# Introduction to Cyber Warfare

## קורס 7510 – 40 שעות

### אודות הקורס

בעולם בו מערכות המחשוב הפכו לחלק בלתי נפרד מחיינו ופגיעה במערכות מחשוב גורמות לנזקים פיננסים בחברות, תחום הגנת המידע הפך להיות תחום פעילות בעל חשיבות עליונה עבור כל חברה. מטרתה של הגנת המידע היא להגן על המערכות הממוחשבות מפני כל הסיכונים האפשריים העלולים לאיים עליהן. בהגנת המידע יש להתחשב בשלושה גורמים עיקריים: חיסיון המידע, זמינות המידע ואמינות המידע.

### מטרות הקורס

- להקנות למשתתפים את הכלים הניהוליים והטכנולוגים בעולם הסייבר, להסביר את עקרונות הגנת המידע, תקני אבטחת המידע וסקירת סוגי התקיפה הנפוצים בעולם.

### קהל יעד

- הקורס מיועד לבעלי רקע טכנולוגי והבנה טכנית אשר מעוניינים להכיר בצורה רוחבית את עולם הסייבר, מונחים וצורות תקיפה והגנה. **חובה** נסיון פרקטי בעולם המחשוב דוגמת כתיבת קוד / ניסיון בשרתים /IT / LINUX / תקשורת וכו'.

### דרישות קדם

- ניסיון פרקטי בעולם המחשוב דוגמת כתיבת קוד / ניסיון בשרתים /IT / LINUX / תקשורת וכו'.
- או תואר בהנדסה/ מדעי המחשב

### תכני הקורס

**חלק 1: יסודות תקשורת ולינוקס**

- רקע על עולם הסייבר ותקיפות
- מכונות וירטואליות הכרת LINUX והקמת סביבת מעבדה
- מבואות לרשתות
  - TCP/IP
  - DHCP&DNS&ARP
  - FIREWALLS&ROUTING
  - HTTPS&HTTP

**חלק 2: טכנולוגיות השגת מידע והבנת חולשות**

- Information Gathering
- Nmap
- Vulnerability & Exploit
- מתקפת DDOS+ DOS
  - התקפה על משאבי השרתים עצמם
  - התקפה על תצורת הרשת
  - התקפה כנגד רכיבי התוכנה על המחשב המותקף

**חלק 3: מעבדות תקיפה**

- ARP Spoofing
- DNS Spoofing
- Amplification
- Privilege Escalation
- BotNet
- SQL INJECTION
- XSS
- Bind and Reverse SHELL
- Brute-force logins and passwords
- cmd OS injections
- remote file and resource inclusion
- Code execution

**חלק 4: מעבדה מסכמת והגנות**

- APT Kill Chain
- הגנות שונות
- CIA
- Whitelists & Blacklists
- Firewalls
- WAF
- NAC
- App-lockers
- הגנת Honeypot