Ethical Hacking

security seen from an offensive perspective

Gabriel Avramescu
OSCP, CEH, CHFI, ECSA, CEI, ISO 27001 Lead Auditor, CREST CRT, CCNA SECURITY
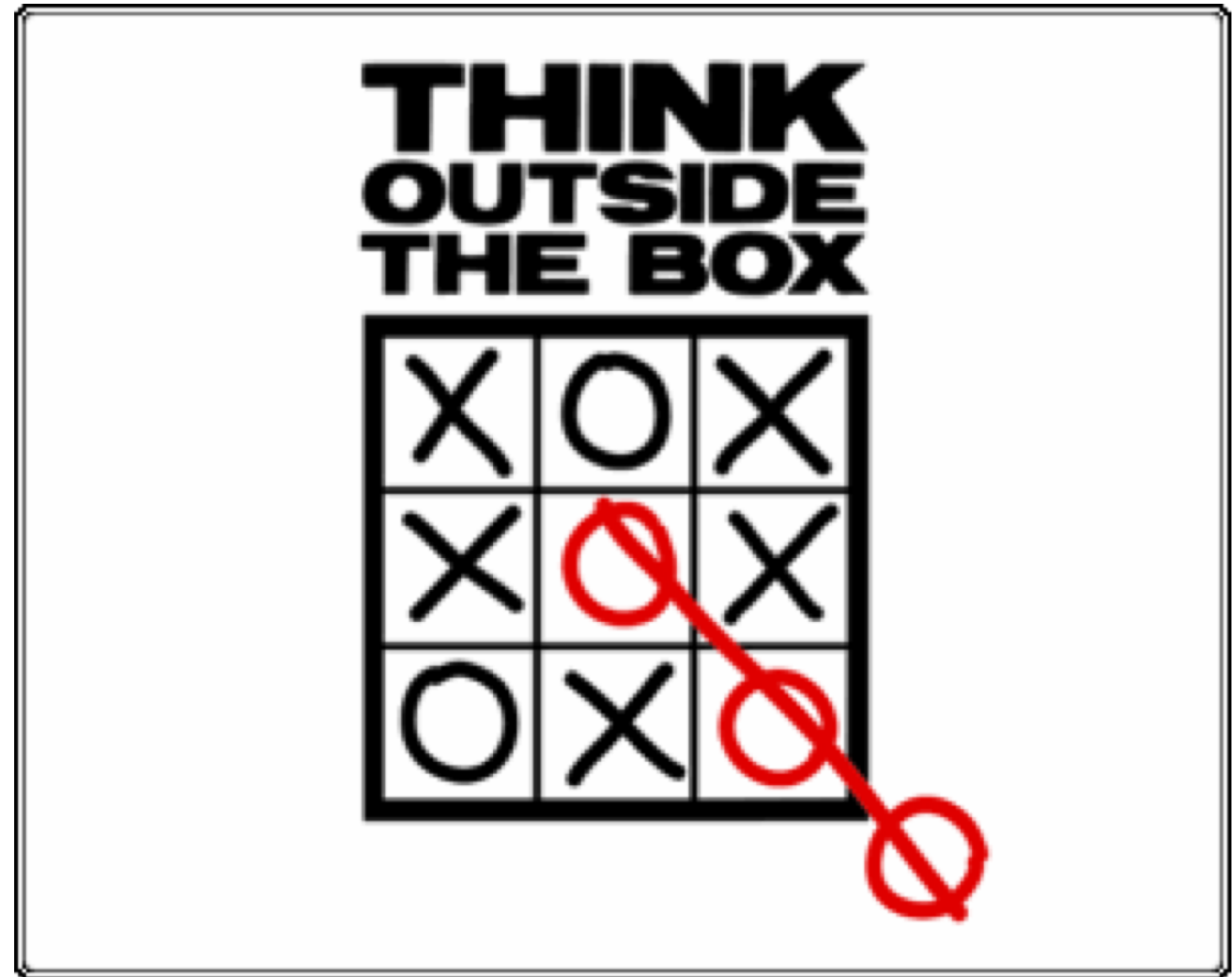www.ituniversity.ro

BEFORE TAKING THIS COURSE, STUDENTS SHOULD

- Basic Computer Networking, OS and Web concepts

Course learning objectives

- Develop "Out-of-box" thinking

- See security from an offensive perspective

Course learning modules

- Penetration testing overview

- Various types of footprinting, footprinting tools, and countermeasures

- Network scanning techniques and scanning countermeasures

- Enumeration techniques and enumeration countermeasures

- System hacking methodology

- Different types of Trojans, Trojan analysis, and Trojan countermeasures

- Packet sniffng techniques and how to defend against sniffing, session hijacking

- Social Engineering techniques, identify theft, and social engineering countermeasures

- Different types of webserver attacks, attack methodology, and countermeasures

- Different types of web application attacks, web application hacking methodology, and countermeasures

- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-security tools

- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools

Practice, practice, practice …

- Damn Vulnerable Web Application, WebGoat, Metasploit - Rings a bell?

- Networking, Metasploit demos- to see the importance of servers upgrade

- Attacker's mindset: "what an attacker would do?"

- Demos, demos, demos (practice vs theory)

About your trainer

- Gabriel Avramescu

- Penetration Tester and Security Consultant

- Trainer, Speaker

- Certifications: OSCP, CEH, CHFI, ECSA, CEI, ISO 27001 Lead Auditor, CREST CRT, CCNA SECURITY

- Email: gabriel.avramescu@ituniversity.ro

- Phone: +40 724 485985

Introductions

- Name

- Company

- Your job role

- Your current experience, certifications

- Do you meet the course prerequisites?

- What you expect from this class

Day 1

1. **Introduction to Ethical Hacking**

2. **Information Gathering - Footprinting, Reconnaissance**

3. **Scanning, Enumeration**

4. **System Hacking**

5. **Malware Threats**

6. **Sniffing and Session Hijacking**

*Each module include labs or demos

Day 2

7. Social Engineering

8. Hacking Web Applications and Web Servers

9. Cryptography

10. Hacking Wireless Networks

*Each module include labs or demos

Environment

Materials for:

- Theory

- **Practice**

- Videos

For labs virtual machine with:

- Two Virtual Machines

  - Kali Linux With Nessus

  - Metasploitable VM with different vulnerabilities

Administrative Items

- Course environment

- Materials in your student packet

- Lab exercise procedures

- Topics not on the agenda

- Evaluations

- Restrooms

- Fire exits

Logistics

Program: 09:00 – 17:00

Morning

- 10 minutes breaks

Lunch

- 1 hour

Afternoon

- 2 x 10 minutes breaks

THANK YOU!