Otwieranie zamka

„Łotrzykowie dużo wiedzieli o otwieraniu zamków na długo przed tym, jak ślusarze rozmawiali o tym między sobą. Jeśli zamek, jeśli został wykonany w jakimkolwiek kraju lub przez jakiegokolwiek producenta, nie jest tak nienaruszalny, jak dotychczas uważano, z pewnością w interesie uczciwych osób leży poznanie tego faktu, ponieważ nieuczciwi są znośni. Pewność praktycznego zastosowania wiedzy a rozpowszechnianie wiedzy jest konieczne, aby zapewnić uczciwą grę tym, którzy mogą cierpieć z powodu ignorancji." Locks and Safes: The Construction of Locks: A. C. Hobbs, 1853

W tej części omówiono czarną magię , jaką jest otwieranie zamków. Zachęcam wszystkich czytających do nauczenia się tej umiejętności (choćby dlatego, że daje dużo radości). Jeśli jesteś członkiem zespołu operacyjnego zajmującego się fizycznymi testami penetracyjnymi, jest to coś, co musisz opanować, a opanowanie wymaga dużo praktyki. Możesz czytać dowolną liczbę książek lub oglądać tyle filmów instruktażowych, ile chcesz, ale dopóki nie staniesz przed pierwszym zamkiem z wytrychami w ręku, nie zaczniesz się uczyć. Otwieranie zamków to termin określający obejście i otwarcie mechanizmu blokującego bez użycia klucza. Sposobów na to jest co najmniej tyle, ile jest typów zamków. Chociaż, oczywiście, niektóre odnoszą się do nas bardziej niż inne. Pod każdym względem tani zamek bębenkowy otwierany tradycyjnymi wytrychami i drogi zamek elektroniczny Winkhaus Blue Chip otwierany za pomocą magnesów można opisać jako otwieranie zamka. Jedną z głównych kwestii, które chcę wcześniej podkreślić, jest to, że celem otwierania zamka jest robienie tego bez wykrycia, bo w przeciwnym razie nie ma to większego sensu. Każdy mechanizm blokujący można obejść w destrukcyjny sposób, zwykle dość łatwo. Pomimo tego, że narzędzia do otwierania zamków są regulowane w wielu krajach i mają silne konotacje kryminalne, w rzeczywistości nie są one narzędziami, których używa wielu przestępców właśnie z tego powodu. Na przykład, jeśli włamywacz zamierza włamać się do twojego domu i ukraść telewizor, nie ma sensu tracić czasu na otwieranie drzwi wejściowych. Prawdopodobnie po powrocie do domu zauważysz brak wspomnianego telewizora. Ergo, przestępca jest znacznie bardziej skłonny po prostu kopnąć drzwi wejściowe (lub wejść przez okno). Otwieranie zamków wiąże się z dużym szczęściem i konsumpcją czasu (szczególnie pod presją). Jednak jak odpowiedział Gary Player, gdy ktoś skomentował, jakim był szczęśliwym golfistą: „Im więcej ćwiczę, tym więcej szczęścia mam".

Otwieranie zamków jako hobby

Jak wszystko inne w tym tekście, chcę skupić się na praktyczności. Oznacza to przede wszystkim robienie dokładnie tego, co powiedziałem i pokażę ci, jak otwierać zamki. Należy jednak ostrzec, że otwieranie zamków jest niezwykle uzależniającym czasem i że w pewnym momencie (miejmy nadzieję, że wkrótce) będziesz chciał wyjść poza proste metody, które mogę przedstawić w jednej części. Na szczęście istnieje wiele klubów i stowarzyszeń, do których możesz dołączyć, aby mieszać się z innymi podobnie myślącymi duszami (szczególnie w Niemczech i Holandii, gdzie otwieranie zamków jest sportem wyczynowym). Kluby te są miejscami, w których najwięcej badań prowadzi się nad tematami i metodami pokonywania nowych mechanizmów blokowania i opracowywania nowych metod naruszania starych. Jeśli chcesz dowiedzieć się więcej o otwieraniu zamków i jego praktycznych konsekwencjach, zachęcam do zapoznania się z TOOOL - The Open Organisation Of Lockpickers. Ci faceci są aktywni w Stanach Zjednoczonych (http://www.toool.us) i w Holandii (http://www.toool.nl), ale wszystkie rozdziały są bardzo zachęcające do pytań i nowych osób. Niemożliwe jest zrozumienie, jak otwierać zamki bez kluczy, jeśli nie masz pełnego pojęcia, jak działa zamek. Poszczególne mechanizmy działają na różne sposoby, ale terminologia jest taka sama i jeśli rozumiesz koncepcje kryjące się za najpopularniejszym typem zamka - bębenkiem pokazanym na rysunku 5.1 - to inne mechanizmy nie będą zbytnio przeszkadzać. Rysunek 5.2 przedstawia widok z boku. Poniższa lista zawiera listę części zamka.

