INE5680 – Segurança da Informação e de Redes – 2013.2   
CRONOGRAMA  
Aula Teóricas, Aulas Práticas e Provas

16/08 Plano de Ensino. Questionário sobre experiência dos alunos.   
 Organização dos Grupos. Novo ambiente de aulas práticas.  
 Introdução à Segurança Computacional: segurança da informação, segurança de redes,   
 segurança de aplicações, segurança de sistemas. O Ambiente Cooperativo.   
 Modelo de Segurança. Protocolo de Segurança, Vulnerabilidades, Ameaças, Riscos,   
 Severidade. Ataques, Intrusões (Invasões), Requisitos de Segurança. Política de   
 Segurança.  
  
23/08 Formas de Ocultação de Mensagens: Código, Esteganografia, Técnicas Clássicas de Criptografia: Modelo de Criptosistema Convencional (algoritmo, chave, cifra, criptonálise, tipos de ataques), Técnicas de Substituição, Técnicas de Transposição. Conceitos da Teoria da Informação (Difusão, Confusão, Segurança Perfeita). Aritmética modular. Gerador de Números Aleatórios. Entropia, Construindo Chaves. Ou Exclusivo. Modos de Cifra. Algoritmos Criptográficos Simétricos. Tarefa 1: Criptografia Simétrica com DES.  
   
30/08 Gerenciamento de Chaves Simétricas. O que são Funções Hash. Acordo de Chave Diffie-Hellman. Mais Funções Hash. Criptografia de Chaves Públicas. Gerenciamento de Chaves Públicas. Assinaturas Digitais. Tarefa 2a: Criptografia Assimétrica com RSA. Tarefa 2b: GnuPG - Criptografia Assimétrica com El Gamal e Assinatura Digital com DSA. Tarefa 2c: Segurança de Email com Mozilla Thunderbird. Tarefa 2d: Envio de email.

06/09 Integridade e Autenticação de Mensagens. Código de Autenticação de Mensagens (MAC). Tarefa 3: Autenticação e Segurança na Comunicação Web (OpenSSL). Tarefa 4: Redes Privadas Virtuais (OpenVPN).

13/09 Certificados Digitais. Infraestrutura de Chaves Públicas. Palestra: Infraestrutura de Gerenciamento de Privilégios (certificados de atributo). Tarefa 7: Questionário da palestra.

20/09 Protocolos Criptográficos Básicos. Protocolos Criptográficos Intermediários. Tarefa 8: Protocolos Criptográficos Básicos.

27/09 Protocolos Criptográficos Avançados. Palestra. Tarefa 9: Questionário da palestra.  
  
04/10 Prova 1 (Avaliação da Primeira Parte).

11/10 Serviços de Segurança, Mecanismos de Segurança. Arquitetura de Segurança. Níveis de Segurança. Visão Geral das Técnicas de Segurança: Controle de Acesso, Credenciais. Tipos de Ataques em Redes, Aplicações e Sistemas. Anatomia de Ataques.Conceito de DMZ. Tarefa 9: Firewall (Iptables, Microtick) e NAT. Sistemas de Detecção de Intrusão (Host, Rede), Honeypots.

18/10 Ferramenta de Reconhecimento de Portas e Serviços (Tarefa 10: Nmap). Ferramenta de Análise de Vulnerabilidades (Tarefa 11: Nessus/OpenVAS).

25/10 Ataques na Web. Ferramentas de Vulnerabilidades na Web (Tarefa 12: Nikto).   
 Segurança na Comunicação Web (OpenSSL).

01/11 Ataques e Tarefa 13: Ferramenta para Avaliação de Segurança de Bancos de Dados.

08/11 Auditoria e Teste de Penetração e Tarefa 14: Metasploit e Metasploitable Linux

22/11. Tarefa 15: Ferramentas para Verificação e Segurança em Sistemas Windows Server.

29/11 Tarefa 16: Apresentação Oral - 13 grupos (Auditoria e Gestão de Segurança da Informação).  
   
06/12 Continuação da Tarefa 16: Apresentação Oral - 12 grupos (Avaliação de Ferramentas).

---------------------------------------------------------

09/12 – Prova de Recuperação Final sobre a Primeira Parte