

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: Network Monitoring and Detection

2.Course code: M.06.016.1

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, ass. Eng. Pavel Bliznakov

9.Course learning outcomes:

The aim of the course is to familiarize UTP students with basic network metrics, configuration of network equipment and hosts to provide those metrics, configuration of monitoring platforms, packet inspection and forging techniques so they have a better insight of what an attacker might use packet encapsulation to force his traffic within the network, intrusion detection and malware interception. The students will be able to determine various types of malicious traffic and track its origins.

Students completed their training in the discipline should acquire:

Basic knowledge of network metrics interpretation; SNMP configuration and metrics extraction; configuration of monitoring tools to present the metrics in graphical form for long term or “post-mortem” analysis and scheduling alarms; inspect traffic content and forge network packets; use of honeypots to track attackers behaviour or intercept malware circulating in the network; detect botnet attacks and track their origins.

Practical skills for detecting malicious traffic and trace its origins.

Competences: Use tools such as netstat, nmap, tcpdump on a Linux system to monitor network traffic. Setup SNM service on switches, routers and Linux hosts to obtain various network interface metrics. Configure monitoring software such as Nagios and Cacti, respectively for active notifications and data analysis. Inspect network packets and force forged packets within a network. Deploy honeypots within a network to intercept malicious traffic and collect malware circulating within the network.

11. Prerequisites:

Basics of Programming, Operating Systems, Linux OS, Python programming, C programming.

12. Course contents:

Introduction to networks. Network monitoring tools in Linux - nmap, tcpdump. SNMP configuration on Linux hosts, switches, routers and metrics extraction. Monitoring with Nagios and Cacti. Network traffic capture with tcpdump and analysis with Wireshark. Forging packets and send them over the network. Methods for detecting malicious traffic. Using honeypots for detecting malicious traffic over the network. High-interactive honeypots. Low-interactive honeypots. Collecting malware with honeypots. Detecting that a given host is a honeypot. Definitions of bot and botnets. Determine the origin of botnets. Techniques for defence against bots and botnets.

13. Bibliography

Basic literature:

1. Niels Provost, Thorsten Holz, “Virtual Honeypots. From botnets tracking to intrusion detection” ISBN: 978-0-321-33632-1, Pearson Education Inc, 2008
2. Chris Sanders, Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis, ISBN-10 : 0124172083, ISBN-13 : 978-0124172081, Syngress, 2013

3. Slawek Ligus, Effective Monitoring and Alerting: For Web Operations, ISBN-10 : 1449333524, ISBN-13 : 978-1449333522, O'Reilly Media, 2012
4. Sause, Markus G. R. , Jasiūnienė, Elena, Structural Health Monitoring Damage Detection Systems for Aerospace, ISBN 9783030721923, 9783030721923, Springer, 2021
<https://library.oapen.org/handle/20.500.12657/50942>,

Additional literature:

1. Zhijiang Chen, Guobin Xu, Vivek Mahalingam, Linqiang Ge, James Nguyen, Wei Yu, Chao Lu, A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures, Big Data Research, Volume 3, 2016, Pages 10-23, ISSN 2214-5796

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.

The formation of the final assessment is formed by assessment from a test and assessment from ongoing control (points from the laboratory exercises, defense of individual developments and conducted control works for checking the theoretical and practical digestibility).

15. Language of instruction: English