ברמת על לא בקוד) :

**דוגמא:**

**צד לקוח:**

שם היכולת: הרשמה למערכת

מהות היכולת: רישום משתמש חדש במערכת (קליטת פרטיים אישיים נדרשים)

אוסף יכולות:

* ממשק משתמש – מסך הרשמה
* קליטת נתונים
* בדיקת תקינות
* שליחה לשרת בבקשת POST
* קבלת תשובה מהשרת
* הצגת דף תשובה למשתמש

שם היכולת: שליחת בקשה לסריקת פורטי TCP

מהות היכולת: לחיצה על כפתור באתר שיבקש ממחשב מסוים להתחיל בסריקת פורטים.

אוסף יכולות:

* שליחת הבקשה לשרת.

שם היכולת: שליחת בקשה לסריקת פורטי UDP

מהות היכולת: לחיצה על כפתור באתר שיבקש ממחשב מסוים להתחיל בסריקת פורטים.

אוסף יכולות:

* שליחת הבקשה לשרת.

רשימת אובייקטים: ממשק משתמש, הצפנה/פיענוח, תקשורת

רשימת אובייקטים: הצפנה/פענוח, תקשורת, בסיס נתונים

**פרק ד' - 'שם המערכת' - העיצוב**

1. תיאור הארכיטקטורה של המערכת המוצעת

* תיאור החומרה
* רכיבים שונים והקשרים ביניהם
* לצרף שרטוט – חובה!

1. תיאור הטכנולוגיה הרלוונטית

* פירוט ההחלטות שנלקחו בחשבון בעת בחירת הטכנולוגיה   
  (שפת תכנות, OS, תקשורת, תחומי עיניין, ועוד...)

1. תיאור מודולים בהם נעשה שימוש

* **שרטוט המראה את הזרימה בין המודולים המרכזיים (להקפיד בשרטוט על מקרא אחיד תוך ביצוע אבחנה בין מה נמצא בלקוח ומה בשרת, שימוש ב draw.io) – החלק בו אתם קובעים את תצורת המערכת**
* סקירת כל המודולים המרכיבים את המערכת וקשרי הגומלין ביניהם:
  1. מודולים שאתם מייבאים – מספיקה שורה אחת המסבירה למה מיועד המודול.
  2. מודולים שלכם - יש לפרט ברמת אובייקטים (שם האובייקט והתכונות שבו) וכן כלל הפעולות שבמודל (כותרות וטענת כניסה ויציאה לכל פעולה – באנגלית כפי שיקראו בתוכנה)

1. תיאור סביבת הפיתוח

* שפת התכנות שנבחרה לכתיבת הפרויקט
* פירוט כלי הפיתוח הנדרשים לפיתוח
* פירוט הסביבה והכלים הנדרשים לבדיקות

1. תיאור האלגוריתמים המרכזיים בפרויקט: (לבחור 4 בעיות עיקריות בפרויקט ולנתח לפי האמור בסעיף זה)

* ניסוח וניתוח של הבעיה האלגוריתמית
* תיאור אלגוריתמים קיימים לפתרון הבעיה
* הפנייה למקורות רלוונטיים
* סקירת הפתרון הנבחר (תוך נימוק הבחירה בו ושלילת הפתרונות האלטרנטיביים, או פיתוח מקורי)

1. תיאור מסכי הפרויקט:

* לכל מסך מיועד בפרויקט (שרטוט ידני, בהמשך יצורפו מסכי המערכת):
  1. מה מטרת המסך
  2. שרטוט של המסך (מה כולל)
  3. ולהיכן הוא מוביל (ברמת מסכים)

1. תיאור פרוטוקול התקשורת
2. תיאור מבני הנתונים

* פירוט מבני הנתונים (מסד נתונים, קבצים, מקומיים וכו')
* פירוט מאגרי המידע של המערכת (בדומה למסדי נתונים) ברמת שדות, טיפוסים, אורכים וכו'
* מסד נתונים: שם המסד, שם הטבלאות, לכל שדה: שם, טיפוס. לתת דוגמא לערכים אפשריים. להגדיר לכל טבלה במסד – מי המפתח הראשי בה.

