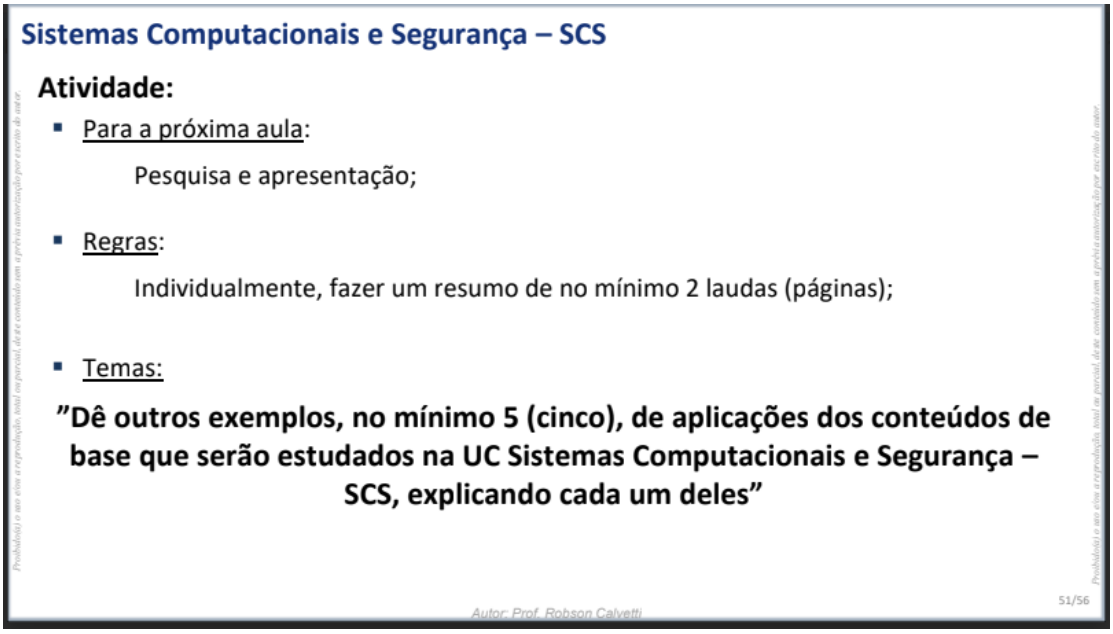
ATIVIDADE PRÁTICA-00

Erick Domingues Soares- 82414486



Sistemas Computacionais e Segurança – SCS

Atividade:

- Para a próxima aula:

  Pesquisa e apresentação;

- Regras:

  Individualmente, fazer um resumo de no mínimo 2 laudas (páginas);

- Temas:

"Dê outros exemplos, no mínimo 5 (cinco), de aplicações dos conteúdos de base que serão estudados na UC Sistemas Computacionais e Segurança – SCS, explicando cada um deles"

Autor: Prof. Robson Calvetti

51/56

1. **Autenticação e Controle de Acesso em Sistemas Empresariais:**

    - **Descrição Detalhada:** A autenticação é o processo de verificar a identidade de um usuário, enquanto o controle de acesso refere-se às permissões concedidas a esse usuário para interagir com o sistema. Em sistemas empresariais, isso envolve o uso de senhas robustas, autenticação multifatorial (MFA), e sistemas de gerenciamento de identidade e acesso (IAM). A MFA pode incluir algo que o usuário sabe (senha), algo que o usuário tem (um token de segurança), e algo que o usuário é (biometria).

    - **Aplicação Prática:** Imagine uma empresa que utiliza um sistema ERP (Enterprise Resource Planning) para gerenciar suas operações. O sistema ERP deve garantir que apenas funcionários autorizados possam acessar informações sensíveis, como relatórios financeiros e dados de clientes. A empresa implementa um sistema de autenticação de dois fatores, exigindo que os funcionários ingressem uma senha e um código enviado para seus dispositivos móveis. Além disso, o sistema usa o controle de acesso baseado em funções para garantir que um gerente possa acessar relatórios financeiros enquanto um funcionário de nível mais baixo não pode.