• Kadłub - jest to część zamka, która się nie obraca.

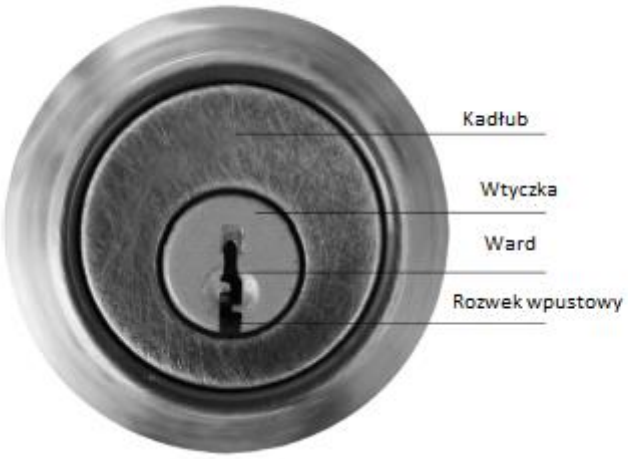
• Wtyczka - będzie się obracać po włożeniu prawidłowego klucza.

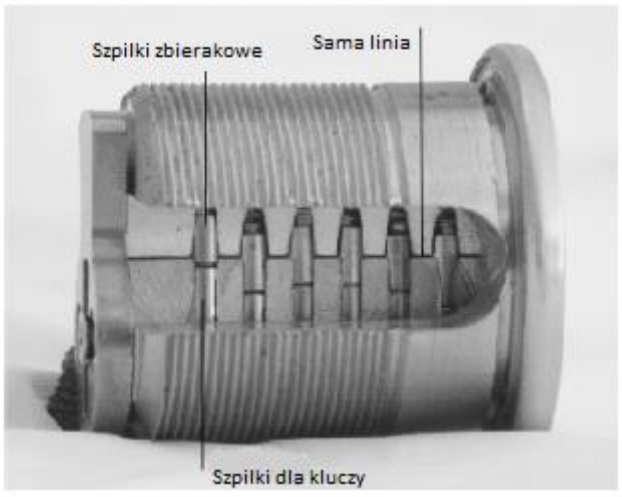
• Rowek wpustowy - Nic dziwnego, że w tym miejscu znajduje się klucz.

• Ward - te występy pozwalają tylko na klucze o odpowiednim wycięciu być włożone w rowek.

• Kołki zabierakowe - Kołki zabierakowe znajdują się nad kołkami klucza i są dociskane przez sprężyny.

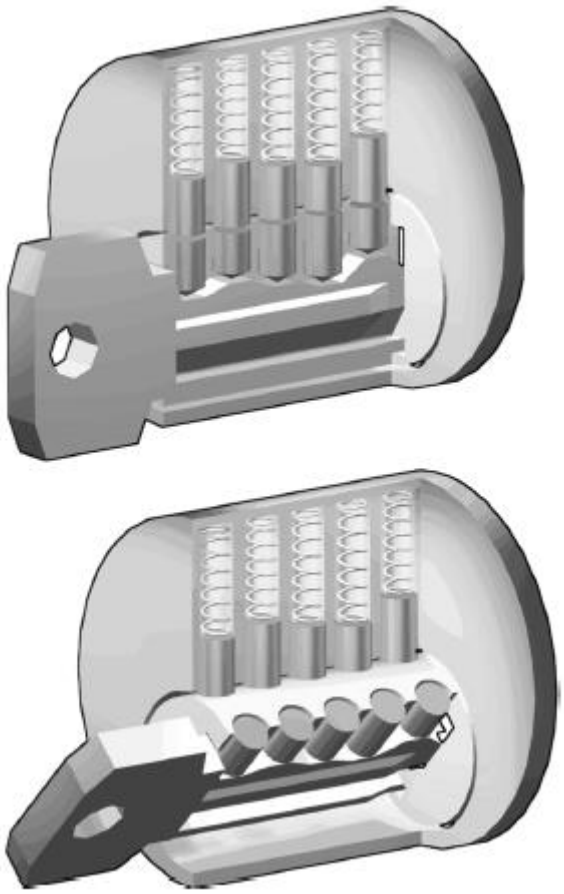
• Kołki do kluczy - Kołki do kluczy są wkładane do wtyczki przez sam klucz.





