Segurança da Informação
IC/UFF 2019/2 (Grad/Mestr/Dout)
Professor: Raphael Machado

Organização e Proposta do Curso

Sobre o Professor

- Atua na área de segurança desde 2003 (e com TIC desde o milênio passado=)
- Experiência de Pesquisa, Ensino, Governo, Defesa e Mercado
- Não é "hacker" -> atua em muitas áreas da segurança, mas sempre em mais alto nível

Objetivos do Curso

- Compreender riscos e modelos de ataque associados às diferentes aplicações de tecnologia da informação
- Conhecer as ferramentas e métodos de ataque e de defesa
  - Não é um curso de Criptografia – embora a Criptografia seja uma ferramenta fundamental para a construção de arquiteturas de segurança.
- Conhecer as diversas áreas da segurança nos setores corporativo, de estado e em pesquisa.

Objetivos... Em outras palavras

- Convencer o aluno de que Segurança da Informação...
  - é uma questão real (e que ataques cibernéticos são um problema capaz de grande impacto "real")
  - é um tema transversal, perpassa todas as áreas de negócio (e da sociedade)
  - dá origem a interessantes temas de pesquisa e desenvolvimento
- Apresentar ao aluno os fundamentos e conceitos que o permitirão trabalhar no tema de segurança – ou, pelo menos, compreendê-lo
- Apresentar ao aluno, temas de trabalho, desenvolvimento tecnológico e pesquisa científica na área de segurança

Abordagem do Curso

- Diferentes visões e aplicações de segurança
  - Governo, Mercado, Academia,...
- Curso fortemente orientado a ataques.
  - Muito além de Alice e Bob
- Curso fortemente orientado a padrões.
  - Buscar conhecimento na fonte
- Curso alterna momentos “informativos” e “formativos”
  - Predominantemente informativo: transmissão de informações (ex.: histórico de ransomware)
    - Pode ser considerado um curso ”fácil”
  - Alguns tópicos formativos: conceitos/fundamentos (ex.: criptografia)

Organização do curso

- Total de 32 dias letivos
  - 20 dias de aulas
  - 2 dias de simulados
  - 4 dias de prova
  - 4 dias para correções de prova, dúvidas e recursos
- Estilo de aula
  - Aulas planejadas para ~1h30min de conteúdo
  - Primeiros 10 min e últimos 20 min para dúvidas/orientações
  - Conteúdo complementado por projetos de pesquisa
    - Opcionais para graduação (até 1 ponto extra na média)
    - Obrigatórios para pós-graduação (vale 50% da nota)

Notas e Critério de Aprovação

- P1: Primeira Prova
- P2: Segunda Prova
- VR: Verificação de Reposição
  - Prova de Substituição: substitui a menor nota entre P1 e P2 (inclusive, caso o aluno tenha faltado)
- VS: Verificação Suplementar
- T: Nota de Trabalhos (projetos de pesquisa)

- Graduação
  - M = 0.5*P1 + 0.5*P2 + 0.1*T
  - Se M>=6: aprovado
  - Se M<4: reprovado
  - Se 4<=M<6: fazer VS
    - VS será a média final
- Mestrado/Doutorado
  - M = 0.25*P1+0.25*P2+0.5*T
  - Se precisar fazer a VS, a média final é (M+VS/2)

Regras:

- Provas básicas: Prova 1 (P1) e Prova 2 (P2) -> Fortemente recomendado que o aluno faça as duas provas.
- Trabalho (T): Nota de 0 a 10 alcançada pelo aluno após a execução das atividades e projetos propostos ao longo do curso.
- Verificação de Reposição (VR). O aluno pode escolher por fazer a VR, que irá obrigatoriamente substituir a menor nota entre P1 e P2. A VR funciona como segunda chamada.
- Média das Provas (MP):
  - Caso não tenha feito VR: MP = (P1+P2)/2
  - Caso tenha feito VR: MP = (max{P1,P2}+VR)/2
- Média final (MF):
  - Graduação: MF = MP + 0,1*T
  - Mestrado e Doutorado: MF = 0,5*MP + 0,5*T
- Alunos com 4<=MF<6 podem fazer Verificação Suplementar (VS)
- Média Suplementar (MS): média final após VS
  - Graduação: MS = VS
  - Mestrado e Doutorado: MS = (MF+VS)/2 + 0,5*T

Temas de projetos de pesquisa

- Segurança de software (vulnerabilidades)
  - Implementar programa/aplicação simples com vulnerabilidade listada no SANS/CWE Top 25 (ou outra de relevância)
- Segurança de redes (ferramentas)
  - implementar rede (possivelmente, usando virtualização) contendo ferramentas básicas de segurança (IDS, IPS, FW, SIEM,...)
- Honeypot/honeynet
  - implementar host vulnerável, deixa-lo acessível e coletar dados de atacantes
- Números aleatórios
  - identificar três fontes distintas de números aleatórios e estudar a aleatoriedade

Temas de projetos de pesquisa

- Análise Estática de Código
  - demonstrar casos de uso das seguintes técnicas: grafo de controle de fluxo, grafo de chamada, tainting, value set analysis
- Análise Estática de Código - identificação de vulnerabilidades
  - Comparar pelo menos duas ferramentas com relação à identificação de vulns
- Ataques a sistemas industriais em rede
  - Desafio: dado objetivo (ex.: aumento de 45% a 55% de threshold) identificar sistema e minimizar número de perdas de pacotes para atingir o objetivo
- Padrões de cybersecurity em setores específicos
  - quais são as organizações e os padrões? existem regulamentos? Em que países? existe certificação? Como funciona?
- Projeto de pesquisa específico alinhado com professor