1. סקירת חולשות והאיומים   
   למערכת ואת הפתרונות שלכם לאיומים, יש לסקור ע"פ מאפייני המערכת השונים:

שכבת האפליקציה:

* עבודה עם בסיס נתונים sql injection ...
* עבודה עם אתרי web ...
* תהליך ה login אימות ווידוא, הרשאות
* MITM : הצפנה, איזו סוג?
* DOS/DDOS : יכול להיות? איך מתמודדים
* העלאת קבצים : hash

שכבת התעבורה:

* פרוטוקול TCP , לחיצת יד משולשת??
* הצפנה?

הפעלת המערכת

* אילו חולשות קיימות ( 'הזרקת קוד' , sql injection וכו') ואיך טופלו ועוד...

**פרק ה' - 'שם המערכת' - הקוד**

1. עבור (שעושים קטעי קוד מיוחדים משהו מיוחד, משהו מסובך, משהו בדרך שונה, משהו יפה בעיניכם ויש לכלול בתוכם את קטעי הקוד הרלוונטים לאלגוריתמים המרכזיים שציינתם בפרק הקודם):

* הסבר על היכולת
* הקוד עצמו (כתוב ע"פ כללי התכנות הנכון ומלווה בהערות כנדרש)
* (למצוא לפחות 7 קטעי קוד מעניינים ...)
* רצוי תמיד לבחור את אלא שהסברתם קודם לכן את האלגוריתם שלהם

1. בנוסף יש לצרף את **שאר קוד המערכת** , לא נדרש הסבר לצד כל קוד אבל כן את שם הקובץ.  
   המלצה - לבצע 'שמירה' של הקוד לקבצי PDF אן העתקה לתוך קבצי word ולא לצרף כתמונה

**פרק ו' - 'שם המערכת' – בדיקות ('קופסא לבנה')**

1. פירוט הבדיקות

* פירוט הבדיקות שהופיעו בפרק האפיון ברמת הביטים – לתאר בפירוט מה נדרש לבצע ומה בוצע בפועל. וכמובן על בדיקה צריכה להתבצע יותר מפעם אחת ועד שהיא עוברת

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **שם הבדיקה** | **מטרת הבדיקה** | **מה נדרש לבצע** | **מתי** | **מה בוצע בפועל** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* יש לתעד כל בדיקה שמבוצעת, חייבים לחזור לפחות פעמיים על כל בדיקה – כל חזרה תתועד בשורה נפרדת עם תוצאות הבדיקה

**פרק ז' - 'שם המערכת' – מדריך למשתמש**

1. מדריך התקנה (סביבת עבודה)
2. מדריך למשתמש הכולל עבור כל תהליך/יכולת במערכת:

* הסבר על התהליך/יכולת
* תרשים זרימה (במקרה של תהליך)
* צילומי מסך מלווים בהסברים בשפה פשוטה

במידה ויש יותר ממשתמש אחד למערכת , לבנות פרקים שונים לדוגמא: מדריך למשתמש קצה, מדריך למנהל מערכת וכו'

**פרק ח' - 'שם המערכת' – רפלקציה**

1. מבט אישי על העבודה ועל תהליך פיתוחה:

* אתגרים שהיו לי בדרך
* אירועים מעניינים שקרו במהלך הפיתוח
* התמודדות עם קשיים, איך מה עשיתי
* הערכת הפתרון לעומת התכנון והמלצות לשיפורו
* תודות חשוב מאוד לחברים, למשפחה, למורים...

יש למלא עד עמוד ולא להתבייש בכתיבה – כאן לא המקום לצניעות.

**פרק ט' - 'שם המערכת' – ביבליוגרפיה**

1. רקע תיאורטי
2. ספרות מקצועית ספציפית לנושא העבודה (רשימת ספרים, מאמרים והפנייה לכתובות אתרים, סרטונים המכילים חומר רקע ששימש לפיתוח העבודה)
3. הערה: לא מספיק להתייחס לספרים המיועדים ללימוד שפה או כלים יישומיים ומדריכים למיניהם.
4. קישורים לאתרים באינטנרט – קישורים ל stackOverflow עם הסבר על הנושא שנחקר (לא תחביר...)

יש להקפיד להציג את הרשימה לפי כללי ה – APA ראו להלן

<https://www.oranim.ac.il/sites/heb/research-information-resource/library/consultation/writing-bib/apa/pages/default.aspx>

נספחים  
  
מסכי MVP (כולל לינק למצגת MVP)

מסכי ניהול הפרוייקט באמצעות Trello

כאן ניתן להוסיף הסברים על הטכנולוגיות שנעשה בהם שימוש, או כל מידע שיכול להועיל לקורא