A practical approach to network forensic, system forensic, memory forensic and data mining

Alexandre Dulaunoy and Raphael Vinot

Table of Contents

Courses at Université de Lorraine, MSSI 2016-2017.

> Feynman’s Maxim: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries.
>
> — Richard Feynman, Los Alamos

The courses are given by Alexandre Dulaunoy and Raphael Vinot.

Course Overview

Computer security incidents happen every day in small or large private or public organizations but also computer equipments used by citizen world wide. In case of incident, victims want to know what exactly happen to their systems, information to understand the impact on their organization or/and on their life. Security researchers need to analyse such compromised systems to better understand techniques, tactics and motivation of the attackers/adversaries.

The aim of the course is to provide a basic ground of all the techniques used in computer forensic and offer a toolbox to the student for their future activities in the computer security field.

The course includes a project to support or perform computer forensic to turn the theory into a practical session. The course requires a high involvement from the participants. **The course will be based on various datasets provided to the student at each session**. The datasets include network packet capture of a black-hole network until Today (which will be the core dataset for the sessions), a subset of potentially leaked information, a series of malware samples and threat-intel raw information.

With the respective datasets, student will learn the various techniques and tools used to process, analyze, review, classify and use them and finally benefit from those. The core objective is **learn techniques that will support day-to-day activities of analysts or incident responders**.

During the sessions, different programming techniques will be approach in order to support the analysis process of the datasets:

- **Parallel and basic distributed programming** (e.g. shared-memory data storage like Redis).
- **Data storage strategies** of network capture along with **the pitfalls of the respective analysis tools** (e.g. network forensic or analysis tools).
- Exchange data formats for supporting the **sharing information among security communities** (e.g. JSON-based formats to support threat-intel exchange).
- Evaluation of the data (e.g. validation of information gathered).

WARNING

Student will get access to real malicious data and information but also personal identifiable information (PII). A high level of ethic is required during his/her participation.

Project Detail

During the period of the course, there will be a specific project to realize. The project is fully integrated into the course sessions that means some topics covered will help to enhance or complete your work.

Project definition should be known for the 2017-02-05.

A project can be:

- A free software tool or extension to support forensic investigation (including network forensic, system forensic, malware analysis) or threat-intel
- A detailed and exhaustive analysis of computer evidences found in the wild

Project will be released under a free software license and using one of the following programming language: Python, Perl, Ruby, Go, Lua, Bash or Zsh. As the development of the project will be done on an operational system, the project along with its tools might evolve following the feedback received from the attackers themselves. The project can be an improvement to an existing free software security project including extensions, documentation, improvements or even bug fixes to computer forensic software. If you don't have any ideas, I'm sure we can find something in a world surrounded by information security issues, insecure technologies and potential innovative technical solutions (also sometime insecure).

A project can be also an analysis of specific evidences collected in the field (e.g. malware discovered, malicious website, hard-disks found in a recycling center) where you explain what you did as a forensic investigator.

You must also create a GitHub account where all your project including its documentation will be available (publicly) and release under a free software license.

Workstation Requirements During Classes

The major part of the work during the classes is a mixture of practical exercises, real-life experiments and sometime a kind of theory. The main requirement is that your workstation is an operational Unixbased system (e.g. a recent GNU/Linux distribution like Ubuntu 16.xx or a BSD flavor like OpenBSD or FreeBSD) with system administrator privileges.

Language

Courses will be given in French with the technical support being in English. Your project will be in English as your code and documentation will be available to the Internet community at large.

Evaluation

The evaluation will be mainly based on your project. **The evaluation is not an objective and the objective is to have fun while learning all together.**

Caveats

You may find that the subject very broad or even too complex. The objective is that you keep a focus on a specific aspect of computer forensic (network, system, malware analysis, data mining) to be used for your project. If you have any issue with the course (including the way I teach it), don't hesitate to talk about as early as possible.

Sessions

Date/Time/Where	Subjects and Supports	Additional Information and Dataset
20170114/9:00-13:00 @E116	* Introduction and Challenges in Incident Response * Darknet and Black Hole Monitoring a Journey into Typographic Errors	Blackhole dataset
20170121/9:00-13:00 @E116	* The Attackers' Principles The shortest, fastest and cheapest path : a common method for compromising information system * An introduction to network forensic - Courses notes 2016-2017	* Mirai Source code * Network pcap of the honeypot
20170128/9:00-13:00 @E116	* Classifying malware using network traffic analysis. Or how to learn Redis, git, tshark and Python in 4 hours.	* Sample set of pcap from malware executed in a sandbox - SHA1:5f5e931ec72b28fbdc7b733aaa1fe5cfc55c71b3 pcap_2012-09-16.zip * MalwareClassifier expected result after the session

20170204/9:00-13:00 @E116	* AIL Analysis Information Leak Framework	* 23.tar.gz SHA1: ad6763323ebb7e34f1cff97e7728d721ecab4d08
20170211/9:00-13:00 @E116	* Forensic Analysis The Treachery of Images	* sfsimage using squashfs to create forensic evidence container * SHA1 90b7e3f68eb91338b4adfb930f0c618514e83657 - raw.dd.raw (given during the session)
20170304/9:00-13:00 @E116	* An Introduction to Information Sharing using MISP * MISP Usage * MISP Administration	* VM of MISP 2.4.67 - SHA512 b01c771d6aa7dce52e0360e36fd369d184145513eedf647faef016c8f84500ae3e1200a7835dbb9e7ad0ad9c58b381de3acc49885f4a8e3920dfed14f6c4cec4
20170311/9:00-13:00 @E116	* PyCIRCLean: a versatile Python framework to check and/or sanitize files	* CIRCLean workshop * Project review
20170317/9:00-13:00 @E116	* An Introduction to Incident Detection and Response Memory Forensic Analysis	

Bibliography

- [SilenceWire] Michal Zalewski. 'Silence on the Wire, a Field Guide to Passive Reconnaissance and Indirect Attacks'. No Starch Press 2005. ISBN 1-59327-046-1.

- Know Your Enemy : Learning about Security Threats (2nd Edition) by Honeynet Project The (2004), Addison Wesley,ISBN:0321166469

- [ims] The Internet Motion Sensor: A Distributed Blackhole Monitoring System by M Bailey, E Cooke, F Jahanian, J Nazario, D Watson

- A Virtual Honeypot Framework by Niels Provos, USENIX Security '04 Paper

- Towards an estimation of the accuracy of TCP reassembly in network forensics by Gerard Wagener, Alexandre Dulaunoy and Thomas Engel. Published in FGCN (2) 2008: 273-278

- [InternetSinks] Yegneswaran, Vinod, Paul Barford, and Dave Plonka. 'On the design and use of Internet sinks for network abuse monitoring'. Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2004

Format

PDF document of this page