	Cyber Security	Tutor	H	Data
10.04	Cloud Cyber Security	Ioan Constantin	3	Mi, 10.04.2019, 08:00-11:00
10.04	Anatomy of a Cyber Attack	Ioan Constantin	3	Mi, 10.04.2019, 11:00-14:00
11.04	Digital Forensics	Ioan Constantin	4	Jo, 11.04.2019, 08:00-12:00
11.04	APT Hunting using Machine Learning	Ioan Constantin	2	Jo, 11.04.2019, 12:00-14:00

	Cyber Security
10.04	Cloud Cyber Security (3H)
Tutor	Constantin Ioan
Date	10.04.2019
Time:	08:00 – 11:00
Requirements	Class-room video projector with HDMI input Class-room Wireless Internet Access

	Topic(s)	**Time**	**Notes**
1	**Concepts and Defintions** Moving our digital infrastructure to the cloud Cloud services and associated vulnerabilities Basic concepts: -Cyber Security perimeters -Physical Security perimeters -IaaS / SaaS vs. Datacenters and 'Hard Iron'	60	Presentation
2	**Scaling cyber security from LANs to the Internet** The impact of virtualization on cyber security -Hypervisor security -VM security -Containers -Open Stack and VMWare Expanding the security perimeter Future Networks Security -IoT and 5G IaaS and SaaS Challenges	60	Presentation -Definitions -Examples
3	**Public clouds vs. Private clouds** Securing the access points Securing the infrastructure	50	Presentation
4	**Q&A**	10	Open Questions

	Cyber Security
10.04	Anatomy of a Cyber Attack (3H)
Tutor	Constantin Ioan
Date	10.04.2019
Time:	11:00 – 14:00
Requirements	Class-room video projector with HDMI input Class-room Wireless Internet Access

	Topic(s)	**Time**	**Notes**
1	**Concepts and Defintions** What is a cyber attack? Understanding the motivation behind cyber attacks Vulnerabilities and exploits	20	Presentation
2	**Anatomy of a Cyber Attack** The four stages of a Attack: survey, delivery, breach, affect Types of attacks: active vs. passive, inside vs. outside Active attacks: -Denial of Service -Distributed Denial of Service -Spoofing -Network attacks (Man In The Middle, ARP poisoning, Floods) -Host-based attacks (Overflows: buffer, heap, stack) Passive attacks: -Network attacks (Wiretapping, Port&Idle Scanning) -Phishing -Spear-phishing -Social Engineering -Host-based attacks (Worms, viruses, Trojans)	120	Presentation -Definitions -Examples -Overview of tools used such as: exploit kits, botnets, botnet networks, Command and Control servers, vulnerabilities
3	**Examples of Cyber Attacks** -Stuxnet (2009-2011) -Mirai Botnet as a cloud-based attack	40	Presentation
4	**Q&A**	10	Open Questions

	Cyber Security
11.04	Digital Forensics (4H)
Tutor	Constantin Ioan
Date	11.04.2019
Time:	08:00-12:00
Requirements	Each student should have a working computer (Laptop or Workstation) running Microsoft Windows, Up-to-date Linux distributions or Mac OS. Each student shall have access to an Administrative account on their computer and shall have the possibility to install software Class-room video projector with HDMI input Class-room Wireless Internet Access

	Topic(s)	**Time**	**Notes**
1	**Concepts and Defintions** What is computer forensics? Why is it necessary? Use Cases and Regulatory	60	Presentation
2	**Investigation in data storage** Types of data storage Storage media Data: The basics Data: File Structures Data: File Formats Data: File Systems Metadata Cloud Data Logs Temporary data: caches, virtual memory, hibernation files	60	Presentation -Definitions -Examples
3	**Recovering information** -Using hardware and software tools	20	-Overview of tools -Key takeaways
4	**Hands-On Session** Students are provided with a packets capture file(s) and are tasked to find specific information within the file using the tools and technologies presented.	90	-Hands-On Lab
5	**Q&A**	10	Open Questions

	Cyber Security
11.04	APT Hunting Using Machine Learning (2H)
Tutor	Ioan Constantin
Date	11.04.2019
Time:	12:00 – 14:00
Requirements	Class-room video projector with HDMI input Class-room Wireless Internet Access

	Topic(s)	**Time**	**Notes**
1	**Introduction** What is an APT?	20	Presentation
2	**History** Coordinated attacks against infrastructure and large enterprises from the late 90’s up to 2019	20	Presentation
3	**APT Hunting** Known Unknowns and Unknown Unknowns Injection vectors APTs in stages Zero-Day Vulnerabilities and the inefficiency of legacy ‘signature-based’ detection Infrastructure Monitoring	40	
4	**Data Sets and Machine Learning** Behavior Analysis, Baselines and Anomaly detection (outliers) Using the Elastic Stack Data Sets Data Enrichment	30	Presentation
5	**Q&A**	10	Open Questions