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**: **2007.2**
Código: INE5630 **Nome**: Segurança em Computação Distribuída
Horas-Aula: 72 **Teóricas**: 72 **Práticas**: Não há laboratório especializado
Código(s) do(s) pré-requisito(s): INE5625 (Computação Distribuída)
Prof.: João Bosco M. Sobral, Dr
Tema: Segurança de Redes e Aplicações
Home Page: http://www.inf.ufsc.br/~bosco/ensino/ine5630.html

2. OBJETIVOS:

2.1-Geral

Conhecer os princípios, técnicas e ferramentas que servem de suporte para a segurança de redes e aplicações em ambientes computacionais distribuídos.

2.2-Específicos

Aprender os conceitos fundamentais. Avaliar ameaças à segurança de rede. Identificar ataques. Exemplificar políticas de segurança de rede. Compreender o desenvolvimento de aplicações seguras. Conhecer os níveis de segurança em redes. Familiarizar-se com as técnicas mais utilizadas na implementação de uma infra-estrutura segura em ambientes distribuídos.

3. EMENTA:

Conceitos básicos de segurança de redes. Categorias e a anatomia de ataques. Formas de ataque. Política de segurança. Softwares de defesa. Conexão segura com a Internet. VPN. Segurança de Aplicações. Segurança em Redes sem Fio.

4..PROCEDIMENTOS DIDÁTICOS:

AEX=Aula Expositiva; **LAB**=Aula de laboratório; **APR**=Aula prática; **OTR**=Outros.

T Ó P I C O S	Proc. Didático	Horas
0. Plano de ensino. 1. Introdução à Segurança de Redes. 2. Cenário de rede para estudo de caso da segurança de uma empresa. O ambiente cooperativo e os problemas existentes. 3. A necessidade de segurança de rede. 4. Visão geral sobre vulnerabilidades, ameaças e riscos.	AEX	2
5. Categorias, anatomia (reconhecimento, comprometimento e efetivação). Técnicas de varredura. Análise de vulnerabilidades. 6. Formas de Ataques: obtenção de informações, negação de serviços, ataques ativos contra o TCP, ataques no nível de aplicação (códigos maliciosos). 7. Indícios de ataques, identificando um comprometimento.	AEX uso de ferramentas	4
8. Pensando em Política de Segurança: estudos de caso	AEX	2
9. Firewalls, Proxy e Segurança em Software Livre: Linux. 10. Conceituando DMZ e Honeypots.	AEX uso de ferramentas	4
11. Conectando-se com Segurança à Internet. 12. Sistemas de Detecção e Prevenção de Intrusões.	AEX uso	4
13. Redes Privadas Virtuais, IP Security.	AEX	4

T Ó P I C O S	Proc. Didático	Horas
	uso de ferramentas	
14. Forense Computacional.	palestra	2
15. Verificação de recuperação de incidentes; avaliação e fortalecimento da Segurança. 16. Modelo de Segurança para Ambientes Cooperativos: níveis hierárquicos de defesa e o gerenciamento da complexidade.	AEX	2
17. Insegurança na Web. 18. Ataques na Web. 19. Segurança na Web. 20. Categorias de segurança de aplicações Web. 21. Avaliação da segurança das aplicações Web.	AEX	4
22. Segurança de Emails: OpenPGP, S/MIME. 23. Privacidade no navegador	AEX e APR	4
24. Evolução das redes sem fio e tipos de tecnologia (WPAN, WLAN, WWAN). 25. WPAN e Bluetooth. WLAN e o Padrão IEEE 802.11.	AEX	4
26. Métodos de transmissão na camada física.	AEX	4
27. Produtos para redes sem fio.	apresentação de trabalhos	4
28. Mecanismos Básicos de Segurança 802.11: WEP 29. Ameaças e Riscos.	AEX	4
30. Técnicas e Ferramentas de ataque em redes sem fio.	apresentação de trabalhos	8
31. Mecanismos de Segurança em redes sem fio: 802.1x, WPA e 802.11i.	AEX	2
32. Métodos de Defesa em redes sem fio	AEX	4
33. Estudos de Caso em redes sem fio: pequena, média e grande empresa.	trabalho escrito	
34. Tópicos para trabalhos de pesquisa	apresentação de trabalhos em grupos	10

5. FERRAMENTAS DE SOFTWARE:

scanner de portas, analisador de vulnerabilidades, software para VPN, navegador, cliente de email, IDS, ferramenta de redes se fio.

5. TÓPICOS PARA TRABALHOS DE PESQUISA:

Ver *home page* da disciplina http://www.inf.ufsc.br/~bosco/ensino/ine5630.html

6. AVALIAÇÃO DA APRENDIZAGEM:

- O aproveitamento do aluno na disciplina será medido através de trabalhos práticos sobre o uso e a avaliação de ferramentas de software ou trabalhos em grupo.
- **A cada trabalho será atribuído um percentual máximo.**
- Serão propostos dois trabalhos em grupo (de 2 ou 3 alunos, dependendo do tamanho da turma). Esses trabalhos serão apresentados em aula pelo grupo, que receberão um percentual, para formar a nota do trabalho.
- Caso a apresentação do trabalho seja oral e o trabalho realizado em grupo, a nota do trabalho será atribuída, individualmente, a cada aluno membro do grupo, levando-se em consideração, a organização do trabalho, a profundidade e a qualidade da apresentação de cada um dos membros do grupo.
- Caso a apresentação do trabalho seja através de relatório, a nota do trabalho levará em consideração a organização do mesmo, conforme a forma de elaboração passada aos alunos, a profundidade abordada e o benefício para um projeto de segurança.
- **A nota final será a soma dos percentuais obtidos nos trabalhos.**

7. BIBLIOGRAFIA e REFERÊNCIAS:

- *Horton, Mike. **Segurança de Redes**. Editora Campus/Elsevier, 2004.*
- *Dhanjani, Nitesh. **Segurança no Linux e Unix**. Editora Campus/Elsevier, 2004.*
- *Nakamura, Emilio Tissato e Geus, Paulo Lício de. **Segurança de Redes em Ambientes Corporativos**. Editora Futura, 2002.*
- *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.*
- *Melo, S., Trigo, C. H., **Projeto de Segurança em Software Livre: Teoria e Prática**, Alta Books, 2004.*
- *Wenstrom, M., **Managing Cisco: Network Security**, Alta Books, 2002.*
- *Burnett, S, Paine, S, **Criptografia e Segurança: o Guia Oficial RSA**, Editora Campus, RSA Press, 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.*