

## Course Overview

### Course Title:

Ethical Hacking Workshop

### Duration:

5 days, 20 Hrs  
4 hours per day

### Class Format Options:

Instructor-led classroom  
Training.

Training is 100% Practical, No  
theoretical part.

### Who Should Attend:

- Cyber Security Professionals
- SOC Managers
- SOC Engineers
- IT Auditors
- System Administrators
- IS Managers
- Penetration testers
- Incident Handlers
- Digital Forensics Examiners

### Prerequisites:

The trainees should be certified in either EC-Council CEH \ Mile2 CPTe, or at least attended the aforementioned training courses.

### Provided Materials:

- Windows VM for hackers.
- Kali Linux 1.9 - Latest Versions

EHW is extremely advanced hacking course, the trainee should check the prerequisite and confirm acceptance.

**Ethical Hacking Workshops** is an advanced cyber security course aims to teach trainees on the proper technique to conduct ethical hacking. It covers hacking tools used by hackers; The **EHW** is designed for those people who wish to conduct ethical hacking both internally and externally from a hacker perspective, and the tools used by a hacker, all labs will be conducted based on black box testing.

Furthermore, this training course is based on the latest release of Kali Linux and how to use the proper hacking tools that is used by real hackers.

**Ethical Hacking Workshop** does not contain a theoretical part, this course contain only a lab part for using hacking tools thus it is 100% practical, the trainees will have a proper training on hacking tools and how to use them in a practical environment.

### EHW Labs

- o **Lab 1:** CVE - Common Vulnerability and exposure LAB.
- o **Lab 2:** Sec tools LAB.
- o **Lab 3:** Hacking Database LAB.
- o **Lab 4:** Metasploit – Passive LAB.
- o **Lab 5:** Mask HTTP Traffic lab and tricks | Deep Web LAB.
- o **Lab 6:** Active Information gathering LAB.
- o **Lab 7:** Using Extensions LAB.
- o **Lab 8:** Vulnerability Assessment LAB.
- o **Lab 9:** Web Application Vulnerability Assessment Tools LAB.
- o **Lab 10:** SMB & SNMP LAB.
- o **Lab 11:** Network Sniffing LAB.
- o **Lab 12:** Port Scanning tools LAB.
- o **Lab 13:** Kali Linux LAB.
- o **Lab 14:** OWASP TOP 10 – SQL injection LAB.
- o **Lab 15:** Password cracking LAB.
- o **Post Class Lab:** Armitage LAB.

The above EHW labs do not reflect by any means the training course practical section, however, it can be considered as the course outline.