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:José Elias de Lima

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: É um meio para definir requisitos de garantia de segurança e quais as técnicas para satisfazer isso, podendo ser resumido em modos, ataque à segurança, que nada mais é que ato de burlar a segurança, um exemplo seria um ataque passivo, onde o atacante invade a rede e fica observando a comunicação sem modificar nada, serviços de segurança, é aquele que é ofertado pela camada de protocolo, um exemplo seria o serviço de autenticação que garante a comunicação correta e que a informações compartilhadas sejam dos indivíduos esperado e por último o mecanismo de segurança que nada mais é que mecanismos que são implementados nas camadas de protocolos ou no protocolo, exemplo seria, assinatura digital um forma do remetente garantir que é ele mesmo que está enviando a mensagem.

2. Qual é a diferença entre ameaças à segurança passivas e ativas?
R: Uma ameaça passiva é um ataque que tenta descobrir informações do sistema sem modificar nada. Já uma ameaça ativa seria quando há invasão e algo a mais como uma modificação ou interação.
3. Liste e defina resumidamente as categorias de ataques passivos e ativos à segurança.
R:Existem dois tipos de ameaça passiva a primeira é vazamento de conteúdo que nada mais é que alguém ter acesso a troca de mensagem um outro tipo seria a análise de tráfego, quando o invasor não consegue ler as mensagens mas mesmo assim tem acesso ao destinatários das mensagens e tamanhos dela, podendo descobrir a natureza da comunicação. Já uma ameaça ativa pode ser, disfarce, se passando por outro diferente, repasse, como nome já diz recebe algo e repassar sendo que seria algo proibido, modificação de mensagem, seria modificar uma parte da mensagem e negação de serviço, que impede o uso ou o gerenciamento normal da comunicação.

4. Liste e defina resumidamente as categorias dos serviços de segurança.
R: Serviços de segura é dividido em cinco categorias, são eles, autenticação, nesse caso garante que a comunicação é entre as partes corretas, controle de acesso que é limitar e dominar o acesso ao sistema por meio de links, confidencialidade de dados que é proteção para que o atacante não tenha acesso às características dos dados, integridade dos dados garante que haja modificação dos dados e por último irretratabilidade que se trate de toda mensagem não pode ser impedida pelo emissor ou receptor.

5. liste e defina resumidamente as categorias dos mecanismos de segurança.
R: Mecanismo de segurança são dividido entre os implementados na camada de protocolo como a codificação que é transformar dados em algo inteligível, assinatura digital que é uma forma de provar a origem do dados, controle de acesso que é diversos mecanismo que impôem acesso a recursos, integridade dos dados que é garantir inviolabilidade dos dados e sua troca , troca de autenticação é um mecanismo que garante a identidade de uma entidade por meio da troca de informação, preenchimento de tráfego é incluir bits em espaços vazios para que o invasor não analise o tráfego, controle de roteamento é seleção de rotas físicas caso encontre falhas de segurança, notarização é a existência de um terceiro confiável para garantir a trocar de informação e os que não são específicos da camada são funcionalidade confiada que é dito correto atendendo alguns critérios, rótulo de confiança que é uma marcação a um recurso podendo ser um dado que nomeia os atributos de segurança desse recurso, detectção de eventos, que nada mais é do que detectar eventos de segurança relevantes, trilha de auditoria de segurança que é quando o dados são utilizados para uma auditoria de segurança e por último recuperação de segurança que é tomar medida de recuperação de mecanismo.

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: Um exemplo de confidencialidade é sua senha, que é única e só ele sabe, pois se mais alguém souber seu dinheiro estará desprotegido, alto grau de importância, já exemplo integridade seria uso do cartão pois com apenas o cartão só os dados poderiam ser consultados daquela conta, temos então um alto grau de importância na integridade e quanto a disponibilidade temos o uso combinado de da senha e cartão, pois com eles o usuário pode acessar sua conta em qualquer caixa eletrônico.

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.
R:

Ataques _____ Serviços De segurança	vazamento de conteúdo	análise de tráfego	disfarce	Repasse	Modificação de mensagens	negação de serviço
autenticação			X			
Controle de acesso			X	X		
Confidencialidade de dados	X	X		X	X	
integridade de dados		X			X	
irretratabilidade				X		X

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

Ataques / Mecanismos de segurança	vazamento de conteúdo	análise de tráfego	disfarce	Repasse	Modificação de mensagens	negação de serviço
Codificação	X				X	
assinatura digital			X	X		
Controle de acesso			X	X		
integridade de dados	X				X	
Troca de autenticação		X	X			
preenchimento de tráfego	X	X				
Controle de roteamento						X
notarização	X	X	X	X		