**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**  **10 de outubro de 2023.** |
| --- |

**Nome Completo:**

* Izabel Yale Neves Nascimento
* Jonas Ferreira Leal Junior

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?**

A arquitetura de segurança OSI traz uma visão geral de pontos importantes sobre a segurança de comunicações em redes de computadores, ela se baseia nas recomendações X.800 e RFC 4949 e apresenta definições de ataque à segurança, mecanismos de segurança, serviços de segurança, ameaça e ataque, sendo este último dividido em ataques passivos e ataques ativos.

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

Ameaças passivas à segurança é uma falha de segurança em que há possibilidade de um usuário capturar e observar o conteúdo de objetos enviados pela rede, violando assim a privacidade, mas não a integridade da comunicação. Já uma ameaça ativa a segurança, são brechas em um sistema que permitem que este usuário mal intencionado comprometa a integridade da comunicação, alterando informação da mensagem ou até mesmo mudando-a completamente para atender aos seus fins.

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

**Ataque passivo:**

* **Vazamento de dados**, muito comum atualmente, consiste em coletar informações sobre uma comunicação ou usuário e expor publicamente esses dados.
* **Análise de tráfego**, consiste em coletar dados e utilizar algum processamento que encontre relações entre esses dados e a partir daí extrair informações

**Ataques ativos:**

* **Disfarce**, acontece quando se passa por outra a fim de obter dados ou permissões não autorizadas.
* **Repasse**, consiste em capturar dados de forma passiva e na sequência retransmitir esses dados de forma a atender o propósito do usuário atacante.
* **Modificação de mensagem,** nessa situação o atacante modifica parte da mensagem original, adia ou reordena as mensagens para obter alguma vantagem.
* **Negação de serviço**, um método de ataque popular que visa tornar um serviço indisponível em sua totalidade ou parcialmente, a fim de obter vantagem, seja na exploração de brechas de segurança ou vantagem oriunda da indisponibilidade do serviço por meio do atacado.

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

**Serviços de Segurança**

* **Autenticação**: Certeza que as entidades que fazem parte da comunicação é quem diz ser.
* **Controle de acesso**: Prevenção de acesso ou uso de recursos não autorizados.
* **Confidencialidade**: Garantir que os dados não sejam acessados por entidades não autorizadas
* **Integridade**: Certeza que os dados serão enviados e recebido pelas partes autorizadas sem violação
* **Irretratabilidade**: Garantia de que cada uma das entidades fizeram parte da comunicação.

1. **Liste e defina resumidamente as categorias dos mecanismos de segurança.**

Implementação em protocolos da camada OSI **(Mecanismos específicos)**

* **Codificação**: uso de algoritmo matemático para encriptar dados;
* **Assinatura digital**: Mecanismo que possibilita provar a origem e integridade dos dados;
* **Controle de acesso**: Restrição de acesso a um recurso;
* **Integridade de dados**: Mecanismos que garantem que o dado será recebido da mesma forma que foi enviado pela fonte
* **Troca de autenticação:** Mecanismo de troca de informação com finalidade de garantir que a entidade é quem diz ser
* **Preenchimento de tráfego:** Inserção de bits nas lacunas de um fluxo de dados, a fim de frustrar tentativas de análise de tráfego;
* **Controle de roteamento:** Permite mudar o caminho por onde os dados trafegam, com o intuito de evitar brechas de segurança
* **Notarização:** Utilização de um terceiro confiável para garantir a confiabilidade da troca de informações

Independente de protocolos **(Mecanismos difusos)**

* **Funcionalidade confiada:** Funcionamento e/ou conduta aprovado pelo usuário, por exemplo, os termos de uso que devem ser lidos ao criar uma conta em algum site.
* **Rótulo de segurança:** uma classificação atribuída a recursos para definir níveis de acesso liberados para usuários autorizados.
* **Detecção de eventos:** Monitorar atividades no sistema para detecção de comportamentos suspeitos.
* **Trilha de auditoria de segurança:** Coleta de dados que podem ser utilizados para realizar auditoria de atividades do sistema.
* **Recuperação de segurança:** Plano de ação com medidas a serem tomadas em caso de surgimento de problemas como falhas de software, invasões, indisponibilidade, etc. Esse mecanismo também pode se dar na prevenção, como alertas em estatísticas do software e simulações.

1. **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.**

Confidencialidade: Restringir acesso somente a usuários autorizados, evitando a divulgação de informações sensíveis. Por exemplo, saldo ou crédito de uma conta, dados como endereço, nome, extratos.

Integridade: Garantir que o ATM funcione somente da maneira que foi projetado para funcionar. Impedir que um usuário altere por exemplo o seu saldo sem realizar saques ou depósitos, que não seja possível realizar saques de uma conta que não seja o titular.

Disponibilidade: Assegurar acesso rápido e confiável ao usuário autorizado, evitar o máximo possível travas e momentos em que o sistema não responde ao usuário. Exemplo disso é instabilidade ou falta de comunicação do ATM com o sistema do banco, sistema operacional do ATM travar ou reiniciar durante o uso, funções do ATM sem funcionar ou funcionando com deficiência, como leitor biométrico que não pega, ou leitores de cartão que travam e não libera o cartão.

1. **Para responder as letras abaixo, por favor, consulte o livro-texto da disciplina:**  
   **ATAQUES**:
2. **Desenhe uma matriz similar ao Quadro 1.4 que mostre o relacionamento entre serviços de segurança e ataques.**

* 1. Vazamento de dados
  2. Análise de tráfego
  3. Disfarce
  4. Repasse
  5. Modificação de mensagens
  6. Negação de serviço

|  | **ATAQUES** | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **SERVIÇO** | a | b | c | d | e | f |
| Autenticação |  | S | S |  |  |  |
| Controle de acesso | S | S |  |  |  |  |
| Confidencialidade | S |  |  |  |  |  |
| Integridade de dados |  |  |  | S | S |  |
| Responsabilização |  | S |  |  |  |  |
| Disponibilidade |  |  |  |  |  | S |

1. **Desenhe uma matriz similar ao Quadro 1.4 que mostre o relacionamento entre mecanismos de segurança e ataques.**

|  | **ATAQUES** | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **MECANISMOS** | a | b | c | d | e | f |
| Codificação | S |  |  |  |  |  |
| Assinatura digital |  |  | S |  |  |  |
| Controle de acesso |  | S | S |  |  |  |
| Integridade de dado |  |  |  |  | S |  |
| Troca de autenticação |  | S | S |  |  |  |
| Preenchimento de tráfego |  | S |  |  |  |  |
| Controle de roteamento | S | S |  |  |  | S |
| Notarização |  |  | S | S |  |  |
| Funcionalidade confiada | S |  | S |  | S |  |
| Rótulo de segurança |  |  | S | S | S |  |
| Detecção de eventos |  |  |  |  | S | S |
| Trilha de auditoria de segurança | S |  | S |  | S |  |
| Recuperação de segurança |  |  |  |  |  | S |