IF68E - Plano de aula 2011/2

- Segurança e Auditoria de Sistemas
- Aulas: 4M2-4M5 (quartas-feiras de 08:20 a 12:00), sala B-202.

~~Podem~~ Irão ocorrer mudanças neste cronograma, com a devida divulgação aos alunos.

Atenção:

- As atividades indicadas com  serão avaliadas através de relatórios.
- Todos os relatórios devem ser enviados ao professor até um dia antes da prova bimestral.
- O formato do relatório é livre, mas sugere-se o formato de artigo da SBC.

10/08 - Aula 01

- Apresentação da disciplina
- Conceitos básicos
- Infraestrutura de segurança

17/08 - Aula 02

- Criptografia: cifragem e decifragem; criptografia simétrica; criptografia assimétrica
- Atividade: cifradores

24/08 - Aula 03

- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas
-  Atividade: Certificados digitais
- Leitura: Modelos de criptografia de chave pública alternativos (SBSeg 2009)

31/08 - Aula 04

- Autenticação: usuários e grupos; técnicas de autenticação; senhas
-  Atividade: Quebra de senhas

14/09 - Aula 05

- Autenticação: senhas descartáveis; desafio/resposta; certificados de autenticação; técnicas biométricas; Kerberos; infraestruturas de autenticação
-  Atividade: autenticação SSH por certificados

21/09 - Aula 06

-  Prática: Experimento PAM Authentication do SEED Project
- Texto de apoio: PAM system administrator's Guide

28/09 - Aula 07

-  Prática: Experimento Packet Spoofing do SEED Project
- Atenção: não é necessário resolver o problema 5 (`telnet`).
- Arquivo de sniffing do tutorial PCap: sniffex.c

05/10 - Aula 08

- **Prova 1** (conteúdo: aulas 01 a 05)
- Entrega dos relatórios das aulas 3 a 6 por e-mail, na véspera.

19/10 - Aula 09

- Entrega/discussão da prova
- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis.

26/10 - 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
-  Prática: Experimento Set-UID Program Vulnerability do SEED Project (questões 1 a 4)

09/11 - Aula 11

- Prática: Experimento Set-UID Program Vulnerability (continuação)
-  Prática: Experimento Capability exploration do SEED Project (questões 1 e 2)

16/11 - Aula 12

-  Prática: Experimento Buffer overflow vulnerability do SEED Project
- Responder as seguintes questões:
  - Explique como funciona a técnica ASLR
  - Explique como funciona o bit NX
  - Explique como funciona a proteção de pilha oferecida pelo compilador

23/11 - Aula 13

- Auditoria: coleta de dados; análise de dados; auditoria preventiva

-  Prática: Explorando sistemas de logs

30/11 - Aula 14

-  Prática: Uso de ferramentas de auditoria:
  - Ferramentas: Nessus (licença *HomeFeed*), Metasploit, Snort e NMap.
  - Escolha **duas** das ferramentas acima indicadas.
  - Para cada ferramenta, apresente:
    - objetivo;
    - principais funcionalidades;
    - passos necessários para instalação;
    - 3 roteiros distintos de uso, com resultados reais.

 Aplique as ferramentas escolhidas somente na rede local do laboratório!

07/12 - Aula 15

- Aspectos de governança da segurança: estudo dirigido sobre temas como:
  - ISO/IEC 27001
  - SAMM - Software Assurance Maturity Model
  - SSE-CMM - Systems Security Engineering Capability Maturity Model
  - CISSP - Certified Information Systems Security Professional
  - BSIMM/BSIMM2 - The Building Security In Maturity Model
  - SOMA - Security Operations Maturity Architecture
  - OSSTMM - Open Source Security Testing Methodology Manual
  - OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation
  - ITIL - Information Technology Infrastructure Library
  - COBIT - Control OBjectives for Information and related Technology

14/12 - Aula 16

- **Prova 2** (conteúdo: aulas 09 a 15)
- Defesa das atividades práticas