Dados de identificacão

Disciplina	Computer Systems Security
Período Letivo	2021/1
Professor Responsável	Weverton Luis da Costa Cordeiro
Sigla	CMP230
Carga horária (horas)	4

Dados adicionais

Data efetiva de início	3 de agosto

(Art. 9o, §1o - O plano de ensino adaptado deverá refletir, no que couber, as datas efetivas de início e realização das atividades.)

Súmula

Princípios e fundamentos de segurança de sistemas computacionais: criptografia (tradicional e moderna), autenticação, autorização e auditoria. Segurança em redes de computadores e sistemas distribuídos. Políticas de segurança de sistemas computacionais.

(Art. 5o, §1o - A súmula, os conteúdos a serem abordados e os objetivos de aprendizagem não poderão ser modificados.)

Objetivos

Estudar segurança em três aspectos distintos da computação: segurança de dados, segurança em redes e segurança de computadores pessoais. Apresentar os principais tipos de ataques e as principais ferramentas utilizadas para sua prevenção. Permitir que o aluno compreenda e saiba analisar as características de um sistema de computação quanto a sua segurança.

(Art. 5o, §1o - A súmula, os conteúdos a serem abordados e os objetivos de aprendizagem não poderão ser modificados.)

Conteúdo Programático

Título	Conteúdo	Semana	Formato
Introdução	Introdução à disciplina. Propriedades de segurança da informação: confidencialidade, integridade, disponibilidade. Ataques de confidencialidade, integridade e disponibilidade. Princípios de segurança. Introdução à criptografia. Segurança de perímetro.	1	Remoto
Criptografia clássica	Criptografia tradicional: cifras de substituição, permutação, steganografia, de livro, máquinas de cifragem. Introdução à criptoanálise	2 e 3	Remoto
Cifras de Substituição	Tipos de cifras de substituição. Tipos de cifras de substituição polialfabéticas: Vigenère, AutoKey, Livro, Vernam. Cifras de transposição. Cifra de Beale, Playfair, Hill, ADFGVX. Introdução à Steganografia	4 e 5	
Cifras de Fluxo e de Bloco	Projeto de cifras de fluxo (stream) e de Bloco. Modos de operação. Vetor de Inicialização. Algoritmos de preenchimento (padding). Livro de Código Eletrônico (ECB). Encadeamento de Cifras de Bloco (CBC). Cipher Feedback (CFB). Output Feedback (OFB). Counter (CTR). Cifras de Substituição-Permutação. Confusão e Difusão. Cifra de Feistel. Cifras de Bloco Modernas	6 e 7	Remoto
DES	Data Encryption Standard (DES). Triple DES	8	Remoto
AES	Advanced Encryption Standard (AES). Projeto Rijndael	9	Remoto
Criptografia Assimétrica	Introdução à Criptografia Assimétrica. Criptografia de Chave Pública. Algoritmo RSA. Ataques. Diffie-Hellman, El Gamal, Curvas Elipticas	10	Remoto
Mecanismos de Autenticação	Funções Hash. Códigos de Autenticação de Mensagens. Assinaturas Digitais	11	Remoto
Segurança em Redes de Computadores	Segurança em Redes de Computadores	12 e 13	Remoto
Políticas	Políticas de Segurança	14 e 15	Remoto

(Art. 5o, §1o - A súmula, os conteúdos a serem abordados e os objetivos de aprendizagem não poderão ser modificados.) Ajustar a Selecionar o

Metodologia

Estratégias didáticas em atividades remotas	A disciplina será apresentada na forma de aulas teórico-práticas e pela execução de seminários com apresentação de tópicos relacionados ao curso pelos estudantes. A parte teórica será realizada através da apresentação de conceitos via videoaulas (formato assíncrono) e por leituras e exercícios recomendados. Os conceitos abordados na parte teórica serão complementados e reforçados por atividades e exercícios práticos, também em modo assíncrono. Tarefas de programação serão realizadas em linguagens de programação com compiladores e ferramentas disponíveis em código livre, código aberto, ou freeware. Todas as atividades serão propostas, entregues e avaliadas usando o Moodle da disciplina. Em caso de dúvidas, os alunos poderão contar com atendimento do professor, em momentos síncronos conforme cronograma a ser divulgado no Moodle no decorrer do semestre. Esses encontros poderão acontecer preferencialmente no horário regular da disciplina, a fim de evitar conflitos com outras atividades dos discentes.

