

Lockpicking - A arte de abrir fechaduras

[21 de outubro de 2015](#) [4 de novembro de 2015](#) / [s0ph0s](#)

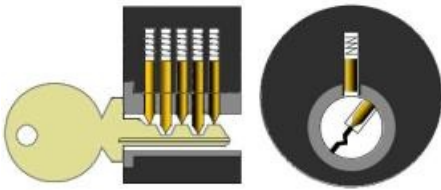
Muitos já viram em filmes hollywoodianos pessoas que abrem fechaduras de carros, casas, cofres e cadeados, e sim, é realmente possível fazer isso, essa técnica é chamada de *Lockpicking*. Iremos abordar neste artigo conceitos e detalhes dessa técnica, lembrando que o mal uso dela é considerado crime como o [Artigo 24](#) prevê na lei.

Definição e aplicação de Lockpicking

É o estudo de como funcionam as fechaduras, como as de portas e cadeados, utilizando ferramentas específicas para cada tipo de fechadura a ser utilizada no teste de segurança. Lockpicking hoje é visto como um hobby que é muito utilizado nas competições de eventos de segurança/hacking (Defcon, HackFest, Roadsec, Bsides, entre outros). Além disso, é considerado uma técnica de PenTest considerada NO TECH HACKING para analisar a segurança física de um local, como estações de servidores, portas de acesso, entre outras coisas.

Mecanismo de funcionamento das fechaduras

Existem diversos tipos de segredos de fechaduras como já citamos, a de carro, cadeado, cofre, porta e a técnica é muito semelhante entre alguns desses modelos. Sendo assim, veremos alguns mecanismos de fechadura, e falaremos sobre o seu funcionamento.



Na imagem acima que podemos usar como exemplo de fechadura de uma porta, que praticamente é o mesmo esquema de segredo do cadeado (tambor é o mesmo tipo). O sistema da fechadura da imagem acima é demonstrado através de 5 pinos, 5 molas e 5 cavidades e 1 cilindro (que envolve tudo dentro dele). Na hora que você insere a “chave” padrão da fechadura, ela exerce a força sobre os 5 pinos que tem base reta, empurrando os demais e nivelando ao ponto de permitir o tambor girar. O importante notar é que esses pinos e molas não são iguais entre si, dificultando, em teoria, a abertura das fechaduras. Dessa forma, esse mecanismo faz delas seguras (mas demonstraremos que não são). E também por esse fato se complica ao você tentar fechar quando uma fechadura depois de aberta.

Conhecendo as ferramentas para Lockpicking

Para cada tipo de técnica de abertura de fechadura existe diversas ferramentas para seu respectivo caso. Por isso, antes de iniciar o procedimento, é necessário analisar:

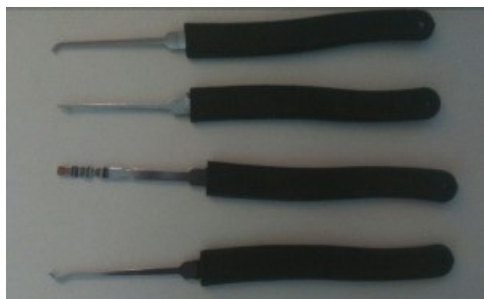
- O mecanismo da fechadura.
- A ferramenta adequada pro uso.
- A técnica de abertura.

As ferramentas mais utilizadas são:

Chave de tensão: ela que faz o giro do cilindro, portanto precisa ser um pouco resistente (recomenda-se de aço). Ou também, caso queira, pode-se usar um clips dobrando ele em “L”.

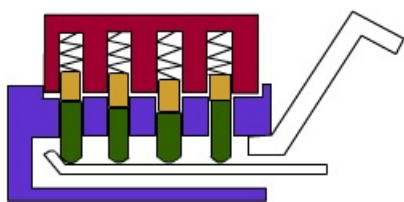


Pick: é usada para manipular os pinos dentro da fechadura. Abaixo temos alguns modelos delas.



Abrindo a fechadura

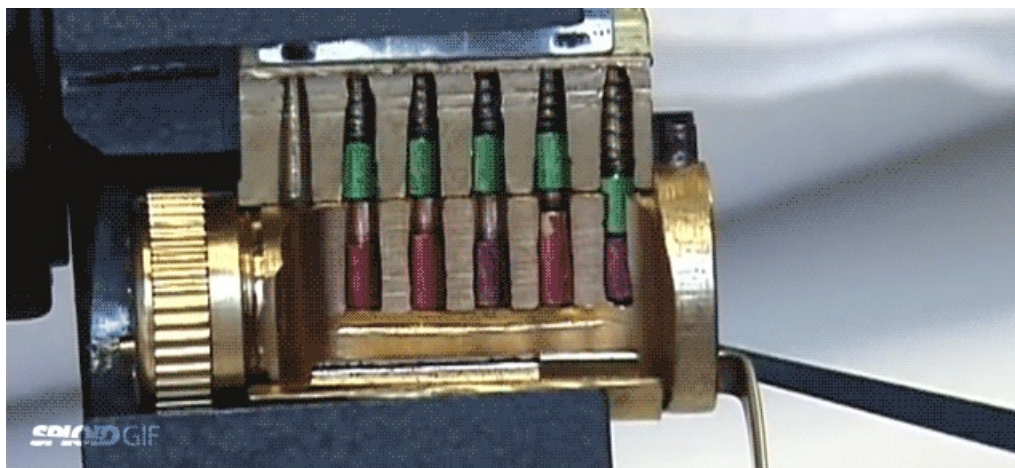
A técnica de abrir consiste no sistema de força bruta, onde você exercerá uma pressão por várias vezes até forçar o nivelamento, abrindo o segredo. No sistema de cadeado, como no exemplo abaixo, colocamos a *chave de tensão* na parte de cima do tambor, pressionando para o sentido horário (para o lado que abre), e ao mesmo tempo inserimos o *pick* para frente e para traz, até o cadeado abrir.



www.lockpickingfrance.org

Para cada tamanho de cadeado existe uma quantidade maior de pinos e molas, fazendo com que a técnica demore um pouco mais para ser realizada com sucesso, devido a quantidade de pinos que devem estar nivelados.

Nas fechaduras de portas de casa a técnica é semelhante, mas a dificuldade é um pouco maior devido haver a necessidade de empurrar pino por pino para o nivelamento deles, demorando um tempo maior e exercendo um pouco mais engenhosidade.



Veja o vídeo abaixo demonstrando o exemplo prático e teórico.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com, ou ative o JavaScript caso ele esteja desativado em seu navegador.

Conclusão

Existem muito mais técnicas de lockpicking do que apresentada neste artigo, umas delas são ferramentas elétricas, chaves mixas que agilizam todo esse trabalho. Nos próximos artigos falaremos mais sobre essa técnica, as quais mostraremos o funcionamento do sistema de fechadura de chaves tetras, cadeados de numeração, modelo de chave de carro, entre outros, as quais todos podem serem facilmente burlados. Lembrando que abordaremos o lado teórico e engenhoso disso tudo, nunca ressaltaremos para fins maliciosos, afinal o hacker é determinado pelas habilidades específicas as quais possuem e não a conduta moral a qual seguem.

Referências e indicações:

<http://www.lockpickingfrance.org/picks-p.html>

<http://www.ebah.com.br/content/ABAAAfYg0AK/lockpicking-a-arte-abrir-cadeados-fechaduras>

<http://deviating.net/lockpicking/videos.html>

<http://toool.us/>