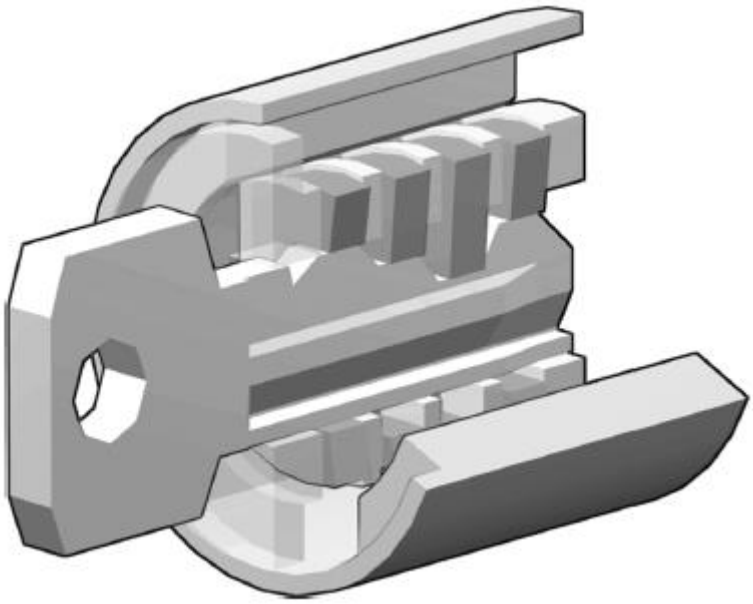
• Sama linia - kiedy właściwy klucz jest włożony do zamka, sworznie zabierakowe i sworznie klucza spotykają się na linii prostej, umożliwiając obrócenie wtyczki i otwarcie zamka. W przypadku włożenia niewłaściwego klucza (lub braku klucza) kołki przekraczają linię wzniosu, uniemożliwiając obracanie się wtyczki. Zwróć uwagę, że wszystkie szpilki zabierakowe mają tę samą długość, podczas gdy długość kołków jest różna.

Trudno jest właściwie uchwycić terminy po prostu na podstawie schematów liniowych i tekstu, dlatego rozważ rysunek , który przedstawia kołki, gdy różne klucze są włożone do zamka.

