

Trabalhos e Projetos

Atividades do Curso





Trabalhos e Projetos

- › Permitem aprofundar e consolidar temas do curso
- › Valem pontos na média
 - Graduação: até um ponto (a mais) na média final
 - Pós-Graduação: valem metade da média
- › Estratégia (programa de milhagem): "acumular pontos" ao longo do curso
- › Regra de outro: plágio é inaceitável e injustificável
- › Cada entrega deverá vir acompanhada de:
 - relatório curto explicando a "teoria" sobre o assunto estudado
 - documento e vídeo (screencast) explicando o funcionamento do ambiente/programa/aplicação e a exploração da vulnerabilidade



Segurança de software (vulnerabilidades) - até 3 pontos

- › Implementar programa/aplicação simples com vulnerabilidade listada no SANS/CWE Top 25
- › Poderão ser implementados até 3 programas/aplicações
 - não pode haver sobreposição de vulnerabilidades entre diferentes alunos
 - preferencialmente, explorar ambientes diversos (SO, C/C++, appweb,...)

Segurança de redes (ferramentas) - até 2 pontos

- › implementar rede (possivelmente, usando virtualização) com ferramentas básicas de segurança (IDS, IPS, FW, SIEM,...)
 - pode ser feito em grupo pontuação é dividida pelo número de participantes do grupo
 - 1 ponto por tipo de ferramenta identificada
- › 0,2 a 1 ponto por cenário de uso (dependendo da complexidade)
- › Exemplo
 - topologia com filtro de pacotes (FW), bastião, IDS, SIEM (4 pontos)
 - cenário de scan interno detectado por IDS (+0,2 ponto)
 - Cenário de scan externo filtrado por IDS (+0,2 ponto)
 - cenário de ataque: exploração de vulnerabilidade do FW, bypass do bastião, acesso a hosts internos, alerta SIEM (+1 ponto)
- › Pontuação adicional se implementar honeypot (até 2 pontos)
 - 1 ponto pela implementação, 1 ponto pelo estudo dos ataques



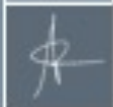
Números aleatórios – até 2 pontos

- › Identificar fontes distintas de números aleatórios e estudar a aleatoriedade
 - descrever como os números aleatórios são gerados
 - executar suítes do NIST, Dieharder, TestU01, PractRand e o gjrnd
 - medir entropia com 800-90B
- › 0,5 ponto por fonte "pronta"
- › 1,0 ponto por fonte "construída"
- › discutir com professor o que caracterizaria as fontes como "prontas" e "construídas"



Análise Estática de Código - até 1 ponto

- › - demonstrar casos de uso das seguintes técnicas
 - grafo de controle de fluxo
 - grafo de chamada
 - tainting
 - value set analysis
- › - os códigos analisados devem ser desenvolvidos pelo aluno



Análise Estática de Código - identificação de vulnerabilidades - até 1 ponto

- › Comparar pelo menos duas ferramentas com relação à identificação de vulns
- › Os códigos analisados devem ser desenvolvidos pelo aluno
- › 0,05 ponto por vuln identificada por todas as ferr.
- › 0,2 ponto por vuln não-identificada por alguma ferr.

Padrões de cybersecurity em setores específicos - até 1 ponto (individual)

- › Quais são as organizações e os padrões? Existem regulamentos? Existe certificação? Como funciona?
- › - setores
 - marítimo
 - energia
 - nuclear
 - veículos autônomos
 - saúde
 - segurança pública
 - governo
- › O aluno deve apresentar “proposta” de setor antes de executar pesquisas aprofundadas. Isso para garantir que existe quantidade adequada de material a ser estudado.



Outros temas – até 2 pontos cada

- › Alguns dos temas são projetos de pesquisa em parceria com colaboradores
 - Tais colaboradores estariam envolvidos com o projeto
- › Pontuação exata depende do grau de complexidade do projeto e dos resultados alcançados
- › Próximos slides apresentam os projetos