שלב ד'

אם הגעתם לכאן אתם בהחלט אנשי סייבר מוכשרים מאוד. המערכת שלכם מאפשרת לכם לבצע מספר מתקפות מאוד מעניינות ולאסוף מידע מאוד חשוב מהרשתות הפנימיות של אותו מחשב מותקף. כעת אנחנו נכנסים לשלב האחרון של פרויקט הסיום. בשלב זה נעסוק קצת יותר בדברים שקשורים למערכת ההפעלה ובכך נשלים את המערכת שלנו.

תזכורת הנחיות

- אתם יכולים להשתמש באילו שפות תכנות שתרצו - מומלץ לקרוא היטב את ההנחיות ולחשוב מה תהיה שפת המימוש המתאימה ביותר.
- על הקוד שלכם להיות מתועד להפליא. תמיד תחשבו על היום שתגייסו עובד שימשיך את הפיתוח של מה שבניתם ואנו מבטיחים לכם שלא תרצו שבכל דבר שלא ברור לו או לה הם יבואו לשאול אתכם מה עשיתם - תעדו היטב את הקוד!
- העבודה בצוות צריכה לעזור לכם ולכן חשבו היטב כיצד לחלק את העבודה, הגדירו מראש שיטות עבודה, חתימות לפונקציות וכל דבר אחר שיחסוך בעיות בשלב חיבור החלקים השונים שפיתחתם.
- התחילו בקריאה והבנה של המשימות. חשבו והשתמשו באינטרנט על מנת להבין אילו שפות תכנות מכילות את הספריות המתאימות שיעזרו לכם לממש בצורה מהירה, יעילה ומיטבית את מה שאתם צריכים. לפעמים מדובר בהבדלים משמעותיים.
- כאשר השלמתם את השלב ואתם מרגישים טוב עם עבודתכם, יש להציג למדריך על מנת לעבור לשלב הבא.

תרגיל 13:

הרבה פעמים הדרך הטובה ביותר לגלות ספאמות או דפוסי פעולה של משתמש, היא על ידי מעקב אחר הפעולות ומעקב אחר המקשים עליהם הוא לוחץ. בשלב זה עליכם לפתח רכיב שיאפשר למחשב התוקף להקליט את ההקלדות שמבוצעות במחשב במותקף. מרגע שליחת הבקשה, המחשב המותקף יקליט את לחיצות המקלדת (key logger) וישלח לשרת התוקף את התווים שנלחצו. המחשב התוקף יוכל להפעיל ולהפסיק את ההקלטה בכל רגע שתחפצו. על מנת ליצור תהליך הגיוני, המחשב המותקף לא יישלח כל תו שנלחץ, אלא יאסוף את כלל התווים שנלחצו במשך דקה, ובכל פעם ישלח את המידע לשרת התוקף.

תרגיל 14:

אחד האתגרים שהאקרים מתמודדים איתם הוא היכולת להפעיל command line מרחוק. זה בדיוק מה שאתם תפתחו בשלב זה. בעת שליחת הפקודה למחשב המותקף ייפתח cmd במחשב המותקף ויריץ את הפקודות שנשלחות ע"י השרת התוקף. ה- output של פקודות המחשב המותקף יישלחו לשרת התוקף. שימו לב, כאשר הנכם מריצים command line באופן ישיר דרך הלקוח שמותקן על המחשב המותקף, הדבר יוביל לזיהוי מהיר של הדבר במנהל המשימות של מערכת ההפעלה. על מנת לטשטש את היכולת לגלות את הפעלת ה- cmd עליכם להזריק את הפעלת ה- cmd לתהליך אחר שרץ על המחשב. ניתן להשתמש ב- svchost, chrome או כל דבר אחר שנוח לכם. באופן זה ה- cmd ירוץ מתהליכים אלו ויהיה הרבה יותר קשה לזיהוי על ידי מנגנוני אבטחה כאלה ואחרים.