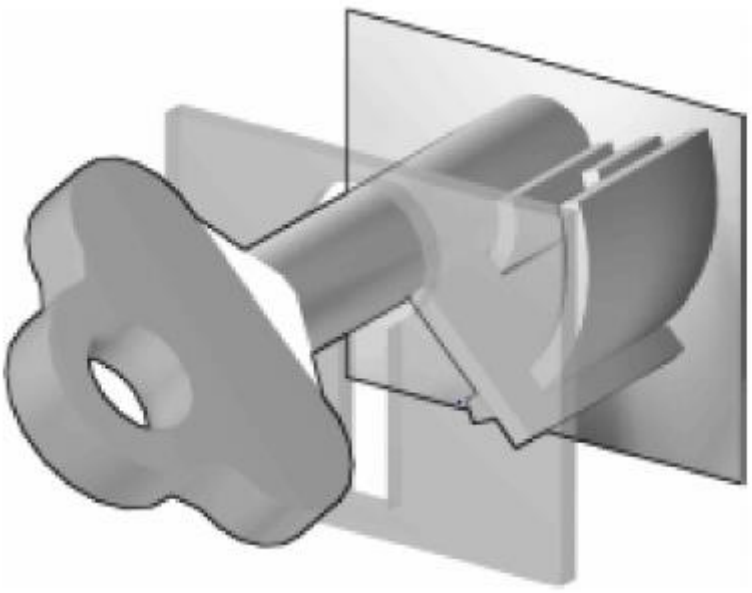


Na ilustracji u góry włożono niewłaściwy klucz. Zabierak i kołki kluczyka nie spotykają się na linii prostej i zamek nie otwiera się. Na obrazku u dołu wstawiony jest właściwy klucz. Sworznie spotykają się na wzniosie, umożliwiając otwarcie zamka. Jak już wspomniano, to długość szpilek jest zmienna; zmiana odwrotnie odpowiadająca wierzchołkom i rowkom na kluczu. W ten sposób tylko właściwy klucz pozwoli na otwarcie zamka. Do momentu włożenia klucza kołki klucza opadają prawie do samego końca w rowku, a przestrzeń nad nimi jest zajęta przez kołki zabierakowe, utrzymując mechanizm zablokowany. W skrócie, tak działa zamek bębenkowy, chociaż istnieją różnice, takie jak liczba użytych par pinów. Zwykła liczba to cztery lub pięć. Niektóre szpilki są bezpieczniejsze niż inne i zawierają dodatkowe mechanizmy zabezpieczające. Omówię je później, kiedy będę mógł otwierać zamki. Jednak używane są inne mechanizmy blokujące i możesz je napotkać. Narażasz każdy z nich w nieco inny sposób:

• Zamki waflowe - są podobne do zamków bębnowych, ale są dużo łatwiejsze do ominięcia. Dominująca różnica z twojej perspektywy polega na tym, że płytki nie są sparowane (tak jak szpilki są pokazane w przykładach). Jeśli naprawdę śledzisz, być może już rozumiesz, dlaczego jest to problem. Zamki waflowe są używane w szafkach na dokumenty (między innymi), więc warto mieć możliwość ich ominięcia.



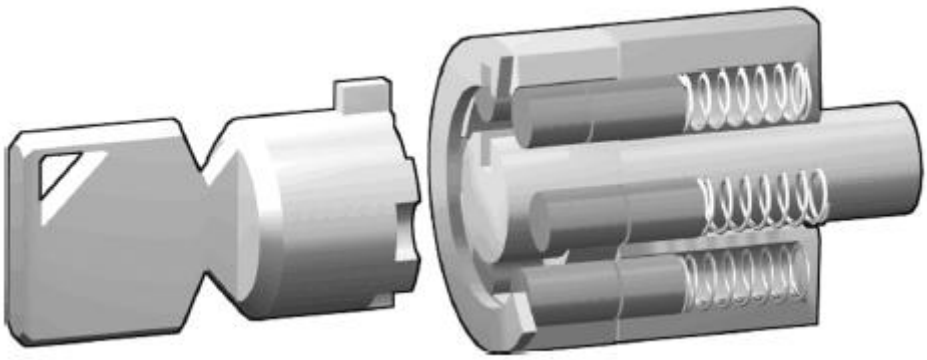
• Zamki chronione - zamki chronione to najstarsze mechanizmy blokujące w historii (nadal w użyciu). Jedyną rzeczą, która uniemożliwia ich wytrącenie, jest zastosowanie „zabezpieczeń" lub przeszkód, które uniemożliwiają otwarcie zamka bez włożenia prawidłowego klucza. Te zamki są nadal dość popularne w Wielkiej Brytanii, ale w USA są ograniczone do tanich aplikacji o niskim poziomie bezpieczeństwa. Dobrze wykonany „szkieletowy klucz" otworzy szeroką gamę zamków chronionych i zestawów dostępnych w Internecie za bardzo niewielkie pieniądze.



• Kłódki - są używane wszędzie, od zamków rowerowych po bramki i śmietniki. Nietrudny do wybrania i faktycznie interesujący, jak zwykle więcej niż jeden sposób na zaatakowanie mechanizmu blokującego.

• Zamki rurowe - są one uwzględnione bardziej ze względu na kompletność niż cokolwiek innego, ponieważ jest mało prawdopodobne, aby zespół operacyjny spotkał się z nimi w terenie. Zamki rurowe

są stosowane w automatach sprzedających i zamkach rowerowych. Jednak są one również używane w blokadach laptopów, co uzasadnia ich włączenie tutaj. Dzięki odpowiednim narzędziom można je łatwo otworzyć.



Wprowadzenie do otwierania zamków

Po przejściu preambuły możemy zabrać się do pracy. Pierwszy omawiam sprzęt potrzebny do rozpoczęcia pracy. Praktycznie cały sprzęt, którego używam do kompletacji pokazałem poniżej. Pełen asortyment produktów można zobaczyć pod adresem www.southord.com, które są dostępne u dystrybutorów na całym świecie. Będziesz potrzebować:

• Standardowy zamek bębenkowy - kup go w lokalnym sklepie. Unikaj takich terminów, jak „odporny na wytrych" i „dowód na pobranie". Te zamki zawierają dodatkowe funkcje bezpieczeństwa, które tylko skomplikują sprawę dla początkującego, chociaż spojrzysz na nie w odpowiednim czasie.

