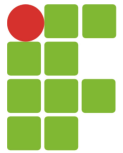
Ataque de Dicionário

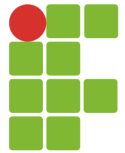
Segurança de Dados - Manutenção e Suporte em Informática

Prof. Daniel Saad Nogueira Nunes

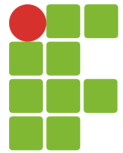
IFB – Instituto Federal de Brasília,
Campus Taguatinga



Sumário

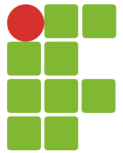


Sumário

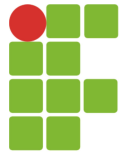


Ataque de Dicionário

- Um ataque de dicionário é um ataque baseado em força-bruta guiada em que se tenta adivinhar uma senha a partir de uma lista de prováveis senhas (dicionário ou *wordlist*).
- Esse ataque tem muito sucesso quando a senha escolhida pelo usuário é fraca, pois ela provavelmente está presente em algum dicionário.
- A versão *off-line* do ataque do dicionário pode ser efetuada quando o arquivo de senhas está disponível para o atacante.
- Abordaremos neste material um ataque de dicionário baseado em um arquivo de senhas do UNIX (arquivo shadow).

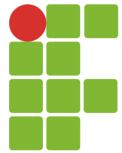


Sumário



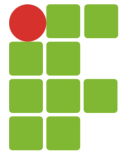
Dicionários

- Os dicionários são listas de prováveis senhas, as quais podem ser utilizadas durante um ataque.
- Diversos dicionários estão amplamente disponíveis na Internet em *sites* como:
  - `https://wiki.skullsecurity.org/Passwords`
  - `https://github.com/BRDumps/wordlists`
  - `https://github.com/danieldonda/wordlist`

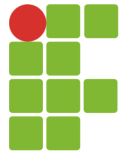


Dicionários

- Alguns dicionários como o `Rock-you.txt` se tornaram famosos no decorrer do tempo por obterem relativo sucesso sobre senhas fracas.
- Dependendo do objetivo, o atacante pode considerar usar dicionários específicos ou em determinada língua.

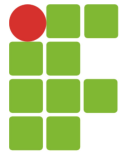


Sumário



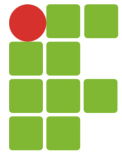
Arquivos Shadow

- Os arquivos de senha também são conhecidos como arquivos *shadow*.
- Nestes arquivos as senhas são armazenadas através de funções de *hash* criptográficas, isto é, as senhas não são armazenadas às claras. Desta forma, com uma simples leitura é impossível adivinhar a senha de cada usuário.
- Normalmente existe um controle de acesso sobre estes arquivos de modo que um usuário comum, sem privilégios, não consiga efetuar uma leitura sobre eles.



Arquivos Shadow

- Entretanto, devido à vulnerabilidades do Sistema Operacional, ou devido à um ataque feito por um *insider* ou *outsider*, este arquivo pode ser vazado.
- O atacante que detém o arquivo *shadow* pode então efetuar um ataque de dicionário.
- Vamos examinar a estrutura de um arquivo *shadow* do UNIX.



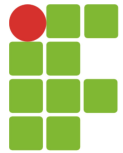
Arquivo Shadow do UNIX

- Cada linha de um arquivo shadow do UNIX possui uma informação sobre um usuário e tem o seguinte formato:

  1 2 3 4 5 6 7 8

  saad:$1$7UsC0KDy$3QLXB9Ghi5wlbW0E2RGO41:3883:0:17658:7:::

  - Cada campo está separado pelo símbolo de :
  - O campo 1 corresponde ao nome de usuário (*username*).
  - Em particular, a próxima informação possui três campos e corresponde à informação da senha e sal do usuário $(2, 3, 4)$, respectivamente temos: a função de *hash* utilizada, o sal utilizado, e o *hash* da senha $+$ sal.



