Segurança nos sistemas de autenticação

Para acesso aos sistemas computacionais que usamos no dia a dia faz-se necessário garantir a autenticação de quem vai utilizar o sistema.

Qual a forma mais comum de autenticação?

É um conjunto utilizado por décadas…

Usuário e Senha

Segurança nos sistemas de autenticação

Com relação a segurança nos sistemas de autenticação de usuários há dois aspectos principais a serem levados em conta.

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

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

Segurança nos sistemas de autenticação

Tipos de Ataques

- Adivinhar a senha do usuário
- Acessar o repositório onde as senhas estão armazenadas
- Capturar a senha digitada pelo usuário
- Impedir que um usuário legítimo faça a autenticação
- Bular o mecanismo de recuperação de senhas
- Roubar sessões válidas

Qual desses ataques é o mais comum e o mais simples de ser executado?

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário

É o ataque que tenta descobrir as senhas de usuários utilizando diversas combinações de senhas. Pode ser executado manualmente, ou com auxílio de ferramentas automatizadas.

Quanto tempo leva para se obter sucesso?

Está diretamente ligado a complexidade e a quantidade de caracteres utilizados nas senhas, ou seja, quanto mais complexo e maior comprimento da senha, mais tempo é necessário para descobrir a senha.

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.

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque com informações do usuário

Consiste em obter dados pessoais do usuário como nome, sobrenome, data de nascimento, número do telefone, placa do carro, nome do cachorro, time preferido, comida preferida, etc., e testar essas informações como sendo a senha do usuário.

Qual a principal vantagem desse tipo de ataque?

Não é necessário grande conhecimento técnico, e sim, conhecimento sobre o usuário que será atacado. A busca nas redes sociais e nas ferramentas de busca tem se mostrado muito eficiente para conseguir essas informações.

Como evitar?

Sistemas considerados seguros impedem que um usuário utilize informações pessoais como nome, sobrenome, data de nascimento e outras informações pessoais na senha, reduzindo a eficiência deste ataque.

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque com senhas padrões

Muitos equipamentos de rede saem de fábrica com um conjunto de configurações padrão, dentre elas usuário e senha. Esse ataque consiste em testar combinações de usuários e senhas padrões para o sistema atacado.

Qual a principal vantagem desse tipo de ataque?

Pode ser feito manualmente, em poucos minutos e não há complexidade técnica para executá-lo.

Como evitar?

SEMPRE fazer a troca da senha padrão em todos os equipamentos e sistemas antes de começar a utilizá-los.

http://www.defaultpassword.com/

https://cirt.net/passwords

https://default-password.info/

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
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.

Principal característica desse ataque

Para executar esse ataque é preciso algum conhecimento técnico e, dependendo do tamanho do dicionário, o ataque pode demorar horas, ou dias, até testar todos os itens.

Como evitar?

A melhor proteção contra esse ataque é ter um dicionário próprio no sistema e impedir que os usuários utilizem senhas presentes no dicionário.

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de dicionário

Sites onde é possível conseguir wordlists
ou dicionários

http://www.openwall.com/wordlists/

https://packetstormsecurity.com/Crackers/wordlists/

https://wiki.skullsecurity.org/Passwords

http://www.md5this.com/tools/wordlists.html

https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de dicionário

Existem também ferramentas que manipulam as palavras do "dicionário" para o que é conhecido como escrita "LEET", que consiste em trocar algumas letras, geralmente as vogais, por números. Por exemplo, a palavra "homem" na escrita "LEET" se torna "h0m3m".

http://www.digininja.org/projects/rsmangler.php

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Consiste em testar milhares, milhões ou até mesmo todas as combinações possíveis de senhas para um usuário. Quanto menor for a senha do usuário, menor é a quantidade de combinações e é possível descobrir sua senha mais rápido. Quanto maior a senha do usuário, maior é a quantidade de combinações que precisam ser testadas, e, conseqüentemente, mais tempo será necessário para executar este ataque.

Para executar esse ataque é necessário um bom conhecimento técnico, muita capacidade de processamento e muito tempo para obter o resultado, pois, como a quantidade de combinações é muito grande, pode-se demorar desde poucos minutos (senhas pequenas) até alguns anos (senhas grandes e complexas) para testar todas as senhas.

Qual a principal vantagem desse tipo de ataque?

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.