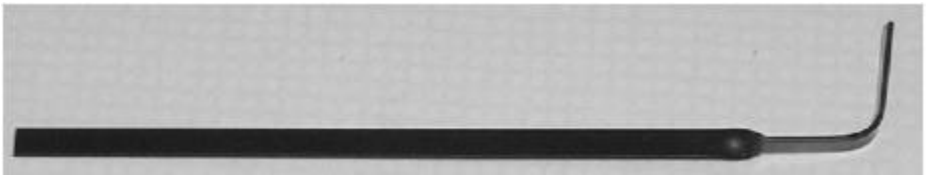
• Zestaw wytrychów - nie musisz wydawać dużych pieniędzy. Wystarczy prosty zestaw z kilkoma wytrychami i kilkoma kluczami dynamometrycznymi. Zwykle wybieram większe zestawy, ale to dlatego, że mam zwyczaj ich łamania, a nie dlatego, że dają większy zakres techniki.

• Blokada ćwiczebna - nie jest to bezwzględny wymóg, ale jest bardzo przydatny dla początkujących, ponieważ możesz zobaczyć efekt, jaki masz na kołkach, co daje lepsze zrozumienie tego, co robisz źle i kiedy robisz to dobrze. (Patrz rysunek 5.9.)

Otwieranie zamków

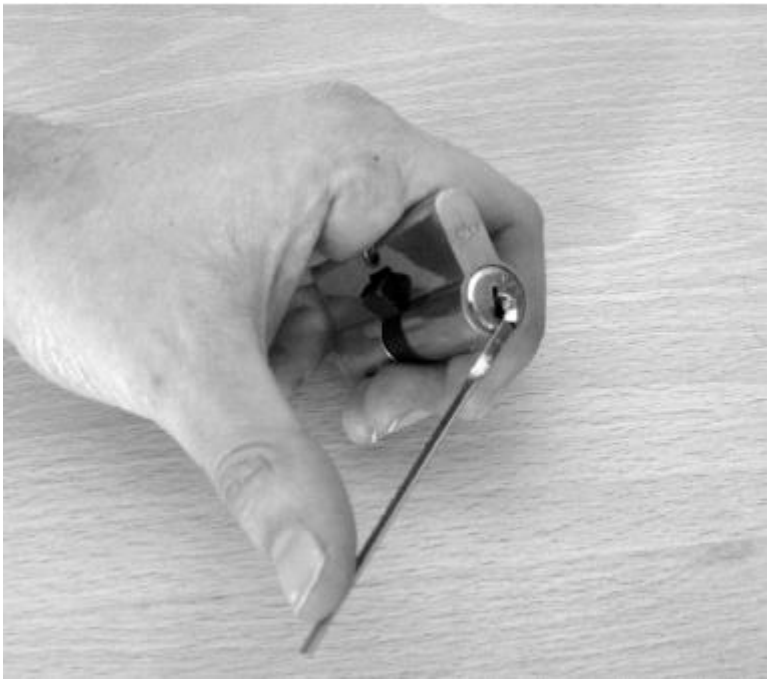
Z poprzedniej sekcji wiesz, jak klucz otwiera zamek; szpilki są ustawiane na miejscu, aż spotkają się na linii prostej i wtyczka może się obracać. Jednak za pomocą odpowiednich narzędzi można podnosić szpilki pojedynczo i osiągnąć ten sam efekt. Jeśli możesz umieścić moment obrotowy na mechanizmie blokującym, jeden (lub czasami więcej) kołków klucza utknie między górną częścią wtyczki a kadłubem, wiążąc go na miejscu. Powodem tego jest po prostu to, że zamki nie są precyzyjnie obrabiane, więc będzie niewielka różnica między szerokością kołków, szczelinami między kołkami a cylindrem i tak dalej, ale najważniejsze jest to, że tylko jeden kołek będzie związany. Gdy ten pin zostanie podniesiony na miejsce, poczujesz delikatne kliknięcie, wtyczka lekko się obróci, a kolejny pin zostanie związany. Powtarzasz ten proces, aż wszystkie kołki zostaną podniesione do linii prostej i zamek się otworzy. Przyjrzyjmy się temu bardziej szczegółowo. Najpierw weź wytrych

i klucz dynamometryczny z zestawu do otwierania zamków.

