1. **O que deve ser levado em conta no desenvolvimento de um sistema de autenticação**

Entender quais são os ataques aos quais os sistemas de autenticação estão expostos

Entender as formas e tecnologias de proteção dos sistemas de autenticação.

1. **Cite pelo menos dois tipos de ataques conhecidos aos sistemas de autenticação**

Adivinhar a senha do usuário, Acessar o repositório onde as senhas estão armazenadas

1. **Qual a maior vulnerabilidade existente em um sistema de autenticação que permita o uso da técnica de invasão de adivinhação da senha do usuário?**

Esse é um ataque muito efetivo quando não existem mecanismos que limitem a quantidade de erros na autenticação. Porém, quando existem tais mecanismos, o ataque tem probabilidade muito baixa de ter sucesso.

1. **Descreva como é feito o ataque conhecido como ataque de dicionário.**

Consiste em criar ou obter um arquivo, que é chamado de “dicionário” e que possui muitas palavras. Quanto maior a quantidade de palavras, melhor é o dicionário. Depois de conseguir um dicionário, testam-se as palavras do dicionário como sendo a senha do sistema que se deseja atacar. Como muitos usuários não utilizam senhas complexas, e sim palavras comuns como nomes de time de futebol, nomes de cidades, nomes de pessoas, etc., este ataque acaba sendo muito efetivo.

1. **O que é “LEET”?**

Consiste em trocar algumas letras, geralmente as vogais, por números. Existem também ferramentas que manipulam as palavras do "dicionário"

1. **Qual a principal vantagem do ataque de força bruta?**

Este ataque poderá testar todas as combinações de senhas, significa que em algum momento ele irá descobrir a senha utilizada pelo usuário. De modo geral, todas as senhas podem ser quebradas por este método

1. **Porque o uso de redes wifi públicas não é seguro**

O wifi público não é seguro pois tem a capacidade de um hacker posicionar-se entre você e o ponto de conexão. Em vez de falar diretamente com o ponto de acesso, estará enviando suas informações para o hacker.

1. **Como criar uma senha segura?**

Utilizar senha com 12 caracteres ou mais, com símbolos, números, letras maiúsculas e minúsculas. Sendo assim, Tornando mais difícil de ser descoberta.

1. **Detalhe um plano de segurança para uma nova aplicação que você seja responsável por desenvolver.**

Projetar um mecanismo de bloqueio da conta do usuário após uma determinada de tentativas. Que consiste em bloquear algum hacker que testará milhões e milhões de combinações.