Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística

Plano de Ensino

1) Identificação

Disciplina: INE5680 - Segurança da Informação e de Redes
Turma(s): 08238A, 08238B
Carga horária: 72 horas-aula Teóricas: 44 Práticas: 28
Período: 2º semestre de 2014

2) Cursos

- Sistemas de Informação (238)

3) Requisitos

- INE5625 - Computação Distribuída

4) Ementa

Introdução à Segurança. Conceitos básicos. Técnicas clássicas de criptografia. Criptografia Simétrica. Acordo de chave de Diffie-Hellman. Criptografia de Chave Pública. Gerenciamento de chaves públicas. Funções Hash. Assinaturas Digitais. Certificação Digital. Protocolos de Autenticação. Protocolos Criptográficos. Segurança de aplicações. Redes Privadas Virtuais. Tecnologias disponíveis para defesa. Gestão da Segurança da Informação.

5) Objetivos

Geral: Introduzir a área de segurança computacional, com relação as suas subáreas de: segurança da informação, segurança de redes, segurança de sistemas e segurança de aplicações. Estudar técnicas focadas em segurança da informação, capacitando o aluno para o desenvolvimento de sistemas seguros através da modelagem de protocolos para segurança da informação (protocolos criptográficos), além de torná-lo apto à formalização e prova de segurança de protocolos para segurança da informação.

Específicos:

- Conhecer fatos e problemas sobre segurança computacional.
- Compreender conceitos, princípios, mecanismos e métodos para segurança.
- Aplicar algoritmos de criptografia.
- Especificar protocolos criptográficos.
- Empregar ferramentas que servem de suporte à segurança computacional.
- Conhecer os fundamentos para Gestão de Segurança da Informação.
- Desenvolver expressão oral e escrita.

6) Conteúdo Programático

6.1) Apresentação da disciplina e plano de ensino [2 horas-aula]
- Apresentação de tarefa Servidor Web e BD

6.2) Plano de Ensino, Ambientes cooperativos [2 horas-aula]
- O que é Segurança: Informação, Rede, Sistema, Aplicação

6.3) Necessidade de segurança [2 horas-aula]

6.4) Introdução à Segurança da Informação [2 horas-aula]

6.5) Criptografia Simétrica [2 horas-aula]

6.6) Riscos que rondam as organizações [2 horas-aula]
- Os potenciais atacantes
- Vulnerabilidades, Ameaças, Riscos, Ataques, Intrusões [2 horas-aula]
- Os pontos explorados

6.7) Criptografia Assimétrica [2 horas-aula]

6.8) Planejamento e Anatomia de ataques [2 horas-aula]
- Ataques para obtenção de informaçoes
- Ataques de Negação de Serviços Coordenados
- Ataque ativo contra TCP
- Ataques no nível da aplicação

6.9) Varredura de Portas e Serviços [2 horas-aula]
6.10) Funções Hash [2 horas-aula]
6.11) Análise de Vulnerabilidades em Serviços [2 horas-aula]
6.12) Assinatura Digital [2 horas-aula]
6.13) Protocolo de Autenticação de Acesso Remoto [2 horas-aula]
6.14) Infra-estrutura de chaves públicas [2 horas-aula]
6.15) Segurança de Aplicação de Email [2 horas-aula]
6.16) Protocolos criptográficos [2 horas-aula]
6.17) Segurança de servidor web [2 horas-aula]
6.18) Técnicas e Tecnologias disponíveis para defesa [2 horas-aula]
- Firewall
- Proxy
- DMZ
- NAT
- Host de segurança
- Honeypots
- IDS
- Roteador de perímetro
- Política de segurança

6.19) Protocolos básicos [2 horas-aula]
6.20) Redes Privadas Virtuais [2 horas-aula]
6.21) Protocolos intermediários [2 horas-aula]
6.22) Modelo de Segurança em Ambientes Cooperativos [2 horas-aula]
6.23) Protocolos Avançados, Certificados de Atributo [2 horas-aula]
6.24) Apresentação oral de tópicos selecionados pelos alunos [6 horas-aula]
6.25) Aulas práticas [10 horas-aula]
6.26) Tarefas teóricas/práticas [8 horas-aula]

7) Metodologia

A disciplina será ministrada em aulas teóricas (AT) e aulas práticas (AP). Podendo haver palestras (P) e apresentações orais por parte dos alunos. Será dada ênfase, durante todo o período, para aulas práticas fazendo parte da avaliação. Tarefas de recuperação serão divulgadas, por ocasião da prova 2.

8) Avaliação

Os alunos serão avaliados através dos seguintes Instrumentos de Avaliação:

-Provas: 2 provas escritas individuais;

-Tarefas: tarefas práticas e tarefas teóricas.

Os seguintes critérios serão observados para fins de avaliação:

-compreensão dos conteúdos discutidos, participação nas atividades, responsabilidade e pontualidade e prazos de entrega;

-frequência suficiente (75%).

