אבטחת מחשבים ורשתות תקשורת

(372-1-4601)

מטלה מס' 3

מתרגל אחראי: חן דויטשמן

הנחיות כלליות:

- .1 העבודה מורכבת משני חלקים חלק תיאוראי וחלק מעשי.
- ענו. שאלות על העבודה יש לשאול אך ורק בפורום הייעודי ב-Moodle. שאלות אשר ישאלו בדוא"ל לא יענו.
 - .3 על התשובות להיות מלאות ומפורטות.
- 4. כחלק מתהליך בדיקת העבודה תתבצע בדיקה לזיהוי עבודות מועתקות. כל מקרה של העתקה יטופל ע"י ועדת משמעת אוגיברסיטאית.

:הוראות הגשה

- 1. ההגשה היא בזוגות בלבד.
- 2. על התשובות שלכם להיות מוקלדות במחשב או סרוקות בכתב יד נקי וברור.
 - .3 יש לענות על השאלות ולהפיק קובץ PDF עם התשובות שלכם.
 - .4 רק אחד מחברי הצוות יגיש את המטלה.
- .5 שם הקובץ יהיה ID1_ID2.pdf כאשר ID1 ו-ID2 מוחלפים בת.ז של מגישי המטלה.

בהצלחה

חלק תיאורטי (70 נק')

(50 Lg) א' (10 נק') שאלה מס' 1 Buffer overflow

:c בשפת הכתובת הבאה הפונקציה הבאה

```
void func () {
char* date = getDateString();
int dateLength = strlen(date);
char b[64];
gets(b);
char logMessage[128];
strcpy(logMessage, date);
strcpy(logMessage + dateLength, b);
writeLog(logMessage);
}
```

כמו כן נתון כי:

- הפונקציה getDateString מחזירה *char מחזירה setDateString המכיל את התאריך ברגע הקריאה
 - הפונקציה writeLog מקבלת []char וכותבת את תוכנו לקובץ לוג.
 - .c ו-strlen, gets הינן כפי שהן מתוארות בתיעוד של שפת strcpy.
 - ?ה (2 נק') מהי מטרת הפונקציה?
- 2. (3 נק') הקומפיילר אשר באמצעותו מקומפל קוד זה משתמש ב-Stack Canary בגודל 4 bytes. שרטט'י את המחסנית לאחר באמצעותו מקומפל קוד זה משתמש ב-לול'י השרטוט את כתובת החזרה מהפונקציה.
- 3. (7 נקי) ידוע שהקוד קומפל תוך שימוש ב-Terminator Canary, לכן מימוש התקפת buffer overflow ע"י הכנסת החזרה לבצע התוך וניחוש ה-Canary לא יעבוד. בכל זאת ניתן לבצע התקפת buffer overflow ובכך לדרוס את כתובת החזרה מהפונקציה, וזאת מבלי לשנות את ה-Canary. הסבר/י כיצד ניתן לבצע זאת.
 - אך לא 0xDEADBEEF וישנה אותו לערך (return address) אך לא 0xDEADBEEF א נק') תנ/י דוגמה לקלט אשר ידרוס את כתובת החזרה (Canary ישנה את ערך ה-

(5] ב' (10 בק') שאלה מס' Buffer overflow ב' שאלה

נתון הקוד הבא אשר server כלשהו משתמש בו:

```
1  void func () {
2  char[] b[64];
3  printf("Type a Log Message");
4  gets(b);
5  writeLogMessage(b);
6 }
```

כמו כן, נתון כי:

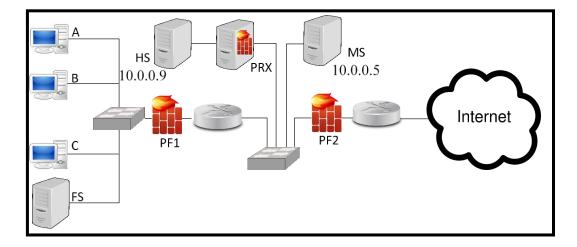
- הקומפיילר אשר באמצעותו מקומפל קוד זה משתמש ב-Random Stack Canary בגודל 4 bytes אשר אשר אשר לא מכיל תווי Termination.
 - ה-Canary איננו משתנה בכל ריצה חדשה של הקוד.
 - מבצע אתחול מחדש תהליך אשר לוקח שנייה אחת. server נדרס, ה-Canary נדרס, ה-Canary מבצע אתחול

תוקף מעוניין למצוא את ה-Canary של התוכנית.

