מבחן בהנדסה לאחור - 236496

סמסטר חורף תשפ"א

מועד ב׳, 18.03.2021

מרצה: עומר קדמיאל

מתרגל: עידן רז

חלק שני

משך חלק זה של הבחינה: 3 וחצי שעות.

בחלק זה של הבחינה ישנן 3 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 17:30. יש להגיש קובץ ZIP (ואך ורק ZIP) ובו כל קבצי ההגשה. ההגשה כוללת בדיוק את הקבצים הבאים:

1. קובץ בשם part2.pdf 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:

ברצוננו לבצע ROP על קטע קוד שהכנסנו למערכת (קטע הקוד הוא בגודל דף בזיכרון). קיימים בידינו מגוון גאדגטים סטנדרטים (העברה מרגיסטר לרגיסטר, מהזיכרון ואל הזיכרון ופעולות אריתמטיות). קיימות שתי בעיות:

a. הגאדגט היחיד הרלוונטי אשר יש בו את esp הינו mov ebp, esp (ניתן להניח כי קיימות פקודות pop כרגיל)
b. קיימת פונקציה שזו חתימתה:

_cdecl MyVirtualAlloc (source, size)

אשר מעתיקה קטע לאזור חדש עם הרשאות מלאות (read, write, execute) ומחזירה מצביע לstruct אשר ב-offset 4 בו נמצאת הכתובת של הקטע.

אין לנו כתובת מדויקת של הפונקציה, אולם קיים memory leak, וידועה כתובת הבסיס של ה-dll בו היא נמצאת.

1. האם הגאדגט המתואר בסעיף a לעיל הינו גאדגט סביר? כיצד ניתן להסביר את קיומו?
2. כתבו קוד (ב-C) המתאר כיצד ניתן להגיע להרצת קוד תוך שימוש בפונקציה המופיעה לעיל. למען הסר ספק – אין להשתמש ב-virtualprotect או ב-virtualalloc. פתרון אשר קורא באופן ישיר לפונקציה יקבל ניקוד חלקי. ניתן להגדיר משתנים לפי הנדרש (כתובת הקטע להרצה, כתובת הבסיס) וניתן להשתמש בפונקציות נוספות מkernel32.
3. הסבירו את ההבדלים בין calling conventions שונים בהקשרי ROP. התייחסו לפחות ל-stdcall ול-cdecl.
4. כתבו את שרשרת הROP הרצויה בהינתן שכתובת ה-dll נמצאת ב-[[ecx]] וכתובת הקוד אותו אנחנו רוצים להריץ נמצא ב-edx. ניתן להניח כי שרשרת הROP יכולה להכיל את כל התווים.

שאלה 2 (25 נקודות) – רטוב:

למבחן מצורף הקובץ secret.exe. התוכנה secret.exe מדפיסה מחרוזת מוצפנת כלשהי.
תוכן המחרוזת שמודפסת נקבע ע"י הפונקציה secret_function - פונקציה זו מקבלת מספר משתנה של ארגומנטים, מבצעת בעזרתם חישוב מסובך ומחזירה תו במחרוזת. ידוע שהפונקציה לא משנה את הארגומנטים שמועברים לה.
הארגומנט הראשון שלה הוא מספר הארגומנטים הנוספים וכל שאר הארגומנטים הם מספרים שלמים.
הפעלות לדוגמה של הפונקציה הן: secret_function(1, 10), secret_function(3, 1, 2, 3).
על מנת לפענח את המחרוזת, עליכם לגרום לכך שערך החזרה של הפונקציה יהיה כערך החזרה שלה אם היינו מוסיפים לכל הארגומנטים שלה (לא כולל הראשון) את המספר 2.
לדוגמה, הקריאה secret_function(3, 1, 2, 3) אמורה להחזיר ערך כאילו קראנו ל secret_function(3, 3, 4, 5).

עליכם לבצע hooking באמצעות **DLL Injection** על התכנית secret.exe כך שהמחרוזת תודפס בצורה המפוענחת שלה. את ה Hook יש לבצע על הפונקציה secret_function בלבד! **אסור לבצע כל שינוי נוסף בתכנית.**
עליכם לבצע זאת באמצעות **hooking רגיל** בלבד, כפי שנלמד בקורס, **ללא שימוש בIAT hooking או Hot patching**.
הקפיצה יכולה להופיע בשני מקומות: או בתחילת הפונקציה (כלומר להתחיל בבית הראשון של הפונקציה) או בסוף הפונקציה (לא ניתן להניח כי אין פקודות חשובות לאחר הret).
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.