Course Description

Title: When You Look into the Black Mirror Who Is Looking Back?
Fields of activity: Applied Sciences , Computational Sciences , Computer Engineering , Computer Science/Automatic Control/Informatics , Control Engineering/Systems engineering , Economics/Business Administration/Marketing , Electrical/Electromechanical Engineering , Electronic/Electrotechnical Engineering , Industrial Engineering , Industrial Management , Mathematics
Examination type: Presentation
Number of ECTS credits issued: Not known yet
Learning Goals and Objective: The course provides an overview of the key concepts and challenges related to the incident response process in a big organization and how digital forensics can help an organization in an effective incident response. At the end of the course we expect participants to be able to explain how they can identify a potential attack, the possible impact on an organisation and how they can respond in such situations. The course will consist of lectures and practical parts including structured exercises where you will be an incident responder as well as digital forensic analyst.

BEST Copenhagen
Polyteknisk Forening
Anker Engelundsvej 1
DK-2800 Kgs. Lyngby

Tel/Fax: +45 77424405
E-mail: copenhagen@best.eu.org
www.BEST.eu.org/copenhagen

Syllabus

Name of activity	Incident Response
Number of working hours	4 hours
Type of activity	Lecture
Lecturer	Dheeraj Kumar Bansal
Short summary of content	Students are going to learn background and basics of the incident response process
Bibliography	N/A
Expected effect	Students will be able to apply incident handling processes-including preparation, identification, containment, eradication, and recovery-to protect enterprise environments

Name of activity	Digital Forensics
Number of working hours	4 Hours
Type of activity	Lecture
Lecturer	Dheeraj Kumar Bansal
Short summary of content	Students are going to learn basics of digital forensics
Bibliography	N/A
Expected effect	Students will be able to understand how digital forensics can be leveraged during an incident response process and what kind of information can be obtained using forensics

Name of activity	Linux and Forensics
Number of working hours	4 Hours
Type of activity	Lecture
Lecturer	Dheeraj Kumar Bansal
Short summary of content	Students will learn basic linux commands that can be used to perform forensics analysis
Bibliography	N/A
Expected effect	Students will understand how they can leverage linux tools to perform forensics analysis

Name of activity	Linux Basics
Number of working hours	2 Hours
Type of activity	Laboratory
Lecturer	Dheeraj Kumar Bansal, Johan Peder Møller, Per Andreas
Short summary of content	Students will solve challenges in an online lab
Bibliography	N/A
Expected effect	Students will get some practical knowledge of linux

Name of activity	CTF Challenge
Number of working hours	10 hours
Type of activity	Laboratory
Lecturer	Dheeraj Kumar Bansal, Johan Peder Møller, Per Andreas
Short summary of content	Students will take part in an online challenge
Bibliography	N/A
Expected effect	Students will use the knowledge from the lectures to solve the practical challenges and use the knowledge in their final project

Name of activity	Incident Response Case
Number of working hours	4 hours
Type of activity	Project Work
Lecturer	Dheeraj Kumar Bansal, Johan Peder Møller, Per Andreas
Short summary of content	Students will work on an Incident Response case in a group and prepare a final presentation for the exam
Bibliography	N/A
Expected effect	Students will use the knowledge from the lectures to work on the case and come up with a final presentation of their conclusions

Name of activity	Final Presentation
Number of working hours	2 Hours
Type of activity	Examination
Lecturer	Dheeraj Kumar Bansal, Johan Peder Møller, Per Andreas
Short summary of content	Students are going to present their project
Bibliography	N/A
Expected effect	Students in groups will do a small presentation of their project that they have been working on in the last 2 days.

Pre-materials

Name	SIFT Workstation
Topic/field	Digital Forensics
Short description	Use the link to install SIFT workstation. We are going to use it for the course lab exercises

Name	Intelligence Concepts—The SANS Incident Response Process
Topic/field	Incident Response Process
Short description	The article provides basics about the Incident Response Process

Name	Introduction to computer forensics
Topic/field	Digital Forensics
Short description	The article provides basics about the Incident Response Process

Name	UNIX Tutorial for Beginners
Topic/field	Unix and Linux Operating System
Short description	The article provides students with basic knowledge of Unix and Linux Operating Systems