# מבחן בהנדסה לאחור - 236496

סמסטר אביב תשפ"א

**מועד ב׳, 21.10.2021**

מרצה: עומר קדמיאל

מתרגל: עידן רז



## חלק שני

משך חלק זה של הבחינה: 3 שעות.

בחלק זה של הבחינה ישנן 2 שאלות. ענו על כולן.

**מותר להשתמש בכל חומר עזר, אך אין לשוחח, להתייעץ, לקבל רמז, לתת רמז, או להיעזר בשום אדם אחר על המבחן, על תוכנו, והתשובות לשאלות. <u>יש לפתור את השאלות לבד.</u>**

נא לכבות מכשירים סלולריים ושעונים חכמים.

בכל מקרה של שימוש בחומר חיצוני יש לתת הפניה אליו.

תוכנות מותרות: התוכנות אשר נלמדו בקורס. בפרט, אין להשתמש בכלי Decompilation!

ענו תשובות ברורות ככל האפשר. **<u>נמקו את כל תשובותיכם</u>**.

במידה שניתן לענות על שאלה במספר דרכים, **<u>ניקוד מלא יינתן לפתרונות קצרים ופשוטים</u>**.

**<u>השאלות והקבצים המצורפים דומים אך אינם זהים לכל הסטודנטים</u>**.

**הגשה אלקטרונית באתר המקצוע עד השעה 17:00**. יש להגיש קובץ ZIP (ואך ורק ZIP) ובו כל קבצי ההגשה. ההגשה כוללת בדיוק את הקבצים הבאים:

1. קובץ בשם ID_part2.pdf (כאשר ID זאת תעודת הזהות שלכם) עם התשובות בכתב <u>לכל</u> השאלות.
2. הקבצים אשר תצרו בשאלה 2 – Injector.cpp, hook.cpp, Injector.exe, hook.dll.

**<u>הערה לכל המבחן: בתרגילים הרטובים, אם אינכם מצליחים להגיע לפתרון שרץ בפועל, תארו במילים מה ניסיתם לעשות - זה עשוי לזכות אתכם בניקוד חלקי!</u>**

# בהצלחה!

## שאלה 0:

נא להעתיק את הקטע הבא בתחילת ה-PDF ולמלא את שמכם המלא ותעודת הזהות שלכם כאישור לכך שקראתם אותו.

אני _____, ת.ז. _____, מאשר/ת כי אני מכיר את מדיניות הקורס והפקולטה בנושא יושר אקדמי במהלך הבחינה. בפרט, אני מאשר/ת כי אני מודע/ת לכך שבמהלך הבחינה אסור לי לתקשר עם אחרים בכל אמצעי כל שהוא, למעט עם צוות הקורס.

## שאלה 1 (25 נקודות) - יבש:

על מנת להתמודד עם מנגנוני תקיפה הוסיפו במערכת מנגנון שרץ ברקע ובודק שאין עמודים עם הרשאות RWX. כמו כן, המנגנון בודק שהרשאות המחסנית לא השתנו (למחסנית יש הרשאות RW). אם המנגנון מזהה הפרה של התנאים הנ"ל הוא מתריע על כך לadmin של המערכת (הניחו כי זהו מנגנון מושלם שיכול לזהות כל מקרה בו דף עם הרשאות RWX או שהרשאות המחסנית שונו).

תוקף הצליח להכניס את הקוד שלו לbuffer שנמצא על המחסנית ב ebp-0x410 במהלך ריצת הפונקציה. הקוד נמצא בתחילת הbuffer והוא באורך 0x400 בתים.

א. הסבירו בעזרת אילו פונקציות WinApi (וללא שימוש בפונקציות ספריה אחרות) ניתן להגיע להרצת קוד מבלי שהמנגנון יתריע על כך.
ב. תחת ההגבלה של סעיף א', כתבו קוד ב-C המגיע להרצת קוד מבלי שהמנגנון יתריע על כך. ניתן להניח כי קיים משתנים כרצונכם – הסבירו מה תפקידו של כל משתנה.
ג. מה משמעות stdcall בהקשרי ROP וכיצד ישפיע הדבר על ROP שנכתוב?
ד. לאור הסעיפים הקודמים ותחת ההגבלה של סעיף א', כתבו שרשרת ROP המבצעת את הפעולות הרלוונטיות. ניתן להשתמש בכל גאדגט שנראה בהרצאות ובתרגולים. נדרש ליצר קוד יעיל וקצר ככל האפשר.
הערות:
   - לא ניתן להניח כי ESP ידוע מראש.
   - בסעיף זה ניתן להניח כי אפשר להכניס תווי NULL.
   - אין להשתמש בגאדגטי popa , push.

## שאלה 2 (25 נקודות) – רטוב:

למבחן מצורף הקובץ secret.exe. התוכנה secret.exe מדפיסה מחרוזת מוצפנת כלשהי.
תוכן המחרוזת שמודפסת מסתמך נקבע ע"י הפונקציה secret_function (כתובת 0x4014AD) המקבלת int ומחזירה char.
על מנת לקבוע את התוכן הפונקציה נעזרת בפונקציה נוספת- secret_helper_function (כתובת 0x401460) המקבלת int ומחזירה int.
על מנת לפענח את המחרוזת, עליכם לגרום לכך שבכל הפעלה של secret_function, הערך המוחזר יהיה הערך המקורי שמוחזר ועוד **סכום** הערכים שאיתם נקראה הפונקציה secret_helper_function באותה הפעלה.
לדוגמא, אם במהלך הפעלה כלשהי של secret_function הפונקציה secret_helper_function נקראה 3 פעמים עם הערכים 1,2,3 עליכם להוסיף 6 לערך שהיה מוחזר בריצה רגילה של התכנית.

עליכם לבצע hooking באמצעות **DLL Injection** על התכנית secret.exe כך שהמחרוזת תודפס בצורה המפוענחת שלה.
בשאלה זו מותר לכם לבצע Hook על שתי פונקציות, כאשר כל Hook חייב להופיע בתחילת הפונקציה!
**אסור לבצע כל שינוי נוסף בתכנית.**
עליכם לבצע זאת באמצעות **hooking רגיל** בלבד, כפי שנלמד בקורס, **ללא שימוש בIAT hooking או Hot patching**.

שימו לב שהמחרוזת המפוענחת צריכה להכיל את הת"ז שלכם.

עבור שאלה זו עליכם להגיש את הקבצים הבאים:

- injector.cpp - קוד המקור של ה-injector.
- injector.exe - ה-injector המקומפל.
- hook.cpp - מכיל את הקוד עבור האתחול של ה-hook, ואת פונקציית ה-hook עצמה.
- hook.dll - ה-dll המוזרק.
- צרפו צילום מסך של המתרחש לאחר הרצה מוצלחת של ההוק ב-part2.pdf.

**על שמות הקבצים ב-ZIP להיות זהים לאלו המופיעים ברשימה לעיל.**