

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3 COMMUNICATION AND COMPUTER TECHNOLOGY
Specialty: COMMUNICATION NETWORKS AND CYBERCRIME INVESTIGATION
Educational-qualification degree: MASTER

LEARNING COURSE DESCRIPTION

1.Course title: Linux Forensics

2.Course code: M.06.018.1

3.Type of the course: Compulsory

4.Level: Master

5.Year of study: second

6.Semester: third

7.Number of credits: 6

8.Name of the lecturer: Assoc. Prof. Dr. Eng. Pavlinka Radoyska, Stanislav Atanasov

9.Course learning outcomes:

The aim of the course is to cover basics of forensics gathering on Linux. How to determine timeline, how to trace issues and search for hidden clues in live or dead systems. It will start with basics understanding of Linux file systems and encryption and continue with more advanced topics like identifying backdoors and malwares.

Students completed their training in the discipline *should acquire:*

*Basic knowledge of forensics under *nix based OSes, chain of custody and gathering of provable information.*

Practical skills for gathering information and understanding of how to review and understand how given system works.

Competences: After completing the course the students will be able to:

- Understand how to review a system from forensics investigator role
- Use basic digital forensics tools to gather information
- Perform basic digital forensics investigations.

11. Prerequisites:

Basics knowledge of computer's hardware and software, Basics knowledge of Linux, Basics knowledge of networking.

12. Course contents:

Linux File Systems, LUKS, LVM. Building a toolbox and using netcat to minimize RAM impact. Collecting volatile data, determine if dead analysis is needed, dumping RAM. Getting the filesystem image. Analysing filesystem images – Mounting images. Analysing filesystem images – Recovering deleted files. Analysing filesystem images - The Sleuth Kit (TSK) and Autopsy. Analysing the timeline. Deeper dive in the Filesystem. Deeper dive in the Network.

13. Bibliography

Basic literature:

1. Practical Forensic Imaging, Bruce Nikkel, ISBN-13: 978-1-59327-793-2
2. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, ISBN: 978-1-118-82499-3
3. Kali Linux - An Ethical Hacker's Cookbook, Himanshu Sharma, ISBN: 978-1-787-12182-9
4. Digital Forensics and Incident Response, Gerard Johansen, ISBN: 978-1-787-28868-3

14. Assessment methods and criteria:

The course ends with an exam. In addition the performance of the student and the obtained notes during practical labs are taken into account.

15. Language of instruction: English