CI1007 - Cronograma 2019/2

- As atividades indicadas com  serão avaliadas;
- Os projetos devem ser entregues usando o Moodle.
- Leia com atenção as Regras das Atividades de Laboratório.

7/8: Aula 1

- Apresentação da disciplina
- Conceitos básicos

- Leitura complementar:
  - Computer security, C. Landwehr, 2001
  - Basic Concepts and Taxonomy of Dependable and Secure Computing. A. Avizienis et al, 2004
  - A Review of Information Security Principles, 1997

9/8: Aula 2

- Criptografia: conceitos básicos; algoritmos simétricos
- Atividade em sala sobre cifradores simétricos
-  Atividade: Base de Vulnerabilidades (prazo: aula 4)

14/8: Aula 3

- Criptografia: algoritmos assimétricos
-  Atividade: O algoritmo RSA (não precisa fazer o 3.6) (prazo: aula 7)

- Conteúdo complementar:
  - Video: Acordo de chaves de Diffie-Hellman (video 1, video 2)
  - Texto: How RSA Works with Examples
  - Vídeo: o algoritmo RSA (video 1, video 2)
  - Vídeo: Elliptic Curves Cryptography

16/8: Aula 4

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

- Leitura complementar:
  - Certificate MITM attack 1, 2011
  - Certificate MITM attack 2, 2019

21/8: Aula 5

- Atividade (Lab 1-2 do DINF): Certificados digitais (entregar relatório no Moodle)
- Leitura complementar: Modelos de criptografia de chave pública alternativos. Goya et al, minicurso do SBSeg 2009.

23/8: Aula 6

- Autenticação: usuários e grupos; técnicas de autenticação; senhas; senhas descartáveis
- Sortear Tópicos em autenticação para os seminários
- Leitura complementar:
  - The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, IEEE Symposium on Security and Privacy, 2012.
  - Designing Password Policies for Strength and Usability, Shay et al, 2016.

28/8: Aula 7

- Autenticação: desafio/resposta; técnicas biométricas; infraestruturas de autenticação; Kerberos
- Leitura complementar:
  - Introdução à Biometria. Costa et al, SBSeg 2006.
  - Gerenciamento de Identidades Federadas. Wangham et al, SBSeg 2010.

30/8: Aula 8

-  Atividade (Lab 1-2 do DINF): Quebra de senhas

4/9: Aula 9

-  Atividade: seminários sobre Tópicos em autenticação

6/9: Aula 10

- Atividade (cont.)

11/9: Aula 11

- Atividade (cont.)

13/9: Aula 12

-  Prova 1 (conteúdo: conceitos básicos, criptografia, autenticação)

18/9: Aula 13

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias; políticas baseadas em domínios
- Sortear Tópicos em controle de acesso para os seminários

20/9: Aula 14

- Controle de acesso: políticas baseadas em papéis; políticas baseadas em atributos.
- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows
- Credenciais de um processo em UNIX: credentials.c
- Leitura complementar:
  - RBAC: Role-Based Access Controls, 1992; Role-Based Access Control Models, 1996.
  - ABAC: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, 2014.
  - UCON: The UCONabc usage control model, 2004.
- Atividade (alunos do *stricto sensu*): resumo sobre modelos de controle de acesso: Clark-Wilson, Brewer-Nash (*Chinese wall*), Graham-Denning (Harrison-Ruzzo-Ullman), Take-Grant, Low Watermark, Lipner Integrity, Object capabilities, com 2 páginas no formato IEEE 2 colunas (prazo: 4/10)

25/9: sem aula (SIEPE)

27/9: sem aula

2/10: Aula 15

Não houve aula

4/10: Aula 16

- Atividade: seminários sobre Tópicos em controle de acesso

9/10: Aula 17

- Atividade (cont.)

11/10: Aula 18

- Atividade (cont.)

16/10: Aula 19

- Controle de acesso: mudança de privilégios
- Revisão da prova

- Escolha dos Tópicos em governança da segurança para os seminários
- Escolha das demonstrações de ataques

18/10: Aula 20

- Atividade: Buffer overflow (demo)

23/10: Aula 21

- Malware (prof. André Grégio)

25/10: Aula 22

- Auditoria: coleta de dados; análise de dados; auditoria preventiva
- ~~Atividade: a definir~~

30/10: sem aula (semana acadêmica)

1/11: sem aula (semana acadêmica)

6/11: Aula 23

- Atividade: Seminários sobre Tópicos em governança da segurança

8/11: Aula 24

- Seminários (cont.)

13/11: Aula 25

- Detecção de Intrusão (prof. André Grégio)
- Leitura complementar:
  - NIST Guide to Intrusion Detection and Prevention Systems (IDPS), 2007
  - Intrusion Detection Systems: A Survey and Taxonomy, 2000.

15/11: sem aula (feriado)

20/11: Aula 26

- Atividade: demonstrações de ataques (tem peso 2 na avaliação)

22/11: Aula 27

- Demonstrações de ataques (cont.)

27/11: Aula 28

- Demonstrações de ataques (cont.)

29/11: Aula 29

- Demonstrações de ataques (cont.)

4/12: Aula 30

-  Prova 2 (conteúdo do bimestre)

11/12: exame final

-  Prova sobre todo o conteúdo das duas provas bimestrais.