G. Bina
Secure Your Cyber-Space & IT

Ethical Hacking and APTs

A 3 day seminar which demonstrate Israeli cyber-attack and cyber- defense techniques and information security methodologies

Developed by Dr. Col. (res.) Gabi Siboni

Ethical Hacking and APTs

A 3 day Seminar

Introduction

To beat a hacker you need to think like one! This course intend to bring a computer-savvy crowd to a state of awareness and basic understanding of what is hacking, attack surfaces and how APTs constructed. We will demonstrate how an attacker operates, chooses targets and vectors. You will be exposed and gain knowledge of how a real live attack takes place and what is the mind-set of your attackers for the purpose of finding and fixing computer security vulnerabilities.

About the Course Owner and Developer

This course is developed by Dr. Col. (res.) Gabi Siboni, Director of the Cyber Security Program at The Institute for National Security Studies, Tel Aviv University and serves as Chief Methodologist of the IDF's Research Center for Force Utilization and Buildup – Experimentation Laboratory.

Dr. Siboni is a domain expert in national security, military strategy and operations, military technology, cyber security and warfare, and force buildup and a thought leader in business operations risk management.

Who Should Attend?

Information security managers, developers and CIOs who are seeking to leverage their understanding in the concept of hacking and to gain knowledge on hacker’s way of thinking, motivation and to master hacking technologies.

Requirements

Each student needs to have an understanding of networking protocols such as TCP, IP, UDP, general OSI and more. Each student needs to have a working knowledge of the Windows operating system and the ability to work with it fluently. It is highly recommended that students have a background in programming or scripting in any language to gain better understanding of materials. Students are to come with laptops with at least 4 GB of free space and at least 2GB of RAM. Practical work will be part of the course.

Course Curriculum

This unique curriculum presents the state of the art Israeli cyber-attack and cyber-defense techniques and information security methodologies.

Topic	Contents
Introduction to Hacking	Hackers' Categories, A bit of history, Hacking in 2014, APTs
Methodology & Concepts	Hacking Methodology, Concepts and Attack Surfaces
Reconnaissance	OSINT, Google as a Tool, Managing your Recon Map, Social Networks as a viable source, Harvesting the data
Network Attack	How they look like, Where and how the occur, Threats to today's infrastructure, Wireless security infrastructure
Web Applications	How to start, What are web applications, Server side attacks (SQLi, RFI/LFI), Client side attack (XSS , CSRF)
Virology	What are malwares, How they are built, What they can do, Case Studies, Behavioral Analysis
The Art of Exploitation	What is MSF, How does it work, Leading a job end to end

* * Learning materials will be provided to participants by a magnetic means