ב״ה

תרגיל מספר 2 בקורס Web Application Security

1. מה ההבדל ומה היחס בין SSL Session ובין SSL Connection?
2. בהנחה שתוקף הצליח לפרוץ את הצפנת הערוץ מה client ל server ולקרוא את התעבורה, האם הוא יוכל גם לקרוא את התעבורה בין ה server ל client? וכיצד זה מסביר את הצורך גם ב Client finish message וגם ב Server finish message?
3. מנה מספר טעויות אופיניות בשימוש בהצפנה להגנה של סודיות של נתונים (לפחות שלש טעויות נפוצות).
4. הסבר מדוע מפתח האפליקציה צריך לדאוג לא רק לכך שהאפליקציה תהיה מאובטחת, אלא גם שתשתית המיחשוב עליה רצה האפליקציה תהיה מאובטחת. הבא מספר דוגמאות לבעיות אבטחת מידע ברמת תשתית המיחשוב להמאפשרות תקיפת המערכת
5. מנה והסבר לפחות ארבעה תהליכי אבטחת מידע הנחוצים על מנת להגן על תשתית המיחשוב עליה רצה האפליקציה בפני התקפות
6. למה חשוב להריץ את האפליקציה עם ההרשאות המינימליות? הסבר את החשיבות הן ביחס להרשאות למערכת ההפעלה, והן ביחס להרשאות לבסיס הנתונים.
7. הסבר את העיקרון של Defense in Depth, והבא לפחות שתי דוגמאות לישום העקרון מהחנות הוירטואלית שנתחנו בהרצאה
8. הסבר את העקרון של Reduce Attack Surface, והבא לפחות שתי דוגמאות לישום העקרון מהחנות הוירטואלית שנתחנו בהרצאה
9. הסבר את העקרון של Separation of Duties and Least Privileges, והבא שתי דוגמאות לישום העקרון מהחנות הוירטואלית שנתחנו בהרצאה
10. הסבר את המשפט ״ The Web Application is part of the Enterprise Security Perimeter״ – והדגם אותו במערכת מהחנות הוירטואלית שנתחנו בהרצאה, והסבר כיצד באמצעות האפליקציה ניתן לתקוף את שאר מרכיבי המערכת

הנחיות: יש להגיש את התרגיל מודפס בהרצאה שתתקיים ביום ראשון ה 9 למאי 2010 (או לתא שלי עד לאותו תאריך)

בברכה

ד״ר דוד מובשוביץ