UNIVERSIDADE FEDERAL DE SANTA CATARINA
C E N T R O T E C N O L Ó G I C O
Departamento de Informática e de Estatística

P L A N O D E E N S I N O

1. IDENTIFICAÇÃO DA DISCIPLINA: **Semestre**: **2009.2**
Código: INE5630 **Nome**: Segurança em Computação Distribuída
Horas-Aula: **72** **Teóricas**: **56** AEX/OTR **Práticas**: **16** APR
Código(s) do(s) pré-requisito(s): INE5625 (Computação Distribuída)
Prof.: João Bosco M. Sobral, Dr
Tema: Segurança da Informação, Segurança de Redes e de Aplicações
Home Page: http://www.inf.ufsc.br/~bosco/ensino/ine5630.html (depois escolher links conforme o andamento da disciplina)

2. OBJETIVOS:
2.1-Geral
Conhecer fatos e problemas sobre segurança computacional. **Compreender** os principais conceitos, princípios, métodos, procedimentos. **Aplicar** algoritmos e protocolos criptográficos. **Empregar** ferramentas que servem de suporte para a segurança computacional da informação, segurança de redes e a segurança de aplicações em ambientes distribuídos.

2.2-Específicos
(1) O aluno deverá **conhecer** ameaças e ataques a sistemas; (2) **compreender** conceitos, princípios em criptografia, métodos de criptografia e procedimentos de gerenciamento de chaves criptográficas; (3) **empregar** algoritmos e procedimentos em criptografia simétrica, assimétrica e em assinaturas digitais; (4) **montar** aplicações seguras utilizando certificação digital; (5) **construir** uma rede privada virtual simples (VPN); (6) **escrever** artigo em grupo para desenvolver a linguagem; (7) **usar** ferramentas de reconhecimento, análise de vulnerabilidades para a segurança de redes (8) **apresentar** oralmente um trabalho sobre tema escolhido de acordo com as áreas da disciplina, para desenvolver o encadeamento de raciocínio e habilidade na fala.

3. EMENTA: O que é Segurança Computacional. O ambiente cooperativo. Vulnerabildades, Ameaças e Riscos. Introdução à Criptografia. Criptografia de Chave Simétrica. Gerenciamento de Chaves Simétricas. Criptografia de Chave Pública. Resumos de Mensagem. Assinaturas Digitais. Certificação Digital. Redes Privadas Virtuais. Anatomia de ataques intrusivos. Tipos de Ataques. Visão sobre Políticas de Segurança. Segurança de Acesso Remoto. Firewalls. Sistemas de Detecção de Intrusão. Internet com Segurança. Modelos de Segurança para ambientes cooperativos.

4..PROCEDIMENTOS DIDÁTICOS:
AEX=Aula Expositiva; **LAB**=Aula de laboratório; **APR**=Aula prática; **OTR**=Outros.

T Ó P I C O S EM SEGURANÇA DA INFORMAÇÃO (36h)	**Proc. Didático**	**Horas**
0. Apresentando o Plano de ensino. 1. Conceitos básicos sobre segurança computacional. 2. O ambiente cooperativo e os problemas existentes. 3. Visão geral sobre vulnerabilidades, ameaças e riscos. 4. Introdução à Criptografia	AEX	8

T Ó P I C O S EM SEGURANÇA DA INFORMAÇÃO (36h)	Proc. Didático	Horas
5. Criptografia de Chave Simétrica. 6. Gerenciamento de Chaves Simétricas. **Tarefa prática 0: usar algoritmos de criptografia simétrica. (10%)** **Tarefa teórica 1: descrever um protocolo de autenticação. Realizada à parte.** **(10%)**	AEX e APT	4 4
6. Criptografia de Chave Pública e o Problema da Distribuição de Chaves.	AEX	4
7. Assinatura Digital, Resumos de Mensagem, Códigos de Autenticação de Mensagens. Assinaturas Verificáveis. Compreendendo os algoritmos de assinatura.	AEX	4
8. **Tarefa Prática 3: como usar o GnuPG (5%)**	APT	4
9. Infra-Estrutura de Chaves Públicas. Introdução aos Certificados. **TÓPICOS EM SEGURANÇA DE APLICAÇÕES** **Tarefa Prática 4: segurança em correio eletrônico. (5%)** **Tarefa Prática 5: segurança de aplicação Web com certificação de cliente e servidor. Realizada à parte. (15%)**	AEX e APT	4
10. Redes Privadas Virtuais (VPN): motivação, conceitos e estruturação **Tarefa Prática 6. Realizada à parte. (15%)**	AEX	4
T Ó P I C O S EM SEGURANÇA DE REDES (36h)	**Proc. Didático**	**Horas**
11. Anatomia (reconhecimento, comprometimento e efetivação) de ataques. Técnicas de varredura e **Apresentação Prática (Nmap)**. Análise de vulnerabilidades e **Apresentação Prática (Nessus)**.	AEX e APT	4
12. Tipos de Ataques: Sem intrusão: obtenção de informações, negação de serviços, força-bruta. Com intrusão: sniffers, backdoors, keyloggers, rootkits, ataques ativos contra TCP/IP, ataques no nível de aplicação (códigos maliciosos)	**Apresentação de Trabalhos em Grupos (5%)**	8
13. Pensando em Política de Segurança: estudos de casos e exemplo de política de segurança em ambiente corporativo.	AEX	2
14. Proxy de Web, Firewalls	AEX	2
15. Sistemas de Detecção de Intrusão.	AEX	2
16.Segurança no Acesso Remoto: métodos de autenticação. Conectando-se à Internet com Segurança: roteador de perímetro, DMZ	AEX	4
17. Modelo de Segurança para Ambientes Cooperativos: níveis hierárquicos de defesa	AEX	2
18. **Tarefa 7: Apresentação de Trabalhos em grupo (15%)**	OTR	4
19. **Tarefa 7: Apresentação de Trabalhos em grupo**	OTR	4
20. **Tarefa 7: Apresentação de Trabalhos em grupo**	OTR	4
21. **Tarefa 8: Elaboração de artigo sobre tema escolhido, realizada à parte. (20%)**		
OBS: A apresentação de trabalhos complementa os tópicos deste plano de ensino.		

