IF68E: Segurança e Auditoria de Sistemas

- **Disciplina**: IF68E - Segurança e Auditoria de Sistemas
- **Carga Horária** (horas): teoria 60h, prática 00h, total 60h
- **Pré-requisito**: IF65D - Redes de Computadores 1
- **Professor**: Carlos A. Maziero

- Plano de aula 2014-2

Objetivos

Investigar as principais questões associadas à segurança de sistemas computacionais, bem como as técnicas e mecanismos usados para assegurar as propriedades de segurança; investigar os problemas de segurança computacional, bem como as técnicas e ferramentas disponíveis para mitigá-los. Proporcionar aos alunos conhecimentos em desenvolvimento de políticas de segurança e instalação, configuração e administração de produtos que auxiliem na manutenção dessas políticas.

Ementa

Auditoria de sistemas. Segurança de sistemas. Metodologia de auditoria. Análise de riscos. Plano de contingência. Técnicas de avaliação. Aspectos especiais: vírus, fraudes, criptografia, acesso não-autorizado.

Conteúdo

- **Conceitos básicos**: propriedades e princípios de segurança; ameaças; vulnerabilidades; ataques; tipos de malware; infraestrutura de segurança.
- **Fundamentos de criptografia**: cifragem e decifragem; criptografia simétrica; criptografia assimétrica; resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas.
- **Autenticação**: usuários e grupos; técnicas de autenticação: senhas, senhas descartáveis, desafio-resposta, certificados de autenticação, técnicas biométricas; Kerberos; infra-estruturas de autenticação.
- **Controle de acesso**: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias: matriz de controle de acesso, tabela de autorizações, listas de controle de acesso, listas de capacidades; políticas obrigatórias: modelo de Bell-LaPadula, modelo de Biba, categorias, políticas baseadas em domínios, políticas baseadas em papéis; mecanismos de controle de acesso: infra-estrutura básica, controle de acesso em UNIX, controle de acesso em Windows; outros mecanismos; mudança de privilégios.
- **Auditoria**: coleta de dados; análise de dados; auditoria preventiva; detecção de intrusão; metodologias de auditoria; análise de riscos; plano de contingência; ferramentas de auditoria.

Metodologia

- **Teoria**: aulas expositivas, com análise e discussão dos temas abordados e textos de apoio.
- **Prática**: atividades referentes aos temas abordados nas aulas teóricas (regras das atividades de laboratório).

Avaliação

```
float p1, p2 ;       // provas (bimestrais)
float t1, t2 ;       // trabalhos (médias bimestrais)
float m, freq ;      // média, frequência

m  = (p1 + t1 + p2 + t2) / 4 ;

printf ("%sprovado\n", freq < 0.75 ? "re" : m >= 6.0 ? "a" : "re") ;
```

Bibliografia

Básica:

- *Security in Computing, 4th Edition*. C. Pfleeger, S. Pfleeger. Ed Prentice-Hall, 2006.
- *Practical UNIX and Internet Security, 3rd Edition*. S. Garfinkel, G. Spafford, A. Schwartz. O'Reilly Media, 2003.
- *Information Security: Principles and Practice, 2nd Edition*. Mark Stamp. Ed. Wiley, 2011.
- *Segurança de Redes em Ambientes Cooperativos, 4a edição*. E. Nakamura, P. Geus. Ed. Novatec, 2007.

Complementar:

- *Security Engineering: A Guide to Building Dependable Distributed Systems (2nd edition)*. Ross Anderson. Ed. Wiley, 2008.
- *Handbook of Applied Cryptography*. A. Menezes, P. van Oorschot, S. Vanstone. CRC Press, 2001.
- *Applied cryptography: protocols, algorithms, and source code in C, 2nd edition*. B. Schneier. Ed. Wiley, 1996.

Outros recursos:

- Capítulo de livro sobre segurança em Sistemas Operacionais
- Sites interessantes em segurança de sistemas
- Página desta disciplina no Moodle
- Imagens de VMs do projeto SEED (cópia local)

Observações

- Podem ocorrer mudanças nesta página, com a devida divulgação prévia aos alunos.