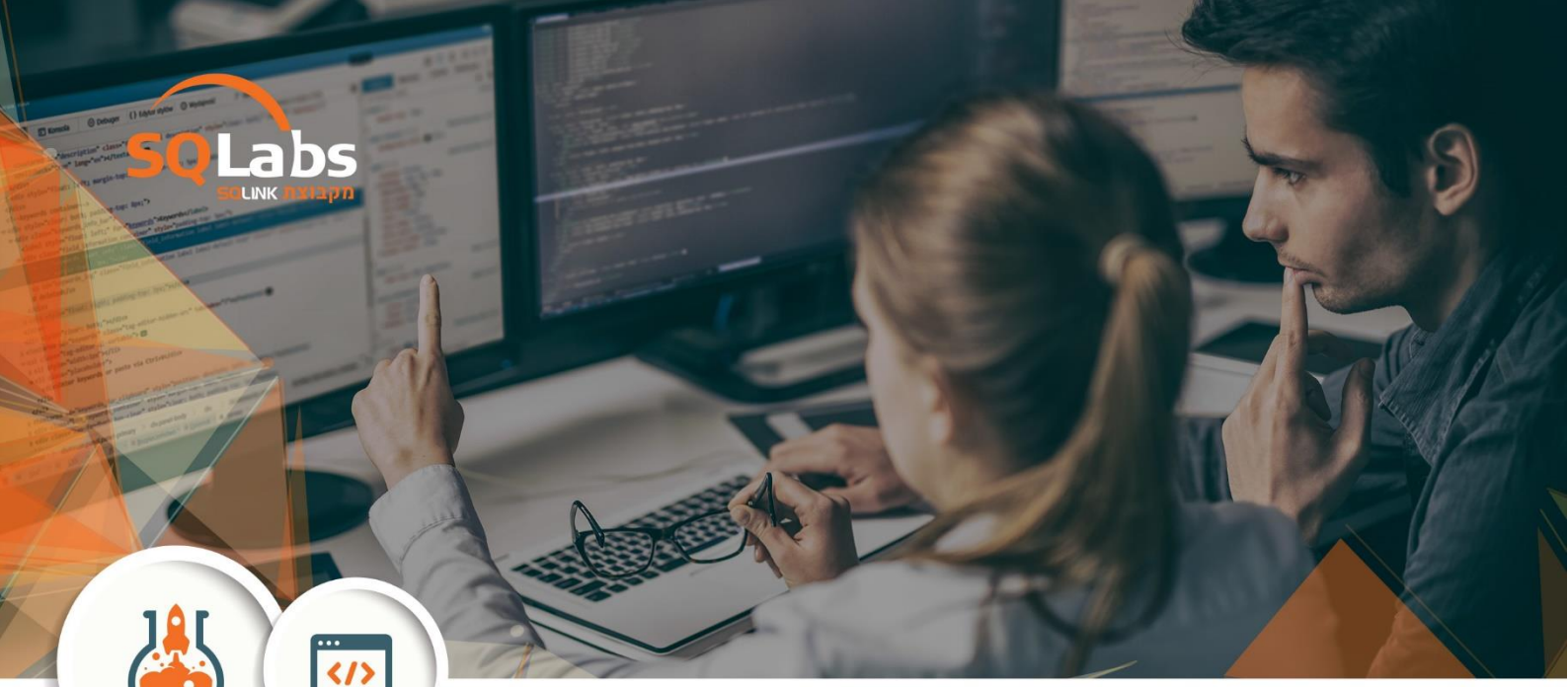

Advanced Cyber and hacking – 32 Hours

Course goals

Extend the knowledge of the participants beyond the basic cyber concepts into the real modern techniques used out there, while obtaining hands on experience with various popular tools and methods – from the world of user tracking using the web, Android attacks, understanding the hashing concept (such as in OS authentication) and how it is being attacked, and understanding the key elements in the penetration testing domain.

Target audience

Anyone with the following knowledge:

- Basic programming capabilities (in any language).
- Basic background in cyber is required, including familiarity with the following topics:
  - Computer networks key concepts (Router, IP and MAC addresses, proxy)
  - Basic communication protocols (DNS, ARP, ICMP, TCP, UDP, HTTP)
  - Basic cyber concepts (DoS, MITM, bufferoverflow, XSS, SQLi)
  - Basic defense concepts (Firewall, IDS/IPS, WAF, Anti-Virus)
  - Hands on experience with any Linux distribution (Such as: Debian, Ubuntu, Kali)

Detailed curriculum:

Session 1 – Basic web technologies

- Working with HTML
  - Background
  - Basic tags and page structure
  - HTML5 – new tags and capabilities
- CSS
  - Overview
  - Basic and advanced selectors
  - Animations

Practical exercise: Working with HTML5 and CSS

Session 2 – More web technologies - JS

- JavaScript
    - Overview
    - Basic programming concepts
    - JS – variables and user input

Practical exercise: Building web pages with tools learned

Session 3 – Advanced JS

- Advanced Javascript in HTML5 (Cookies, GeoLocation, LocalStorage, AJAX)

Practical exercise: Building web pages with tools learned

Session 4 – User fingerprinting and Web tracking

- Java applets background
- Basic flash programming and concepts
- Web tracking basics using JS, Applets and Flash
- User fingerprinting

Practical exercise: Build Flash content utilizing learned capabilities

Session 5 – Certificates and SSL

- What are certificates and their basic types
- Encryptions basics
- CAs
- SSL and TLS (Concept, Handshake process...)
- Hashing and Code signing
- Authentication and OS critical files

Practical exercise: Analyzing and installing certificate, working with Hashes

Session 6 – Android attacks

- Built-in Android security tools and concepts
- Common attack vectors
- Best practices for protection
- Risks of a successful attack
- Android attacks
    - mRAT based
    - MITM
    - Other

Practical exercise: Perform various Android attacks

Session 7 – Penetration testing

- Overview and concepts
- Techniques
- Injection attacks (Advanced SQLi, OS injection...)

Practical exercise: Practice various attacks and key pen-testing concepts

Session 8 – Account hijacking

- Overview and concepts
- Techniques
    - Dictionary and Brute force
    - Password reset
    - Phishing

Practical exercise: Practice various account attack techniques