Questões práticas

- Grupo (email)
  - https://groups.google.com/d/forum/prog2-uff-2019-2
- Site
  - https://sicccIber.com.br/ensino/programacao-de-computadores-ii/programacao-de-computadores-ii-uff-2019-2/

Questões operacionais

- Lista de presença em todas as aulas e provas
  - Lembrar ao professor de passar a lista
- "Simulados" para entender o "estilo" da prova
- Trabalhos: apresentações acontecerão em dia extra
  - Podemos agendar videoconferência
- Provas
  - VR substituirá menor nota entre P1 e P2
  - Vista de provas: Professor fica com as provas, aluno pode tirar foto
  - VR e VS "sob agendamento"

Cronograma

- Aguardar outros professores marcarem provas
  - Será divulgado no site do curso
- Feriados
  - 7-set, 12-out, **14-out (seg)**, 15-out, 26-out, **28-out (seg)**, 2-nov, 15-nov, 16-nov, **20-nov (qua)**, 21-nov, 23-nov
- Dias sem aula (por outros motivos)
  - **21-ago (qua), 2-set (seg) e 4 set (qua)**
- Dias de Aula
  - Agosto(5): 12, 14, 19, 26, 28
  - Setembro(7): 9, 11, 16, 18, 23, 25, 30
  - Outubro(8): 2, 7, 9, 14, 16, 21, 23, 30
  - Novembro(7): 4, 6, 11, 13, 18, 25, 27
  - Dezembro(5): 2, 4, 9, 11, 16

Sequência de atividades

- Parte 1 (14 dias) Agosto-Setembro-Outubro
  - 10 aulas teóricas/práticas/labs
  - 1 dias de simulados
  - 1 aula de correção de simulado (aula seguinte), revisão e dúvidas
  - Prova 1
  - Correção da Prova 1, dúvidas e recursos
- Parte 2 (14 dias) Outubro-Novembro
  - 10 aulas teóricas/práticas/labs
  - 1 dias de simulados
  - 1 aula de correção de simulado (aula seguinte), revisão e dúvidas
  - Prova 2
  - Correção da Prova 2, dúvidas e recursos
- Provas Finais (4 dias) Dezembro
  - Verificação de Reposição
  - Correção da VR, dúvidas e recursos (sob agendamento)
  - Verificação Suplementar
  - Correção da VS, dúvidas e recursos (sob agendamento)
- Divulgação das notas finais

Questões operacionais – Dias de Prova

- Consulta permitida - Folha A4 manuscrita
- Obrigatorjedade de assinar lista de presença - e verificar o "recebido" (rubrica) do professor.
- Horário rigoroso de entrega da prova
- Nome na prova a caneta
- Prova pode ser a lápis
- Atraso máximo de 30 minutos (ninguém pode sair antes disso)
  - Caso alguém chegue após 30 minutos, só poderá fazer a prova se ninguém tiver saído.
- Prova das duas matérias no mesmo dia (pode entrar 10 minutos antes - haverá sobreposição)
  - Aluno da matéria de 20:00 pode fazer a prova de 18:00 a 20:00 e sair 20:30
- questão da letra na redação das respostas na prova Letra (caligrafia) na redação das respostas na prova
- Não se levantar ou entregar prova qdo o prof. não estiver em sala

Material Didático

- Livros didáticos
  - Stallings, Computer Security
  - (Stallings, Cryptography and Network Security)
- Material apresentado a cada aula
  - Artigos científicos
  - Estudos, reportagens, white papers
  - Vídeos, Webinars, Podcasts
  - Livros de divulgação
  - Normas, Guias e Manuais

Apresentação

Conteúdo do Curso

Conteúdo do curso

- PARTE 1: APRESENTAÇÃO
  - 1. Apresentação: O Impacto da (In)Segurança
  - 2. Conceitos e Nomenclatura Básica
  - 3. Padronização de Segurança
  - 4. Segurança de Sistemas de Informação
  - 5. Riscos, Ameaças, Ataques e Atacantes

Conteúdo do curso

- PARTE 2: AMEAÇAS
  - 6. Vulnerabilidades de software
  - 7. Malware: Software Malicioso
  - 8. Ataques de Negação de Serviço
  - 9. Engenharia Social
  - 10. Ameaças Avançadas e Persistentes

Conteúdo do curso

- PARTE 3: FERRAMENTAS DE SEGURANÇA
  - 11. Identificação e Autenticação de Usuário
  - 12. Controle de Acesso
  - 13. Criptografia
  - 14. Sistemas de Detecção de Intrusão
  - 15. Segurança de Redes com Firewalls

Conteúdo do curso

- PARTE 4: PADRÕES DE SEGURANÇA
  - 16. Padronização
  - 17. Avaliação da Conformidade
  - 18. Segurança de Software e o Common Criteria
  - 19. Segurança de Módulos Criptográficos e o FIPS 140-2
  - 20. Sistemas de Gestão de Segurança da Informação e a ISO/IEC 27001
  - 21. Padrões Nacionais de Segurança

Conteúdo do curso

- PARTE 5: DESENVOLVIMENTO SEGURO E AVALIAÇÃO DE SEGURANÇA
  - 22. SDLC
  - 23. Desafios e Importância de Avaliar Segurança
  - 24. Riscos, requisitos, soluções aceitáveis e caracterização do Ativo
  - 25. Criptografia e Arquitetura de Segurança
  - 26. Análise de Código, Vulnerabilidades de Software e Aspectos de Implementação
  - 27. Testes Operacionais e Testes de Penetração
  - 28. Auditoria de Sistemas de Gestão

Conteúdo do curso

- PARTE 6: Sociedade, Governo e Setor Produtivo
  - 29. Gerenciamento de Riscos Cibernéticos
  - 30. Infraestruturas Críticas e Defesa Cibernética
  - 31. Regulação do Setor Cibernético