שלב ב'

אם הגעתם לשלב זה, למעשה יש ברשותכם מערכת השתלטות מרחוק המאפשרת לבצע עדכוני תוכנה מרחוק ולתקשר באופן מוצפן. זה בהחלט הישג מרשים ולא מובן מאליו. עכשיו מתחיל הכיף האמיתי. משלב זה כל העדכונים של המערכת צריכים להיות מבוצעים באמצעות רכיב העדכון של המערכת ולא ע"י שינוי ידני של קוד הלקוח. אתם כמובן יכולים "לרמות" אבל זה הופך את האתגר להרבה פחות כיף ומעניין. נסו לדמות סביבת עבודה אמיתית של אנשי סייבר ולהתמודד עם הבעיות והסוגיות שיצוצו לאורך הדרך ולא לחפש "קיצורי דרך".

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 4:

בשלב זה עליכם לפתח את הרכיב הראשון למערכת אשר יאפשר לשרת לבקש מהלקוח אינפורמציה כלשהי. על מנת להבין מהי אותה אינפורמציה עליכם להריץ את התכנית שקיבלתם. כפי שוודאי תשימו לב, התכנית דורשת סיסמה בתחילתה. עליכם למצוא דרך להבין מה התכנית הנ"ל עושה ברגע שמזינים את הסיסמה הנכונה (או עוקפים אותה) ולפתח רכיב למערכת שלכם אשר מבצע את אותה פעולה שמבצעת התכנית ללא נושא הסיסמה כמובן . השרת יעביר ללקוח את הפקודה המתאימה - על פי מה שאתם תגדירו וכשהלקוח יקבל את הפקודה, הוא יאסוף את כל האינפורמציה הרצויה, כמו בתכנית שקיבלתם, יבנה תשובה מסודרת על סמך המידע, ויחזירה לשרת.

* **הערה חשובה** - לפני שתפנו לממש בעצמכם את הפונקציה הזו, וודאו היטב שאתם מבינים מה התוכנה המצורפת עושה. פנו למלווה הקבוצה שלכם והסבירו לו מה התוכנה עושה ומה אתם מתכוונים לעשות, בטרם תתחילו לממש. אל תתחילו במימוש לפני שתקבלו אישור ממלווה קבוצה.

תרגיל 5:

בתרגיל זה עליכם להוסיף רכיב נוסף למערכת. הרכיב צריך לאפשר לכם מרחוק, ע"י המחשב התוקף, לפתוח אילו פורטים שתחפצו וליצור דרכם התקשרות. למעשה בפקודת המחשב התוקף אתם תגדירו את הפורט במחשב המותקף, את כתובת ה- IP והפורט של שרת כלשהו (יכול להיות של השרת התוקף). המחשב המותקף יפתח ערוץ תקשורת מעל הפורט הנבחר וישלח אחת לדקה תו כלשהו על מנת לשמר את הקשר. במידה והפורט בשרת סגור, על הלקוח לנסות לכל היותר שלוש פעמים ליצור את ההתקשרות ובמידה והפורט בשרת עדיין סגור, להפסיק.

תרגיל 6:

אנחנו מעוניינים לקבל גם מידע אודות מערכת הקבצים במחשב המותקף. בשלב זה עליכם לפתח רכיב שמאפשר לקבל את רשימת הקבצים, ההרשאות והסטטוס שלהם בכל תיקייה שרק תחפצו. המחשב התוקף יעביר פקודה למחשב המותקף, בה הוא מבקש לקבל את רשימת הקבצים בנתיב מסוים ועל המחשב המותקף יהיה לבנות את התשובה ע"פ התוצאות ולהחזיר למחשב התוקף. עליכם להגדיר

תיקיית בסיס במידה והתוקף לא העביר נתיב ספציפי.

תרגיל 7:

עכשיו, כאשר אנחנו יודעים למפות את קבצי המחשב המותקף, אנחנו רוצים שתהיה לנו אפשרות לבצע שינויים קלים. עליכם לפתח רכיב שיאפשר להסתיר ולהציג קבצים מוסתרים בשלב ראשון. קובץ מוסתר הינו קובץ שה- attribute שלו הוא +h. לאחר מכן נרצה שתהיה לנו אפשרות למחוק קובץ, או להעביר קובץ לנתיב אחר. על מנת להשלים תרגיל זה וודאו שישנן שלוש פקודות שונות שניתן להעביר למחשב המותקף: הפיכת קובץ למוסתר, מחיקת קובץ והעברת קובץ לנתיב אחר. במידה שכל אחת מהפקדות הנ"ל עובדות שיחקתם אותה!

תרגיל 8:

עליכם לפתח ממשק ויזואלי למערכת השליטה מרחוק (השרת התוקף). על הממשק לתת כלי קצת יותר אינטואיבי שיאפשר בצורה יחסית פשוטה לשגר פקודות למחשב המותקף, לקבל את התשובות ולבצע את הפעולות. לדוגמה במחיקת קובץ ניתן יהיה לראות את רשימת הקבצים בתיקייה. בלחיצה על הקובץ ניתן יהיה לבצע מחיקה. זה שלב יחסית פתוח שבו עליכם לחשוב איך נכון לממשק חלק זה.

בהצלחה!