Disciplina: Segurança de rede de computadores (2022.2)
Nome completo: Carlos André de Almeida Cavalcante

1) **O que é a arquitetura de segurança OSI?**
   R: É a arquitetura desenvolvida pelo padrão internacional X.800 da ITU-T, ela define um método sistemático de definições a requisitos de segurança e caracterização de técnicas que os satisfazem, ou seja, oferece uma visão geral sobre os ataques, mecanismos e serviços de segurança.

2) **Qual é a diferença entre ameaças à segurança passivas e ativas?**
   R: Diria que a principal diferença entre ameaças passivas e ativas está na característica da possibilidade detecção da ameaça, como uma ameaça passiva tem a intenção de apenas escutar os dados ela é indetectável, já a ativa tem a intenção de modificar, trocar a ordem ou negar o serviço.

3) **Liste e defina resumidamente as categorias de ataques passivos e ativos à segurança.**
   R: As categorias de ataques passivos temos
   i) O vazamento de conteúdo de mensagem: consiste na escuta e obtenção de dados confidenciais ou sensíveis em mensagens, conversa telefônica, correio eletrônico, etc.
   ii) Análise de tráfego: resumisse em analisar o padrão de mensagens, seu local de origem e destino, identidades de origem e destino da mensagem, frequência e tamanho da mensagem, tais informações são úteis para descobrir a natureza da comunicação que está ocorrendo.

   Já as categorias de ataques ativos são
   i) Disfarce: uma entidade adquire privilégios por meio de autenticações frágeis, fazendo que a mesma possa utilizar tais privilégios.
   ii) Repasse: envolve a captura passiva de uma unidade de dados e sua subsequente retransmissão para produzir um efeito não autorizado.
   iii) Modificação da mensagem: alguma parte da mensagem é interceptada e modificada ou ainda que a mesma adiada ou reordenada.
   iv) Negação do serviço: interrompe ou barra o uso do serviço de comunicação.

4) **Liste e defina resumidamente as categorias dos serviços de segurança.**
   R: Os serviços de segurança são divididos em cinco categorias cada qual serviços específicos, são elas
   I) Autenticação: diz respeito que se tem a certeza que a entidade que está se comunicando é aquela que afirma ser.
      a) Autenticidade de entidade pareada: usada em associação com uma conexão lógica para fornecer confiança na identidade das entidades conectadas.

b) Autenticidade de origem de dados: em uma transferência sem conexão, oferece certeza de que a origem dos dados recebidos é conforme alegada.

II) Controle de acesso: prevenção de uso não autorizado de um recurso.

III) Confidencialidade dos dados: proteção dos dados contra divulgação não autorizada.

a) Confidencialidade de conexão: proteção de todos os dados do usuário em uma conexão.
b) Confidencialidade sem conexão: proteção de todos os dados do usuário em um único bloco de dados.
c) Confidencialidade com campo seletivo: confidencialidade de campos selecionados dentro dos dados do usuário em uma única conexão ou em um bloco de dados.
d) Confidencialidade do fluxo do tráfego: proteção das informações que poderiam ser derivadas dos fluxos de tráfego.

IV) Integridade de dados: certeza que os dados recebidos são exatamente conforme enviados pela entidade autorizada.

a) Integridade de conexão: integridade de todos os dados do usuário em uma única conexão e detecta qualquer modificação, inserção, exclusão ou repasse de quaisquer dados dentro de uma sequência inteira, com tentativas de recuperação.
b) Integridade da conexão sem recuperação: integridade de todos os dados do usuário em uma única conexão e detecta qualquer modificação, inserção, exclusão ou repasse de quaisquer dados dentro de uma sequência inteira, sem tentativas de recuperação.
c) Integridade da conexão com campo seletivo: integridade de campos selecionados nos dados do usuário de um bloco de dados transferido por uma conexão e determina se os campos selecionados foram modificados, inseridos, excluídos ou repassados.
d) Integridade sem conexão: integridade de um único bloco de dados sem conexão e pode tomar a forma de detecção da modificação de dados. Além disso, pode haver uma forma limitada de detecção de repasse.
e) Integridade sem conexão com campo seletivo: integridade de campos selecionados dentro de um único bloco de dados sem conexão; determina se os campos selecionados foram modificados.

V) Irretratabilidade: oferece proteção contra a negação, por parte de uma das entidades envolvidas em uma comunicação, de ter participado de toda ou parte dela.

a) Irretratabilidade da origem: prova de que a mensagem foi enviada pela parte especificada.
b) Irretratabilidade do destino: prova de que a mensagem foi recebida pela parte especificada.

