בס"ד

מטלה מספר 3 – מערכת תקיפה והגנה על רשת אלחוטית

רקע

- מטלת הקורס המרכזית הינה פיתוח ובניית מערכת תקיפה על רשת תקשורת בשביל השגת נכס ופיתוח מערכת הגנה. באישור מיוחד, ניתן להמיר למערכת תקיפה חדשנית באישור המרצה.
- לצורך בחינת ביצועי התקיפה יש להשיג נכס, מידע או הרשאות שלא ברשות וכדומה ולבסוף מערכת הגנה שמתריעה או מונעת את התקיפה.
- אין מגבלה על סוג הטכנולוגיה האלחוטית מתקשורת סלולארית ועד לNFC.
- למטלה שתי מטרות, הראשונה ליישם את הידע הנרכש בקורס באחד התחומים שנלמדו והשנייה מיומנות בבניית כלי תוכנה בהקשר הקורס.
- ציון המטלה מותנה בעמידה בשני שלבים: הגשת קבצי המטלה במודל והדגמת המערכת ובחינת ביצועיה ע"י המרצה. כל סטודנט יידרש להדגים ולהיבחן על חלקו במערכת ובהתאמה לכך יינתן ציון.

דרישות המטלה

- פיתוח מערכת תקיפה שתמומש בכלי תוכנה יעיל, דהיינו ממשק אחד שמנהל ומנטר את ההתקפה עד להשגת הנכס.
- פיתוח כלי מותאם אישית, אפשר להשתמש בקוד קיים אבל יש להתאימו לשימושים ולעבודה תחת ממשק אחד.
- אין להשתמש בקוד מקומפל בסגנון AIRCRACK אלא אם כן התקבל אישור מפורש מהמרצה.
- כתיבת בסביבת עבודה לינוקס

טיפ: כדאי להימנע מVM עקב בעיות תאימות שנובעות מהצורך לגישה מלאה לחומרה.

רעיון למערכת תקיפה

בטכנולוגית WLAN השגת נתוני משתמש באמצעות התקפת Evil twin.

- זיהוי AP ולקוח המחובר אליו.
- הפעלת AP חלופי תואם אבל "רשע".
- שידול הלקוח להתחבר אל הAP ה"רשע" לדוגמא באמצעות השבתת הAP ה"טוב".
- לאחר וידוי שהלקוח התחבר, הפעלת פורטל או אמצעי תקיפה אחר
- קבלת נתונים מהלקוח
- סוף

כלי הגנה, פועל ברקע לפני ההתקפה, מזהה את ההתקפה ומתריע או משבית את התוקף.

ציון

הציון נקבע על בסיס ידע, הבנה, השקעה, יישום והישג. לצורך כך ייקבע זמן לכל קבוצה להדגים את ביצועי המערכת כאשר כל חבר קבוצה מדגים בפני המרצה חלק מהמערכת כאשר תוך כדי ההדגמה המשתתפים ייבחנו על המערכת שבנו. הציון לכל חבר קבוצה בנוי מרכיב אישי על סמך חלקו בהדגמה וממרכיב קבוצתי.

לרגל הנסיבות המיוחדות, ההדגמות ייעשו מרחוק בפלטפורמת זום בהתאם לנסיבות כאשר למרצה תהיה אפשרות להשתלט על מחשב בסביבת ההדגמה בכדי לבחון את הקוד וביצועי ההגשה