(Art. 11 - Os Planos de Ensino adaptados poderão prever atividades síncronas e assíncronas. §1o – As atividades síncronas que visem

Estratégias didáticas em atividades presenciais	Não serão realizadas atividades presenciais.
Recursos disponibilizados	As atividades previstas, assim como as instruções para sua realização, serão disponibilizadas no Moodle Acadêmico da UFRGS em área associada à disciplina. Eventuais recursos adicionais como ferramentas de desenvolvimento, necessários à realização das atividades práticas, serão indicados no próprio Moodle através de links para download. Todos os softwares empregados serão livres de licenças comerciais (código aberto, código livre ou freeware). Também serão disponibilizados no Moodle, links para livros e artigos disponíveis via acesso online, e sem custos para os alunos, indicados para leitura e estudo, visando auxiliar na realização das atividades propostas.

(Art. 10 - Os planos de ensino adaptados deverão prever obrigatoriamente a utilização de um dos Ambientes Virtuais de Aprendizagem

Recursos computacionais	Para acompanhar as atividades previstas neste plano de ensino será necessário acesso regular à Internet. É necessário ainda um navegador web (browser) e de software que permita a leitura de arquivos PDF, assim como, softwares para a elaboração de documentos texto e planilhas eletrônicas. As atividades instrucionais assíncronas e síncronas (sessão de dúvidas) serão gravadas através de ferramentas de videoconferências e disponibilizadas no Moodle Acadêmico da UFRGS, e podem ser acompanhadas através de tablet, smartphone ou computador. Para atividades síncronas não é necessário o uso de câmeras. O endereço da sala virtual empregada para as eventuais sessões síncronas será fornecido no Moodle da disciplina. Para a realização das atividades práticas será necessário um computador pessoal com sistema operacional Linux (nativo ou em uma máquina virtual).
Carga Horária	
Teórica	40h
Prática	20h
Experiências de Aprendizagem	Os discentes serão estimulados a realizar as seguintes atividades de aprendizagem: 1) Visualização de videoaulas (modo assíncrono) seguido de leituras recomendadas que complementem e reforcem os conceitos apresentados nas videoaulas; 2) Implementação de trabalhos de programação; 3) Execução de listas de exercícios de fixação de conteúdo recomendadas; 4) Realização de atividades de verificação de aprendizagem dos conteúdos vistos até a data das mesmas.
Critérios de Avaliação	teóricos, esses serão realizados na forma de 2 atividades teóricas (AT) assíncronas referentes aos conteúdos desenvolvidos durante as várias etapas do semestre. Em relação a trabalhos práticos, esses consistirão na execução de dois trabalhos práticos (TP) e uma atividade de seminário (AS), a se realizado pelos estudantes (individualmente ou em grupo). As apresentações dos seminários acontecerão em seminários síncronos online. A médica final (M) será calculada da seguinte forma: M = 0,4 * (AT1 + AT2) + 0,4 * (AS) + 0,2 * (TP1 + TP2) A conversão da média numérica para conceito será feita da seguinte maneira: M >= 9,0 : Conceito A 9,0 > M >= 7,5 : Conceito B 7,5 > M >= 6,0 : Conceito C M < 6,0 : ver Atividades de Recuperação Será considerado aprovado o aluno que obtiver média final (MF) maior ou igual a 6,0. forma remota e assíncrona. §1º - A metodologia avaliativa remota a ser utilizada deve estar detalhada no Plano de Ensino adaptado. §2º - No
Atividades de Recuperação Previstas	Os discentes que não alcançarem média final para aprovação (M >= 6,0) poderão realizar uma atividade de recuperação teórica (RT) e/ou uma atividade de recuperação prática (RP), sobre qualquer dos conteúdos apresentados na disciplina. Essas atividades de recuperação serão realizadas de forma remota e assíncrona, nos mesmos moldes das atividades de verificação de aprendizagem executadas no decorrer do semestre. A nota da atividade de recuperação teórica (RT) substituirá 50% da nota M, correspondente aos exercícios teóricos. A nota da atividade de recuperação prática (RP) substituirá 50% da nota M, correspondente aos trabalhos práticos.
Bibliografia	Sem alterações Segue bibliografia complementar. F.L. Bauer. Decrypted Secrets - methods and maxims of cryptology, 2nd edition.Springer Verlag, 2001. Simon Singh. The Code Book. Ed. Doubleday, 1999 (tradução pela Ed. Record - O livro dos códigos) Gary, K.C. An Overview of Steganography for the Computer Forensics Examiner. 2004. Stallings W. Criptografia e Segurança de Redes. 2006 Paar C; Pelzl, J. Understanding Cryptography: A Textbook for Students and Practicioners. 2010. Goodrich, Michael T.; Tamassia, Roberto. Introdução à Segurança de Computadores. Porto Alegre: Bookman, 2013. 568p. domínio público ou ser disponibilizada pelo docente.)