UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
PRÓ-REITORIA DE ENSINO DE GRADUAÇÃO
Rua Dom Manoel de Medeiros, s/n – Dois Irmãos 52171-900 Recife-PE
Fone: 0xx-81-332060-40 proreitor@preg.ufrpe.br

PLANO DE ENSINO

I – IDENTIFICAÇÃO

CURSO: Bacharelado em Sistemas de Informação

MODALIDADE: Presencial

DISCIPLINA: Segurança e Auditoria de Sistemas de Informação

PRÉ-REQUISITO:

(X) OBRIGATÓRIA ( ) OPTATIVA

DEPARTAMENTO: Departamento de Estatística e Informática

PROFESSOR RESPONSÁVEL : Rodrigo Elia Assad

Ano: 2014

Semestre Letivo: (x) Primeiro ( ) Segundo

Total de Créditos (se for o caso):

Carga Horária: 60h

II - EMENTA (Sinopse do Conteúdo)

Histórico da Segurança da Informação. Evolução, Fatos e eventos históricos, Tipos de hackers, Engenharia social. Virologia Computacional. Malwares, Anti-vírus e anti-spywares. Criptografia. Criptografia x criptoanálise. Algoritmos simétricos e assimétricos. Infra-estrutura de chave pública e privada. Educação, Tecnologia e Segurança da Informação – Cartilha Diálogo Virtual. Internet, E-mail, Broswer, Lan House, Redes de Relacionamento, P2P, Justiceiros. Mensageiro Instantâneo, Chat, Roubo de

Dados, Blogs, Vírus e Pragas Virtuais. Crime Digital, Invasão, Denúncia, Responsabilidade Social, Software Livre, VoIP. Segurança para Internet – Cartilha Cert.br. Conceitos de Segurança, Análise de Malwares, Avaliação de sites suspeitos e fraudes on-line, Denúncias na Web. Segurança em Códigos. Bugs, exploits e vulnerabilidades. Depuração de aplicações. Sql Injection, Cross Site Scripting. Auditoria de vulnerabilidades em sites Internet. Firewalls. Conceitos e arquiteturas. Projeto de firewall em camadas. Zonas Desmilitarizadas. Redes Privadas Virtuais – VPN. Segurança em Redes sem Fio. Norma Internacional: ISO/IEC 17799:2000

III - OBJETIVOS DA DISCIPLINA

Apresentar aos alunos os conceitos fundamentais sobre segurança de sistemas através de uma abordagem prática com a execução de exercícios executados em sala de aula e nos laboratórios da universidade.

IV - CONTEÚDO PROGRAMÁTICO

1) Introdução
2) Funcionamento dos principais componentes de segurança (proxies, IDS, Firewall, Anti-Vírus, VPN). Arquiteturas de segurança de redes.
3) Configuração de serviços de rede de forma segura
4) Entender os principais tipos de ataques: spoofing, arp spoofing, flood, buffer overflow, XSS, Sql Injection, etc.
5) Compreender e avaliar o impacto da utilização de criptografia e funcionamento de uma infra estrutura de chave pública.
6) Especificar e implantar os passos necessários para a implantação de uma política de segurança para uma instituição.

V – MÉTODOS DIDÁTICOS DE ENSINO

(x) Aula Expositiva
(x) Seminário
(x) Leitura Dirigida
(x) Demonstração (prática realizada pelo Professor)
(x) Laboratório (prática realizada pelo aluno)
(x) Trabalho de Campo
(x) Execução de Pesquisa
(x) Outra. Especificar: Implementação prática de um componente de um sistema operacional.

_____

VI - CRITÉRIOS DE AVALIAÇÃO

a) Provas
b) Participação em sala de aula
c) Apresentação do seminário
d) Execução do exercício passado

CRONOGRAMA	
DATA	CONTEÚDO
Aula 1	Apresentação da disciplina e métodos de avaliação
Aula 2	Histórico de segurança
Aula 3	Topologias de segurança, apresentar os conceitos sobre Firewall, proxies, VPN, switching
Aula 4	Topologias de segurança, apresentar os conceitos sobre Firewall, proxies, VPN, switching
Aula 5	Arquiteturas de Firewall
Aula 6	Arquiteturas de Firewall
Aula 7	Arquiteturas de Firewall
Aula 8	Revisão sobre sistemas operacionais
Aula 9	Montagem do laboratório, configuração do roteamento entre e acesso a uma DMZ e testes de acesso.
Aula 10	Montagem do laboratório, configuração do roteamento entre e acesso a uma DMZ e testes de acesso.
Aula 11	Considerações e configuração de regras de Firewall
Aula 12	Considerações e configuração de regras de Firewall
Aula 13	Configuração de um proxy
Aula 14	Prova
Aula 15	Tipos de ataques: spoofing, arp spoofing,buffer overflow, cross site scripting, sql injection, etc
Aula 16	Tipos de ataques: spoofing, arp spoofing,buffer overflow, cross site scripting, sql injection, etc
Aula 17	Tipos de ataques: spoofing, arp spoofing,buffer overflow, cross site scripting, sql injection, etc
Aula 18	Tipos de ataques: spoofing, arp spoofing,buffer overflow, cross site scripting, sql injection, etc
Aula 19	Tipos de ataques: spoofing, arp spoofing,buffer overflow, cross site scripting, sql injection, etc
Aula 20	Ferramentas de auditoria de redes
Aula 21	Ferramentas de auditoria de redes
Aula 22	Criptografia
Aula 23	Criptografia
Aula 24	Criptografia
Aula 25	Criptografia
Aula 26	Revisão para a prova
Aula 27	Prova
Aula 28	Politicas de segurança
Aula 29	Politicas de segurança

Aula 30	Politicas de segurança
Aula 31	Prova
Aula 32	Duvidas e revisões
Aula 33	Duvidas e revisões
Aula 34	Duvidas e revisões

VIII – BIBLIOGRAFIA (Conforme normas da ABNT)

BÁSICA:

1. Nakamura Emilio & Geus, Paulo, Segurança de Redes em Ambientes Corporativos , 291 p, Novatec, Berkeley, 2002
2. Sêmola, Marcos, Gestão da Segurança da Informação – Uma Visão Executiva , 156 p., Ed. Campus, 2003;
3. Kurtz, George; Scambray, Joel; McLure, Stuart, Hackers Expostos , 832 p., Ed. Campus, 2003;

COMPLEMENTAR:

1. CARUSO, Carlos A. A., STEFFEN, Flávio D. Segurança em Informática e de Informações. São Paulo: Senac, 1999.
2. PELTIER, T. R. Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management; Boca Raton: Auerbach, 2002.
3. Martins, José Carlos Cordeiro, Gestão de Projetos de Segurança da Informação , 384 p., Ed. Brasport, 2003;
4. Ulbrich, Henrique Cesar; Della Valle, James, Universidade Hacker – 2a. Edição , 348 p., Ed. Digerati, 2003;
5. CARVALHO, Daniel B. Segurança de Dados com Criptografia. Rio de Janeiro: Book Express, 2001.

Recife, 20 de Abril de 2014

Rodrigo Elia Assad

Professor Responsável