Red Team Master

There is only way to become really good at cybersecurity: you must know both how to attack and how to defend. First of all, you have to learn to think like a hacker, so you deeply understand what the threats are. Then you'll need to know how to protect yourself from the attacks. We start with precise descriptions and examples of network attacks to show you how the malicious hackers can break into your network—and what harm they can do. Then we'll look at another attack vector: websites and web-applications. You'll see the most vulnerable places and understand what cybercriminals will do if they find them. Then we'll discover the third vector of attacks: humans. Refined hackers know how to hack a human brain first to hack digital assets. You'll find out what social engineering, phishing, and spear-phishing's, and why they're becoming especially dangerous today. By the end of this course, you'll be able to locate all your vulnerabilities and remediate them before malicious hackers find and exploit them.

You must know!

Duration:
40 Hours

Who should attend?
IT security professionals, Malware Analysts that want to get better understanding of attacker's perspective, Security Analysts who want to advance their knowledge in the cybersecurity field, Digital Forensics experts, Others with the passion and eagerness to discover and learn new topics.

Prerequisites:
Basic understanding of networking: TCP/IP, Routing, Forwarding. Reading and understanding code, Basic understanding of well-known protocols such as HTTP/HTTPS,

Red Team Master

Course Modules

Module 1 – System Fundamentals

- Introduction to Cybersecurity
- Basic Concepts
- CIA vs. DAD
- Attack & Defense point of views
- Learning the state of mind of an attacker
- Architecture Fundamentals
- Basic OS Internals
- Buffers & Memory Management
- x86 Assembly Basics
- Python Basics

Module 2 – Infrastructure Attacks

- Reconnaissance and Information Gathering
- System and Network Enumeration
- Traffic Sniffing and Packet Analysis
- Weaponizing Man-in-the-Middle attacks
- Social Engineering Tools and Techniques
- Utilizing Vulnerability Assessment Tools
- Exploitation Tools and Techniques
- Post Exploitation Tools and Methods
- Anonymity and Evasion

Module 3 – Wireless Attacks

- Introduction to Wireless Security
- Introduction to the 802.11 (Wi-Fi) Protocol
- Introduction to SDR Hacking
- Wi-Fi Networks Enumeration
- Wi-Fi Network Attacks
- Enumerating Cellular Networks with SDR Devices

Module 4 –Web Application Attacks

- Introduction and OWASP Top 10
- Build a Proper State-of-Mind and Ask the Right Questions
- Using Burp Suite Web-Proxy for web vulnerability research
- Automate Web Attacks with Python

Module 5 –Hacking the Human in Cyber Crime Attack

- Social Engineering Techniques
- Making a Phishing Email with SET
- Creating a Malicious File with SET
- Creating and Delivering Malicious USB Card
- Learning Spear-Phishing Methods for VIP
- Gathering Emails and Phone Numbers with Maltego
- Looking for Secrets in Social Media with Online Tools
- Playing on Human Emotions and Weaknesses to Get the Information
- How to Hack Without Getting in Touch with a Target

INT

המרכז הבינלאומי
ללימודי הייטק וחדשנות

מתקדמים
לקריירה בהייטק

*6377

תל אביב
המרץ 2