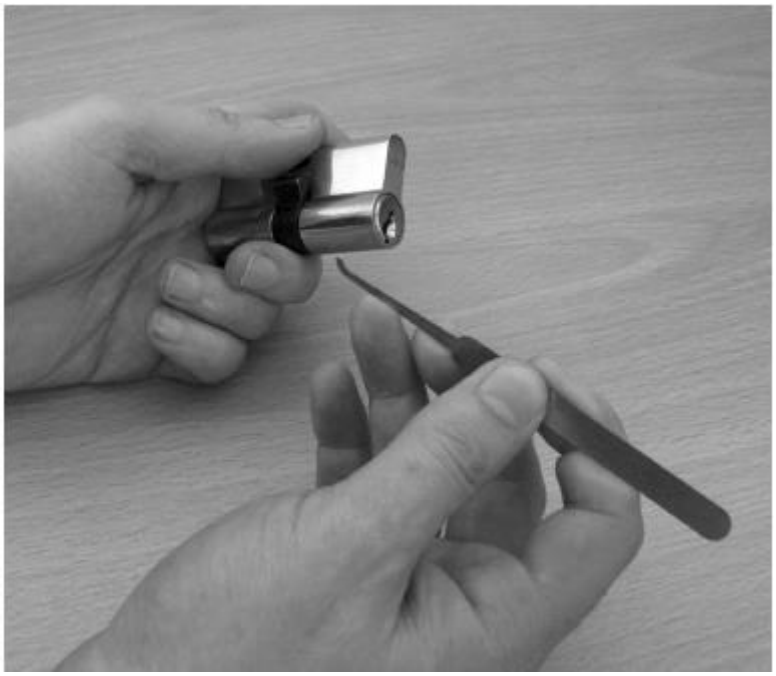


Za pomocą tych dwóch prostych narzędzi można otworzyć praktycznie każdy zamek bębenkowy. Poniższe kroki przedstawiają ten proces bardziej szczegółowo:

1. Weź blokadę do ręki i włóż klucz dynamometryczny, jak pokazano na rysunku. Nacisk wywierany na klucz powinien być minimum niezbędny do przekręcenia wtyczki i powinien być stały – około tej samej siły nacisku potrzebnej do przytrzymania klawisza na klawiaturze komputera.



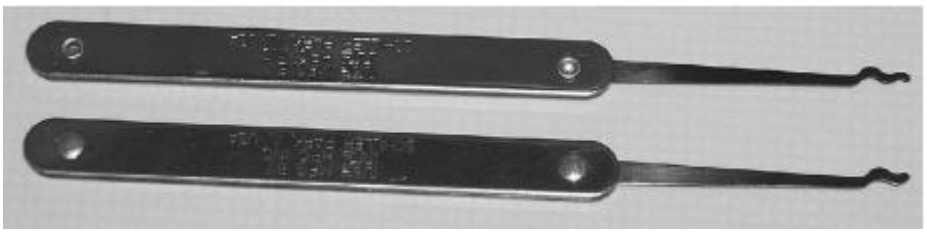
2. Włóż wytrych i delikatnie przesuń końcówkę wzdłuż kołków na górną część rowka, zaczynając od tyłu i przesuwając się w kierunku przodu. Wszystkie szpilki oprócz jednej powinny poruszać się swobodnie pod twoim dotykiem. Jedna szpilka będzie sztywna, ponieważ utknęła między płytami wtyczki i kadłuba.

