מבחן בהנדסה לאחור - 236653

סמסטר חורף תשע״ט

מועד ב׳, 28.02.2019

מרצה: עומר קדמיאל

מתרגל: טל שנקר

חלק שני

משך חלק זה של הבחינה: 3 שעות.

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

בחלק זה 3 עמודים, כולל עמוד זה. וודאו שכל הדפים נמצאים (יש הדפסה משני צידי הדף).

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 part2_sol.pdf עם התשובות בכתב <u>לכל</u> השאלות.**
2. **את הקבצים אשר תצרו בשאלה 2.**

<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 1 (25 נקודות) - יבש:

א. ברצוננו לבצע הוקינג על תוצאת החזרה של פונקציה.

a. מדוע מציאת סוף הפונקציה וביצוע שינוי שם הוא בעייתי?

b. כיצד יש לבצע זאת?

c. האם ניתן להשתמש ב-IAT הוקינג במקרה זה? הדגימו כיצד או הסבירו מדוע לא.

ב. סטודנט הציע רעיון חדש – במקום להשתמש ב-return oriented programming הוא הציע להשתמש ב- jump oriented programming (או בקיצור JOP), קרי לחפש את כל ה-jump-ים בתוכנית ולהשתמש ב-gadget-ים שהם מייצרים:

a. אלו jump-ים ניתנים לניצול ואלו לא? התייחסו גם לקפיצות מותנות וגם לקפיצות לא מותנות.

b. האם אחת השיטות חזקה יותר מהאחרת? כלומר, האם קיימת לוגיקה הניתנת למימוש בשיטה אחת ולא ניתנת למימוש כלל בשיטה השנייה?

c. במערכת ללא ASLR, בנו שרשרת ROP\JOP המריצה את calc.exe באמצעות winexec, בהתבסס על ה-gadget הנתון ע״י הפקודה jmp eax. השתמשו בגאדג'טים סבירים (בפרט, אין להשתמש בגאדג׳ט של pusha) ובנו שרשרת קצרה ככל הניתן. ניתן להניח קיום של גאדג׳ט getESP.

ג. בהינתן מחבר USB עוין, מנה את השיטות האפשריות להערכתך להגיע להרצת קוד על המחשב אליו הוא מחובר.

שאלה 2 (25 נקודות) - Hooking:

למבחן מצורף הקובץ program.exe. התוכנה program.exe מכילה את הפונקציה Secret אשר לא ברור לנו מה היא מבצעת. מטרתכם בשאלה זו תהיה לבצע רישום של ערכי החזרה של הפונקציה Secret. **רשמו ב-part2_sol.pdf מהי סדרת הערכים שמייצרת הפונקציה Secret.**

עליכם לבצע hooking באמצעות **DLL injection** על program.exe כך שבכל ריצה שלה, יווצר קובץ בשם secret_log.txt. קובץ זה יכיל את ערכי החזרה של הפונקציה Secret במהלך ריצת התוכנית, כל אחד בשורה נפרדת. כלומר, לאחר 20 קריאות ל-Secret הקובץ יכיל 20 שורות כאשר בכל אחת מופיע ערך חזרה של קריאה כלשהי ל-Secret. עליכם לבצע זאת באמצעות **hooking רגיל** בלבד, כפי שנלמד בקורס, **ללא שימוש ב IAT hooking או Hot patching.** את ה Hook יש לבצע על הפונקציה Secret בלבד!

עבור שאלה זו עליכם להגיש את הקבצים הבאים:

- injector.cpp - קוד המקור של ה-injector.
- injector.exe - ה-injector המקומפל.
- dllmain.cpp - מכיל את פונקציית ה-DllMain של ה-dll אותו אתם מזריקים.
- dllhook.cpp - מכיל את הקוד עבור האתחול של ה-hook, ואת פונקציית ה-hook עצמה.
- dllhook.dll - ה-dll המוזרק.
- secret_log.txt - הקובץ הנוצר בזמן הרצת הפתרון שלכם.

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