- ?Canary- מממוש נאיבי למתקפה שתמצא את ה-Canary. תוך כמה זמן בממוצע התוקף ימצא את ה-ל מחוץ. (1 נק') הציעו מימוש נאיבי למתקפה שתמצא את ה-
- 2. (5 נק') הציעו דרך יעילה יותר עבור התוקף למצוא את ה-Canary בזמן סביר (מספר דקות). הסבירו תשובתכם ונתחו את מספר הניסיונות הממוצע והמקסימלי הדרוש לצורך ביצוע מתקפה זו.
- Canary- ערך ה-Canary, ערך הריסת מחדש עקב אתחול מחדש מבצע אתחול פעם בכל פעם כעת כעת כעת כעת לא הסעיף הקודם כאשר כעת בכל פעם שהשרת מבצע אתחול מחדש עקב דריסת הקודם כאשר כעת בכל $(\text{mod } 2^{32})$.

שאלה מס' Firewalls – 3 (נק')

לפניכם תרשים של רשת ארגונית:



SMTP שרת (HS) HTTP שרת (FS) FTP שרת (A,B,C), שרת מייל שרת מייל שרת מייל (HS) ושרת בתרשים, הרשת מורכבת משלוש עמדות קצה (A,B,C), שרת שרת מייל (HS) deep packet inspection (לא Stateless packet filter). כמו כן, הרשת מוגנת ע"י שלושה חומות אש: שתיים מסוג שתיים מסוג שרת פרוקסי המסוגלת לפעול ברמת האפליקציה (PRX). (PRX)

- .1 (4 נקי) ענו נכון/לא נכון והסבירו בקצרה את תשובתכם לגבי כל אחת מהטענות הבאות:
- i. בל פנייה לשרת HS (בין אם הפניה מגיעה מחוץ לארגון או מתוכו) עוברת דרך לפחות חומת אש אחת.
 - .ii אשר מגיעה מתוך הרשת הארגונית עוברת דרך שתי חומות אש. .ii
 - .HS <u>ניתן</u> ליצור חיבור <u>ישיר</u> אל שרת .iii
 - .FS לשרת C ביתן ליצור חוק המונע גישה של עמדה .i
- 2. (2 נקי) בארגון עלה חשד כי אחד העובדים מהעמדות C-A שולחים בקשות HTTP זדוניות לעבר שרת .HS מה על הארגון לעשות על מנת לזהות את העובד מהעמדה הסוררת? האם נדרש מהארגון לשנות את מבנה הרשת. פרטו!
 - 3. (**5 נק'**) מלאו את טבלת החוקים של PF2 לפי המדיניות הבאה (יש להקפיד על סדר החוקים):
 - 1. מותר לגשת מחוץ לארגון אל שרת MS, אך רק ע"י הפרוטוקול והפורט המתאים (מהו?).
 - פרט לגופים מתחרים (אשר כתובות ה-IP שהם מתחילות ב-212), מותר לגשת מחוץ לארגון אל שרת IP, א<u>ד רק ע"י</u> ב-21 הפרוטוקול והפורטים המתאימים (מהם?).
 - 3. יש לאפשר מענה על <u>כל בקשה</u> מתוך הרשת הארגונית.
 - .4 כל השאר אסור.

Rule ID	In/Out	Src. IP	Dst. IP	Protocol	Src. port	Dst. port	Ack	Action

- 4. **(בקי)** את/ה מנהל/ת אבטחת המידע (CISO) בארגון שלך. התאמ/י לכל תרחיש את סוג ה-firewall הבסיסי ביותר שמקיים את הדרישה. הסבר/י בקצרה את תשבותך.
 - א. מעוניינים לסנן הודעות מייל שעלולות להכיל קישורים ממקור שאינו מוכר לארגון.
 - ב. מעוניינים לסנן הודעות מייל שמגיעות מתוך הארגון אך עם IP מחוץ לארגון.
 - ג. מעוניינים בפתרון אבטחה שלם הכולל sandboxing ,URL, סינון sandboxing וכו'..
 - ד. מעוניינים לסנן תעבורת TCP עוינת למטרות שמגיעה ממדינה עוינת.

