

IF68E - Plano de aula 2014/2



- 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: 25/9

- Apresentação da disciplina
- Conceitos básicos

Aula 2: 26/9

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

Aula 3: 2/10

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

Aula 4: 3/10

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

Aula 5: 9/10

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

Aula 6: 10/10

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

Aula 7: 16/10

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

Aula 8: 17/10

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

Aula 9: 23/10

- Autenticação: técnicas biométricas; Kerberos.
- Leitura: [Introdução à Biometria](#). Costa et al, SBSeg 2006.
- **Atividade 5:** [autenticação SSH por certificados](#)

Aula 10: 24/10

- Autenticação: infraestruturas de autenticação.
- **Atividade 6:** Experimento [PAM Authentication](#) do [SEED Project](#) (texto de apoio: [PAM system administrator's Guide](#))
- Sortear apresentações da próxima aula

Aula 11: 30/10

- **Atividade 7:** Overview sobre infraestruturas de autenticação em rede (SASL, CHAP, EAP, RADIUS, SRP, LDAP, SAML) ou distribuída (OpenID, CardSpace, U-Prove, Shibboleth, SPKI/SDSI, OAuth, PGP Web of Trust); apresentações de 10 minutos cada, em grupos de 2 alunos.
- Leitura: [Gerenciamento de Identidades Federadas](#). Wangham et al, SBSeg 2010.

Aula 12: 31/10

- Overview sobre autenticação distribuída (cont.)
-  ~~**Atividade 7:**~~ [Aspectos de Governança da Segurança](#) ~~(prazo: aula 13)~~ (retirei esta atividade por causa da semana de informática)

Aula 13: 6/11

- Semana de Informática (atividades extraclasse)

Aula 14: 7/11

- Semana de Informática (atividades extraclasse)

Aula 15: 13/11

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

Aula 16: 14/11

- **Prova 1** (conteúdo do bimestre)

Aula 17: 21/11

- Controle de acesso: políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis.
- Leitura: [Attribute-Based Access Control](#) (NIST)
- Sorteio das [demonstrações de ataques](#)

Aula 18: 27/11

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

Aula 19: 28/11

- Apresentação da prova
- Defesa das atividades do bimestre

Aula 20: 4/12

- **Atividade 8:** Experimento [Same-Origin Policy](#) do [SEED Project](#) (leia com **muita atenção** a seção 3 do documento)

Aula 21: 5/12

-  **Atividade 9:** Experimento [Set-UID Program Vulnerability](#) do [SEED Project](#) (prazo: 1/3)
- Credenciais de processo em UNIX: [credentials.c](#)

Aula 22: 11/12

-  **Atividade 10:** Experimento [Buffer overflow vulnerability](#) do [SEED Project](#) (prazo: 1/3)
- 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 23: 12/12

- Atividade 10 (cont.)

Aula 24: 18/12



- **Atividade 11:** Experimento [Capability exploration](#) do [SEED Project](#) (prazo: 1/3)

Aula 25: 19/12

- Atividade 11 (cont.)

Recesso: de 23/12/14 a 31/1/15

Aula 26: 5/2

- 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 27: 6/2

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

Aula 28: 12/2

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

Aula 29: 13/2

- Ferramentas de auditoria (cont.)

Aula 30: 19/2



- **Atividade 14:** [demonstrações de ataques](#) (**peso 2**, prazo: PDFs até dia 4/3)
- Grupos 3, 13, 14, 17.

Aula 31: 20/2

- **Prova 2** (conteúdo do bimestre)

Aula 32: 26/2

- Demonstrações de ataques (cont.)
- Grupos 1, 5, 9, 12.

Aula 33: 27/2

- Demonstrações de ataques (cont.)
- Grupos 2, 4, 7, 11.

Aula 34: 5/3

- Demonstrações de ataques (cont.)
- Grupos 6, 8, 10, 15, 16.

Aula 35: 6/3

- 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_2014-2

Last update: **2015/02/14 23:20**

