Hacks em fechadura(s) para teste de intrusão físico

Casos de estudo

Quem sou eu?

- Filipe Cordeiro (Linkedin)
- Offensive Security Consultant
- Mobile Hacking Hobbyist
- LockPicking Lover <3
- unl0g1c (Telegram)
- DCPT, CRTP, eWPT, CMPen

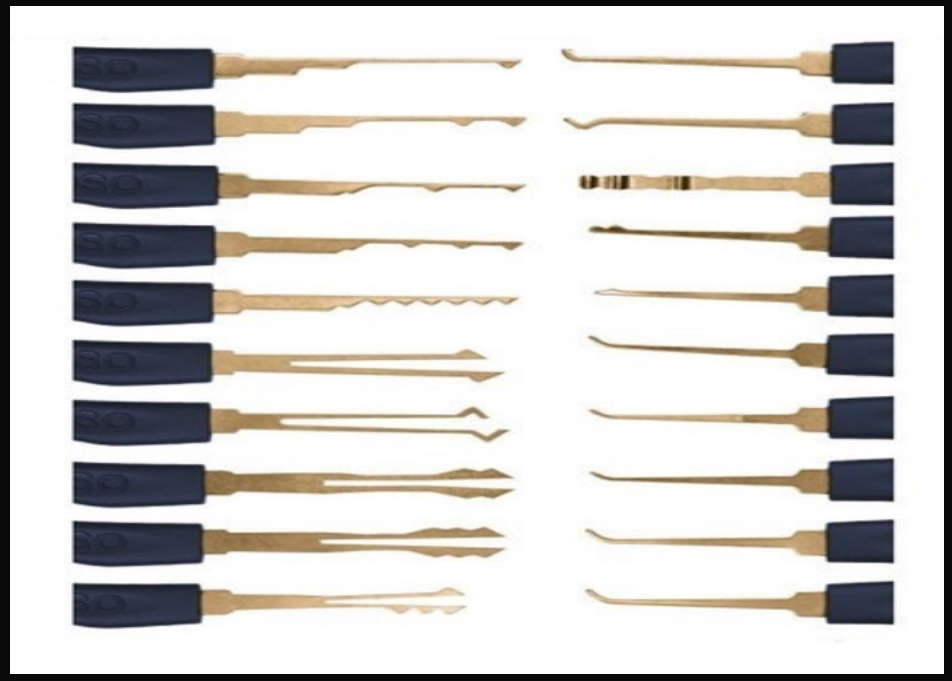
Overview

- Chaves micha, bump keys ou lockpick?
- Alguns tipos de fechaduras
- Técnicas de bypass comuns em fechaduras
- Qual é a utilidade de tudo isso?
- Show me the hacking

Chaves micha, bump keys ou lockpick?

- Chave Micha, também conhecida como chave mestra, é uma chave que foi projetada para abrir fechaduras;
- Uma bump key é uma chave que foi modificada para ser usada em uma técnica chamada "bumping" (ou "key bumping");
- Um lockpick (ou kit de lockpicking) é um conjunto de chaves micha projetadas para abrir fechaduras;
- Bom e velho grampo de cabelo.

Chaves micha, bump keys ou lockpick?



Alguns tipos de fechaduras

- Fechadura externa (tambor)
- Fechadura multi ponto
- Fechadura gorja/gorje
- Fechadura tetra
- Fechadura digital

Técnicas de bypass comuns em fechaduras

- Tetra:
  - Utilizando da micha para fechadura tetra e concluindo as voltas necessárias para a sua abertura.
- Externa:
  - Apoiador + micha de ponta, pressionando o apoiador para o lado que abre a porta e michar.
- Gorje/Gorja:
  - Posiciona a micha dentro da fechadura até localizar uma mola, após isso virar a micha para trás.