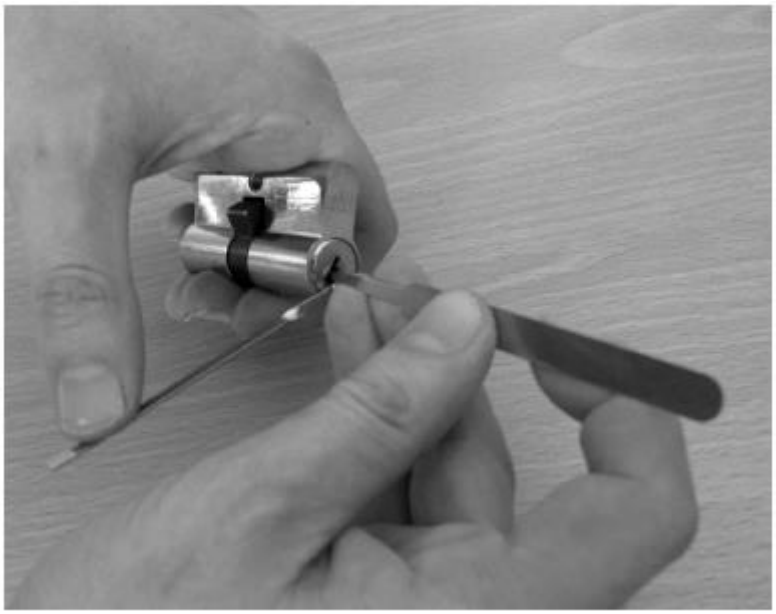


3. Delikatnie i powoli unieś zawiązany sworzeń. Wskoczy na swoje miejsce, a wtyczka lekko się obróci w odpowiedzi na nacisk klucza skrętnego, powodując związanie nowego sworznia, a bolec wpadnie z powrotem w rowek. Podczas podnoszenia związanego kołka ważne jest, aby nie spieszyć się ani nie wywierać zbyt dużego nacisku, w przeciwnym razie istnieje ryzyko, że dolny kołek klucza zostanie uwięziony między wtyczką a kadłubem, a to oznacza zaczynanie od nowa.

4. Powtarzaj proces, aż wszystkie kołki zostaną podniesione do linii wzniosu i zamek otwarty.

Brzmi prosto? Cóż, w zasadzie tak jest, ale wymaga dużo praktyki, aby uzyskać prawidłowy wynik. Wspomniałem wcześniej o TOOOL. OOO oznacza Oefenen, Oefenen, Oefenen (praktyka, praktyka, praktyka). Część dotycząca Stanów Zjednoczonych twierdzi, że to skrót od Over and Over and Over. Ta sama różnica. Istnieje skrót, zwany grabieniem, którego możesz użyć, aby pomóc Ci w otwieraniu zamków z bolcem. Jest to metoda szybkiego ustawiania kręgli poprzez grabienie ich specjalnymi kilofami, które, jak można się spodziewać, nazywane są grabiami.





Mechanizmy odporne na wybieranie

Jedyną rzeczą, która w ogóle umożliwia otwieranie zamków, jest ciągłe stosowanie projektów, o których wiadomo, że są wadliwe od (dosłownie) stuleci. Dostępne są zamki o wysokim poziomie bezpieczeństwa, których w żadnym wypadku nie da się wykryć w żadnych praktycznych okolicznościach. Jednak te zamki są drogie w porównaniu z zamkami za 30 USD, które większość ludzi ma na swoich drzwiach. To powiedziawszy, producenci zamków mają kilka sztuczek w rękawach, aby uczynić zamek bardziej odpornym na wytrych bez uciekania się do skomplikowanych i zbyt drogich projektów. Kluczowym słowem jest odporność, a nie dowód. Te środki zaradcze mają postać specjalnie zmodyfikowanych szpilek wymienionych jeden lub więcej kluczyków lub kołków w zamku. Ma to na celu udaremnienie prób otwierania zamków. Trzy główne typy kołków zabezpieczających w produkcji to:

• Szpilki szpulki - jest to najpopularniejszy rodzaj szpilek zabezpieczających i może być bardzo frustrujący dla początkującego. Trzpień szpulki jest znacznie węższy w średnicy wzdłuż środka niż na obu końcach. Może to spowodować ,że sworzeń, który ma zostać uwięziony wzdłuż linii wzniosu podczas podnoszenia. Frustracja polega na tym, że przy pierwszym napotkaniu kołków szpulki dotykowe sprzężenie zwrotne jest takie samo, jak w przypadku pomyślnego ustawienia kołka, a wtyczka będzie się obracać w podobny sposób, z wyjątkiem tego, że obrót jest przesadzony i to jest klucz do identyfikacja obecności szpulek. Po zidentyfikowaniu trzpienia szpulki należy ustawić. Aby to zrobić, lekko zmniejsz napięcie klucza dynamometrycznego i używając mniejszego nacisku niż normalnie, podnieś sworzeń do łoża. Wznów normalne napięcie i normalnie wyjmij resztę szpilek.