(5)שאלה מס' (5) שאלה מס' (5)

ענו על השאלות הבאות בקצרה:

- .privacy והסבירו מה מטרתו. ציינו יתרון אחד וחסרון אחד בהיבט google FLoC והסבירו מה 4) .1
 - .SolarWinds hack-אועל קראו על ה-2 .5) .2
 - א. (1 נק') פרטו בקצרה על התקיפה.
 - ב. (1 נק') באיזו סוג התקפה מדובר?
 - מהו התוקפים? attack vector שבו השתמשו התוקפים?
 - ד. (1 נק') מהו הנזק לו גרמו התוקפים?
 - ה. (1 נק') באילו דרכים הייתם ממליצים להתגונן מפני תקיפות דומות בעתיד?
- 3. (1 נקי) בונוס: היכנסו ל-chrome://settings/passwords/check?start=true (הדביקו את הכתובת בשורת הכתובת בדפדפן היכנסו ל-compromised). החליפו 3 סיסמאות שלכם/ן שזוהו כ-compromised וצרפו צילומי מסך של מייל האישור מהאתר על החלפת הסיסמה.

שאלה מס' 5 – (15 נק')

בתרגול למדנו כי המחסנית (Stack) גדלה לכיוון הכתובות הנמוכות בזיכרון.

בשאלה זו נניח כי המחסנית גדלה בכיוון ההפוך (לכיוון הכתובות הגבוהות בזיכרון).

- ?User space- ממצא מעל למחסנית? מה תפקידו? איך ניתן לפנות אליו מה (Space) מצא מעל למחסנית? 1.
 - ?ה ניתן לבצע מתקפת Buffer Overflow במצב זה? .2
- ם. במידה ולא, פרט/י כיצד ההגנה מתבצעת. במידה ולא, פרט/י כיצד ההגנה מתבצעת. התייחס/י לכתובות החזרה (RA) ומצביעי המחסנית (ESP,EBP) בתשובתך וספק/י דוגמת קוד רלוונטית אשר

וור יוסל לכות בחד הווה ה (KA) המצב ע המהסב ה (ESI, ESI) בהשובהן הסכקל האמה קה היהום האשר תאשש את טענתך.

b. במידה וכן, פרט/י כיצד התקיפה מתבצעת. התייחס'י לכתובות החזרה (RA) ומצביעי המחסנית (ESP,EBP) בתשובתך וספק/י דוגמת קוד רלוונטית אשר תאשש את טענתך.

(50 - 6) - 6 שאלה מס'

ענו על השאלות הבאות בקצרה:

- .UDP-י TCP נק") הסבר/י בקצרה על ההבדל בין פרוטוקול 3
- .TCP של Three Way Handshake-של בקצרה על מנגנון ה-1. נקי) הסבר/י בקצרה על מנגנון ה-1.
- 5. (**3 נק')** הסבר/י בקצרה על התקפת SYN flood. בתשובתך פרט למה משמשת התקיפה וכיצד ניתן למנוע אותה (2 דרכים לפחות).
 - .SYN-ACK על התקפת בקצרה על הסבר/י בקצרה (3 נק') הסבר/י בקצרה של החקפת

חלק מעשי (30 נק')

עם web אשר הינה אפליקציית (Buggy Web Application קיצור של הינה אפליקציית) אשר הינה אפליקציית של העורך פתרון תרגיל זה, נשתמש ב-נשתמש ב-נשתמש ב-שנות שנמצא במודל כדי להתקין את הכלים הנדרשים לחלק זה של המטלה. setting up bwapp שנמצא במודל כדי להתקין את הכלים הנדרשים לחלק זה של המטלה.

כעת פתחו מספר משתמשים במערכת כמספר מגישי העבודה (פתיחת משתמש חדש במערכת נעשית תחת הלשונית New User).

לאחר מכן, התחברו למערכת עם אחד מהמשתשמים שפתחתם.

הערה: פתרון מלא לשאלות הבאות צריך לכלול הסברים מלווים בצילומי מסך וקטעי קוד בהם השתמשתם.