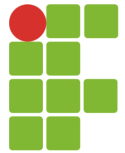
Arquivo Shadow do UNIX

- Cada linha de um arquivo shadow do UNIX possui uma informação sobre um usuário e tem o seguinte formato:

  1 2 3 4 5 6 7 8

  saad:$1$7UsC0KDy$3QLXB9Ghi5wlbW0E2RGO41:3883:0:17658:7:::

  - Tipos de função de hash:
    - 1: MD5.
    - $2a$: Blowfish.
    - $2y$: Eksblowfish.
    - 5: SHA-256.
    - 6: SHA-512



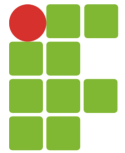
Arquivo Shadow do UNIX

- Cada linha de um arquivo shadow do UNIX possui uma informação sobre um usuário e tem o seguinte formato:

1 2 3 4 5 6 7 8

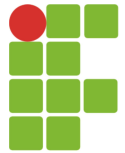
saad:$1$7UsC0KDy$3QLXB9Ghi5wlbW0E2RGO41:3883:0:17658:7:::

  - O campo 5 indica a última vez em que a senha foi alterada no formato EPOCH (dias após 1 de janeiro de 1970).
  - O campo 6 representa o número de dias que o usuário tem para alterar a senha, caso contrário ela se tornará inválida.
  - O campo 7 expõe o período de inatividade, isto é, o número de dias após a senha ficar inválida necessário para que a conta seja desativada.
  - O campo 8 contém a data de expiração da conta no formato EPOCH.

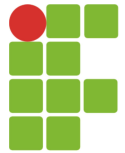


Arquivos Shadow

- Tendo a posse de um arquivo *shadow*, e possível utilizar uma ferramenta como a `John the Ripper` para efetuar um ataque de dicionário a partir de um arquivo de prováveis senhas.

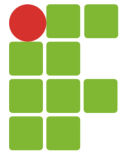


Sumário

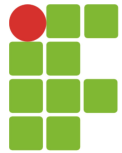


John The Ripper

- A ferramenta `John the Ripper` é uma ferramenta muito utilizada para testar a fraqueza das senhas dos usuários.
- Também é utilizada por atacantes para efetuar quebras de senha.
- Atualmente está disponível para várias plataformas como: Windows, MAC e Linux.
- Abordaremos o seu uso em sistemas baseados em GNU/Linux.

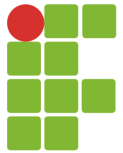


Sumário

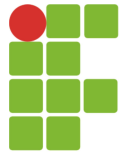


Instalação

- Em sistemas derivados do Debian (ex: Ubuntu), é possível instalar a ferramenta com uma simples linha de comando: `sudo apt-get install john`.
- Em sistemas derivados do Arch-Linux, um comando similar pode ser emitido: `sudo pacman -S john`.
- Em outros sistemas, é possível verificar se a ferramenta está disponível nos repositórios oficiais do gerenciador de pacotes.
- Em último caso, é possível compilar o fonte a partir do arquivo disponível no site oficial (`https://www.openwall.com/john/`) e construir o executável.

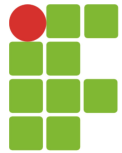


Sumário



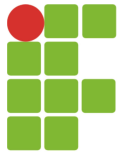
Utilização da Ferramenta

- A ferramenta possui três modos básicos de operação:
  1. *Single*: modo padrão da ferramenta: ela tenta quebrar as senhas disponíveis no arquivo através de um dicionário de senhas fracas.
  2. *Wordlist*: neste modo é necessário especificar o dicionário contendo as possíveis tentativas de senha.
  3. *Incremental*: ataque força-bruta clássica que tenta todas as possibilidades de senha.
- Estamos mais interessados no uso da ferramenta informando um dicionário.

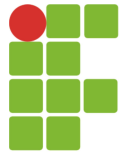


Utilização da Ferramenta

- Para utilizar a ferramenta, basta utilizar o seguinte comando: `john --wordlist=<caminho dicionario> shadow.txt`
- Todas as senhas quebradas serão armazenadas em um arquivo `john.pot`.
- Para verificar quais senhas foram quebradas, basta utilizar o seguinte comando: `john --show shadow.txt`.



Sumário



Considerações Finais

- Verificamos os conceitos básicos sobre ataque de dicionário e aprendemos a manipular de maneira básica a ferramenta `John the Ripper`.
- Ela consegue executar um ataque a partir de um dicionário de senhas fracas.
- Para ter sucesso, um atacante pode ter que utilizar múltiplos dicionários.
- Algumas senhas podem não ser quebradas devido à natureza do ataque.