

Plano de Ensino – 2023/1

Código	DCC831
Disciplina	TTECC: Cibersegurança
Turma	N/A
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	Data	Conteúdo previsto	Modalidade
1		Apresentação do curso	Presencial
2		Introdução à cibersegurança. Black hats x White hats.	Presencial
3		Introdução à segurança da informação e segurança de redes	Presencial
4		Segurança da Internet	Presencial
5		Princípios da cibersegurança e principais frameworks de cibersegurança	Presencial
6		Principais ameaças e principais ataques de redes	
6		Vulnerabilidades	Presencial
7		Lab de Princípios de Segurança de Redes	Presencial
8		Introdução ao Common Vulnerability Scoring System - CVSS	Presencial
9		Mecanismos de filtragem	Presencial
10		Protocolos de segurança e IPSec	Presencial
11		Lab de classificação de vulnerabilidade	Presencial
12		Seminários	Presencial

13		Classificação de vulnerabilidade	Presencial
14		Lab de classificação de vulnerabilidade	Presencial
15		Seminários	Presencial
16		Predição de risco de vulnerabilidade	Presencial
17		Lab de previsão de risco de vulnerabilidade	Presencial
18		Seminários	Presencial
19		IDS/IPS, SIEM, Monitoramento de redes	Presencial
20		Lab de IDS/IPS	Presencial
21		Seminários	Presencial
22		CERT	Presencial
23		SPAM e classificação de emails	Presencial
24		Seminários	Presencial
25		Privacidade e Lei Geral de Proteção dos Dados	Presencial
26		Seminários	Presencial
27		Virtualização e Segurança de Ambientes em Nuvem	Presencial
28		Malwares e princípios de desenvolvimento de software seguro	Presencial
29		CERT, arquiteturas de segurança e aspectos metodológicos relacionados à segurança de redes	Presencial
30		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 Binaries Towards Understanding the Pain and Pills

https://ieeexplore.ieee.org/abstract/document/7985685?casa_token=akhXG6WCyEAAAAA:4a9WpbBy-Lb6FOvUiHpXrq318PWPUlgQxuDWARVUEgYbQlSqpVXJpKmg9JpilpegMiHmr 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=JaxScrN2Ni8AAAAA:yq65mBxi72UD2gRDzJtL0ICFQJZIDOA8_xjuMiP0pgqQCzS7LjU6v8q 08SHxCCPr_jGBw33P9RWyzA

Avaliações

1	Laboratórios: 30 pts	30 pontos	presencial
2	Seminários: 50 pts	50 pontos	presencial
3	Leitura/participação: 20 pts	20 pontos	presencial