Universidade Federal do 

Agreste de Pernambuco

Av. Bom Pastor s/n - Boa Vista

55292-270 Garanhuns/PE

+55 (87) 3764-5500

http://www.ufape.edu.br

| Bacharelado em Ciência da Computação  CCMP3079 Segurança de Redes de Computadores  Prof. Sérgio Mendonça  Atividade Cap. 01 - Introdução  10 de outubro de 2023. |
| --- |

Nome Completo: **Luiz Fellipe de Almeida Rodrigues Barbosa**

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?

**R - A arquitetura de segurança OSI define os requisitos e técnicas para garantir a segurança em redes de computadores de uma organização. Ela serve como um guia para organizar a implementação de medidas de segurança. Esta arquitetura se concentra em três aspectos principais: ataques à segurança, mecanismos de segurança e serviços de segurança. Podendo serem resumidos da seguinte forma:**

* **Ataque à segurança:** refere-se a qualquer ação que comprometa a segurança da informação de uma organização.
* **Mecanismo de segurança:** são processos ou dispositivos projetados para detectar, prevenir ou recuperar-se de ataques à segurança.
* **Serviço de segurança:** engloba as funções oferecidas pelos mecanismos de segurança para proteger a rede e os dados contra ameaças.

**Essa abordagem ajuda a compreender melhor os riscos de segurança e a implementar medidas adequadas para proteger as redes e os sistemas de uma organização.**

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

**R - As ameaças à segurança passivas são caracterizadas pelo monitoramento ou bisbilhotagem das transmissões de dados, com o objetivo de obter informações sem modificar o fluxo de dados. Exemplos incluem vazamento de conteúdo de mensagem e análise de tráfego. Por outro lado, as ameaças à segurança ativas envolvem a modificação do fluxo de dados ou a criação de fluxos falsos, como disfarce, repasse, modificação de mensagens e negação de serviço. De modo geral, as ameaças passivas visam obter informações sem alterar os dados, enquanto as ameaças ativas envolvem a modificação ou interrupção do fluxo de dados.**

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

**R -**

**Ataques Passivos:**

1. **Vazamento de Conteúdo de Mensagem:** Bisbilhotar transmissões para obter informações sensíveis ou confidenciais.
2. **Análise de Tráfego:** Observar padrões de comunicação, mesmo que o conteúdo esteja encriptado, para deduzir informações sobre a natureza da comunicação.

**Ataques Ativos:**

1. **Disfarce:** Fingir ser outra entidade para obter acesso não autorizado.
2. **Repasse:** Capturar e retransmitir dados para produzir um efeito não autorizado.
3. **Modificação de Mensagens:** Alterar partes de uma mensagem legítima para alcançar um resultado não autorizado.
4. **Negação de Serviço:** Inibir ou impedir o uso normal de instalações de comunicação, seja direcionado ataques a um alvo específico ou perturbando toda uma rede.

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

**R -**

1. **Autenticação:** Garante a certeza de que a entidade comunicante é realmente quem afirma ser. Isso inclui autenticação da entidade pareada, que verifica a identidade das entidades em uma conexão, e autenticação da origem de dados, que autentica a origem de uma unidade de dados.
2. **Controle de Acesso:** Previne o uso não autorizado de recursos, controlando quem pode acessá-los, sob que condições e o que é permitido para quem acessa.
3. **Confidencialidade dos Dados:** Protege os dados contra divulgação não autorizada. Isso pode incluir a confidencialidade da conexão, confidencialidade sem conexão, confidencialidade com campo seletivo e confidencialidade do fluxo de tráfego.
4. **Integridade dos Dados:** Garante que os dados recebidos sejam exatamente conforme enviados por uma entidade autorizada, sem modificações, inserções, exclusões ou repasses. Isso pode envolver integridade da conexão com recuperação, integridade da conexão sem recuperação, integridade da conexão com campo seletivo, integridade sem conexão e integridade sem conexão com campo seletivo.
5. **Irretratabilidade:** Impede que o emissor ou o receptor neguem uma mensagem transmitida, fornecendo prova de que a mensagem foi enviada pela parte especificada (irretratabilidade de origem) ou prova de que a mensagem foi recebida pela parte especificada (irretratabilidade de destino).
6. **Serviço de Disponibilidade:** Garante que um sistema ou recurso do sistema seja acessível e utilizável sob demanda por uma entidade autorizada, de acordo com as especificações de desempenho. Isso inclui proteção contra ataques de negação de serviço e depende do gerenciamento adequado dos recursos do sistema.

