TRAINING NAME: Computer security, the "Dark side" view

DURATION: 3 days (additional 2 days of hands-on only is available)

TRAINING OVERVIEW:

This course introduces participants to the world of ethical hacking. Training begins with the insight into the protocols, tools, networking, and common network, OS, and application attack vectors and then continues with additional lectures which provide attacker's and defender's point of view, including several attack demonstrations with detailed explanations. For the participants that would like to practice and further experience some of the topics, additional 2 days hands-on only training is available.

To understand the hacking and implications of it, risk management will be briefly discussed, as it is usually considered as foundation of security. Hacking phases will be reviewed, including the cyber kill chain and micro segmentation. Concept and usage of the penetration testing will be explained, as an important tool for corporate world to minimize the exposure to hacking. Participants will learn about networking protocols and MitM (Man-in-the-Middle) attacks, Windows authentication and Windows attacks, and Linux basics, authentication, and Linux attacks.

Course will be concluded with the introduction to web application security, WiFi security and respective hacking concepts. For those that would like to learn and explore more about web application security, five-day "Web application (in)security" training is a must.

KEY LEARNING OUTCOMES:

- Understand basic security concepts.
- Understand the importance of risk management in information and computer security.
- Understand the hacking phases and how to prevent the attacks by using the cyber kill chain.
- Understand what the penetration test is and how to utilize it in your environment.
- Understand basics of networking and networking protocols
- Understand the network and MitM attacks.
- Understand the Windows authentication and password storing.
- Understand the Windows password and other Windows attacks.
- Understand the Linux authentication and password storing.
- Understand the Linux password and other Linux attacks.
- Basic understanding of the web application attacks.

THIS TRAINING IS IDEAL FOR:

- Anyone interested in ethical hacking and computer/information security in general.
- Anyone interested in understanding network, Windows and Linux attacks and protection techniques.
- Software developers, DevOps specialists, security analysts, enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for secure development, deployment, maintenance, and security in general.

PREREQUISITES:

- Basic understanding of networking principles, architecture, and protocols is preferred but not mandatory.
- Basic understanding of Windows and Linux administration is preferred but not mandatory.

TRAINING AGENDA:

Security concepts – in this short, introductory module participants will learn about basic security concepts such as the CIA and DAD triangle, Defense in depth, etc.. Current risks and threats will be discussed too.

Essential terminology – in this module participants will learn more about essential security terms. That includes X-teaming (focusing on the blue/red/purple team) as well as the data protection concepts in all states (@rest, in-transit and in-use). Participants will also learn about zero-trust model and SDP (Software Defined Perimeter).

Risk management basics – In this module, basic risk management concepts will be reviewed, and qualitative and quantitative risk management process will be explained. Importance of the Risk management in the business environment will be covered, as well as the options for organizations to deal with the risks they are exposed due to the cyber threats. Additionally, the threat modeling will be introduced as a concept, including the GRC (Governance, Risk Management and Compliance), security policies and audits.

Hacking phases – participants will learn about hacking methodology (reconnaissance, scanning, gaining access, maintaining access, covering tracks). Attack demonstrations will provide 360-degree perspective on the hacking process, showing the initial compromise through vulnerable application, and then using the compromised computer as a pivot to compromise the entire organization including the AD (Active Directory).

Penetration testing – this module reviews the attacks conducted by professional penetration testers, including the penetration testing purpose and phases (they are slightly different from hacking phases, and yet, almost the same). Besides that, responsibilities of both the penetration testers and customers, including the risks that arise from conducting the penetration test, will be discussed. Anonymized penetration testing report will be shared with the delegates to provide an insight into the type of vulnerabilities that can be identified during the penetration testing projects.

Network basics and MitM attacks – participants will learn about the basic networking concepts required for understanding of the network sniffing and MitM attacks. The OSI and TCP/IP models will be discussed, and how the data is moving from one computer to another. It will be then followed by the insight into MitM attacks and respective entry points, like ARP spoofing (IPv4). During the attack demonstration, Wireshark and Network miner will be used to analyze the traffic, while Bettercap tool will be used to create the MitM attacks including the attacks on HTTPS protocol.

Authentication and Windows/Linux passwords attacks – Protocols, tools and techniques used for authentication and authorization on both, Windows and Linux, are in the focus of this module. Participants will learn how to create good passwords and how to crack the password using dictionary, brute force and pre-calculated hashes attacks. Authentication methods will be defined including the biometrics and dongle-based authentication. The structure of both, Windows and Linux password storing will be defined. During the attack demonstrations, participants will have an opportunity to learn how to reset domain administrator password, local Windows, and Linux passwords.

WEB application attacks – participants will learn about web technologies mostly used today and HTTP protocol. Some of the web application attacks will be reviewed too, like SQL injection, XSS, parameter tampering and directory traversal. Attack demonstrations will be performed using the tools like Burp and Zap. This module is an introduction to "Web application (in)security" course.

Wi-Fi attacks – Use of wireless connectivity is constantly increasing. However, networks are usually unsafe. This module covers Wi-Fi security concepts and options that are available to hack WEP, WPA, WPA2 and WPA3 protocols.

ABOUT THE TRAINER:



Robert Petrunić works as a senior information security consultant in Eduron IS, the company dedicated to IT security education, penetration testing and computer forensics.

Robert is Microsoft certified trainer since 2002, EC-Council certified trainer since 2008 and $(ISC)^2$ certified trainer since 2014. Today, he lectures mostly hacking and security related courses for red teams and DFIR (Digital Forensics and Incident Response) related courses for blue team members. Since 2004, he worked primarily in the security field, and Microsoft acknowledged this in 2008, by assigning him the most valuable Microsoft's professional recognition for nine years in a row.

For the last eighteen years Robert is working on programs related to ethical hacking and IT security awareness for systems administrators, developers, and IT security consultants. He is also often a lecturer at regional IT conferences.

Robert holds many industry certifications, such as $(ISC)^2$ CISSP and CCSP, Offensive Security OSCP, OSCE and OSWP, EC-Council CPENT, CEH, CHFI, CND, ECIH to name the few.