ENISA CERT TRAINING

Tentative agenda for workshop

Supported and organised by: CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

TLP GREEN

AUGUST 2015

Tentative agenda for the ENISA CERT training workshop

4-6th August 2015

29 Raiņa bulvāris, CERT.LV, Riga, Latvia

To-do before the training:

1. Check if your laptop meets the following requirements:
   a. Computer that can run Virtual Images, by using either VirtualBox or a similar application
   b. The laptop should preferably have at least 4 GB of RAM, capable processor (i5 or i7), and at least 20 GB of free HD space
   c. You should be able to install applications and use USB memory sticks on your computer (preferably USB 3.0)

2. Download virtual images (Open virtualization format) from the following links.
   http://www.enisa.europa.eu/ftp/enisa-main.ova
   http://www.enisa.europa.eu/ftp/styx32.ova
   http://www.enisa.europa.eu/ftp/opsu-12-2-x86.ova

Load the images into the virtualisation environment and test if they work properly by powering them on.

More specific instructions and 'how-to' could be found here:
https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/virtual-image-how-to

Day 1 (4th August) Mobile forensics

START TIME	TITLE OF ACTIVITY	ORGANISER
09:00	Registration	
09:15	Seminar introduction and organization of the day	ENISA; Lauri Palkmets
09:30	**Mobile forensics**	ENISA; Yonas Leguesse
11:00	*Coffee break*	
11:15	**Mobile forensics**	ENISA; Yonas Leguesse
12.30	*Lunch break*	
13:30	**Mobile forensics**	ENISA; Yonas Leguesse
15:00	*Coffee break*	
15:15	**Mobile forensics**	ENISA; Yonas Leguesse
16:45	**Wrap up discussion; Q/A**	ENISA; Yonas Leguesse
17:00	*End of the training day*	

This course of mobile forensics is based on ENISA training material (https://www.enisa.europa.eu/activities/cert/training/training-resources/technical-operational#mobile_threats) and will introduce concepts, tools and techniques used for Mobile Incident Handling. The students will familiarise themselves with the risks found on Mobile platforms and also ways of identifying and mitigating such risks.

During the training participants will learn about different tools available for artifact analysis on the Android operating system. Using the provided virtual machine, the participants will be able to follow a hands-on tutorial.

Training objectives:

- Understand Mobile Platforms
- Familiarisation with tools related to Mobile Forensics
- Familiarisation with Mobile Applications
- Perform static mobile malware analysis
- Perform automated mobile malware analysis

Expected audience:

Incident handlers' with a good understanding of:

- Fundamentals of networking
- Basic Programming (Java)
- Basic analysis skills

Day 2 (5th August) Memory Forensics

START TIME	TITLE OF ACTIVITY	ORGANISER
09:00	Registration	
09:15	Seminar introduction and organization of the day	ENISA; Lauri Palkmets
09:30	**Memory forensics**	ENISA; Lauri Palkmets
11:00	*Coffee break*	
11:15	**Memory forensics**	ENISA; Lauri Palkmets
12.30	*Lunch break*	
13:30	**Memory forensics**	ENISA; Lauri Palkmets
15:00	*Coffee break*	
15:15	**Memory forensics**	ENISA; Lauri Palkmets
16:45	**Wrap up discussion; Q/A**	ENISA; Lauri Palkmets
17:00	*End of the training day*	

The course of Memory Forensics is based on ENISA training material (https://www.enisa.europa.eu/activities/cert/training/training-resources/technical-operational#identification_handling , https://www.enisa.europa.eu/activities/cert/training/training-resources/technical-operational#advanced_artifact) and will introduce concepts, tools and techniques used for Memory Forensics.

At the beginning, the trainer will introduce the basic concepts of memory forensics, such as acquisition of memory and its analysis. In the first part the participants will learn how to acquire memory images from Windows and Linux operating systems. During the second and third part, the students will perform basic analysis tasks while working with Windows and Linux memory dumps. Following the analysis tasks, the students are confronted with advanced analysis techniques, such as identifying and isolating a malware sample from a given memory image. Using the provided virtual machine, the participants will be able to follow a hands-on tutorial.

