An introduction to network forensic, system forensic, memory forensic and malware analysis

Alexandre Dulaunoy

Table of Contents

Course Overview 1
Project Detail 1
Operational Aspect 2
Workstation Requirements During Classes 2
Language 2
Evaluation 2
Caveats 3
Sessions 3
Bibliography 4
    Format 5

Courses at Université de Lorraine, MSSI 2014-2015.

> 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

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.

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 2014-12-05.

A project can be:

- A free software tool or extension to support forensic investigation
- 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.

Operational Aspect

The system to be used for the project is shared among the class including the system administration of the system. Security and system administration is part of the overall project. This includes adequate system administration, OpenSSH key management, logging management and security monitoring on wild Internet. Git will be extensively used during the courses.

You must also create a GitHub account where all your project including its documentation will be available (publicly).

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 recent GNU/Linux distribution like Ubuntu 14.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
2014-11-14 10:00 12:00 and 14:00 18:00 @ E116	* The Attackers' Principles The shortest, fastest and cheapest path: a common method for compromising information system * The Void An Interesting Place For Network Security Monitoring * Network forensic 101 TCP/IP pocket guide	pcap file 1 (MD5:65ca24413de7ab0ad6423ed2b6329056 - SHA1:5a012551c9c49815082a27f504430dd214c8610a) pcap file 2 (MD5:db066fcd23e505349978236de5fb8977 - SHA1:1740f89e9dafbde52b1f5005843d4e99932a66ed) - Dataset of 4257 pcap with network traffic from malware executed in a sandbox (given during the course) (MD5:992cb16347bb963242a18560892c4df2 SHA1:5f5e931ec72b28fbdc7b733aaa1fe5cfc55c71b3)
2014-11-21 10:00 12:00 and 14:00 18:00 @ E116	* Practical usage of network captures in incident response (TLP:GREEN) * Passive DNS - Using the DNS for fun and profit * Network Data Capture in Honeynets Berkeley Packet Capture (BPF) and Related Technologies : An Introduction * Notes from previous session	
2014-11-27 10:00 12:00 and 14:00 18:00 @ E116	* Passive DNS - Using the DNS for fun and profit	pcap - challenge - SHA1:b22995dae531f4a2ce69230f0cdc312bc4a08657

2014-12-13 09:00 13:00 @ E116	* Forensic Analysis - an Introduction * File System Forensic and Analysis	- Malware samples (1.3GB) - SHA1:f07daf26445fe599c1a91f728d46246fae0d9bf2 - Disk image (dd.e01) - SHA1:c40dc3f87f6d902ec7355348d85c52668ddcede5
2015-01-10 09:00 13:00 @ E116	* Classifying malware using network traffic analysis. Or how to learn Redis, git, tshark and Python in 4 hours.	* Malware Classifier From Network Capture code published after the workshop
2015-01-17 09:00 13:00 @ E116	* Classifying malware using network traffic analysis. Or how to learn Redis, git, tshark and Python in 4 hours. extension + project reviews	
2015-01-23 09:00 13:00 @ E116	* File System Forensic and Analysis using a write-blocker * Projects review	
2015-02-07 09:00 13:00 @ E116	* Memory acquisition and analysis * Lab memory analysis	
2015-02-28 09:00 13:00 @ E116	* Data Mining Pastes Finding a needle in a haystack How to analyze unstructured data sets?	* Dataset of pastes to be given during the lab * Project and exam review

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