5) Liste e defina resumidamente as categorias dos mecanismos de segurança.

R: Existem mecanismos de segurança específicos a camada de aplicação e não específicos a camada para o específicos são

I) Codificação: O uso de algoritmos matemáticos para transformar os dados para um formato que não seja prontamente inteligível. a transformação e subsequente recuperação dos dados depende de um algoritmo é zero ou mais chaves de encriptação.

II) Assinatura digital: dados anexados a uma unidade de dados que permite que um destinatário dela prove sua origem e integridade e a proteja contra falsificação.

III) Controle de acesso: uma série de mecanismos que impõem direitos de acesso aos recursos.

IV) Integridade de dados: uma série de mecanismos utilizados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.

V) Troca de autenticação: um mecanismo intencionado a garantir a identidade de uma entidade por meio da troca de informações.

VI) Preenchimento de tráfego: a inserção de bits nas lacunas de um fluxo de dados para frustrar as tentativas de análise de tráfego.

VII) Controle de roteamento: permite a seleção de determinadas rotas fisicamente seguras para certos dados e mudanças de roteamento, sobretudo quando uma brecha de segurança é suspeitada.

VIII) Notarização: o uso de um terceiro confiável para garantir certas propriedades de uma troca de dados.

Já mecanismos de segurança não específicos são

I) Funcionalidade confinada: aquilo que é percebido como sendo correto com relação a alguns critérios.

II) Rótulo de segurança: a marcação vinculada a um recurso que nomeia ou designa os atributos de segurança desse recurso.

III) Detecção de eventos: detecção de eventos relevantes à segurança.

IV) Trilha de auditoria de segurança: dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança, que é uma revisão e exame independentes dos registros e das atividades do sistema.

V) Recuperação de segurança: lida com solicitações de mecanismos, como funções 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: Confidencialidade: tal requisito é extremamente importante com relação a cada usuário do caixa, assim que o usuário utiliza o mesmo e finaliza alguma operação o caixa pode reiniciar perguntando se o mesmo deseja realizar alguma outra operação, pois como temos filas nesse tipo de caixa o usuário pode apenas ir embora ao finalizar uma operação, logicamente caso o usuário não interage com o caixa durante um período curto o mesmo pede a senha novamente. Como é um caixa em fila como já dito, algumas informações podem ser visualizadas pela pessoa atrás, nesse caso podesse optar ocultando alguns dígitos ou sobrenome que estão sendo exibidos, preservando a confidencialidade. Considero tal importância como média.
Integridade: aqui podemos exigir etapas extras de autenticação e/ou confirmação para manter integridade dos dados, por exemplo, quando o usuário for efetuar uma transação ou um saque, pedir que insira a senha novamente e identifique que realmente deseja realizar tal operação. Considero tal importância como baixa.
Disponibilidade: existem períodos que esses caixas não estão disponíveis para serem utilizados, tais períodos podem acontecer regularmente desde de que seja rápido seu retorno a estar disponível a ser utilizado. Tal situação pode ocasionar a vinda de usuários desavisados, mas que soa mais como um infortúnio ao mesmo. Considero tal importância como baixa.

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

Serviço X Ataques	AP1	AP2	AA1	AA2	AA3	AA4
Autenticação de entidade pareada			X	X		
Autenticação da origem de dados			X	X	X	
Controle de acesso	X			X	X	
Confidencialidade	X				X	
Confidencialidade do fluxo de tráfego	X	X		X	X	
Integridade de dados				X	X	
Responsabilização	X		X	X	X	
Disponibilidade						X

AP1: Vazamento de conteúdo da mensagem
AP2: Análise de tráfego
AA1: Disfarce

AA2: Repasse
AA3: Modificação da mensagem
AA4: Negação de serviço

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

Mecanismos X Ataques	AP1	AP2	AA1	AA2	AA3	AA4
Codificação	X			X	X	
Assinatura digital			X	X	X	
Controle de acesso			X			X
Integridade dos dados				X	X	
Troca de autenticação			X			
Preenchimento de tráfego	X	X		X	X	
Controle de roteamento	X	X		X	X	
Notarização			X		X	

AP1: Vazamento de conteúdo da mensagem
AP2: Análise de tráfego
AA1: Disfarce
AA2: Repasse
AA3: Modificação da mensagem
AA4: Negação de serviço