Training objectives:

- Familiarize with memory capture techniques and forensics
- Familiarisation with tools used for memory forensics
- Using memory captures to extract unpacked artifacts
- Perform malware analysis using memory dump

Expected audience:

Incident handlers' with a good understanding of:

- Fundamentals of operating systems (Linux, Windows)
- Basic analysis skills
- Basic understanding of malware analysis

Day 3 (6th August) Artifact analysis

START TIME	TITLE OF ACTIVITY	ORGANISER
09:00	Registration	
09:15	Seminar introduction and organization of the day	ENISA
09:30	**Artifact analysis**	ENISA; Razvan Gavrila
11:00	*Coffee break*	
11:15	**Artifact analysis**	ENISA; Razvan Gavrila
12.30	*Lunch break*	
13:30	**Artifact analysis**	ENISA; Razvan Gavrila
15:00	*Coffee break*	
15:15	**Artifact analysis**	ENISA; Razvan Gavrila
16:45	**Wrap up discussion and closing of the workshop**	ENISA; Lauri Palkmets
17:00	*End of the training day*	

The course of Artifact Analysis course is based on ENISA training material (https://www.enisa.europa.eu/activities/cert/training/courses#artifact) and will give the students an overview of the most common tools and methodologies used to perform malware analysis on artifacts, such as binary or documents, found on Windows systems. At the end of the session, students will learn how to configure an artifact analysis environment, store and process artifacts in order to extract host and network-based indicators from a malicious program using dynamic and static analysis techniques.

During the training participants will be presented on behavioural analysis concepts and how these can be used to analyse a sample's interaction with its environment. The training will provide use cases on when such techniques should be used and their limitations. The goal is to train analysts on the basic rules of safe malware analysis and extraction of useful evidence, as part of a forensics investigation. (Please note that malware reverse engineering is out of the scope for this training.)

Training objectives:

- Configure and prepare an artifact analysis environment
- Understand how static properties of suspicious programs can be used to detect malicious samples
- Perform behavioural analysis of malicious Windows executables using a sandboxed environment
- Extract actionable information out of a sample
- Understand the limitations of these techniques

Expected audience:

Incident handlers' with a good understanding of:

- Operating System Concepts
- Fundamentals of networking
- Basic research skills

Trainers:

Mr. Lauri Palkmets

Lauri Palkmets is an Expert in Computer Security and Incident Response at ENISA. At ENISA he has been improving and extending CERT training material, and providing technical trainings for EU Member States. Before joining the agency he was working for the Estonian Defence Forces as head of Cyber Incident Response Capability. Lauri Palkmets holds MSc in the area of Cyber Security from the Tallinn University of Technology and University of Tartu.

PGP Key ID: 0x490F50CF RSA 4096/4096
Fingerprint: 2054 FFAE DE3E 0278 6B04 F6B3 3A1B C911 490F 50CF

Mr. Yonas Leguesse

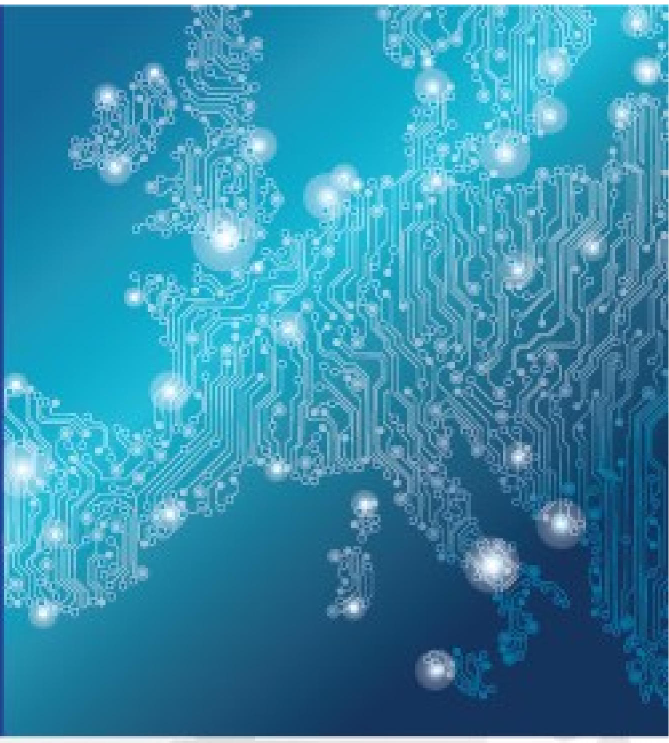
Yonas Leguesse is an Expert in Network and Information Security at ENISA. He is one of the latest additions to the Agency, providing training in various topics, focusing mainly on Mobile Technologies and Incident Handling. Before joining the agency he was working for The Malta Information Technology Agency, and formed part of the Information Security Department. He also has experience in a Law Enforcement Agency, and has a background in software development.

PGP Key ID: 0x57C9852C RSA 4096/4096
Fingerprint: A6A0 B8E3 19CF 1277 5E15 43CF 5B7F 9480 57C9 852C

Mr. Razvan Gavrila

Razvan Gavrila has been a Network and Information Security Expert for the European Union Agency for Network and Information Security since 2011. He is currently working under the Operational Security Unit, contributing to the Agency’s programs in the area of cyber crisis cooperation and exercises.

PGP KeyID: 0x98F70B2F
Fingerprint: 860F 511B 060C DB98 8A6D 1F77 12DB E74D 98F7 0B2F



ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu