

PLANO DE PESQUISA

11º Feira de Ciências, Empreendedorismo e Inovação da Bahia

Título do Projeto: <i>Attack's Management System</i> - Sistema de Gerenciamento de Ataques
Estudantes: Thiago Santos Sousa; João Victor Santana Cavalcante
Professor Orientador: Silvelane Lima de Queiroz Pereira
Colégio: Centro Territorial de Educação Profissional Recôncavo II Alberto Torres
Série/Ano dos Estudantes: 3º ano
Questão ou Problema Identificado: <p>No contexto de sistemas de informação interligados existem informações em constante tráfego com a necessidade de segurança máxima. O software <i>Encryption's Builder Studio</i> (desenvolvido por Thiago Sousa), juntamente com as ferramentas de segurança da startup de desenvolvimento de software <i>EBS - Security Systems</i> destacaram-se propondo que a proteção de dados fosse um ponto relevante, em relação ao armazenamento e tráfego de dados. Porém como uma falta no projeto geral foi visto que o ataque também é um ponto crucial para manter os pilares da segurança da informação, pois para impedir a disseminação de informações falsas, o roubo de dados por invasão de sistemas, os ataques de negação de serviço (DDOS), o plágio de perfis nas redes (não necessariamente em redes sociais), entre outros, torna-se até então necessário o desenvolvimento de contramedidas variadas com o intuito de manter a integridade, confidencialidade e disponibilidade de serviços e informações.</p> <p>Nisto, trabalhando para proporcionar o ambiente digital privado mais seguro, um possível software chamado <i>Attack's Management System</i> pode se tornar um grande aliado no monitoramento e neutralização de ameaças em sistemas de rede privadas, além de ajudar os donos de perfis de grandes redes no monitoramento e neutralização automatizada de ataques.</p>
Hipótese ou Objetivo: <p>Elaborar uma ferramenta de neutralização de ameaças a partir dos mecanismos já existentes. A fim de contemplar o objetivo geral foram listados objetivos mais específicos:</p> <p>Demonstrar como ocorrem ataques cibernéticos</p>

Conscientizar o público geral sobre a prevenção de ataques e neutralização de ameaças

Explorar novas modalidades de ataque cibernético, a fim de desenvolver novas técnicas de proteção

Proteger uma instituição fictícia de um ataque de terrorismo virtual

Avaliar a eficácia dos métodos de neutralização de ameaças

Descrição Detalhada dos Materiais e Métodos (Procedimentos) que serão utilizados:

A pesquisa inicialmente será pautada através de estudos bibliográficos, vídeos, reportagens, artigos científicos, pesquisas, elementos necessários para compreensão e desenvolvimento do tema segurança cibernética, visando desenvolver uma simulação de terrorismo virtual e proteção da instituição.

A simulação de alguns tipos de ataques em organizações será apresentada, juntamente com as contramedidas possíveis.

Serão apresentados os seguintes ataques com as medidas de prevenção e remediação:

- DDOS (Ataque de Negação de Serviço)
- *Phishing*
- Invasão RDP (Windows)

Com as contramedidas para esses tipos de ataque o objetivo é criar um conjunto de ferramentas em um novo software chamado AMS (*Attack Management System*).

Para a pesquisa sobre as principais maneiras que ocorrem os ataques, juntamente com as contramedidas foram utilizados artigos, pesquisas e vídeos na internet.

Para a simulação de ataque e defesa foi utilizado o Microsoft PowerPoint, onde foram criadas apresentações dinâmicas, onde o usuário poderia interagir diretamente. Em breve estará disponível na web.

Como o software ainda não foi desenvolvido, mas já existe a possibilidade de sua criação está sendo criada a documentação de casos de uso do sistema em UML (Linguagem de Modelagem Unificada). Existe uma grande possibilidade de ser desenvolvido utilizando a linguagem Python, porém será integrado com outras aplicações em VPS de C# e até PHP.

As pessoas que estiverem interessadas em adquirir o software podem se cadastrar no EBS-WEB (<https://web.ebs-systems.epizy.com/>), uma aplicação que disponibiliza o acesso às aplicações oficiais da EBS Systems, startup de programação dos alunos de informática do CETEP Alberto Torres.

Bibliografia (Três referências mais importantes)

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers Expostos:- Segredos e Soluções para a Segurança de Redes**. Bookman Editora, 2014.

HOSANG, Alexandre. Política Nacional de Segurança Cibernética: uma necessidade para o Brasil. **Escola Superior De Guerra**, Rio De Janeiro, 2011. Disponível em:
<https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1417/1/Alcyon%20Ferreira%20de%20Souza%20Junior.pdf>