CIRCL - Computer Incident Response Center Luxembourg

TRAINING AND TECHNICAL COURSES CATALOGUE 2014

from Incident Response to Operational Security

TLP:WHITE - version 201401

CIRCL
Computer Incident
Response Center
Luxembourg

INTRODUCTION

CIRCL offers courses to its members and organizations based in Luxembourg.

In our mission to improve information security, CIRCL is sharing its field experience through a set of training or technical courses. Due to diversity of competences within the CIRCL team, we are able to provide a large diversity of information security trainings. Courses target technical experts but also non-technical staff in the topic of incident handling, malware analysis, operational security and system forensic.

CIRCL sees the trainings and technical course as a great opportunity to also learn from the partners and to improve our security handling procedure. By attending the courses, partners are not only helping their own organization but also the overall security in Luxembourg (i.e. it is beneficial for the organization and CIRCL if the technical staff is prepared for Incident Response).

Courses can be held at CIRCL's training room or the premises of the organization unless specific requirements are noted.

Courses however have specific requirements in terms of technical equipment. These requirements are specified in the course description or will be specified before the course starts.

CIRCL provides these courses under tailored terms and conditions in order to fit your organizational structure. Don't hesitate to Contact us for more information.

CIRCL
Computer Incident
Response Center
Luxembourg

Contents

CIRCL
Computer Incident
Response Center
Luxembourg

INTRODUCTION TO INCIDENT RESPONSE

Title	Introduction to Incident Response
Abstract	Incident detection and response introduction theory and practical examples from concrete incidents. The training includes an overview of the most common type of incidents encountered in Luxembourg.
Goals	How are the majority of security incidents detected - How to secure evidences after detecting an incident - How to perform acquisition of evidences (file-system, memory and network) - How to interact with local CERTs and/or international CERTs - How to balance remediation with incident response
Who	IT department staff and manager - Local Incident Response Team
Level	IT support - basic knowledge of operating systems is required
Duration	3 hours
Language	English, French, German or Luxembourgish

CIRCL
Computer Incident
Response Center
Luxembourg

FILE-SYSTEM POST-MORTEM FORENSIC ANALYSIS

Title	File-system Post Mortem Forensic Analysis
Abstract	Forensic Analysis is based on the assumption that everything leaves a trace behind. A trace in an information system can be any data that helps to identify space and time actions. Post mortem analysis is a key tool to discover and analyse security incidents. This course will teach the participant on how to find answers to what has happened by analysing different layer from the physical medium to the file system up to the application level.
Goals	- Perform disk acquisition the right way - Introduce to file system analysis (NTFS/FAT) - Analyse operating system artifacts (MS Windows) - Find evidences in communication applications (e.g. browser or chat history)
Who	IT department staff - Local Incident Response Team
Level	Knowledge of operating systems and IT security is required
Duration	8 hours
Language	English, German

CIRCL
Computer Incident
Response Center
Luxembourg

DIGITAL PRIVACY SALON

Title	Digital privacy salon
Abstract	A digital privacy salon aims to present and explain how to use secure communication tools along with good Internet hygiene and understanding the associated risks.
Goals	Learning how to securely use: - Browsers (e.g. HTTPS, plugins, passwords, tracking, phishing) - Instant messaging (e.g. OTR, Cryptocat) - Emails (e.g. virus, spam, encryption) - Mobile devices (e.g. tracking, secure communication) - Disk encryption (e.g. FireVault, Bitlocker, LUKS, truecrypt) - Online and offline exchange of data (e.g. USB, Sharing platforms) - Network encryption (e.g. VPN, Tor)
Who	Citizens using IT equipment
Level	Beginner
Duration	2 hours
Language	English, French, Luxembourgish, German

CIRCL
Computer Incident
Response Center
Luxembourg

INTRODUCTION TO PENETRATION TESTING

Title	Introduction to Penetration Testing
Abstract	Besides classical security techniques like firewalls, VPN, AV among many others, offensive security is also a mandatory ability nowadays. This course gives an overview on how attackers prepare and execute a targeted attack. APT - Advanced Persistent Threats turn into the most critical risk for companies, today. This course will help the security responsible to see their corporate network from the attackers point of view and choose the necessary security mechanisms.
Goals	Learn to attack your network before others do
Who	IT security teams and administrators
Level	Good level of IT security
Duration	8 hours
Language	English, German

CIRCL
Computer Incident
Response Center
Luxembourg

INTRODUCTION TO (MALWARE) REVERSE ENGINEERING

Title	Introduction to (Malware) Reverse Engineering
Abstract	It is not unusual to detect unknown software on computer systems. Identifying if the software is malicious or benign is a critical (and expensive) task. This course aims to develop skills to perform basic Malware Reverse Engineering. The goal of this course is to set up a malware laboratory for each student and to get introduced into the most successful malware reverse engineering strategies.
Goals	- Get an overview of malware analysis techniques - Create a custom lab environment - Be able to collect indicators if a file is malicious or benign - Develop strategies to collect Indicators of Compromise (IOCs) - Build-up some solid grounds for further studies
Not in scope	- Learn x86 assembler - Get deep into reverse engineering
Who	Security Engineers, Administrators, Managers
Prerequisites	- Linux/UNIX experience - Good knowledge of Windows internals - Knowledge about control flows in programming languages - Understanding of TCP/IP networks, DNS, proxy, firewall - Very basic x86 assembler understanding is an advantage
Duration	16 hours or 24 hours
Language	English, German

CIRCL
Computer Incident
Response Center
Luxembourg

CONTACT

Postal Address

CIRCL - Computer Incident Response Center Luxembourg
c/o "security made in Letzebuerg" (SMILE) g.i.e.
41, avenue de la gare
L-1611 Luxembourg
Grand-Duchy of Luxembourg

Telephone

(+352) 247 88444

Email

info@circl.lu
PGP Fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5

CIRCL
Computer Incident
Response Center
Luxembourg