5. AVALIAÇÃO DA APRENDIZAGEM:

- O aproveitamento final do aluno na disciplina será medido através de tarefas teóricas e práticas. A cada tarefa será atribuído um percentual máximo que comporá a nota final na disciplina. **A nota final será a soma dos percentuais obtidos nas tarefas. Os percentuais máximos são indicados na tabela acima, para cada tarefa.**
- Caso a apresentação do trabalho seja oral e o trabalho realizado em grupo, a nota do trabalho será atribuída ao grupo levando-se em consideração, a clareza da apresentação, a

qualidade do material apresentado e a freqüência do aluno durante as apresentações dos outros grupos.

- Caso a apresentação do trabalho seja através de artigo/relatório, a nota do trabalho levará em consideração a organização e a profundidade abordada.

6. BIBLIOGRAFIA e REFERÊNCIAS:

- *Burnett, S, Paine, S,* ***Criptografia e Segurança: o Guia Oficial RSA****, Editora Campus, RSA Press, 2002.* ***(Livro Texto)***
- *Nakamura, Emilio Tissato e Geus, Paulo Lício de.* ***Segurança de Redes em Ambientes Cooperativos****. Editora Futura, 2007.* ***(Livro Texto)***
- *Dhanjani, Nitesh.* ***Segurança no Linux e Unix****. Editora Campus/Elsevier, 2004.*
- *Melo, Sandro e Trigo, Clodonil H.,* ***Projeto de Segurança em Software Livre****, Alta Books, 2004.*
- *Rufino, Nelson Murilo de O.,* ***Segurança em Redes sem Fio: ambientes Wi-Fi e Blootooth****. Editora Novatec, 2005.*
- *Terpstra, John H. e Love, Paul e Reck, Ronald P. e Scanlon Tim.* ***Segurança para Linux.*** *Editora Campus, 2004.*
- *Digerati Books.* ***Segurança e Espionagem Digital****, 2005.*
- *Marcelo, Antonio.* ***Squid: Configurando o Proxy para Linux*** *(guia rápido para administrador de redes). Editora Brasport, 2005.*
- *Marcelo, Antonio.* ***Firewalls em Linux para Pequenas Corporações*** *(guia rápido para administrador de redes). Editora Brasport, 2003.*
- *Neto, Urubatan.* ***Dominando Linux Firewalls IPtables****. Editora Ciência Moderna, 2004.*
- *Tanenbaum, Andrew S.* ***Redes de Computadores, Quarta Edição*** *(Capítulo 8). Editora Campus, 2003.*
- *Forristal, Jeff e Traxier, Julie.* ***Site Seguro: Aplicações Web*** *(Capítulo 11). Syngress (Alta Books), 2002.*
- *Stallings, W.,* ***Cryptography and Network Security: Principles and Practice****, 3rd ed., Prentice-Hall, 2003.*
- *Kaufman, C., Perlman, R., Speciner, M.,* ***Network Security: Private Communication in a Public World****, Pfleeger, C., Pfleeger, S.L., Security in Computing, 3rd edition, Prentice Hall, 2003.*
- *Coulouris, G., Dollimore, J., Kindber, T.,* ***Distributed Systems: Concepts and Design****, 3nd ed., Addison-Wesley, 2005, capítulo: Security. Prentice Hall, 2002.Russel, R. (Editor).,* ***Rede Segura****, Alta Books, 2002.*
- *Oliveira, W. J.,* ***Segurança da Informação****, Visual Books, 2001.*
- *Forristal, J., Traxler, J.,* ***Site Seguro: Aplicações Web****. Alta Books, 2002.*
- *Scambray, J., McClure, G., Kurtz, G.,* ***Hackers Expostos****, Makron Books, 2001.*
- *Anonymous,* ***Maximum Security****, Sams.Net, 1997.*
- *Carvalho, D. B.,* ***Segurança de Dados com Criptografia: Métodos e Algoritmos****, Book Express, 2001.*
- *Russel, R. at al.,* ***Roubando a Rede****, Alta Books, 2003.*
- *Wang, W.,* ***Roubando este Computador****, Alta Books, 2003.*
- *Wenstrom, M.,* ***Managing Cisco: Network Security****, Alta Books, 2002.*
- *Spyman,* ***Manual Completo do Hacker****, Book Express, 2004.*
- *Caswell, B, Beale, J. Foster, J. C., Posluns, J.,* ***Snort 2, Sistema de Detecção de Intruso****, Open Source, Syngress-Alta Books, 2003.*