תרגיל 15:

בתרגיל זה, נשפיע על תהליכים אחרים שרצים במחשב המותקף. בכדי להסביר את מטרת שלב זה נתחיל במעט רקע. קבצי EXE הם בפורמט PE - Portable Excecutable אשר מורכב ממספר חלקים. אחת המטרות של PE היא לדאוג לתאימות בין גרסאות שונות של מערכת ההפעלה וזהו חלקו הראשון של כותר ה- PE. החלק השני מכיל מספר פרמטרים עשויים להיות חשובים להרצת התכנית.

בין היתר חלק זה מכיל את ה- IAT - Import Address Table וזה הבסיס לשלב זה. בחלק זה אתם תקבלו תכנית שמבצעת שימוש בפונקציות שונות של מערכת ההפעלה. עליכם להבין באילו פונקציות התכנית משתמשת. עליכם לבחור פונקציה אחת שלה תעשו hook ולכתוב קובץ dll משלכם עם פונקציה משלכם שיחליף את הפונקציה שבחרתם. לאחר השלמת התהליך והיכולת לעשות זאת מקומית, תעשו את השינוי הדרושים על מנת שהשרת התוקף יוכל לשלוח קוד להרצה, אשר ייכתב בקובץ dll על המחשב המותקף ויריץ את התכנית exe שקיבלתם כאשר יתבצע hook לפונקציה שבחרתם לפני כן ויבצע את הקוד שנשלח ע"י השרת בעת הקריאה לפונקציה.

<u>תרגיל 16:</u>

כאשר אנחנו רוצים להוציא מידע ממחשב מותקף באופן שלא מעורר חשד, ניתן להחביא את האינפורמציה בתוך תמונה או קובץ אודיו. בשלב זה אתם תקבלו סקריפט אשר מבצע תהליך של הסתרת הודעה בתוך תמונה (png). הסקריפט טוען קובץ עם ההודעה ואת קובץ התמונה, ומייצר תמונה חדשה המכילה את ההודעה. עליכם להבין כיצד התכנית עובדת ע"י תהליך של RE. בנוסף תקבלו תמונה שכבר הוסתר בה מידע. לאחר שהצלחתם לפענח את אופן הסתרת המידע עליכם לחלץ את ההודעה מתוך התמונה שקיבלתם.

<u>תרגיל 17:</u>

בשלב נעשה מימוש בתובנות שהסקתם מהשלב הקודם. עליכם לבנות רכיב שמאפשר לכם להשתמש באותה טכניקה של הסתרת מידע מהשלב הקודם ולממשה על המחשב המותקף. הרכיב שלכם צריך לכלול שני חלקים. חלק שיושב בצד המחשב המותקף שמאפשר להסתיר מידע בתוך תמונות באותו אופן שבוצע בשלב הקודם. החלק השני הינו יחידת פיענוח שיושבת בצד השרת התוקף ומאפשרת להוציא את המידע המוסתר מתוך התמונה. בסופו של תהליך תגדירו איזו אינפורמציה אתם רוצים לקבל מהמחשב המותקף - יכול להיות כל אחת מהפעולות שפיתחתם עד כה ונתיב לקובץ תמונה (יכול להיות כתובת url או נתיב מקומי). במקום שהמידע יעבור באופן שעבר עד כה, הוא יוחבא בתוך התמונה והתמונה תישלח למחשב התוקף.

תרגיל 18:

זהו החלק האחרון, והוא מצריך קצת יצירתיות. בשלב זה עליכם לחקור תחום מעניין שבחרתם ולפתח רכיב המאפשר לכם לבצע את הפעולה על או באמצעות המחשב המותקף. תהיו סקרנים ובחרו תחומים שיותר מעניינים ומאתגרים אתכם. אתם יכולים לקחת את זה לאן שתחפצו. דוגמאות: שליחת cookies לתוקף, בדיקה שלא רצים על VM וכו'.

בהצלחה!