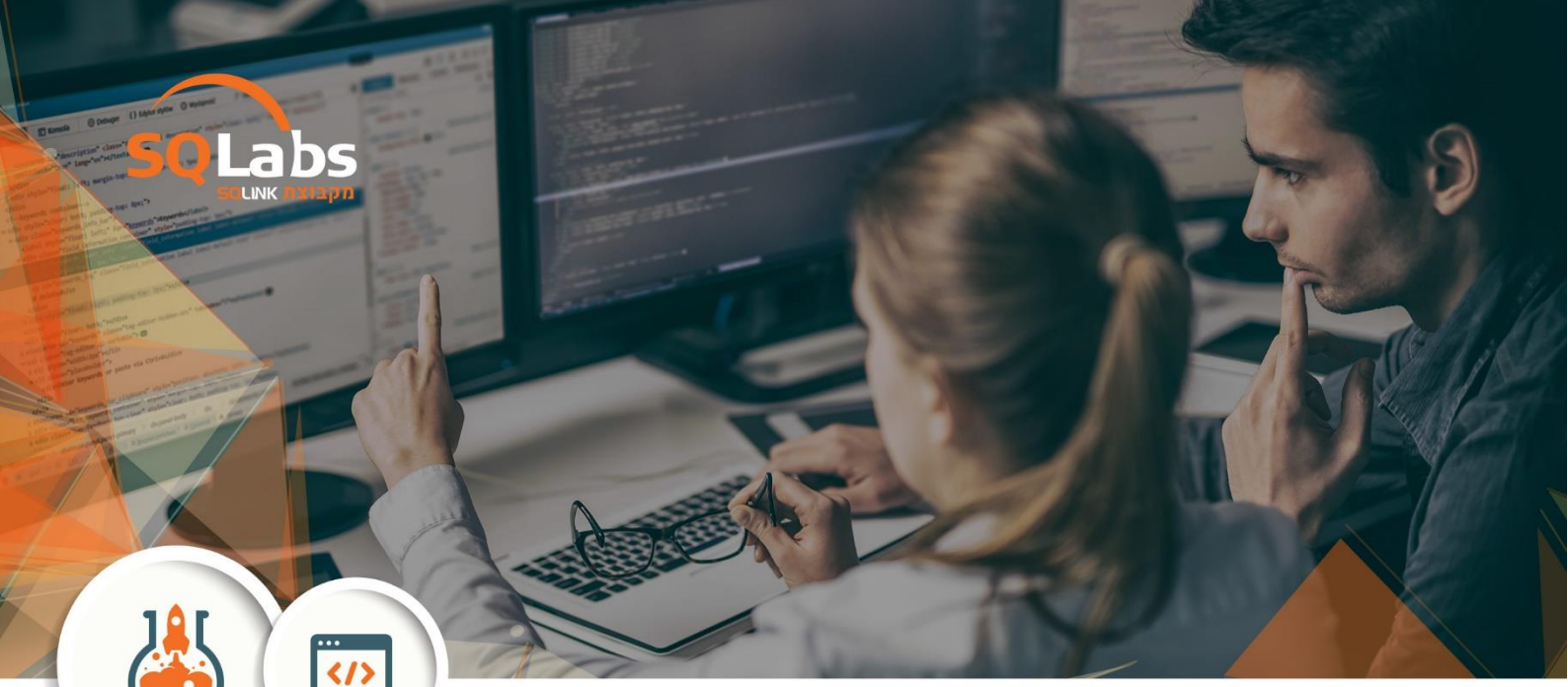

Cyber & Hacking basics – 24 Hours

Course goals

The “Cyber” term is becoming more and more prominent in the last few years, and it seems we keep hearing it almost on a daily basis. Even so, it appears that most of us don’t really understand what “Cyber” really means, and what it encompasses. In this course we are going to be exposed to various topics included in this term, from the world of hacking and phising to the world of cyber attacks against computer networks and web sites. We will get familiar with common industry terms and security tools used by attackers as well as security experts, for protection purposes.

Target audience

A general background in computers is required (basic computer usage). No background in cyber, hacking or programming is needed.

Detailed curriculum:

Session 1 – Basics and overview

- Definition (or lack of it) of Cyber
- What is Hacking all about
- Who are the attackers (From script kiddies to nation-state actors)
- Common attack techniques (Phishing, MITM, Drive-by download, Ransomwares)
    - Recent incidents and examples
- Basic tips for staying secure

Practical exercise: Analyze security level of used machine

Session 2 – Linux for beginners

- What is an OS
- Common OS types
- Linux – Background and history

- Why do Hackers love Linux
- Various Linux distributions
- Virtualization
- Working with Linux
- Common Linux command line tools
- Kali Linux

Practical exercise: Working with Linux

Session 3 – Computer networks

- What are computer networks
- Common internet protocols (DNS, ICMP, TCP, UDP, ARP, HTTP)
- Network components and concepts (Router, Proxy, VPN)
- Network identities and their forgery
- Network traffic sniffing

Practical exercise: Working with Wireshark (Sniffing)

Session 4 – Network attacks

- How hackers protect themselves
- WiFi attacks (Security measures and techniques to break them)
- Man in the middle (Passive, ARP spoofing, DNS spoofing, SSL Striping)

Practical exercise: Hands on experience with various attack techniques

Session 5 – Network attacks Resumed

- DoS (Using single machine, DDoS, DRDoS, PDoS)
- Network attack techniques and tools (nmap, Metasploit, Armitage)

Practical exercise: Hands on experience with various attack techniques

Session 6 – Web attacks

- Web background
- Common attack vectors and countermeasures
    - SQL Injection
    - XSS
    - CSRF
    - Session hijacking (Firesheep example)
- Clickjacking (Using Frames)
- Google hacking

Practical exercise: Perform SQL injections and XSS on dedicated sites