קורס מבדקי חדירה וסקרי סיכונים

16 שעות , 4 מפגשים – **פרונטלי** | 16 שעות, 8 מפגשים – **מקוון**
16 שעות, 7 מפגשים – **היברידי**

אודות הקורס

מקצוע הסייבר ואבטחת המידע הולך ומתפתח במהירות בגלל ניסיונות הפריצה הרבים מצד ההאקרים, שיטות הפריצה המתוחכמות של ההאקרים והנזק הרב שנגרם לארגונים בגלל איומי סייבר, כופר, תרמיות ובעיות באבטחת מידע.

הקורס נבנה בצורה מתודולוגית ובהתאמה לטכנולוגיות העדכניות ביותר בתחומי סייבר, אבטחת מידע, תקשורת ומחשבים, ובהתאם לדרישות של חברות ההייטק והארגונים המובילים.

מטרות הקורס

מטרת הקורס היא הכשרה מעשית של אנשי הגנה ואבטחת סייבר, תוך מתן ידע עדכני ויכולת מעשית גבוהה בנושאי איתור חולשות במערכי הגנת סייבר ובדיקות חדירות (Penetration Testing).

בנוסף, הקורס נותן כלים להערכת חולשות. כלל הנושאים האלו מתורגלים בפועל (Hands-On) על ידי החניכים במהלך הקורס.

קהל יעד

הקורס מיועד לאנשים עם זיקה לעולם הטכנולוגי ולתחום אבטחת סייבר שמעוניינים להעמיק את הידע במבדקי חדירה וסקרי סיכונים.

דרישות קדם

אין דרישות קדם לקורס.

תכני הקורס

- א- Build the foundation Build the foundation
  - א- Basics of networking
  - ב- Cryptography
  - ג- Firewall
  - ד- Vulnerabilities
- ב- Infrastructure Penetration Testing
  - א- Reconnaissance tools
  - ב- Nmap
  - ג- Nmap Scripts
  - ד- Nessus
- ג- Application Penetration Testing
  - א- Reconnaissance tools
  - ב- Session hijacking
  - ג- QWASP
- ד- Structure and Final report