2. **Criptografia de Dados em Transações Financeiras:**

    - **Descrição Detalhada:** A criptografia é usada para proteger dados de ser lido ou alterado por partes não autorizadas. Em transações financeiras online, isso é crucial para garantir a segurança dos dados financeiros durante a transmissão. A criptografia de dados em repouso (armazenados) e em trânsito (durante a transmissão) é aplicada para proteger informações sensíveis, como números de cartão de crédito e detalhes bancários.

    - **Aplicação Prática:** Quando um usuário faz uma compra em um site de comércio eletrônico, como o eBay, os dados do cartão de crédito são transmitidos do navegador do usuário para o servidor do site. Para proteger essas informações, o site utiliza criptografia SSL/TLS (Secure Sockets Layer/Transport Layer Security), que criptografa a comunicação entre o navegador e o servidor. Isso impede que hackers interceptem e leiam os dados do cartão durante a transação. Além disso, os dados são armazenados de forma criptografada no banco de dados do site para proteção adicional.

3. **Segurança em Redes de Computadores:**

    - **Descrição Detalhada:** A segurança de redes envolve proteger a infraestrutura de rede contra acessos não autorizados e ataques cibernéticos. Isso pode incluir a instalação de firewalls para filtrar tráfego indesejado, sistemas de detecção e prevenção de intrusões (IDS/IPS) para identificar e responder a atividades suspeitas, e práticas de segmentação de rede para limitar o impacto de possíveis violações.

    - **Aplicação Prática:** Em uma instituição financeira, como um banco, a segurança da rede é fundamental para proteger dados financeiros e informações pessoais dos clientes. O banco utiliza firewalls para bloquear tentativas de acesso não

autorizado e IDS para monitorar atividades na rede em tempo real. Se uma tentativa de ataque é detectada, o IDS alerta os administradores para que possam tomar medidas corretivas imediatamente. Além disso, a rede interna é segmentada para garantir que uma possível violação em uma parte da rede não comprometa todo o sistema.

4. **Segurança em Aplicações Web:**
    - **Descrição Detalhada:** A segurança de aplicações web envolve a proteção contra vulnerabilidades específicas que podem ser exploradas por atacantes. Isso inclui a implementação de práticas de codificação segura, validação de entradas do usuário para evitar injeções de código, e proteção contra ataques de Cross-Site Scripting (XSS) e Cross-Site Request Forgery (CSRF). A segurança também pode ser reforçada com cabeçalhos de segurança HTTP e políticas de segurança de conteúdo (CSP).
    - **Aplicação Prática:** Considere um site de e-commerce que permite aos usuários criar contas e fazer compras. Para proteger o site contra ataques, o desenvolvedor implementa medidas como validação de entradas para evitar SQL Injection (onde um atacante insere código SQL malicioso em formulários) e utiliza bibliotecas que escapam caracteres especiais para prevenir XSS. O site também usa tokens anti-CSRF para garantir que as solicitações enviadas pelos usuários sejam legítimas. Essas práticas ajudam a proteger os dados dos clientes e a integridade do sistema.
5. **Resposta a Incidentes e Recuperação de Desastres:**
    - **Descrição Detalhada:** Resposta a incidentes envolve a identificação, contenção, erradicação e recuperação de eventos de segurança que afetam a integridade dos sistemas e dados. A recuperação de desastres é o processo de restaurar as operações normais após um evento disruptivo, como uma falha de hardware, um ataque cibernético ou um desastre natural. Isso inclui a criação de planos de resposta a incidentes, a realização de simulações de ataques e a implementação de estratégias de backup e restauração.
    - **Aplicação Prática:** Suponha que uma empresa de telecomunicações sofre um ataque de ransomware que criptografa todos os seus arquivos críticos. O plano de resposta a incidentes da empresa inclui procedimentos para isolar o ataque, notificar os principais stakeholders, e iniciar a restauração dos dados a partir de backups recentes. A empresa realiza regularmente backups completos e incrementais dos dados e armazena esses backups em locais seguros, como na nuvem e em mídias físicas off-site. O plano de recuperação de desastres garante que, mesmo após o ataque, a empresa possa restaurar rapidamente os serviços e minimizar o tempo de inatividade.

Esses exemplos mostram como os conceitos de sistemas computacionais e segurança são aplicados em cenários do mundo real para proteger informações e garantir a continuidade das operações.