IF68E - Plano de aula 2012/2

- Segurança e Auditoria de Sistemas
- Aulas: 2a e 4a, de 18h40 a 20h20, sala B-202

Podem 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.
- Os relatórios devem seguir o formato de artigo da SBC.

Aula 01 - 03/12

- Apresentação da disciplina
- Conceitos básicos

Aula 02 - 05/12

- Infraestrutura de segurança
-  Atividade: Base de Vulnerabilidades

Aula 03 - 10/12

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

Aula 04 - 12/12

- Atividade: cifradores

Aula 05 - 17/12

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

Aula 06 - 19/12

-  Atividade: Certificados digitais
- Leitura: Modelos de criptografia de chave pública alternativos (SBSeg 2009)

Aula 07 - 04/02

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

Aula 08 - 06/02

-  Atividade: Quebra de senhas

Aula 09 - 18/02

- Autenticação: técnicas biométricas; Kerberos; infraestruturas de autenticação

Aula 10 - 20/02

-  Atividade: autenticação SSH por certificados

Aula 11 - 25/02

-  Estudo dirigido: Tópicos em autenticação por senhas

Aula 12 - 27/02

-  Estudo dirigido: Tópicos em autenticação distribuída

Aula 13 - 04/03

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

Aula 14 - 06/03

- Prática: Experimento Secret-key Encryption do SEED Project
- Prática: Experimento One-way Hash Function and MAC do SEED Project

Aula 15 - 11/03

- **Prova 1** (conteúdo das aulas 01 a 13)

Aula 16 - 13/03

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

Aula 17 - 18/03

- Controle de acesso: políticas baseadas em domínios; políticas baseadas em papéis; mecanismos de

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

Aula 18 - 20/03

- Apresentação dos estudos dirigidos
- **Defesa das atividades do bimestre**

Aula 19 - 25/03

- Apresentação dos estudos dirigidos (cont.)

Aula 20 - 27/03

- Escolha dos temas de estudo de caso da aula 28
-  Prática: Experimento Set-UID Program Vulnerability do SEED Project (atividades 1 a 4)

Aula 21 - 01/04

- Prática: Experimento Buffer overflow vulnerability do SEED Project
- 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 22 - 03/04

-  Prática: Experimento Capability exploration do SEED Project (até 3.1, inclusive).

Aula 23 - 08/04

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

Aula 24 - 10/04

-  Prática: Explorando sistemas de logs

Aula 25 - 15/04

-  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;
        - 2 roteiros distintos de uso, com resultados reais.

Aplique as ferramentas escolhidas somente na rede local do laboratório ou em um ambiente de sua responsabilidade!

Aula 26 - 17/04

- Continuação da atividade da aula anterior

Aula 27 - 22/04

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

Aula 28 - 24/04

-  Estudo dirigido sobre aspectos de governança da segurança: escolher um dos temas abaixo (por ordem de relevância):
    - ISO/IEC 27001
    - CC - Common Criteria (ISO/IEC 15408)
    - COBIT BMIS - Business Model for Information Security ($)
    - ITIL Security Management
    - SAMM - Software Assurance Maturity Model
    - CISSP - Certified Information Systems Security Professional
    - OSSTMM - Open Source Security Testing Methodology Manual
    - OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation
    - OWASP - Open Web Application Security Project
    - SSE-CMM - Systems Security Engineering Capability Maturity Model ($)
    - CERT/CSIRT
    - PCI-DSS

Aula 29 - 29/04

- **Prova 2** (conteúdo das aulas 16 a 28)

Aula 30 - 06/05

- Prazo para entrega dos trabalhos (não tem aula)

Aula 31 - 08/05

- Apresentação da prova

- **Defesa das atividades do bimestre**