Cálculo da NF (Nota Final):

MPR (média das provas) = Nota Prova 1 * 0,5 + Nota Prova 2 * 0,5

MT (média das tarefas) = (Média de tarefas práticas * 0,8 + Média de tarefas teóricas * 0,2)

Média do Semestre (final Moodle) = MPR * 0,6 + MT * 0,4

Nota Final = Média do Semestre

Recuperação da aprendizagem:

Se a Media do Semestre (Final no Moodle = Provas, Tarefas, ...) satisfaz

3,0 < = Media do Semestre < 6,0 e o aluno tiver frequência de 75%, terá direito a recuperação do aprendizado.

Nota de Recuperação = 0,20*TT + 0,80*PR,
onde TT=Tarefa Teórica e PR=Prova de Recuperação

Nota final = (Média do Semestre + Nota de Recuperação)/2

Para realização de avaliações em atraso, de acordo com a RESOLUÇÃO Nº 17/CUn/97, de 30 de setembro de 1997:

Art. 70 § 4o - Ao aluno que não comparecer às avaliações ou não apresentar trabalhos no prazo estabelecido será atribuída nota 0 (zero).

Art. 74 - O aluno, que por motivo de força maior e plenamente justificado, deixar de realizar avaliações previstas no plano de ensino, deverá formalizar pedido de avaliação à Chefia do Departamento de Ensino ao qual a disciplina pertence, dentro do prazo de 3 (três) dias úteis, recebendo provisoriamente a menção I.

Conforme parágrafo 2º do artigo 70 da Resolução 17/CUn/97, o aluno com frequência suficiente (FS) e média final no período (**MF**) entre 3,0 e 5,5 terá direito a uma nova avaliação ao final do semestre (**REC**), sendo a nota final (**NF**) calculada conforme parágrafo 3º do artigo 71 desta resolução, ou seja: **NF = (MF + REC) / 2**.

9) Cronograma

PARTE I - SEGURANÇA DA INFORMAÇÃO E APLICAÇÕES
15/08 Plano de Ensino. Introdução à Segurança. Técnicas Clássicas de Criptografia. Modelo de Cifra Simétrica: Cifras de Bloco, Algoritmos de Cifra Simétrica. Modos de operação de cifra de bloco. Tarefa 1: Uso de algoritmos de criptografia.
22/08 Classificação e Tipos de Ataques. Cifras de fluxo. Chaves mestras e distribuição de chaves de sessão. Tarefa 2: Uso de algoritmo de criptografia.
29/08 Criptografia de Chave Pública. Tarefa 3: GnuPG e Segurança de Email. Gerenciamento de Chaves Públicas.
05/09 Códigos de Autenticação de Mensagem. Tarefa 4: Função Hash. Assinaturas Digitais. Protocolos Criptográficos Básicos.
12/09 Tarefa 5: Análise de Vulnerabilidades Web. Tarefa 6: Segurança na comunicação Web.
19/09 Protocolos Intermediários. Tarefa 7: Redes Privadas Virtuais.
26/09 Infraestrutura de Chaves Públicas. Palestra (P): Infraestrutura de Gerenciamento de Privilégios (controle de acesso). Tarefa teórica de especificação de protocolo.
03/10 Protocolos Avançados. Tarefa teórica de especificação de protocolos. Ferramenta de Verificação da Correção de Protocolos de Segurança.
10/10 Prova 1 (P1)
PARTE II – SEGURANÇA DE REDES, SISTEMAS E APLICAÇÕES
17/10 Cenário de Estudo de Caso da Empresa XYZ: DMZ. Política de Segurança. Tarefa 8: Reconhecimento de portas e serviços. Tarefa 9: Análise de vulnerabilidades.
24/10 Tarefa 10: Firewall. Sistema de Detecção de Intrusão.
31/10 Tarefa 11: Testes de Penetração
07/11 Tarefa 12: Testes de Penetração
14/11 Tarefa 13: Testes de Penetração
21/11 Prova 2 (P2) e Divulgação da Tarefa de recuperação e Apresentação de Ferramenta.
28/11 Tarefa 15: Apresentações Orais de grupos de 2 alunos – 15 minutos de apresentações de temas selecionados.
05/12 Apresentação de Ferramenta
12/12 Prova de Recuperação, Aluno entrega Tarefas de Recuperação (TR).

10) Bibliografia Básica

- Criptografia e Segurança de Redes, William Stallings, 4 Edição, Pearson.

- Segurança de Redes, Emílio T. Nakamura e Paulo L. de Geus, 4 Edição, Futura.
- Segurança de Dados, Routo Terada, 2 Edição, Editora Blucher, 2008.

11) Bibliografia Complementar

- Redes de Computadores, Tanembaum e Wetherall, 5 Edição, Pearson.
- Diversos e-books da área da disciplina.