MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO PARANÁ

SETOR DE CIÊNCIAS EXATAS

Departamento de Informática

Ficha 2 (variável)

Disciplina: Segurança Computacional	Código: CI1007
Natureza: (x) Obrigatória ( ) Optativa	(x) Semestral ( ) Anual ( ) Modular

Pré-requisito: CI1055 / CI1068 / CI1003 / CMA111 / CM304 / CI1056 / CI1210 / CI1001 / CMA211 / CM303 / CI1057 / CI1212 / CI1002 / CI1237 / CE009 /	Co-requisito:	Modalidade: (x) Presencial ( ) Totalmente EAD ( ) CH em EAD: _____

CH Total: 60 CH Semanal: 4	Padrão (PD): 44	Laboratório (LB): 16	Campo (CP): 0	Estágio (ES): 0	Orientada (OR): 0	Prática Específica (PE): 0	Estágio de Formação Pedagógica (EFP):

EMENTA

Conceitos básicos. Introdução à criptografia. Autenticação e controle de acesso. Segurança de sistemas e aplicações. Segurança em redes e na Internet. Auditoria. Gestão da segurança. Ética na computação. Computação e a sociedade. Politicas nacionais de segurança da informação.

PROGRAMA

1. Conceitos básicos: princípios e propriedades fundamentais para segurança computacional; ameaças, vulnerabilidades e ataques; base de computação confiável;
2. Introdução à criptografia: cifragem simétrica e assimétrica; hashes; assinaturas digitais; certificados; infraestruturas de chaves públicas;
3. Autenticação: local; em rede; distribuída;
4. Controle de acesso: políticas; modelos; mecanismos;
5. Segurança de sistemas e aplicações: ataques contra sistemas e mecanismos de defesa; segurança de sistemas; segurança em aplicações Web; desenvolvimento seguro;
6. Segurança em redes: filtragem de pacotes; firewalls; DMZ; ataques contra redes; protocolos de segurança;
7. Auditoria: logs; testes de invasão; detecção de intrusão; antivírus; análise de malware;
8. Gestão da segurança: normas e padrões; gerenciamento de vulnerabilidades; ética em segurança.

OBJETIVO GERAL

O aluno deve ser capaz de pensar criticamente sobre os problemas de segurança a que um sistema ou rede estão suscetíveis e soluções possíveis para mitigá-los. Deve também ser capaz de buscar formas de identificar ameaças e

vulnerabilidades, planejar a implementação de soluções para defesa e gerenciar o processo de manutenção de segurança.

OBJETIVO ESPECÍFICO

1. Entender o que é segurança computacional e os princípios fundamentais que norteiam a área;
2. Identificar ameaças, vulnerabilidades e ataques contra sistemas, redes e informação;
3. Aprender conceitos introdutórios sobre criptografia, mecanismos que a implementam e suas aplicações em segurança;
4. Compreender os mecanismos utilizados para prover autenticação e controle de acesso em sistemas e redes;
5. Estudar ataques clássicos e modernos de forma a entender como são feitos, que vulnerabilidades exploram e por que funcionam;
6. Conhecer o funcionamento dos mecanismos de defesa utilizados em sistemas e redes;
7. Instalar e configurar mecanismos de defesa tradicionais para analisar sua eficácia, eficiência e limitações;
8. Implementar ferramentas para varredura de vulnerabilidades, automatização de ataques e/ou detecção de ameaças;
9. Utilizar ferramentas (defensivas e ofensivas) para gerenciamento de vulnerabilidades em um sistema/rede: configuração, instalação, execução, atualização, monitoramento;
10. Conhecer as normas e padrões que regem a segurança da informação e estudar conceitos éticos sobre pesquisa, desenvolvimento e atuação na área.

PROCEDIMENTOS DIDÁTICOS

A disciplina será desenvolvida mediante aulas expositivas para apresentação dos conteúdos curriculares teóricos ou demonstrações feitas pelo professor, e através de atividades de laboratório nas quais as ferramentas e mecanismos serão implementados ou instalados, bem como avaliados na prática em ambiente controlado. Serão utilizados quadro branco, computador e projetor multimídia, computadores com sistema operacional GNU/Linux e ferramentas livres específicas para estudar cada conceito aplicável em laboratório.

FORMAS DE AVALIAÇÃO

- provas escritas abordando os tópicos teóricos;
- trabalhos de implementação/instalação/avaliação de técnicas e ferramentas de segurança;
- apresentação de seminários sobre temas atuais da área;
- A nota final é dada pela média simples das avaliações.

BIBLIOGRAFIA BÁSICA (mínimo 03 títulos)

1. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. 1a. edição. Wiley Publishing, 2001.
2. Willian Stallings. Criptografia e segurança de redes: princípios e práticas. 6a. edição. Pearson, 2015.
3. Emilio Nakamura e Paulo Lício de Geus. Segurança de redes em ambientes cooperativos. Novatec, 2010.

BIBLIOGRAFIA COMPLEMENTAR (mínimo 05 títulos)

4. Michael T. Goodrich e Roberto Tamassia. Introdução à Segurança de Computadores. Bookman, 2013.
5. David Kim e Michael G. Solomon. Fundamentos de segurança de sistemas de informação. LTC, 2014.
6. Mark Stamp e N. J. Hoboken. Information Security: Principles and Practice. Wiley-Interscience, 2006.
7. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. 2a ed. Wiley Publishing, 2008. ISBN : 9780470068526.
8. Matt Bishop. Computer Security: Art and Science. Addison-Wesley Professional, 2005.

**OBS: ao assinalar a opção CH em EAD, indicar a carga horária que será à distância.*

Documento assinado eletronicamente por **CARLOS ALBERTO MAZIERO**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 31/10/2018, às 06:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida aqui informando o código verificador **1304436** e o código CRC **10546D6A**.