

# 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):

|              |                        |                         |                         |                         |                         |                         |                        |                         |
|--------------|------------------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|------------------------|-------------------------|
| <b>Data</b>  | <b>5/6</b>             | <b>12/6</b>             | <b>26/6</b>             | <b>3/7</b>              | <b>10/7</b>             | <b>31/7</b>             | <b>7/8</b>             | <b>14/8</b>             |
| <b>Aula</b>  | <a href="#">Aula 1</a> | <a href="#">Aula 2</a>  | <a href="#">Aula 3</a>  | <a href="#">Aula 4</a>  | <a href="#">Aula 5</a>  | <a href="#">Aula 6</a>  | <a href="#">Aula 7</a> | <b>Aula 8</b>           |
| <b>Prazo</b> |                        | A1                      |                         |                         | A3                      | A4                      | A7                     |                         |
| <b>Data</b>  | <b>21/8</b>            | <b>28/8</b>             | <b>4/9</b>              | <b>11/9</b>             | <b>18/9</b>             | <b>25/9</b>             | <b>2/10</b>            | <b>9/10</b>             |
| <b>Aula</b>  | <a href="#">Aula 9</a> | <a href="#">Aula 10</a> | <a href="#">Aula 11</a> | <a href="#">Aula 12</a> | <a href="#">Aula 13</a> | <a href="#">Aula 14</a> | <b>Aula 15</b>         | <a href="#">Aula 16</a> |
| <b>Prazo</b> |                        |                         |                         | 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**

From:  
<https://wiki.inf.ufpr.br/maziero/> - **Prof. Carlos Maziero**

Permanent link:  
[https://wiki.inf.ufpr.br/maziero/doku.php?id=sas:plano\\_de\\_aula\\_2013-1](https://wiki.inf.ufpr.br/maziero/doku.php?id=sas:plano_de_aula_2013-1)

Last update: **2013/10/14 14:01**

