TRAINING NAME: Computer forensics as an IT asset

DURATION: 4 days

TRAINING OVERVIEW:

This training introduces participants to computer forensics and incident handing, being a hot topic, as a result of increasing number of security incidents caused by evolving and advanced threats faced by the businesses of all sizes. Training begins with the incident handling process overview to get understanding about the various activities that have to be undertaken to investigate and resolve the incident. Computer forensics is the integral part of incident handling process and highly important one, as incident responders need to understand all of the activities that attackers have undertaken to be able to properly contain their further activities and to eradicate them from the compromised IT environment. During the training, participants will learn the computer forensics basics and common tools being used by forensic specialists. While main focus of the training is on how to perform the investigation within corporate environment, evidence has to be presented sometimes in legal proceedings too – training covers guidelines for acquiring and handling the evidences properly, in case if they would need to be used for legal purposes.

Participants will learn about different storage and file system types and how to recover the data and deleted data from it in a forensically sound manner. Memory holds interesting data, like clear text passwords, password hashes, documents, and files. Participants will learn how to use tools to acquire, extract and analyze the computer memory contents. Training covers the steganography, which is interesting topic for most of the businesses because it is, among other things, used to exfiltrate the data in the industrial espionage. Then the network and log forensics will be covered, followed by encrypted data analysis, like EFS (Encrypted File system) file encryption and BitLocker full disk encryption.

Aside the labs, delegates will work on the forensic challenges too, to further reinforce the acquired knowledge.

KEY LEARNING OUTCOMES:

- Understand incident handling concepts and process.
- Understand the foundational concepts related to computer forensic.
- Understand the differences between various storage and file system types.
- Know how to create forensic image of a storage device and analyze it.
- Understand computer memory forensics process and challenges.
- Know how to extract and analyze the data from memory image.
- Understand the steganography, it's usage and analysis options.
- Understand the network and log analysis and it's usage in computer forensics.
- Understand the challenges related to encrypted data, like file and full disk encryption.
- Know how to decrypt EFS encrypted data with an access to a user profile.
- Know how to decrypt the BitLocker encrypted drives when default configuration is used.
- Reinforce the knowledge with hands-on experience.

THIS TRAINING IS IDEAL FOR:

- Anyone interested in computer forensics.
- 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 attacker's perspective" or similar knowledge.
- Advanced knowledge of the computer systems and various types of OS.
- Understanding basics of networking principles, architecture, and protocols is preferred.
- Understanding the basic usage and administration of Windows and Linux OS.

TRAINING AGENDA:

Incident management – participants will learn basics of incident handling based on NIST and ENISA recommendations. Incident handling process will be reviewed through its main stages, starting with activities that can be undertaken to properly prepare for the incident handling, how to identify incidents, how to stop the bleeding (isolate compromised systems), eradicate malware if needed, returning the system back in the production and finishing the hole process with the lessons learned.

About computer forensics – participants will learn basic concepts of computer forensics and the tools used for this purpose. Digital evidence and how to collect it, either for internal investigation or to be used in the legal proceedings will be covered in this module.

Data storage systems – in this module, data storage connector types and data storage types in general (HDD, SSD, optical media) will be reviewed.

File systems – participants will learn about mostly used filesystems like FAT32, NTFS and EXT4. Data recovery will be discussed and during the hand-on exercise, participants will recover deleted data by using standard undelete methods and by using file carving methods. It is recommended to bring used USB key to the class, so that one can try to identify which of the deleted files and folders are recoverable.

Memory forensics – with more advanced and smarter malware, it's becoming more and more difficult to identify how those programs infected the machine. Usually, the only trace they leave is waiting in the memory to be found. Delegates will have a chance to analyze the memory image of infected machine to answer the questions like when, how and through what infection path(s) the machine was compromised.

Steganography – one of the mostly used ways of hiding data from other users is steganography, process of hiding data inside another data. In this module participants will learn about different ways the steganography could be used in digital world, and how to hide the data inside another data.

Network logs forensics – almost each internal forensic analysis must deal with network log analysis. One of the mostly used free network analysis tools is Wireshark. In addition to Wireshark, Network miner tool will be covered too. Each of those tools has different usage during the network forensic investigation - it will be demonstrated live during this session.

EFS and BitLocker– Microsoft Encrypted File System (EFS) is a building block of NTFS file system, available since Windows 2000. This is file level encryption that uses PKI architecture to be as robust and tamper resistance, as possible. During forensic analysis, experts often have to decrypt various types of files including EFS encrypted files. In this module participants will learn about EFS inner workings, PKI architecture and how to break EFS encryption. BitLocker is Windows built-in full disk encryption technology. It is safe and robust if used properly. Unfortunately, default BitLocker installations are susceptible to hacking and simple decryption, which will be demonstrated in this module.

Forensics challenges – in this module, participants will have the opportunity to test their skills through the forensics challenges that will help them to further strengthen the newly acquired knowledge

from different fields like, steganography detection, EFS decryption, network logs analysis and various tools used during the training.

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.