

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 fracas 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 relatório de até deverá ser entregue detalhando como o ataque de dicionário foi realizado. Ele deverá possuir a seguinte relação de elementos:

- **Introdução:** descrição do objeto de estudo e objetivos do trabalho.
- **Conceitos preliminares:** todos os conceitos necessários para que o relatório possa ser entendido.
- **Resultados e Discussão:** os resultados obtidos bem como a discussão dos mesmos, que contempla as observações associadas a estes resultados juntamente com os conceitos e práticas de segurança vistos no decorrer da disciplina.
- **Conclusão:** conclusão do trabalho, recapitulando o que foi feito e verificando se os objetivos foram atingidos ou não.
- **Referências:** referências utilizadas.

4 Considerações

- Este trabalho pode ser feito individualmente, em dupla ou em trio.
- 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.