

שם הקורס: רשתות תקשורת מחשבים ועולם הסייבר
Computer Networks and the Cyber World
שם הפקולטה: הנדסה
שם המחלקה: הנדסת תעשייה וניהול
מספר הקורס: 4260410
שם המרצה: ד"ר רון הירשפרונג (ronyh@ariel.ac.il)
מתכונת הקורס: הרצאה

שנת לימודים: תשפ"ג **סמסטר:** ב' **היקף שעות:** 2 **נקודות זכות:** 2
אתר הקורס באינטרנט: Moodle

א. מטרת הקורס:

הקורס מיועד לתלמידים מתחומים שאינם טכנולוגיים, והוא אינו דורש ידע מוקדם. מטרתו לסקור ולהבין את העולם הטכנולוגי של הסייבר על מרכיביו השונים, תוך התמקדות ברשת האינטרנט המהווה בפועל את יישומו המעשי של עולם זה. במסגרת הקורס ילמדו: מבנה המחשב (שכבות החומרה והתוכנה), אופן הפעולה של רשתות תקשורת (עקרונות, ופרוטוקולים תוך התמקדות במודל 5 השכבות הידוע גם כמודל-TCP/IP), מחשוב ענן והאתגרים הבטיחותיים הכרוכים בו, אבטחת מידע בעולם הסייבר (יסודות וכלים קריפטוגרפים, תקיפות נפוצות, תשתיות תקיפה והגנה).

ב. תוכן הקורס:

ליבת הקורס תתבסס על מודל 5 השכבות (המכונה גם מודל TCP/IP ושעליו מושתת בין השאר רשת האינטרנט). המודל ילמד בסדר Top ⇐ Down.

מהלך השיעורים:

הערה: החומר ילמד בסדר זה. חלק מהיחידות יתפרסו על פני יותר משיעור אחד, ויחידות אחרות על פני פחות משיעור אחד.

יחידת שיעור	נושא השיעור	הערות
1.	מבוא: סקירת נושאי הקורס, הגדרת תחום הסייבר (קיברנטיקה), לוחמת סייבר, סיכונים, מטרות האבטחה (Security Objectives).	
2.	מבנה המחשב ומקומה של מערכת ההפעלה: ארכיטקטורת המחשב ורכיביו (מעבד, היררכיות זיכרון, ממשקים), ייצוג מספרים, מושג ה"אלגוריתם", מערכת ההפעלה, שפות תכנות, COMPILER/INTERPRETER (מהדיר/מפרש), מגבלות משאבים.	
3.	רשתות תקשורת: מיתוג מנות לעומת מיתוג מעגלים, ריבוד, ארכיטקטורת רשתות, מודל שרת-לקוח (CLIENT-SERVER) מודל 5 הרמות של OSI, רשתות קווי ואלחוטיות. רשתות מקומיות (LAN) ואזוריות (WAN). לעומת מודל עמית לעמית (PEER TO PEER). כתובות, מושג ה"פרוטוקול".	

4.	רשת האינטרנט – בסיס היסטוריית רשת האינטרנט, פרוטוקול IP, כתובות IP, ARP, ICMP, ניתוב, NAT, DNS, תקינה.
5.	רשת האינטרנט – שכבת המשלוח ושכבת היישומים תקשורת מוכוונת קשר (Connection Oriented), פתחת תקשורת (Communication port) TCP, UDP, Streaming, פרוטוקולי אפליקציה חשובים (SSH, Telnet, SMTP), סיכונים.
6.	פגיעותה של רשת ה-Web מתקפות על שגבות הרשת השונות, פגיעות דפדפנים ומרכיבי רשת נוספים, תקינה, ואיומים.
7.	מחשוב ענן: מכונות וירטואליות, מהו מחשוב ענן, סוגי מחשוב ענן (טקסונומיה), רגולציה בהתהוות, סיכונים.
8.	כלי קריפטוגרפיה – בסיס: היסטוריה, טכניקות בסיסיות (פונקציות חד-כיווניות, הצפנה, שלמות הודעה), Block cipher, לעומת Stream cipher, הצפנה סימטרית לעומת א-סימטרית, מפתח ציבורי ופרטי.
9.	תקיפות נפוצות: איש באמצע (Man in the Middle - MITM), מניעת שירות (DOS) + מבוזרת (DDOS), גניבה (Hijack), Phishing, SMiShing, Vishing.
10.	PKI: ניהול מפתחות, החלפת מפתחות, אמון (Trust), PGP, היררכיית רשויות תעודות (certificate authorities), (hierarchy).
11.	פרוטוקולי הגנה: תיעול (Tunneling), IPSEC, SSL/TLS.
12.	כלי הגנה: חומת אש (Firewall), NIDS, אנטי-וירוס, מלכודת דבש (Honeypot), תקינה, פרטיות.

דרישות קדם:

- אין

ג. חובות הקורס:

חובות / דרישות / מטלות:

- תרגילי הבית הנם רשות ומשמשים כהכנה טובה לבחינה.
- השתתפות בהרצאת אורח ובמטלת אורח (במידה ויתקיימו).
- הזמן הנדרש לביצוע מטלת האורח כשעה אחת.
- מבחן סופי.

מרכיבי הציון הסופי:

הרצאת אורח ומטלת אורח	*ראו הערה להלן
מבחן סופי	100%

*ההשתתפות בהרצאת האורח ומטלת האורח במידה ויתקיימו הנן חובה. היעדרות שאינה מוצדקת תגרור הורדה מהציון הסופי של 5 נקודות.

ד. ביבליוגרפיה:

- Cyber Security Essentials (by James Graham, Richard Howard and Ryan Olson) Auerbach Publications © 2011
- Computer networking: a top-down approach / James F. Kurose, Keith W. Ross