Plano de Ensino – 2025/2

Código	DCC831/DCC049/DCC030
Disciplina	TTECC: Cibersegurança
Turma	DCC 831/030/049
Professor	Michele Nogueira Lima

Ementa.

Conceitos e princípios de cibersegurança, diferenciação de segurança da informação e de redes, vulnerabilidades, principais ameaças e ataques de redes, Common Vulnerability Scoring System, Common Weakness Enumeration, Common Vulnerability & Exposure, mecanismos de filtragem de tráfego (firewall), VPN e protocolos de segurança, IPSec, IDS/IPS, SIEM, Monitoramento de redes, CERT, arquiteturas de segurança e aspectos metodológicos relacionados à segurança de redes.

Programa

Aula	Conteúdo previsto	Modalidade
1	Apresentação do curso	Presencial
2	Introdução à Cibersegurança. Principais conceitos. Principais ameaças e defesas.	Presencial
3	Reflections on Trusting Trust (atividade de participação)	Online
4	Atributos de segurança	Presencial
5	Criptografia - simétrica	Presencial
6	Criptografia - assimétrica	Presencial
7	Lab de classificação de vulnerabilidade	Online
8	Vulnerabilidades. Classificação de vulnerabilidade.	Presencial
9	Sistemas de gestão de identidades	Presencial
10	Princípios de Segurança de Redes	Presencial
11	Segurança de redes e mecanismos de filtragem	Presencial
12	Segurança da Internet, protocolos de segurança e IPSec	Presencial
13	Internet das Coisas, 5G e Cibersegurança	Presencial
14	Internet das Coisas, 5G e Cibersegurança (cont)	Presencial
15	Demonstração cibersegurança em raspberry PI	Presencial

16	Segurança da aplicação e princípios de desenvolvimento seguro	Presencial
17	Segurança da aplicação e princípios de desenvolvimento seguro (cont)	Presencial
18	Governança de cibersegurança e frameworks	Presencial
19	Virtualização e Segurança de Ambientes em Nuvem	Presencial
20	Predição de risco de vulnerabilidade	Presencial
21	CERT, IDS/IPS, SIEM, Monitoramento de redes	Presencial
22	CERT, IDS/IPS, SIEM, Monitoramento de redes (cont)	Presencial
23	Ética e responsabilidade em cibersegurança e LGPD	Presencial
24	Inteligência artificial em cibersegurança. SPAM e classificação de emails	Presencial
25	Reservada para preparação/apresentação de seminários	Presencial
26	Reservada para preparação/apresentação de seminários	Presencial
27	Reservada para preparação/apresentação de seminários	Presencial
28	Reservada para preparação/apresentação de seminários	Presencial
29	Reservada para preparação/apresentação de seminários	Presencial
30	Reservada para preparação/apresentação de seminários	Presencial

Bibliografia

Digital Security

Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, The Shellcoder's Handbook: Discovering and Exploiting Security Holes

Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications

Michael T. Goodrich & Roberto Tamassia, Introduction to Computer Security

Jon Erickson, Hacking The Art of Exploitation

Pfleeger and Pfleeger, Security in Computing

Ross Anderson, Security Engineering

Charu C. Aggarwal, Outlier Analysis

S1 [I/A] A Large-Scale Empirical Study of Security Patches
https://dl.acm.org/doi/abs/10.1145/3133956.3134072

S2 [I] VulPecker: an automated vulnerability detection system based on code similarity analysis
https://dl.acm.org/doi/abs/10.1145/2991079.2991102

S3 [I] Predicting Vulnerable Software Components via Text Mining
https://ieeexplore.ieee.org/document/6860243

S4 [I] Automated identification of security issues from commit messages and bug reports https://dl.acm.org/doi/abs/10.1145/3106237.3117771

S5 [I] Cross-Project Transfer Representation Learning for Vulnerable Function Discovery https://ieeexplore.ieee.org/document/8329207

S6 [I] VCCFinder: Finding Potential Vulnerabilities in Open-Source Projects to Assist Code Audits
https://dl.acm.org/doi/abs/10.1145/2810103.2813604

S7 [A] Learning to Catch Security Patches
https://arxiv.org/abs/2001.09148

S8 [I] When a Patch Goes Bad: Exploring the Properties of Vulnerability-Contributing Commits
https://ieeexplore.ieee.org/abstract/document/6681339

S9 [A] SPAIN: Security Patch Analysis for BinariesTowards Understanding the Pain and Pills
https://ieeexplore.ieee.org/abstract/document/7985685?casa_token=akhXG6WCyEAAAAA:4a9WpbBy-Lb6FOvUiHpXrq318PWPUIgQxuDWARVUE

gYbQlSqpvXJpKmg9JpilpegMiHmr pJXla0

S10 [A] Historical Analysis of Exploit Availability Timelines

https://www.usenix.org/system/files/cset20-paper-householder.pdf

S11 [A] Patch Based Vulnerability Matching for Binary Programs

https://dl.acm.org/doi/pdf/10.1145/3395363.3397361?casa_token=JaxScr

N2Ni8AAAAA:yq65mBxi72UD2gRDzJtL0ICFQJZIDOA8_xjuMiP0pgqQCzS7Lj

U6v8q O8SHxCCPr_jGBw33P9RWyzA

Avaliações

1	Projetos de Programação: 45 pts	15 pontos cada	presencial
2	Seminário: 30 pts	30 pontos	presencial
3	Leitura/participação: 25 pts	25 pontos	presencial