**טכנולוגיות בסיסיות של מערכות סייבר (שו"ת)**

**מר רוני הירשפרונג (הפקולטה להנדסה)**

**1843-0510**

**(תש"פ)**

הקורס מיועד לתלמידים מתחומים שאינם טכנולוגיים. מטרתו לפרוס את העולם הטכנולוגי של הסייבר על מרכיביו השונים. נקודות החוזק ונקודות התורפה, מטרות האבטחה בסייבר, מבנה מחשבים ורשתות תקשורת, מגבלותיהם ופגיעותם. הקורס סוקר היבטים טכנולוגיים בהתפתחותה ומודל פעולתה של רשת האינטרנט, פרוטוקולים ורגישותם לפריצה, רשת ה WEB-והסכנות שבה, מחשוב ענן והאתגרים הבטיחותיים הכרוכים בו, יסודות וכלים קריפטוגרפים, תקיפות נפוצות, תשתיות תקיפה והגנה (פרוטוקולים וכלים).

 **1843-0510-01 טכנולוגיות בסיסיות של מערכות סייבר
Fundamental Technologies of Cyber Systems
שנה"ל תשע"ז | סמ'  ב' | מר הירשפרונג שמחה רון**

**רשימת קריאה**

Cyber Security Essentials (by James Graham, Richard Howard and Ryan Olson)

Auerbach Publications © 2011

הספר הנ"ל אינו מכסה את כל הנושאים.

רשימת ספרים נוספים ורשימת מאמרים עדכניים יועברו בהמשך.

**סדר השיעורים**

הרצאה 1 - מבוא

סקירת נושאי הקורס, הגדרת תחום הסייבר (קיברנטיקה), לוחמת סייבר, סיכונים, מטרות האבטחה (Security Objectives).

הרצאה 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.

הרצאה 3 - רשתות תקשורת

מיתוג מנות לעומת מיתוג מעגלים, ריבוד, ארכיטקטורת רשתות, מודל שרת-לקוח (CLIENT-SERVER) מודל 5 הרמות של OSI, רשתות קוויות ואלחוטיות. רשתות מקומיות (LAN) ואזוריות (WAN). לעומת מודל עמית לעמית (PEER TO PEER). כתובות, מושג ה"פרוטוקול".

הרצאה 4 - רשת האינטרנט – בסיס

היסטוריית רשת האינטרנט, פרוטוקול IP, כתובות IP, ARP, ICMP, ניתוב, NAT, DNS, תקינה.

הרצאה 5 - רשת האינטרנט – שכבת המשלוח ושכבת היישומים

תקשורת מוכוונת קשר (Connection Oriented), פִּתְחַת תקשורת (Communication port) TCP, UDP, Streaming, פרוטוקולי אפליקציה חשובים (SSH,SMTP,Telnet), סיכונים.

הרצאה 6 - פגיעותה של רשת ה-Web

היסטוריה, מ SGML ל HTML ו XML, HTTP, דפדפנים, תקינה, איומים, פגיעות וסיכונים.

הרצאה 7 - סיכונים במחשוב ענן

מכונות וירטואליות, מהו מחשוב ענן, סוגי מחשוב ענן (טקסונומיה), רגולציה בהתהוות, סיכונים.

הרצאה 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.

הרצאה 9 - תקיפות נפוצות

איש באמצע ( MiM- Man in the Middle), הפרעה לשירות (DOS) + מבוזרת (DDOS), גניבה (Hijack), Phishing, SMiShing, Vishing

הרצאה 10 - PKI

ניהול מפתחות, החלפת מפתחות, אמון (Trust), PGP, היררכיית רשויות תעודות (certificate authorities hierarchy)

הרצאה 11 - פרוטוקולי הגנה

תיעול (Tunneling) , SSL/TLS, IPSEC

הרצאה 12 - הגנה - כלים, תקינה, certification

חומת אש (Firewall), NIDS, אנטי-וירוס, מלכודת דבש Honeypot)), תקינה, פרטיות

הרצאה 13 - טכניקות תקיפה

ראיות (Forensic), טכניקות התחמקות (Covering), Proxy, Intermediaries, Steganography, תשתיות תקיפה (Botnet, Fast–flux), תקיפות בערוץ צדדי (side channel), .Key loggers

מטלת סיום: מבחן.