PENETRATION TEST

Definition of training:
Sometimes the best way to test out the security of a site or IT infrastructure is to try to break into it. Pen testing tries to mimic cyber attacks, hoping to find security vulnerabilities before hackers do. Penetration tests are a vital part of planning a security-first design for real-world applications.

Pen testers provide security assessments by mimicking activities hackers engage in. These pen tests, part of a suite of ethical hacking activities, allow companies to predict and fight against new types of malware and offer mitigations to new security threats. Every time technology evolves, new cybersecurity concerns appear. Penetration testers are now an essential part of the front lines, preventing disruption and securing sensitive data.

Computer systems are more complex than ever and with the addition of black box AI applications, security and remediation are critical to businesses and organizations.

The course will help practitioners from across the security spectrum:
- Learn how to become a penetration tester by using information gathering techniques to identify and enumerate targets running various operating systems and services
- Writing basic scripts and tools to aid in the penetration testing process
- Analyzing, correcting, modifying, cross-compiling, and porting public exploit code
- Conducting remote, local privilege escalation, and client-side attacks
- Identifying and exploiting XSS, SQL injection, and file inclusion vulnerabilities in web applications
- Leveraging tunneling techniques to pivot between networks
- Creative problem solving and lateral thinking skills

Duration:
2 Instructors / 6 Days

Place:
Online Platform

Target group:
Ethical Hackers, Security Practitioners, Engineers, Specialist, Architects, Managers, Threat Intelligence Specialists, Associates, Researchers, Consultants, Threat Hunters, SOC Professionals, Digital Forensic and Malware Specialists, Incident Response Team Members, any mid-level to high-level cybersecurity professionals with a minimum of 2 years of experience, Individuals from the information security profession and who want to enrich their skills and knowledge in the field of cyber threat intelligence, Individuals interested in preventing cyber threats.

Participation prerequisite:
Attendees should be comfortable with using the command line in Linux for a few lab tests (though a walkthrough is provided) and be familiar with security terminology.

Document:
Certificate of participation