TRAINING NAME: Computer security, the "Dark side" view – (hands-on labs extension)

DURATION: 2 days

TRAINING OVERVIEW:

This entirely practical training is an extension of Computer security, the "Dark side" training, during which, participants will have the opportunity to practice and experience on their own, through hands-on labs, some of the attacks demonstrated during the previous lectures.

The main lab in this training is based on the real case and vulnerabilities identified during the penetration test engagement. It shows the process and steps that penetration tester used during the initial compromise and after it. Initial compromise is achieved by utilizing the vulnerability in MS Office and pivoting through the compromised computer to hack the entire domain. Participants will use *nmap*, Metasploit framework and *proxychains* as some of the tools, while social engineering, *footprinting*, password hash dumping, and PtH (Pass the Hash) attack will be some of the techniques that they will practice during the lab.

Participants will have the opportunity to exploit application vulnerable to Log4shell too, which is even today, in 2023., an issue for some organizations, as witnessed during the penetration testing engagements.

KEY LEARNING OUTCOMES:

- Utilizing the hacking phases to compromise vulnerable system.
- Apply the theoretical knowledge to attack Windows authentication and passwords by using multiple techniques.
- Usage of network mapping and attacking tools
- Understand how the hacking process works to be able to define and design better protections.

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:

- Computer security, the "Dark side" view – theory or equivalent knowledge

TRAINING AGENDA:

HoL 1 – 360 degree hacking view. Compromising the windows network behind the firewall. Firewall is fully closed from the outside. Initial foothold is provided by user clicking on the infected word document. Delegates will both create and open the document to understand the process and look and feel of the attack on the client's side. After that, participants will establish a pivoting point on the compromised machine, go through the reconnaissance to better understand the network that is surrounding the compromised computer and scan the network. Based on the scans, participants will compromise Windows print server, dump the password hashes from the computer memory, and use the PtH attack to compromise the domain controller. The full demo recording of the process will be provided together with the step-by step guide in the lab manual.

HoL 2 – Log4Shell vulnerability exists in one of the computers in the lab network. participants have to identify the right machine and compromise it. The full step-by-step guide is provided in the lab manual.

Hol 3 – these are the challenge labs – they differ from previous labs as there is only partial or no step-by step guide for the lab. Participants have to identify the vulnerabilities on their own. They will be also able to register for the trainer hosted online CTF where, providing them with additional opportunity to further brush their hacking experience.

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.