מבחן בהנדסה לאחור - 236496

סמסטר חורף תש"ף

מועד ב׳, 17.03.2020

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.

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.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 1 (30 נקודות) - יבש:

א. מנו שלוש שיטות להכנה מפני חולשת Buffer Overflow. הסבירו מהם היתרונות והחסרונות של כל אחת מהשיטות.

ב. אנו מעוניינים לבצע hook על exception handler על מנת לשנות את ערכי החזרה שלו. אין לנו את היכולת לשנות את הזיכרון המכיל את הקוד של ה handler המדובר. בנוסף, איננו יכולים להשתמש בפונקציות כגון VirtualProtect על מנת לשנות את הרשאות הגישה לאזור זיכרון זה. הסבירו כיצד ניתן להתגבר על הבעיה.

ג. הנדסה לאחור ו-JIT.

1. הסבירו מהו JIT וכיצד נבדל JIT מקומפילציה רגילה בהקשרי RE.
2. אילו כלים אשר שימשו אותנו עבור הנדסה לאחור אינם רלוונטיים תחת JIT?
3. כיצד ניתן להשתמש ב JIT על מנת לסייע בבצוע הנדסה לאחור?

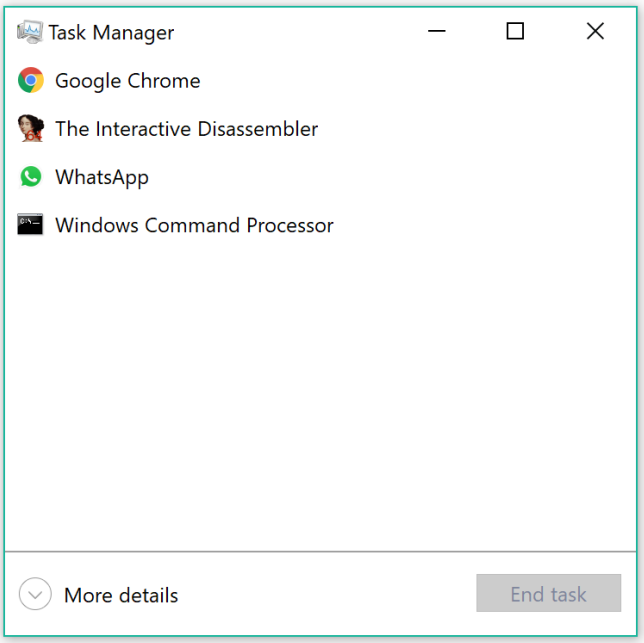
ד. נתונה תכנית אשר מכילה section קוד יחיד בעל הרשאות קריאה והרצה. ידוע כי התכנית מבצעת שימוש בפונקציות ספרייה על אף שה Import Table של התכנית ריק. הסבירו בפירוט כיצד ייתכן שהתכנית משתמשת בפונקציות הספרייה הבאות:

1. Sleep הנמצאת ב Kernel32.dll.
2. BitBlt הנמצאת ב GDI32.dll.

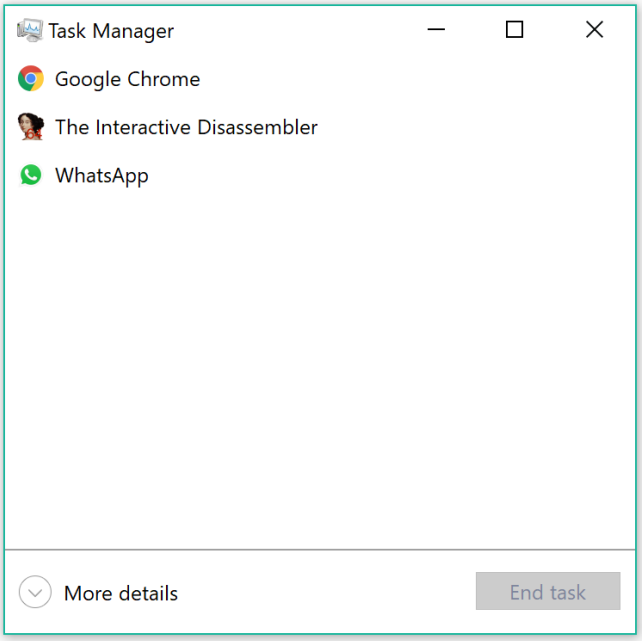
שאלה 2 (20 נקודות) - Hooking:

בשאלה זו תבצעו Hook **ללא שימוש ב hot patching וללא שימוש ב IAT Hooking**. השתמשו בקובץ מנהל המשימות (TaskMgr.exe) הנמצא על מחשבכם (וגם על המכונה הוירטואלית שלכם) ב C:\Windows\System32. עליכם לבצע hook שיגרום להסתרה של אחד התהליכים הרצים במערכת. **לצורך הפתרון עליכם לבצע Hook בזכרון ע"י DLL Injection**. הפונקציה שעליה תבצעו Hook היא **NTQuerySystemInformation** שנמצאת ב ntdll.dll.

הרצה רגילה TaskMgr.exe



הסתרה של cmd באמצעות ה hook



עליכם ליצור Injector.exe שיקבל כארגומנט בשורת הפקודה **רק** את שם התכנית שנרצה להסתיר.

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.