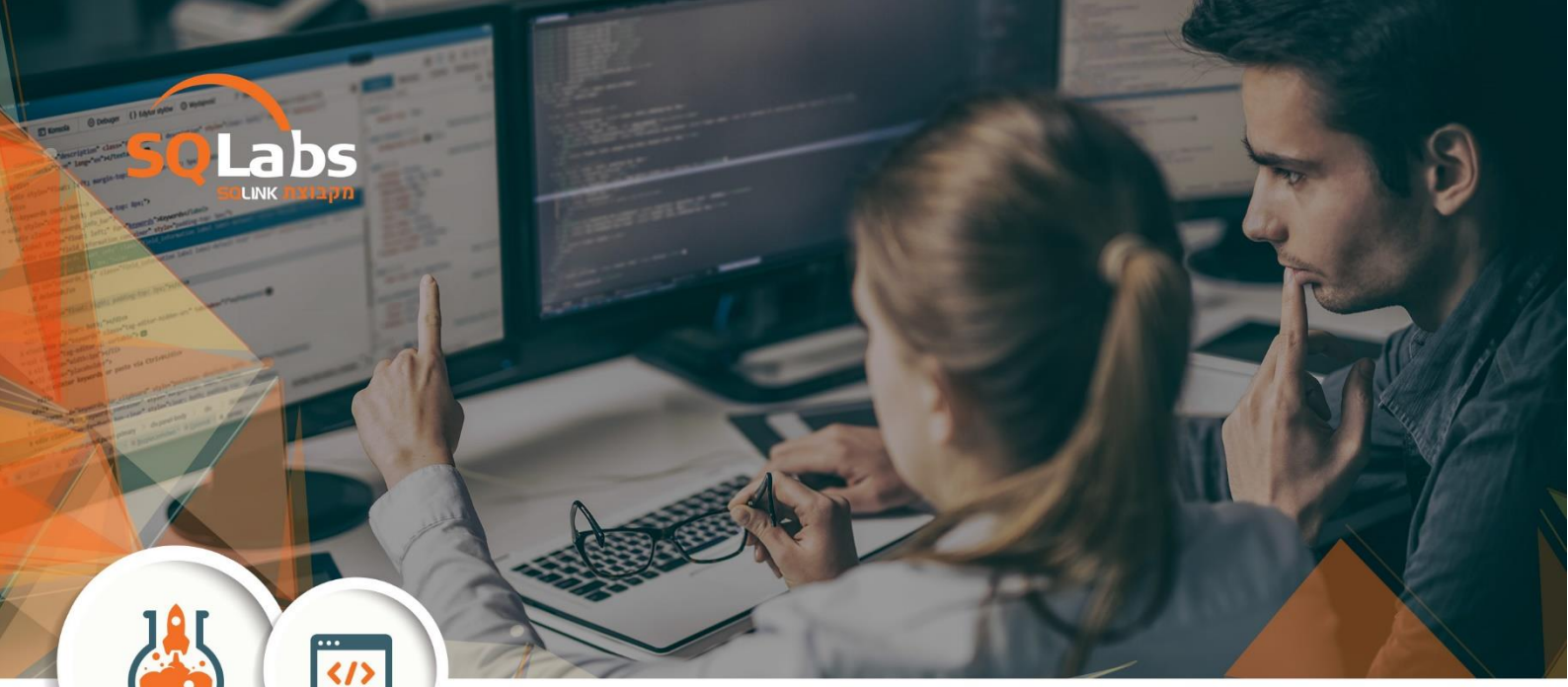


# Cyber & Hacking basics

**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 get familiar with various topics included in this term, from the world of hacking and phishing 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.

**Course Methodology:** Six sessions of about three full hours each. We believe that only practical hands on experience will help fully understand the material at hand. For this reason most sessions includes a practical exercise where the actual hands on experience can be gained.

**Detailed curriculum:**

## Basics and overview

- What is Cyber all about
- Who are the attackers (From script kiddies to nation-state actors)
    - How attackers make money from cyber attacks
    - Common attack types
- Recent incidents and examples
- Basic tips for staying secure

## 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

Practical exercise: Working with Linux

## Computer networks

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

Practical exercise: Working with Wireshark (Sniffing)

## Wi-Fi and MITM attacks

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

Practical exercise: Hands on experience running an MITM attacks on practice VMs

## Remote machine takeover (RCE)

- Finding a remote victim:
    - Using Google Dorks
    - Using dedicated search engines
    - Scanning for a victim
    - Random IP attacks
- RCE example case study:
    - How a vulnerability is created
    - Exploiting a vulnerable application (buffer overflow)
    - Payload – taking over the remote machine
- Working with exploit database (metasploit)

Practical exercise: Taking over remote machine (test VM) using armitage

## Attacking websites

- Web background
- Common attack vectors:
    - Injections: SQLi, OSi, HTMLi
    - XXE
    - XSS
    - CSRF

Practical exercise: Run various attacks on test website