מבחן בהנדסה לאחור - 236496

סמסטר חורף תשפ"א

מועד א׳, 22.02.2021

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:

תוקף בעל ידע ב-ROP הצליח להכניס קוד שלו למערכת שיושב בזיכרון שאינו בר הרצה.

בסעיפים הבאים ניתן להניח כי לרשות התוקף עומדים gadget-ים לבחירתו, המבצעים pop, העתקה מכל רגיסטר לכל רגיסטר ומרגיסטר לזיכרון וחזרה, פעולות אריתמטיות סטנדרטיות על רגיסטרים ודומיהם.

1. מדוע יעדיף תוקף לבצע VirtualProtect ולא VirtualAlloc?
2. הסבירו מה הצעדים הנדרשים על מנת להשתמש ב-virtualAlloc על מנת להגיע להרצת קוד. האם ניתן לממש את הפונקציונאליות החסרה מסעיף 1 באמצעות ROP ו/או באמצעים אחרים? הסבירו ופרטו.
3. יצרו שרשרת ROP המבצעת את הפונקציונאליות הנדרשת בסעיף הקודם בהינתן שהקוד של התוקף יושב ב-[edi]. ניתן להניח כי הקוד של התוקף בגודל דף . תשובה המניחה שקיים דף ריק בכתובת ידועה תזכה לניקוד חלקי. לשם פשטות, בסעיף זה בלבד ניתן להניח כי שרשרת הROP יכולה להכיל את כל התווים.
4. נניח שקיימת בדיקה שבודקת שכל התווים ב-buffer של התוקף הינם תווים הניתנים להדפסה (printable characters). מה התנאים שצריכים להתקיים על מנת שבניית ה-ROP תצליח? פרטו והדגימו התאמות נדרשות.
5. הסבירו במילותיכם כיצד ASLR מתמודדת עם איום ה-ROP, ופרטו אילו חלקים בשרשרת הROP שבניתם ישתנו בעקבות שימוש בASLR (כלומר בטעינה אחרת של התהליך).

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 אינדקס i, מבצעת חישוב מסובך ולבסוף מחזירה את התו ה i במחרוזת המוצפנת.

על מנת לפענח את המחרוזת, עליכם לבצע XOR ציקלי של המחרוזת המוצפנת עם התווים של תעודת הזהות שלכם. כלומר, עבור כל אינדקס i במחרוזת לבצע:

$$plaintext[i] = encrypted[i] \wedge id[i\%9]$$

לדוגמה, אם תעודת הזהות שלכם היא "123456789" והמחרוזת המוצפנת היא "abcd" אז התו הראשון במחרוזת המפוענחת יהיה $'a' \wedge '1' = 'P'$ וכך הלאה.

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!

עליכם לבצע זאת באמצעות **hooking רגיל** בלבד, כפי שנלמד בקורס, **ללא שימוש בIAT hooking או Hot patching**. המקום היחיד אותו מותר לדרוס בפונקציה secret_function הוא תחילת הפונקציה והקפיצה חייבת להופיע בתחילת הפונקציה.

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.
- <u>צרפו צילום מסך של המתרחש לאחר הרצה מוצלחת של ההוק ב-part2.pdf.</u>

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