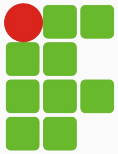
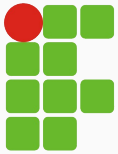


Segurança da informação na WEB

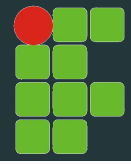
Maximilian Jaderson de Melo

Aula 6 - Senhas e suas vulnerabilidades



Ataques em sistemas protegidos por senha

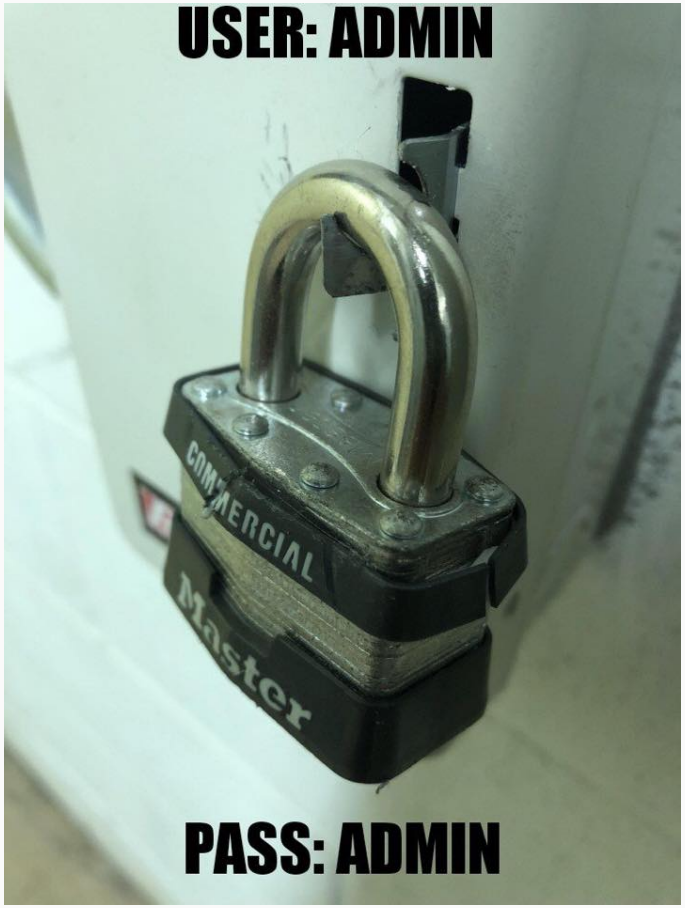
Visão geral



- Funcionalidades da segurança:
  - controle de acesso.
  - validação de credenciais.
  - permissão de acesso a recursos.
  - proteção de dados.
  - definição de trilhas de auditoria.

Senhas

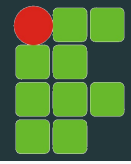
Senhas



A senha

- Combinação de símbolos conhecida somente pelas pessoas autorizadas.
- É um mecanismo de controle de acesso, que supostamente garante credenciais de acesso válidas.

Força bruta



- Consiste na combinação de todas as possibilidades de um dicionário de símbolos possíveis em uma senha. Ex:
  - Símbolos: {a,e}
  - Senhas com 0 símbolos: {}
  - Senhas com 1 símbolo: {a, e}
  - Senhas com 2 símbolos: {aa,ae,ea,ee}
  - Senhas com 3 símbolos: {aaa,aae,aea,aee,eaa,eae,eea,eee}
  - ...

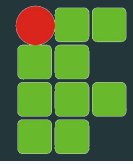
Complexidade do ataque

- Para um dicionário de 26 caracteres temos as seguintes senhas:
  - 1 char: 26 combinações diferentes.
  - 2 chars: $26 \times 26 = 26^2$ combinações diferentes.
  - 3 chars: $26 \times 26 \times 26 = 26^3$ combinações diferentes.
  - ...

Complexidade do ataque

- Pode-se pensar que para “adivinhar” uma senha, tem-se o seguinte número máximo de tentativas
-
$$\sum_{p=0}^{N} A_r(m, p)$$
- Com:
  - m o número de símbolos do dicionário.
  - p o número de caracteres na senha.
  - N o número máximo de caracteres de uma senha.
  - $A_r(m, p) = m^p$

Complexidade do ataque



- A complexidade aumenta a medida que o número de possibilidades aumenta.
- Qual complexidade é maior: aumentando o número de caracteres na senha ou aumentando os símbolos no dicionário?

Comprove

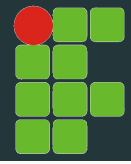
- Considere que o dicionário simples possua 26 símbolos, enquanto o dicionário complexo, considerando 10 símbolos especiais, contém 72 (por quê?). Faça uma tabela relacionando o número de senhas possíveis para os dois dicionários (como no slide seguinte).
  - Verifique a taxa de crescimento de ambos os dicionários.

Comprove

dicionário	2 chars	3 chars	4 chars	5 chars	6 chars
simples					
complexo					

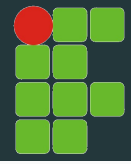
- Analise a taxa de crescimento dos dicionários.

Por que funcionam?



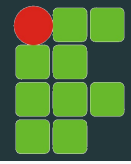
- Esses ataques, apesar de pouco sofisticados, costumam obter resultados positivos.
- Os processadores funcionam em um frequência extremamente alta, conseguindo testar centenas a milhares de combinações por segundo.

E se a senha for muito grande?



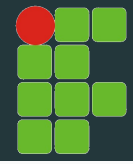
- Isso implica no tempo necessário para quebrá-la, não na impossibilidade!

Ataques guiados



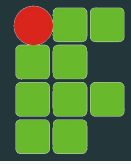
- Pensando em diminuir o tempo consumido, pode ser aplicada alguma heurística.
  - Heurística é uma dica, algum padrão detectado ou conhecido.

Pense estatisticamente



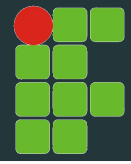
- Considerando um alvo brasileiro. No idioma português, o caractere mais frequente é o ‘a’, seguido do ‘e’, seguido do ‘o’.
- A média do número de letras das palavras no idioma português é de 4.53.
- Há grande probabilidade de uma palavra conter:
  - Vogais: A, E, I, O, U.
  - Consoantes: S, R, N, D, M.

Pense estatisticamente



- A senha provavelmente conterá uma ou mais ou parte de palavra no idioma nativo.
  - Grande probabilidade da palavra possuir relação afetiva com o alvo/ambiente sociocultural do alvo.
  - Engenharia social ajuda aqui.

Wordlist's



- Considerando os fatores citados, existem **estatísticos e sociolinguistas** que trabalham na análise de dicionários eficientes na quebra de sigilo.
- A comunidade de "hacker's" (*script kiddies* em sua maioria) disponibilizam *wordlists* para diversos cenários.
    - Lembrando: o acesso não autorizado de dispositivo informático constitui crime!

Atividade

1. Descreva o funcionamento do ataque de força bruta pura e direcionado.
2. Pesquise sobre pelo menos dois mecanismos para evitar o sucesso de força bruta.

Próxima aula

- Noções de criptografia.

Referências

1. GTA UFRJ
2. TIForense
3. educabras - permutação, arranjo e combinações

Dúvidas, críticas ou sugestões?

maximilian.melo@ifms.edu.br

max.mjm.melo@gmail.com