



פרויקט סיום

ברוכים וברוכות הבאים לפרויקט הסיום. זה היה לא פשוט להגיע עד פה ולמדתם הרבה. בפרויקט הסיום תשתמשו בלא מעט יכולות שרכשתם לאורך התכנית. הפרויקט הינו צוותי ולא יחידני ויאפשר לכם לחלק את העבודה בצורה כזו שתאפשר לכם לבנות פרויקט ברמה גבוהה ועם הרבה רכיבים מעניינים. שיהיה בהצלחה.

אז מה עושים בכלל?

בפרויקט זה עליכם לבנות מערכת השתלטות על מחשב מרוחק המורכבת מלקוח ושרת. השרת הוא המחשב המשתלט ואילו הלקוח הוא התכנית המותקנת על המחשב המותקף. בכל שלב תפתחו רכיבים נוספים למערכת ההשתלטות שלכם, כך שתפתחו אותה עד שתקבלו מערכת איכותית ומגוונת מאוד שמאפשרת לתוקף לבצע כמעט כל דבר שיחפוץ בו. על מנת לאפשר בניית מערכת מתוחכמת שכזו, עליכם להתחיל בבניית התשתית ולשם כך לפתח בשלב ראשון שרת ולקוח שמעליהם תיבנה המערכת כולה.

הנחיות אחרות

- אתם יכולים להשתמש באילו שפות תכנות שתמצאו - מומלץ לקרוא היטב את ההנחיות ולחשוב מה תהיה שפת המימוש המתאימה ביותר.
- על הקוד שלכם להיות מתועד להפליא. תמיד חישבו על היום שבו תגייסו 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.

שלב א

זהו שלב א של הפרויקט, והוא כמו כל שלב בנוי ממספר תרגילים. בשלב זה עליכם לבנות את התשתית שתהווה בסיס להמשך השלבים והתרגילים שתפגשו לאורך הפרויקט. ישנם תרגילים שניתן לבצע במקביל וישנם תרגילים שיש לבצע לפני תרגילים אחרים, כי הם מתבססים על תרגילים קודמים. בעת השלמת השלב תוכלו לעבור לשלב הבא ולהתמודד עם פיתוח של אתגרים יותר מעניינים. בשלב זה יש להשלים את השלבים אחד אחרי השני.

תרגיל 1:

כתיבת שרת לקוח. על מנת לאפשר למערכת שאתם בונים לעבוד יש ליצור פרוטוקול תקשורת שבו הלקוח מדבר עם השרת המשתלט. עליכם להגדיר מעל איזה פורט תעבור התקשורת ואת פרוטוקול ההתקשרות בין הלקוח לשרת. על מנת לבנות זאת בצורה חכמה ולהקל על עצמכם בהמשך, חשבו כיצד ניתן לבנות משהו שיאפשר באופן פשוט להוסיף רכיבים נוספים ויכולות נוספות למערכת שלכם. וודאו שכאשר במחשב המותקף הרצתם את הלקוח ובמחשב התוקף את השרת, הלקוח בודק מדי פעם האם עליו לבצע משהו עבור השרת התוקף ולכם יש אפשרות באמצעות השרת להעביר פקודות ללקוח.

תרגיל 2:

מצוין! ככל הנראה יש לכם את התשתית המתאימה לבניית המערכת שאנחנו רוצים. בכדי להשלים את התשתית ולהתחיל בפיתוח של הרכיבים השונים במערכת שלכם, עליכם להקפיד לעבוד באופן סודי. כרגע, המידע בין הלקוח לשרת ולהיפך עובר בצורה גלויה - לא יאה לאנשי סייבר. בשלב זה עליכם לדאוג להצפנת התעבורה בין הלקוח לשרת. כדי לשפר את רמת האבטחה, עליכם לבנות מודל המאפשר להחליף מדי פעם את המפתח המשמש להצפנת התעבורה. לצורך כך נשתמש במימוש של פרוטוקול החלפת מפתחות המכונה [Diffie-Helman](#).

עליכם להגדיר מפתח פרטי וציבורי לשרת ומפתח פרטי וציבורי ללקוח (למדו כיצד בונים זוגות של מפתחות כאלה). לאחר מכן ממשו את הפרוטוקול של



Diffie-Helman על מנת לאפשר לשרת לבקש מהלקוח לחדש את מפתח ההצפנה הנוכחי. עכשיו דאגו שבכל יממה, יוחלף המפתח המשמש להצפנת התקשורת בין המחשבים (על מנת לוודא את תקינות האלגוריתם מומלץ לשנות את מפתחות ההצפנה כל זמן קצר ולאחר שווידאתם שאכן שינוי המפתחות עובד בהצלחה, להחזיר ל- 24 שעות).

תרגיל 3:

יפה מאוד, השלמתם את התשתית המאובטחת שלכם ועכשיו אפשר להתחיל במימוש של הרכיבים השונים במערכת. אבל רגע, מה יקרה כאשר נרצה להחיל את השינויים והעדכונים על צד הלקוח? הרי אין לנו אפשרות להגיע ולבצע "עדכוני תוכנה". נקודה בעייתית בהחלט! לכן בשלב זה עליכם יהיה לפתח רכיב עדכון למערכת. כלומר הלקוח שלכם צריך להיות מסוגל לקבל פקודת עדכון מהשרת ולעדכן את עצמו. הדבר יאפשר לכם להוסיף בהמשך, בכל שלב שרק תרצו רכיבים נוספים למערכת שאתם בונים, ומרחוק! זהו שלב ד"י מורכב וניתן למימוש בהרבה מאוד אופנים. מומלץ לשבת ולחשוב מהם הדברים שמצריכים עדכון על מנת שהלקוח שאנחנו בונים יבצע עדכון לעצמו. מרגע שפיתחתם אסטרטגיה וביצעתם מחקר בנושא, ממשו את הדרך הטובה ביותר בעיניכם.

בהצלחה!