

## המכללה האקדמית אשקלון החוג למדעי המחשב

### שם הקורס:

אבטחת מידע (סייבר)

### מבנה הקורס:

הרצאה: 2 שעות

תרגיל: 1 שעות

### דרישות הקורס:

תרגילים: 4 תרגילים, חובת הגשה

בחינה, משקל: 90% מהציון הסופי, 10% תרגילי בית

דרישות קודמות: תקשורת מחשבים 1, אלגוריתמים 1

דרישות מקבילות: אין

חובה / בחירה: בחירה

מהלך השיעורים:

◆ ההרצאות מבוססות על מצגות.

◆ התירגולים מבוססים על מצגות.

### מטרת הקורס:

מטרת הקורס היא להקנות ידע, הבנה בתחום אבטחת מידע, בסיום קורס זה יכיר הלומד ויתמחה ב :

1. אבטחת משאבי מערכת המחשב.

2. פרוטוקולי אבטחת תקשורת באינטרנט.

3. התקפות וחדירות למערכת מחשב.

### סילבוס:

הקורס יתרכז בנושאי אבטחת מחשבים (מערכות הפעלה), אבטחת רשתות תקשורת מחשבים והתקפות ברמת

האפליקציה.

• נושאים:

1. מבוא.

2. כתיבת קוד בטוח – עקרונות תכן לכתיבת קוד בטוח.

3. קריפטולוגיה שימושית.

4. החלפת מפתחות ו-PKI.

5. בקרת כניסה – פרוטוקולי challenge response סיסמא חד פעמית, פרוטוקול EKE, קרברוס.
6. איומים ברשת מחשבים – התקפות בשכבת ה-MAC ובשכבת ה-IP.
7. Firewalls – תכן רשתות, stateless ו-stateful, ניתוח חבילות לעומק (inspection deep packet), שרתי proxy.
8. IPsec – פרוטוקול אבטחה ליצירת חיבורים מאובטחים (ורשתות וירטואליות פרטיות).
9. אבטחת רשתות אלהוטיות, פרוטוקול WEP, פרוטוקול WPA ו-802.1X.
10. SSL – פרוטוקול אבטחת תעבורה מבוסס סרטיפיקטים.
11. חישוב אמין בסביבת תקשורת לא אמינה.
12. מחשוב ענן.
13. פרטיות ברשתות – שיטות מעקב אחרי משתמשים, דרכים לחסום אותן, גלישה אנונימית TOR.

ספרים:

1. "Firewall and Internet Security" Cheswick, Bellovin & Rubin
2. "Network Security, Private Communication in a Public World." Kaufman, Perlman & Speciner.
3. W. Stallings, Network Security Essentials, 4<sup>th</sup> ed., 2011, Pearson.
4. D. Stuttard, M. Pinto, The Web Application Hacker's Handbook 2<sup>nd</sup> Ed., Wiley, 2011