UNISUL – UNIVERSIDADE DO SUL DE SANTA CATARINA
CURSO DE CIÊNCIAS DA COMPUTAÇÃO – SEGURANAÇA DE REDES
PROF. SILVANA MADEIRA ALVES DAL-BÓ
ALUNO(A):_____
30/11/2020

**Orientações e critérios de avaliação:**
- avaliação é individual, consequentemente, as respostas são individuais, cópias entre colegas ou da internet serão consideradas plágio;
- seguir a quantidade máxima de linhas de resposta em cada questão;
- enviar o arquivo preferencialmente até as 22h30min (exceções entrar em contato para justificar).

## PROVA TEÓRICA

1. [2.0] Cenário: as violações de segurança em uma organização podem resultar em perdas tanto de receitas, dados sigilosos, segurança física, pessoal etc. Em aula discutimos diversos casos e situações de violações de segurança oriundos de ameaças internas e extensas. Cite duas situações (uma interna e outra externa) que contextualize esse cenário.

**Internas:** funcionários não instruídos aos quesitos de segurança da informação podem ser ameaças internas contribuindo principalmente para facilitar o acesso através de ataques de engenharia social, fornecendo acesso físico ao local ou clicando em links maliciosos (phishing).
**Externas:** phishing é um dos tipos de ataques que embora seja externo, tem maior chances de sucesso quando há ameaças internas, como no caso dos funcionários. DDOS é um exemplo de vetor externo e consiste em negação de serviço, a característica é sobrecarregá-lo tornando indisponível, normalmente existem outros fatores envolvidos juntamente com este ataque.

Máximo 10 linhas

2. Recentemente pode-se acompanhar nos noticiários um ataque hacker ao TSE. Acesse artigo sobre o caso no link:

   https://g1.globo.com/google/amp/jornal-nacional/noticia/2020/11/28/suspeito-de-atacar-o-sistema-de-computadores-do-tse-antes-do-1o-turno-e-preso-em-portugal.ghtml

a. [3.0] Relacione o caso ocorrido com seus estudos sobre Segurança: princípios de segurança (violações), tipo de ataque, características do hacker, etc:

A notícia em si não deixa claro o tipo de ataque. O site do Conjur cita como sendo um ataque massivo, conhecido como ataque DDOS ou negação de serviço. A característica é realizar múltiplas requisições de origens diferentes para tentar derrubar o serviço (o que não ocorreu segundo o TSE), muitas vezes estes ataques são direcionados ao DNS ou firewall, para retirá-los do caminho. Os princípios de segurança envolvidos são da: disponibilidade e confidencialidade.

Máximo 6 linhas

b. [2.5] Que mecanismos de segurança/criptografia poderiam ser incorporados em um plano de continuidade para evitar que novos ataques venham a acontecer nesse caso ocorrido?

Para recuperação dos dados com facilidade: replicação dos dados para outros servidores, backup frequentes. Para evitar futuros ataques e garantir a segurança da rede, aplicar políticas de segurança via firewall mais restritivas, criptografar os dados armazenados para dificultar a leitura em caso de ataques, garantindo a confidencialidade da informação. Realizar conexões e tráfego dos dados via protocolos seguros e isolar os servidores com informações sensíveis das redes acessíveis internamente.

Máximo 10 linhas

3. [2.5] Firewall pode ser definido como um “Componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet, ou entre conjunto de redes.” (Chapman), tem por objetivo proteger uma rede de acessos não autorizados, vazamento de informações e controle de segurança. Comente sobre seu projeto final e de que forma está relacionado ao componente Firewall.

**Tema:**
LGPD – Lei Geral de Proteção de Dados

**Discussão:**
Embora seja um tema mais distante do firewall em si, tal assunto contribui para o cumprimento da LGPD, visto que ela trata da segurança dos dados, confidencialidade, auditoria e outros. O firewall é um agente de extrema importância para tal garantia. Através de regras de acesso conseguimos realizar

auditoria das informações, garantir a confidencialidade e o acesso apenas às pessoas autorizadas.

Máximo 10 linhas