IF68E - Plano de aula 2013/1

Aulas: quartas-feiras de 8h20 a 12h00, sala B-202

Calendário (podem ocorrer mudanças, com a devida divulgação prévia aos alunos):

Data	**5/6**	**12/6**	**26/6**	**3/7**	**10/7**	**31/7**	**7/8**	**14/8**
Aula	Aula 1	Aula 2	Aula 3	Aula 4	Aula 5	Aula 6	Aula 7	**Aula 8**
Prazo		A1			A3	A4	A7	
Data	**21/8**	**28/8**	**4/9**	**11/9**	**18/9**	**25/9**	**2/10**	**9/10**
Aula	Aula 9	Aula 10	Aula 11	Aula 12	Aula 13	Aula 14	**Aula 15**	Aula 16
Prazo				A9	A10	A11		A14

Obs: dia 19/6 não haverá aula (Semana Acadêmica de Informática e Eletrônica).

- As atividades indicadas com  serão avaliadas;
- Os arquivos deverão ser entregues através do Moodle, nas datas e horários indicados;
- Leia com atenção as Regras das Atividades de Laboratório.

Aula 1

- Apresentação da disciplina
- Conceitos básicos
- Sorteio de temas de Aspectos de Governança da Segurança
-  **Atividade 1**: Base de Vulnerabilidades

Aula 2

- Criptografia: cifragem e decifragem; criptografia simétrica; criptografia assimétrica.
- Vídeo: Public Key Cryptography: RSA Encryption Algorithm
- **Atividade 2**: cifradores

Aula 3

- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas
-  **Atividade 3**: Certificados digitais

Aula 4

- Autenticação: usuários e grupos; técnicas de autenticação; senhas; senhas descartáveis; desafio/resposta; certificados de autenticação.

-  **Atividade 4**: Quebra de senhas

Aula 5

- Autenticação: técnicas biométricas; Kerberos; infraestruturas de autenticação.
- Leitura: Introdução à Biometria. Costa et al, SBSeg 2006.
- ~~Atividade:~~ autenticação SSH por certificados
- **Atividade 5**: Experimento PAM Authentication do SEED Project (texto de apoio: PAM system administrator's Guide)

Aula 6

- ~~Estruturas de autenticação distribuída (OpenID, CardSpace, Shibboleth)~~
- Leitura: Gerenciamento de Identidades Federadas. Wangham et al, SBSeg 2010.
- **Atividade 6**: Desafio  : realizar o maior número possível de ataques na atividade TCP/IP attacks do projeto SEED!

Aula 7

-  **Atividade 7**: Aspectos de Governança da Segurança

Aula 8

- **Prova 1** (conteúdo do bimestre)
- **Defesa das atividades do bimestre**

Aula 9

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis.
- Sorteio das demonstrações de ataques
- **Atividade 8**: Experimento Same-Origin Policy do SEED Project

Aula 10

- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows; outros mecanismos; mudança de privilégios.
-  **Atividade 9**: Experimento Set-UID Program Vulnerability do SEED Project

Aula 11

- Leitura preparatória:
  - Smashing the Stack for Fun and Profit, Aleph One, 1996
  - Smashing the Stack in 2010, Graziano & Cugliari, 2010

    - Smashing the Stack in 2011, Makowski, 2011
- **Atividade 10**: Experimento Buffer overflow vulnerability do SEED Project
- No relatório, descreva as atividades efetuadas e explique como funcionam os seguintes mecanismos de proteção:
    - Técnica ASLR (*Address Space Layout Randomization*)
    - Bit NX (*No eXecute bit*)
    - Proteção de pilha oferecida pelo compilador GCC
    - Proteção de execução SUID oferecida pelo shell `bash`
    - Proteção de execução SUID oferecida pela montagem de partições (comando `mount`)

Aula 12

- **Atividade 11**: Experimento Capability exploration do SEED Project.

Aula 13

- Auditoria: coleta de dados; análise de dados; auditoria preventiva
- **Atividade 12**: Explorando sistemas de logs

Aula 14

- **Atividade 13**: Ferramentas de auditoria

Aula 15

- **Prova 2** (conteúdo do bimestre)
- **Atividade 14**: demonstrações de ataques

Aula 16

- **Atividade 14**: demonstrações de ataques (cont.)
- Apresentação da prova
- **Defesa das atividades do bimestre**