שאלה מס' CSRF – 7 (נק')

.Choose Your Bug תחת Cross-Site Request Forgery (Transfer Amount) הכנסו לחור האבטחה

לפניכם מערכת להעברת כספים לחשבון אקראי. נסו את המערכת, הזינו מספרי חשבון וסכומים ובדקו שהמערכת מתנהגת בהתאם למצופה.

- .CSRF על מתקפת בקצרה על מתקפת .11.
- בקי) מצאו דרך בה תוקף יכול לגנוב את כל הכסף בחשבונו של הנתקף ע"י שימוש ב-CSRF. הדגימו את הדרך הזו ע"י שילוב הבקשה בעמוד HTML לגיטימי כלשהו אותו תבנו וודאו שהמתקפה אכן עובדת. תשובה לשאלה זו תהיה סדרת הצעדים (הכנת עמוד ה-HTML, הכנת ההודעה בשילוב Social Engineering, והוכחה שהסכום אכן נגנב).
 - .3 (נק') כיצד ניתן להתגונן מהמתקפה אותה הצעתם? הציגו 3 דרכים.

(נק') Reflected XSS -8 שאלה מס'

.Choose Your Bug החת Cross-Site Scripting – Reflected (GET) הכנסו לחור האבטחה

נסו את המערכת, הכניסו נתונים כרצונכם ושימו לב כיצד המערכת מתנהגת.

- .XSS Reflected אל מתקפת בקצרה על מחבירו בקצרה על מתקפת 1.
- 2. (3 נקי) חשבו על רעיון יצירתי בו אתם רוצים להשיג את כתובת ה-Cookies+IP של המחשב הנתקף. בתשובתכם התייחסו לכל התהליך.
 - XSS מכיל מתקפת לא מכיל מלינק שלינק מידע כדי לבדוק שלינק מחוים לא מכיל מתקפת בדיקה שתבצעו בתור מומחי אבטחת מידע כדי לבדוק שלינק מחוים לא מכיל מתקפת .Reflected

הערה: הניחו כי האתר אינו מוגן מהמתקפה.

שאלה מס' Stored XSS – 9 שאלה

.Choose Your Bug תחת XSS – Stored (Blog) הכנסו לחור האבטחה

לפניכם בלוג בו אתם יכולים להגיב כרצונכם, תגובותיכם נשמרות במערכת כך ששאר המשתמשים יכולים לצפות בהן (בדקו זאת!).

- .XSS Stored אמקתפה על המבירו בקצרה על המבירו בקצרה על .1
- 2. (4 נקי) כתבו תגובה בבלוג אשר תגרום לכך שכל משתמש אשר יכנס לעמוד זה, יפתח לו חלון אשר מכיל את הטקסט:

"hacked by ITNS21 student."

ולאחר מכן יחווה תקיעה משמעותית בדפדפן/קריסה.

3. (7 נק') מצאו דרך בה תוקף עם גישה לעמוד יצליח לקבל את המיקום הגיאוגרפי של המחשב הנתקף ע"י כתיבת תגובה בבלוג. בתשובתך התייחס לפעולות שהתוקף צריך לבצע.

הערה: במידה ובחרתם לעבוד עם bee-box (אופציה מס' 2 במדריך), בצעו את המשימה הבאה במקום: מצאו דרך בה תוקף עם גישה לעמוד יצליח לגרום לדפדפן של המחשב הנתקף לגלוש לאתר לבחירתכם ע"י כתיבת תגובה בבלוג.

על התוקף לקבל חיווי שמעבר הדף הצליח. בתשובתך התייחס לפעולות שהתוקף צריך לבצע.

:הערות

- .NAT ניתן לעבוד עם 2 מחשבים הנמצאים מאחורי
- .Netcat או Wireshark תוכלו לבדוק את עצמכם ע"י שימוש ב-
- פתרון לשאלה זו יהיה קטעי קוד וצילומי מסך של רצף הפעולות שהתוקף מבצע שמוכיח היתכנות של המתקפה.
 נדרש להראות פלט במסך של התוקף עם המיקום הגיאוגרפי של המחשב הנתקף.
 - ס רמז: <u>פה</u>