Cyber Threat Intelligence - an overview and practical approaches using open source security tools

Alexandre Dulaunoy and Raphael Vinot

Table of Contents

Courses at Université de Lorraine, M2SI 2017-2018.

> 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. But as digital forensic or incident response is no more a single-person work, a strong focus on information sharing and threat intelligence management will be done during the sessions.

The aim of the course is to provide a basic ground of all the techniques used in computer forensic, incident response, threat intelligence 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).

> ⚠ 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 2018-02-10.

A project can be in one of the following field:

- A free software tool or extension to support forensic investigation (including network forensic, system forensic, malware analysis) or threat intelligence relying on the MISP threat sharing platform.
- A specific model of analysis for gathering and/or review threat intelligence using the techniques seen during the session or improving existing techniques (e.g. improvement to MISP taxonomies classification, sharing models like MISP objects)

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 if this is a software implementation. The project can be an improvement to an existing free software security project including extensions, documentation, improvements or even bug fixes to open source security 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).

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 Unix-based system (e.g. a modern GNU/Linux distribution like Ubuntu or Debian GNU/Linux) with system administrator privileges. A virtual image will be used mainly for the MISP threat intelligence platform (e.g. virtual box or VmWare workstation).

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) and cyber threat intelligence 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

20170113/9:00-13:00 @UM-AN2-015	- Introduction and Challenges in Incident Response
	- Darknet and Black Hole Monitoring a Journey into Typographic Errors
	- An Introduction to Information Sharing and MISP the Threat Intelligence Platform
		- MISP virtual machines
		- MISP OSINT Feed
		`For the MISP web interface -> admin@admin.test:admin`
		`For the system -> misp:Password1234`

20170120/9:00-13:00 @UM-AN2-015		- 2017-12 - 1 month of pastes
20170127/9:00-13:00 @UM-AN2-015	- AIL - Analysis Information Leak - The Attackers' Principles The shortest, fastest and cheapest path : a common method for compromising information system	- A set of IoT malware targeting Linux

20170203/9:00-13:00 @UM-AN2-015	- Sample code for the workshop: Malware Classifier From Network Captures (git repository) - Classifying malware using network traffic analysis -Or how to learn Redis, git, tshark and Python in 4 hours.	- A set of pcap from malware executed in sandbox - Projects list
20170210/cancelled	- Forensic Analysis The Treachery of Images	- SHA1 90b7e3f68eb91338b4adfb930f0c618514e83657 - raw.dd.raw (given during the session)
20170217/9:00-13:00 @UM-AN2-015	- Python introduction - a bview analysis perspective	

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