IF68E - Plano de aula 2013/2



- 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: 31/10

- Apresentação da disciplina
- Conceitos básicos

Aula 2: 01/11

- Conceitos básicos (cont.)
- Sorteio de temas de Aspectos de Governança da Segurança

Aula 3: 07/11

- **Atividade 1**: Base de Vulnerabilidades (prazo: aula 7)

Aula 4: 08/11

- Criptografia: cifragem e decifragem; criptografia simétrica; criptografia assimétrica.
- Vídeo: Public Key Cryptography: RSA Encryption Algorithm
- Leitura complementar: Algoritmo de troca de chaves de Diffie-Helmann

Aula 5: 14/11

- **Atividade 2**: cifradores

Aula 6: 21/11

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

Aula 7: 22/11

- **Atividade 3**: Certificados digitais (prazo: aula 11)

Aula 8: 28/11

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

desafio/resposta; certificados de autenticação.

Aula 9: 29/11

- **Atividade 4**: Quebra de senhas (prazo: aula 13)

Aula 10: 05/12

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

Aula 11: 06/12

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

Aula 12: 12/12

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

Aula 13: 13/12

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

Aula 14: 19/12

- Aspectos de Governança da Segurança (cont.)

Aula 15: 20/12

- **Prova 1** (conteúdo do bimestre)

Recesso: 21/12 a 19/1

Aula 16: 23/1

- **Defesa das atividades do bimestre**

Aula 17: 24/1

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis.

Aula 18: 30/1

- Sorteio das demonstrações de ataques
- Aspectos de Governança da Segurança (cont.)
- 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.

Aula 19: 31/1

- Controle de acesso (cont).

Aula 20: 06/2

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

Aula 21: 07/2

- **Atividade 8** (cont.)

Aula 22: 13/2

- **Atividade 9**: Experimento Set-UID Program Vulnerability do SEED Project (prazo: aula 27)

Aula 23: 14/2

- **Atividade 11**: Experimento Capability exploration do SEED Project (prazo: aula 29)

Aula 24: 20/2

- *Buffer Overflow Attack* - 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

Aula 25: 21/2

- **Atividade 10**: Experimento Buffer overflow vulnerability do SEED Project (prazo: aula 33)
- 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 26: 27/2

- 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: 28/2

- **Atividade 12**: Explorando sistemas de logs

Aula 28: 6/3

- **Atividade 13**: Ferramentas de auditoria

Aula 29: 7/3

- Ferramentas de auditoria (cont.)

Aula 30: 13/3

- **Prova 2** (conteúdo do bimestre)

Aula 31: 14/3

- **Atividade 14**: demonstrações de ataques (prazo: aula 33)

Aula 32: 20/3

- Demonstrações de ataques (cont.)

Aula 33: 21/3

- Demonstrações de ataques (cont.)

Aula 34: 27/3

- 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_2013-2

Last update: **2014/03/07 16:49**