Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
T +55 (87) 3764-5500
m http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 01 - Introdução
Para apresentação e discussão em sala de aula, em 1º de junho de 2023.

Nome completo: Geisianny Bernardo da Silva

Questões retiradas do livro-texto da disciplina.
Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

1. O que é a arquitetura de segurança OSI?

É um modelo de referência que baseia-se na necessidade das organizações de terem políticas de segurança e serviços que possibilitem avaliar todos os aspectos relacionados à segurança de suas informações.Essa arquitetura focaliza ataques, mecanismos de segurança e serviço, assim, ataque de segurança: qualquer ação que comprometa a segurança das informações pertencentes a uma organização; Mecanismo de segurança: um processo (ou dispositivo que incorpora esse processo) projetado para detectar, prevenir ou recuperar-se de um ataque de segurança; E serviço de segurança: um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e das transferências de informações de uma organização. Esses serviços têm como objetivo frustrar ataques de segurança e podem fazer uso de um ou mais mecanismos para alcançar esse objetivo.

2. Qual é a diferença entre ameaças à segurança passivas e ativas?

Um ataque passivo é a tentativa de descobrir ou utilizar informações ao sistema, mas não afetando os seus recursos. Já um ataque ativo é a tentativa de alterar recursos do sistema ou afetar sua operação.

3. Liste e defina resumidamente as categorias de ataques passivos e ativos à segurança.

Essas categorias descrevem os diferentes tipos de ataques que podem ocorrer, tanto de

forma passiva, onde as informações são observadas e obtidas sem interferência, quanto de forma ativa, onde ações maliciosas são realizadas para explorar vulnerabilidades ou obter informações confidenciais.As categorias de ataques passivos à segurança são: Monitoramento: Envolve a interceptação e monitoramento não autorizado de informações, como tráfego de rede, comunicações ou dados em repouso, sem alterá-los; Espionagem: Refere-se à obtenção não autorizada de informações confidenciais ou estratégicas por meio de escutas, vigilância ou acesso indevido a sistemas ou dispositivos; e análise de tráfego: Consiste em analisar o tráfego de rede para obter informações sensíveis, como senhas, dados pessoais ou detalhes de transações, sem interromper a comunicação. Os ataques ativos: Injeção de código: Envolve a inserção de código malicioso em um sistema ou aplicativo para explorar vulnerabilidades e executar ações indesejadas, como roubo de dados, controle remoto ou comprometimento do sistema; Negação de serviço (DoS): O objetivo é sobrecarregar um sistema, serviço ou rede, impedindo que usuários legítimos acessem ou utilizem recursos. Isso é feito através de tráfego excessivo, exploração de vulnerabilidades ou esgotamento de recursos;Ataques de phishing: São tentativas de obter informações confidenciais, como senhas, números de cartão de crédito ou informações pessoais, fazendo-se passar por entidades confiáveis em comunicações eletrônicas, como e-mails ou mensagens; e ataques de engenharia social: Consistem em manipular ou enganar os usuários para obter acesso a informações confidenciais ou realizar ações prejudiciais. Isso pode envolver persuasão, falsa representação, intimidação ou exploração da confiança das pessoas.

4. Liste e defina resumidamente as categorias dos serviços de segurança.

Esses serviços são fundamentais para proteger sistemas, redes e dados contra ameaças e garantir a segurança das informações.Sendo eles:

As categorias dos serviços de segurança são: Autenticação: Verificação da identidade antes do acesso a recursos protegidos; Autorização: Controle de acesso com base em permissões atribuídas aos usuários autenticados; Criptografia: Proteção dos dados por

meio de algoritmos que tornam as informações ininteligíveis para terceiros não autorizados;Firewall: Monitoramento e bloqueio de conexões indesejadas ou maliciosas em redes; Detecção de intrusões: Monitoramento e alerta sobre atividades suspeitas ou maliciosas; Prevenção de intrusões: Identificação e bloqueio ativo de tentativas de invasão em tempo real; Antivírus e antimalware: Detecção e remoção de software malicioso para proteção contra infecções; E gerenciamento de eventos e informações de segurança (SIEM): Coleta, correlação e análise de eventos de segurança para identificar ameaças e tomar ações adequadas.

5. liste e defina resumidamente as categorias dos mecanismos de segurança.

As categorias dos mecanismos de segurança são: Controle de Acesso: Regula o acesso a recursos, garantindo que apenas usuários autorizados possam utilizá-los; Criptografia: Codifica os dados para proteger sua confidencialidade e integridade; Assinatura Digital: Fornece autenticidade e integridade em transações eletrônicas;Firewalls: Monitoram e controlam o tráfego de rede, protegendo contra acessos indesejados;Detecção e Prevenção de Intrusões: Identificam atividades maliciosas e tomam medidas para detê-las;Segurança em Camadas: Implementam várias camadas de defesa para proteger sistemas e redes; Autenticação Multifator: Exige múltiplos fatores para verificar a identidade dos usuários. e respaldo e Recuperação: Realizam cópias de segurança e permitem a recuperação em caso de falhas.

6. Considere um caixa eletrônico ATM no qual os usuários fornecem um cartão e um número de identificação pessoal (senha). Dê exemplos de requisitos de confidencialidade, integridade e disponibilidade associados com esse sistema e, em cada caso, indique o grau de importância desses requisitos.

No sistema de um ATM eletrônico, os requisitos de confidencialidade, integridade e disponibilidade são essenciais para garantir a segurança e o funcionamento adequado do sistema. A confidencialidade deve ser mantida para os dados do cartão e as senhas dos usuários, evitando assim fraudes financeiros e protegendo as informações pessoais. A integridade das transações é fundamental para garantir que os valores sejam corretamente debitados ou creditados nas contas dos usuários, evitando manipulações ou alterações indevidas. Além disso, é necessário proteger o software e os dados contra alterações não autorizadas, assegurando a confiabilidade do sistema. A disponibilidade do serviço é primordial para permitir que os usuários realizem suas transações a qualquer momento, garantindo a conveniência e a eficiência do serviço. É importante fornecer suporte adequado e realizar manutenções preventivas para evitar interrupções prolongadas e garantir o funcionamento contínuo do caixa eletrônico. A quebra de

confidencialidade, integridade ou disponibilidade pode resultar em consequências graves, como fraudes financeiras, comprometimento das informações pessoais dos usuários e indisponibilidade do serviço, tornando esses requisitos de alta importância.

7. Para responder as letras abaixo, por favor, consulte o livro-texto da disciplina:

(a) Desenhe uma matriz similar ao Quadro 1.4 que mostre o relacionamento entre serviços de segurança e ataques.

- Controle de acesso;
- Controle de roteamento;
- Integridade de dados:
- Autenticação da origem de dados;

(b) Desenhe uma matriz similar ao Quadro 1.4 que mostre o relacionamento entre mecanismos de segurança e ataques.

- Controle de acesso;
- Assinatura digital;
- Autenticação da origem de dados;
- Confidencialidade do uxo de tráfego;
- Integridade de dados;
- Responsabilização.

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed.6. 2014.