Segurança de Dados - Ataque de Dicionário
Manutenção e Suporte em Informática

Prof. Daniel Saad Nogueira Nunes

1 Ataque de Dicionário

Um ataque de dicionário é um método força-bruta direcionado em que utiliza-se uma lista de palavras candidatas à senha para tentar quebrá-la e, potencialmente, obter acesso não autorizado a algum recurso.

Este ataque é bem eficiente quando o usuário escolhe senhas fraca ou comuns, pois provavelmente ela já se encontra em alguma das diversas listas de senha (*wordlists*) disponíveis.

Este tipo de ataque pode ser utilizado em diversas formas para obtenção de diferentes objetivos, como:

- Quebra de senha em redes Wi-Fi com protocolo WPA2.
- Descoberta de senhas de usuários de um determinado serviço ou sistema em que o arquivo de senhas tenha sido indevidamente disponibilizado por um *insider* ou *outsider*.
- Outros.

2 Objetivo

O objetivo deste trabalho é realizar um ataque de dicionário em um arquivo de senhas do Unix (*shadow*) para obtenção das senhas dos usuários.

Para alcançar este objetivo, a ferramenta `John the ripper` deverá ser utilizada em conjunção com diferentes dicionários.

3 Desenvolvimento

Um documento respondendo as seguintes perguntas deverá ser elaborado.

1. Como funciona um ataque de dicionário?
2. Quais os usuários que tiveram suas senhas quebradas e quais as respectivas senhas?
3. Quais foram os dicionários utilizados para efetuar a quebra?
4. Houve algum usuário que não teve a senha quebrada? Em caso afirmativo, qual as possíveis causas.

4 Considerações

- Este trabalho pode ser feito individualmente, ou em dupla.
- Cópias e plágio serão avaliados automaticamente com nota 0 para os envolvidos. Medidas disciplinares também serão tomadas.
- O trabalho deve ser entregue dentro de uma pasta zipada com a devida identificação dos alunos até a data estipulada pelo ambiente virtual de aprendizagem da disciplina.