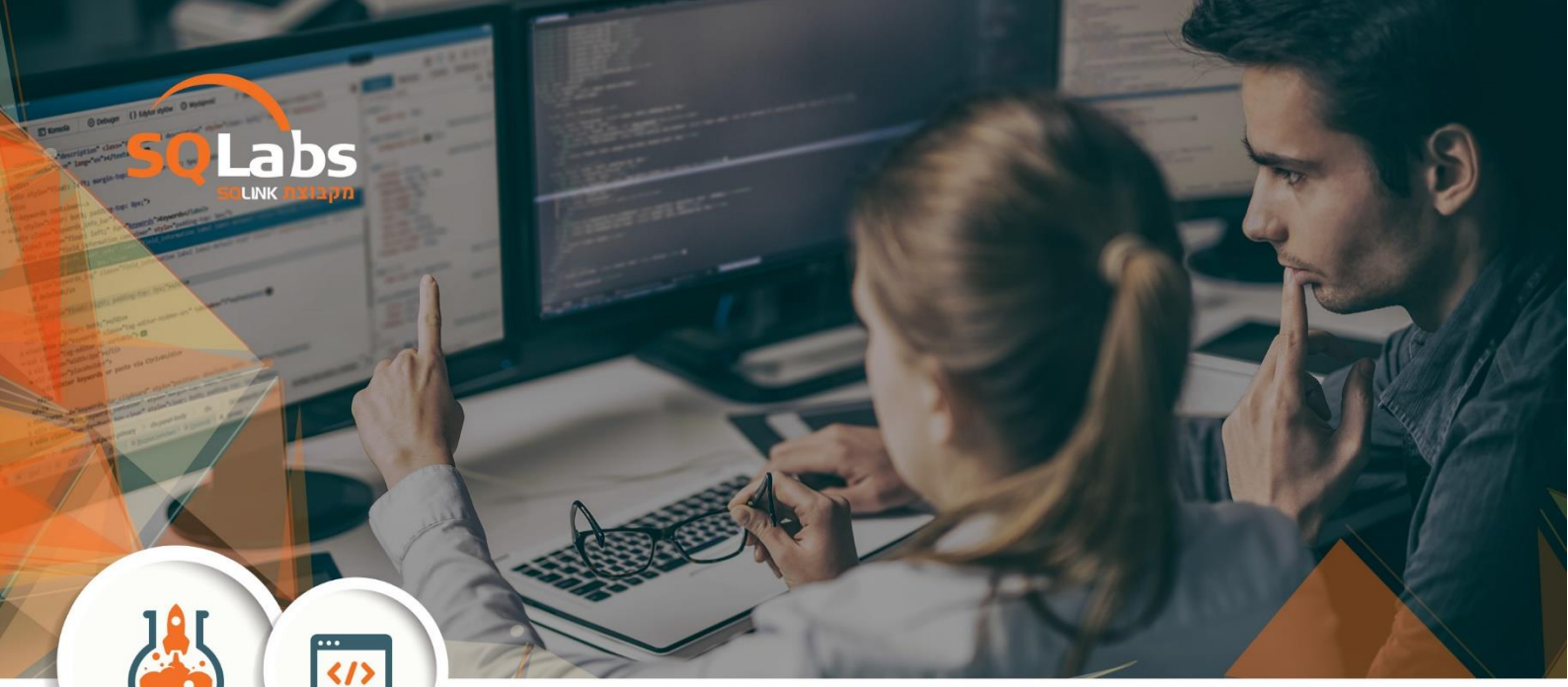

Ethical Hacking and Pentest – 40 Hours

על הקורס

האם תמיד חלמת לחשוף את נקודות התורפה במערכות מחשוב?

בואו לצלול לעולם אבטחת מידע, סייבר ובדיקות חוסן (Pentest), עם קורס המיועד למי שמעוניין להבין את נקודות התורפה במערכות מחשוב ולרכוש כלים מתקדמים לזיהוי, ניתוח ותיקון פרצות אבטחה.

הקורס משלב גישה טכנית ומעשית עם הבנה תיאורטית מעמיקה, תוך שימוש במתודולוגיות המובילות בתחום והסתמכות על סטנדרטים עולמיים כמו אלו של Cisco ו EC-Council
לכל המשתתפים תהיה גישה למעבדת תרגול וחומרי לימוד און ליין .

קהל יעד

בוגרי קורס אבטחת מידע וסייבר

דרישות קדם

- ראיון מקדים
- בוגר קורס סייבר במכללה
- רצון ללמוד את התחום ולהתקדם

לאחר השתתפות ומעבר הקורס נכיר ונלמד את הנושאים הבאים :

Module 1: Introduction to Ethical Hacking and Pentesting

- Overview of cybersecurity and ethical hacking.
- Understanding the roles of ethical hackers and pentesters.
- Ethical and legal considerations in ethical hacking.
- Introduction to industry standards (e.g., OWASP, NIST, CIS).

Module 2: Reconnaissance and Information Gathering

- Open Source Intelligence (OSINT) techniques.
- Active vs. passive reconnaissance.
- Tools for information gathering
- Identifying potential attack surfaces.

Module 3: Network Scanning and Enumeration

- Network scanning techniques and tools
- Identifying open ports and services.
- Detecting operating systems and network devices.
- Enumeration of network shares, users, and protocols.

Module 4: Vulnerability Assessment

- Introduction to vulnerability scanning tools
- Identifying and analyzing vulnerabilities.
- Categorizing vulnerabilities by risk level.
- Reporting and prioritizing remediation efforts.

Module 5: Exploitation and Gaining Access

- Exploiting vulnerabilities in systems and applications.
- Tools for exploitation
- Privilege escalation techniques.
- Maintaining access with backdoors and persistence mechanisms.

Module 6: Web Application Attacks

- Common web vulnerabilities (SQL Injection, XSS, CSRF).
- Techniques for attacking authentication mechanisms.
- Using tools like Burp Suite and OWASP ZAP.
- Securing web applications with best practices.

Module 7: Wireless Network Attacks

- Fundamentals of wireless security (WPA/WPA2).
- Cracking Wi-Fi passwords and exploiting vulnerabilities.
- Tools for wireless attacks (Aircrack-ng, Wireshark).

- Defenses against wireless attacks.

Module 8: Post-Exploitation and Lateral Movement

- Post-exploitation techniques: harvesting credentials and sensitive data.
- Moving laterally within a network.
- Evading detection and maintaining persistence.
- Data exfiltration methods.

Module 9: Defensive Strategies and Reporting

- Hardening systems and networks against attacks.
- Patch management and vulnerability remediation.
- Writing pentest reports.