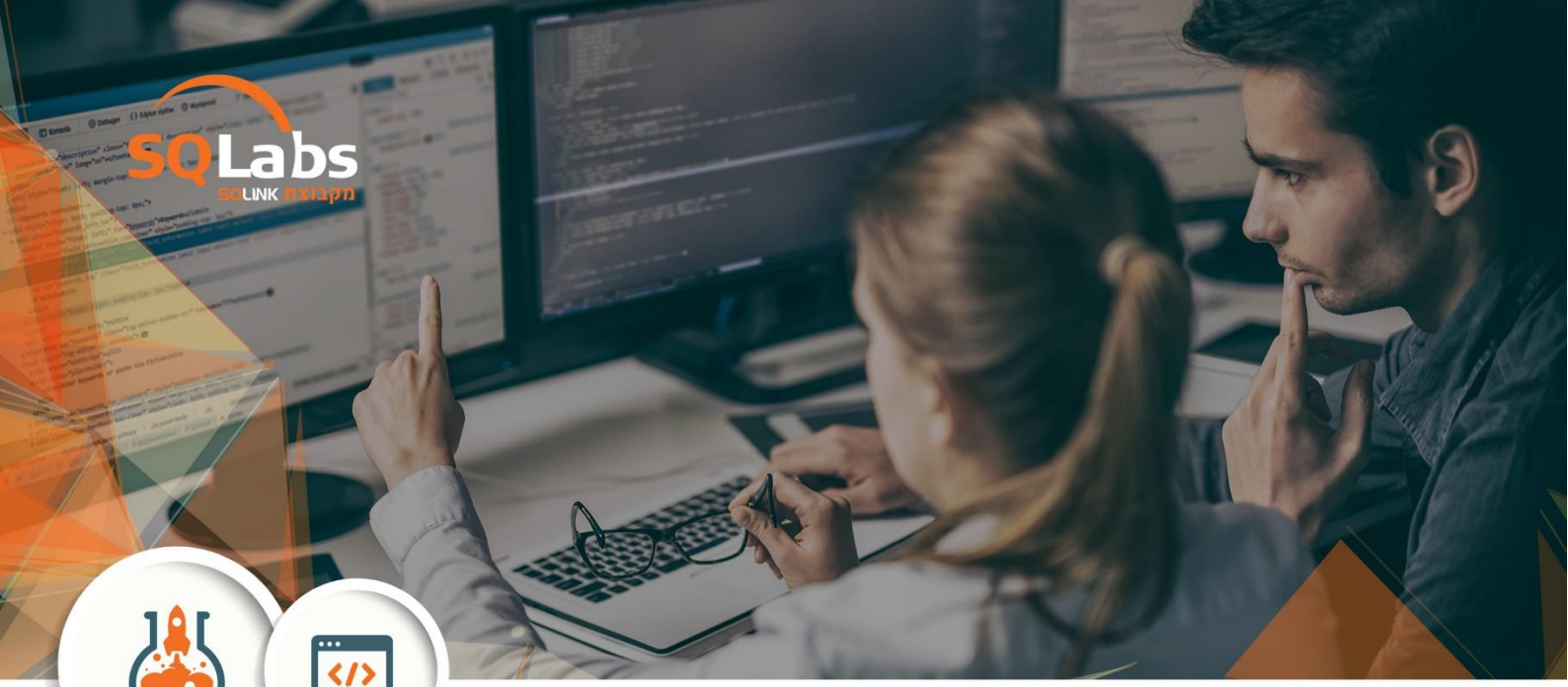

אנטומיה של תקיפת הסייבר 2

HOURS 40

Course Brief

The Cybersecurity Specialization covers the fundamental concepts underlying the construction of secure systems, from the hardware to the software to the human-computer interface, with the use of cryptography to secure interactions. These concepts are illustrated with examples drawn from modern practice, and augmented with hands-on exercises involving relevant tools and techniques. Successful participants will develop a way of thinking that is security-oriented, better understanding how to think about adversaries and how to build systems that defend against them. The students will understand the concepts of reactive vs. proactive security and will have hands on activity's

What we will learn

- What is cyber and the digital universe?
- What is denial of service and how it is performed?
- How is information gathering performed?
- How to gain privileges (with brute-forcing and without)?
- How to inject code into interpreted context?
- How to exploit vulnerable code?
- Security truisms
- What are blacklists and how are they implemented?
- What are whitelists and how are they implemented?
- How to improve authentication mechanisms?
- How to better manage your current assets?

- How to create baselines and detect anomalies?
- How to use and improve the human factor?
- What are APTs?
- What is security by design?

Prerequisites

- **Entry level (first cyber course graduation)**: Technical/scientific mind-set, very good English (reading), search skills (google).

Course Content

Part 1: Threat Landscape

- Flooding
- Spoofing
- Protocol malformations
- Reflections and amplifications
- Scanning, fingerprinting and enumeration
- Manual vs. Automated spidering
- Credential harvesting
- Resource mapping
- Error based information disclosure
- Brute-force logins and passwords
- Password hashes and password dictionaries
- Custom dictionaries and password complexity
- Bypass authentication mechanisms
- Bypass session management
- Bypass OS user and fs permissions
- Bypass security software
- cmd OS injections
- data-store injections
- file injections (XML, json, etc)
- remote file and resource inclusion
- injecting web clients (browsers)
- injecting client applications (office, pdf, etc)
- Buffer, stack and heap overflows
- Browser and plugin exploitation
- Code execution

Part 2: strategies

- What is defense all about
  - IP blacklists
  - Anti-malware defenses
  - URL filtering (... and ad blocking too)
  - Block mail SPAM and spoofs
  - Application firewalls (proxies and reverse-proxies, WAFs, DB-fw)
  - IDS/IPS/HIPS
  - NAC
  - Firewalls and access-lists
  - Application whitelisting
  - Application firewalls (positive proxies and reverse-proxies)
  - strong passphrases
  - certificates
  - cryptography
  - multi-factor authentication
  - permissions and the ‘need to know’ rule
  - admins (locale & domain) and roots
  - audit
  - patch operating systems and applications
  - perform vulnerability scans
  - harden OS and application configurations
  - maintain a ‘master’ system image bank
  - backup and disaster recovery
  - keep detailed logs and network traffic captures
  - Honeypots and decoys
  - Exploit mitigation tools
  - Centralized log collection and analysis (aka SIEM)
  - Network/host-based anomaly detection
  - Heuristic A/V and HIPS
  - New profession: security analyst
  - User education
  - Skill assessment and training (of security teams)
  - Secure coding for developers
  - Penetration test