

WHITE HAT HACKER TRAINING COURSE

TIME (DAY)	5
TRAINING OPTIONS	General Participation & In-House & Online
LANGUAGE	Turkish, English
ACCREDITATION	CPD

COURSE AIM

White hat hacker training is an advanced level of information security training. Unlike theoretical security training, it has been prepared with the philosophy of "Security cannot be provided without knowing the attack methods" by exemplifying the methods of malicious attackers.

Unlike malicious attackers; Individuals with white hat hacker skills aim to simulate the attacks that organizations may experience in advance and use their knowledge and competencies in beneficial matters. In this training, attack techniques and methods used by attackers are examined.

The aim of the White Hat Hacker Training is to enable the participants to specialize in Information Security and to train experts (Pentesters) who can make Security Tests.

WHO SHOULD ATTEND

- A system, Network Administrators and Information Security experts

COURSE CONTENT

- Introduction to Ethical Hacking
- Discovery
- Network Scans
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Information Gathering Methods
- Getting Information From Services
- Metasploit
- Virus, Worm and Trojans
- DOS Session Stealing
- Social Engineering
- Denial-of-Services
- Session Hijacking
- IDS, Firewall and Honeypot bypass
- Introduction to Web Servers
- Web Application Weaknesses
- SQL Injection
- Introduction to Wireless Networks
- Firewall & Honeypot and IDS
- Memory Overflow
- Cryptography - Encryption
- Pentest

IMPORTANT NOTES

NOTE 1: You must have basic Linux, System and Network knowledge to participate in the white hat hacker training.

NOTE 2: In order to get a certificate of achievement in education, the exam passing grade is 70 points, and the Participant Certificate will be given to those who cannot get a valid grade.

NOTE 3: In order to take the exam, at least 70% attendance is required.