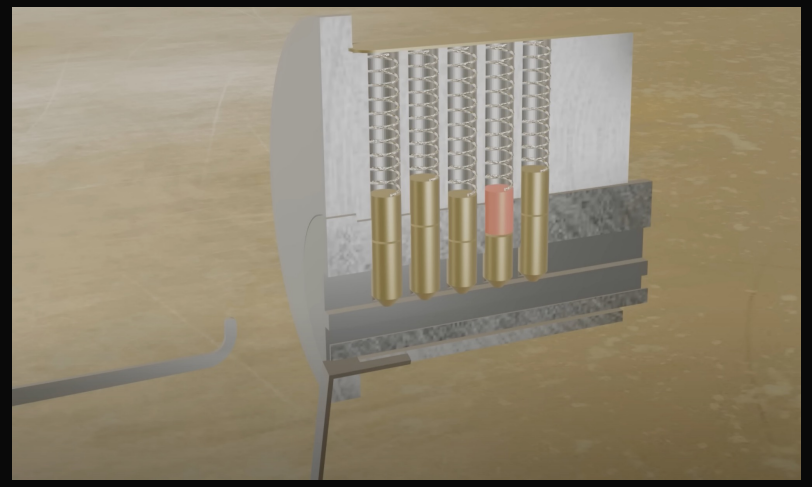
Qual a utilidade disso?

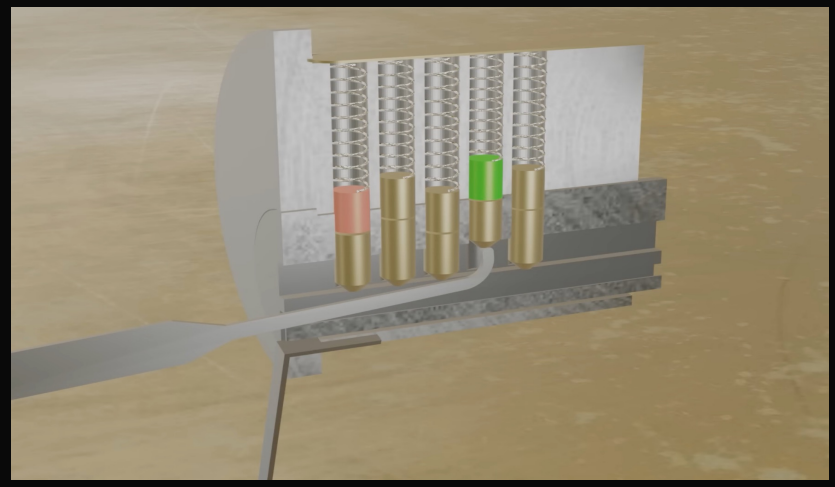
- Teste de intrusão físico
- Salvar algum amigo (rs)
- Se salvar (rs)

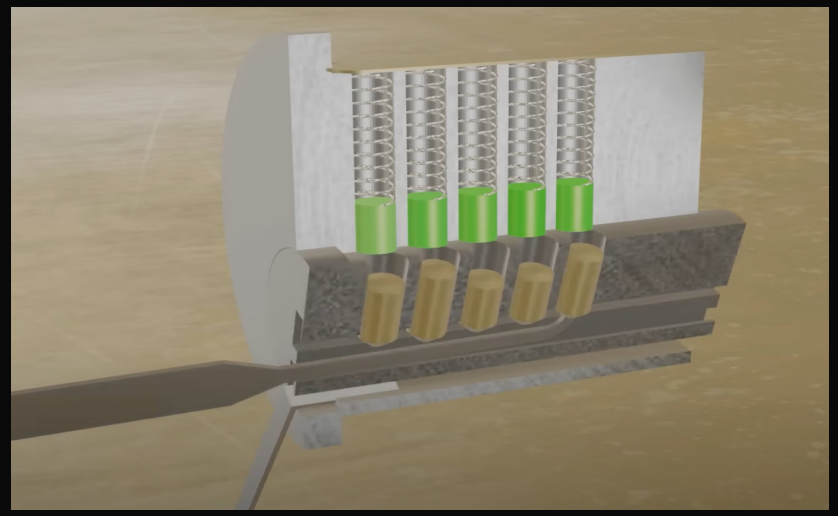
Opinions are my own

Show me the hacking

Show me the hacking







Dicas?

- Fazer curso de chaveiro (aprender com quem sabe)
- Comprar michas profissionais
- Comprar ou forjar keys bump

Isso é tudo? Não!

A área do teste físico + LockPicking é muito extensa e ainda está sendo estudada pelo autor dessa talk.

Fim