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

**R -**

1. **Mecanismos de segurança específicos:**
   * **Codificação**: Utilização de algoritmos matemáticos para transformar os dados em um formato não prontamente inteligível, geralmente com o uso de chaves de encriptação.
   * **Assinatura digital:** Dados anexados a uma unidade de dados que permitem que o destinatário prove sua origem e integridade e protege contra falsificação.
   * **Controle de acesso:** Conjunto de mecanismos que impõem direitos de acesso aos recursos.
   * **Integridade de dados:** Conjunto de mecanismos usados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.
   * **Troca de autenticação:** Mecanismo para garantir a identidade de uma entidade por meio da troca de informações.
   * **Preenchimento de tráfego:** Inserção de bits nas lacunas de um fluxo de dados para frustrar análises de tráfego.
   * **Controle de roteamento:** Permite a seleção de rotas seguras para determinados dados e mudanças de roteamento.
   * **Notarização**: Uso de um terceiro confiável para garantir certas propriedades de uma troca de dados.
2. Mecanismos de segurança difusos:
   * **Funcionalidade confiada:** Aquilo que é percebido como correto de acordo com critérios estabelecidos por uma política de segurança.
   * **Rótulo de segurança:** Marcação vinculada a um recurso que nomeia ou designa os atributos de segurança desse recurso.
   * **Detecção de evento:** Detecção de eventos relevantes à segurança.
   * **Trilha de auditoria de segurança:** Dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança.
   * **Recuperação de segurança**: Lida com solicitações de mecanismos de tratamento e gerenciamento de eventos e toma medidas de recuperação.

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.

**R -**

1. **Confidencialidade:**
   * **Requisito**: Garantir que as informações pessoais dos usuários, como números de conta e senhas, sejam mantidas em sigilo e não sejam acessíveis a pessoas não autorizadas.
   * **Importância**: Muito alta. A confidencialidade é fundamental para proteger os dados sensíveis dos clientes contra acesso não autorizado, prevenindo assim o roubo de identidade e a fraude financeira.
2. **Integridade**:
   * **Requisito**: Assegurar que as transações realizadas pelos usuários não sejam alteradas durante o processo de transferência de dados entre o ATM e o banco.
   * **Importância**: Alta. A integridade garante que as transações sejam processadas conforme a intenção do usuário e que não sejam adulteradas ou corrompidas no meio do caminho, evitando assim a perda de fundos e problemas de contabilidade.
3. **Disponibilidade**:
   * **Requisito**: Garantir que o sistema ATM esteja sempre disponível para os usuários realizarem transações, sem interrupções significativas ou tempos de inatividade prolongados.
   * **Importância**: Muito alta. A disponibilidade é crucial para garantir que os clientes possam acessar seus fundos a qualquer momento, especialmente em situações de emergência. Qualquer interrupção no serviço pode causar inconvenientes aos usuários e afetar a reputação do banco.

Esses requisitos são fundamentais para garantir a segurança e o bom funcionamento de um sistema ATM, e sua importância é refletida na necessidade de implementar medidas robustas de segurança e manutenção para atender a esses requisitos.

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.

| Ataques  X  Segurança | Vazamento de conteúdo | Analise de trafego | Disfarce | Repasse | Modificação de mensagem | Negação de serviço |
| --- | --- | --- | --- | --- | --- | --- |
| Autenticação | X |  | X |  | X |  |
| Controle de Acesso | X |  |  | X |  |  |
| Conf. de Dados | X | X |  |  |  |  |
| Int. de Dados |  |  | X | X | X | X |
| Irretratabilidade |  |  |  |  |  | X |

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

| Ataques  X  Mecanismos | Vazamento de conteúdo | Analise de trafego | Disfarce | Repasse | Modificação de mensagem | Negação de serviço |
| --- | --- | --- | --- | --- | --- | --- |
| Codificação | X | X | X | X | X |  |
| Assinatura Digital |  |  | X |  |  | X |
| Controle de Acesso | X |  |  |  | X | X |
| Integridade de dados |  |  |  |  | X |  |
| Troca de Autenticação | X |  | X |  |  |  |
| Preen. de Trafego |  | X |  |  |  |  |
| Contr. de Roteamento | X |  |  | X |  |  |
| Notalização |  |  |  | X |  |  |