

Network and Computer Security

SYLLABUS

I. IDENTIFICATION

Program: Computer Science		
Course: Network and Computer Security		
Class hours: 72 hours (4 local credits)	Academic year: 2023/1	Phase: Optative class
Professor: Charles Christian Miers		
Contact: charles.miers@udesc.br		

II. SUMMARY

Study of challenges related to security in computing environments. Study of solutions for security in software, operating system, and computer network, as well as studies of protection mechanisms, policies, security culture, and necessary actions in the face of attacks. Systems audit. Particular Aspects: Viruses, Frauds, Encryption, Unauthorized Access.

III. DIDACTIC PROGRAM

The class will cover, but is not restricted to, the following topics:

- Fundamentals of computer security
- Information security standards and procedures
- Cryptography: symmetric, asymmetric, hashes, and public key infrastructure
- Firewall, proxy, and VPN
- Malicious code and malware
- IDS/IPS and Honeypots
- Selected topics

IV. LEARNING METHODOLOGY

The learning methodology will consist of lectures, seminars, activities at both computer laboratories, and homework.

V. ASSESSMENT SYSTEM

The assessment will consist of quizzes and seminars with group presentation throughout the semester.

IV. BIBLIOGRAPHY

- Bishop, Matt. Computer Security: Art and Science. Boston, MA: Addison-Wesley, 2nd Edition. 2018.
- McLure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed 7: Network Security Secrets & Solutions: Network Security Secrets and Solutions. McGraw Hill. 2012.
- Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. Wiley. 2011.
- Stallings, William - Cryptography and Network Security: Principles and Practice. 8th Edition. 2020.
- Public and general security standards.
- Conference papers and scientific journals.
- Technical documents related to the area.