

IF68E - Plano de aula 2014/1



- As atividades indicadas com  serão avaliadas;
- Os arquivos deverão ser entregues através do [Moodle](#), nas datas indicadas (até às 23:55); entregas atrasadas são feitas por e-mail;
- Leia com atenção as [Regras das Atividades de Laboratório](#).

Aula 1: 10/4

- Apresentação da disciplina
- Conceitos básicos

Aula 2: 11/4

- Conceitos básicos (cont.)
- Sorteio de temas de [Aspectos de Governança da Segurança](#)
-  **Atividade 1:** [Base de Vulnerabilidades](#) (prazo: aula 4 aula 6)

Aula 3: 24/4

- Criptografia: cifragem e decifragem; criptografia simétrica; criptografia assimétrica.
- Leitura complementar: [Algoritmo de troca de chaves de Diffie-Hellman](#)
- Vídeo: [Public Key Cryptography: RSA Encryption Algorithm](#)

Aula 4: 25/4

- **Atividade 2:** [cifradores](#)

Aula 5: 8/5

- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas

Aula 6: 9/5

-  **Atividade 3:** [Certificados digitais](#) (prazo: aula 10)

Aula 7: 15/5

- Autenticação: usuários e grupos; técnicas de autenticação; senhas; senhas descartáveis;

desafio/resposta; certificados de autenticação.

Aula 8: 16/5

-  **Atividade 4:** [Quebra de senhas](#) (prazo: aula 12)

Aula 9: 22/5

- Autenticação: técnicas biométricas; Kerberos.
- Leitura: [Introdução à Biometria](#). Costa et al, SBSeg 2006.
- ~~Atividade:~~ [autenticação SSH por certificados](#)

Aula 10: 23/5

- Autenticação: infraestruturas de autenticação.
- **Atividade 5:** Experimento [PAM Authentication](#) do [SEED Project](#) (texto de apoio: [PAM system administrator's Guide](#))

Aula 11: 29/5

- Overview sobre autenticação distribuída (OpenID, CardSpace, Shibboleth, SAML, SPKI/SDSI, OAuth, PGP Web of Trust) (apresentações de 10 minutos cada)
- Leitura: [Gerenciamento de Identidades Federadas](#). Wangham et al, SBSeg 2010.

Aula 12: 30/5

-  **Atividade 7:** [Aspectos de Governança da Segurança](#) (prazo: aula 13)

Aula 13: 5/6

- Aspectos de Governança da Segurança (cont.)

Aula 14: 6/6

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

Recesso: de 12/6 a 12/7

Aula 15: 17/7

- Apresentação da prova
- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias.

Aula 16: 18/7

- Sorteio das [demonstrações de ataques](#)
- Controle de acesso: políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis.
- **Atividade 8:** Experimento [Same-Origin Policy](#) do [SEED Project](#) (leia com **muita atenção** a seção 3 do documento)
- Leitura: [Attribute-Based Access Control](#) (NIST)

Aula 17: 24/7

- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows; mudança de privilégios.

Aula 18: 25/7

- Credenciais de processo em UNIX: [credentials.c](#)
-  **Atividade 9:** Experimento [Set-UID Program Vulnerability](#) do [SEED Project](#) (prazo: aula 24)

Aula 19: 31/7

- Atividade 9 (cont.)

Aula 20: 1/8

-  **Atividade 10:** Experimento [Buffer overflow vulnerability](#) do [SEED Project](#) (prazo: aula 26)
- Leitura preparatória:
 - [Smashing the Stack for Fun and Profit](#), Aleph One, 1996 ([versão PDF](#))
 - [Smashing the Stack in 2010](#), Graziano & Cugliari, 2010
 - [Smashing the Stack in 2011](#), Makowski, 2011
- [Buffer overflow - informações adicionais](#)
- 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 21: 7/8

- Atividade 10 (cont.)

Aula 22: 8/8

- Atividade 10 (cont.)

Aula 23: 14/8

- **Atividade 11:** Experimento [Capability exploration](#) do [SEED Project](#) (prazo: aula 28)

Aula 24: 15/8

- Atividade 11 (cont.)

Aula 25: 21/8

- Auditoria: coleta de dados; análise de dados; auditoria preventiva.
- **Leitura complementar:** [NIST Guide to Intrusion Detection and Prevention Systems \(IDPS\)](#), NIST Special Publication 800-94, 2007.

Aula 26: 22/8

- **Atividade 12:** [Explorando sistemas de logs](#)

Aula 27: 28/8

- **Atividade 13:** [Ferramentas de auditoria](#)

Aula 28: 29/8

- **Prova 2** (conteúdo do bimestre)

Aula 29: 4/9

- **Atividade 14:** [demonstrações de ataques](#) (prazo: aula 31, **peso 2**)

Aula 30: 5/9

- Demonstrações de ataques (cont.)

Aula 31: 11/9

- Demonstrações de ataques (cont.)

Aula 32: 12/9

- 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_2014-1

Last update: **2014/08/01 16:43**