• Kołki grzybkowe - tak zwane, ponieważ główka kołka wbijającego ma kształt grzyba, działają one w podobny sposób jak szpula szpilki. Praktyczna różnica między trzpieniem szpulkowym a trzpieniem grzybkowym jest bardzo mała; oba zostały zaprojektowane tak, aby frustrować otwieracza zamków, powodując uwięzienie sworzni prowadzących między górną częścią wtyczki i kadłuba. Jedyna prawdziwa różnica w porównaniu z narzędziem do wybierania zamków perspektywa jest taka, że przesadny obrót jest odczuwany, gdy trzpień szpulki zostaje uwięziony, jest nieco mniejszy w przypadku trzpienia grzybkowego. Sposoby pokonywania tego typu blokad są identyczne.

• Kołki ząbkowane - Są to (moim zdaniem) najbardziej irytujące ze wszystkich. Mogą to być zarówno klucze, jak i wkrętaki, a ich zabezpieczenie polega na wycięciu z boku ząbków. Ząbkowane części

kolidują z naturalnym przesuwaniem się kołka po linii wzniosu, ponieważ każde ząbkowanie lub grzbiet zaczepia się o wierzchołek wtyczki, gdy jest pod wpływem momentu obrotowego (który będzie w większości). Może to prowadzić do myślenia, że pin został ustawiony, podczas gdy w rzeczywistości tak nie jest. Jeśli wiesz lub podejrzewasz, że używane są kołki ząbkowane, nie ufaj charakterystycznemu kliknięciu kołka ustalającego, ale spróbuj podnieść go dalej. Uczucie zgrzytania (gdy grzbiety przekraczają linię wzniosu) jest klasycznym wskaźnikiem obecności ząbkowanych kołków.

Wskazówki dotyczące ćwiczenia umiejętności otwierania zamków

Otwieranie zamków po prostu nie jest jedną z tych rzeczy, których możesz się nauczyć z książki; będziesz musiał ćwiczyć te koncepcje. Istnieją jednak sposoby, aby nieco ułatwić ten proces. Omówiłem już ćwiczenia praktyczne. Kup sobie jeden zamek ćwiczebny. W tej chwili dostępnych jest kilka całkiem zaawansowanych modeli, które są zarówno wycięte (tj. widziałeś szpilki), jak i można je odtworzyć bez żadnych specjalnych narzędzi. Zamki są wyposażone w szpilki o różnych rozmiarach (a także szpilki zabezpieczające omówione w poprzedniej sekcji) i można je łączyć i dopasowywać, aby ćwiczyć to, czego się nauczyłeś. Pozwoli to zaoszczędzić czas, nie wspominając o pieniądzach. Dwa szczególnie ładne przykłady praktycznych blokad to:

• Ultimate Practice Lock z http://www.learnlockpicking.com.

• EZ ReKey jest dostępny praktycznie z każdego miejsca, gdzie sprzedaje się wytrychy.

Ćwiczenie następujących technik pomoże rozwinąć umiejętności niezbędne do otwierania zamków z bolcem:

• Trzymanie wytrycha - sposób trzymania wytrycha decyduje o tym, jaki sukces odniesiesz z nim. Wolę trzymać go trochę jak ołówek, ale z palcem wskazującym trzymanym na końcu kilofa i kciukiem dotykającym palca wskazującego.

Jednak rozwiniesz styl, który będzie dla ciebie naturalny. Zapamiętaj, zasięg i precyzja ruchu są ważniejsze niż siła. Upewnij się, że w miarę możliwości to palce, a nie nadgarstek, kontrolują każdy aspekt ruchu kilofa, a nie nadgarstek.

• Nacisk podczas kompletacji - jedną z najważniejszych części podczas kompletacji jest wiedza o tym, jaki nacisk należy wywierać na kołki. Za mały nacisk i nie będziesz miał wpływu na kołki napędowe - za duży i uwięzisz bolec. Zapoznanie się z różnymi zamkami w ten sposób jest kluczowe, ponieważ nie

będziesz mieć na to czasu podczas wykonywania zadania. Wyrzuć klucz dynamometryczny i za pomocą podnośnika poczuj opór na kołkach. Ponieważ wszystkie zamki mają nieco inny charakter, to ćwiczenie ćwiczy wyczucie różnych mechanizmów, a co ważniejsze ćwiczy zmysły dotykowe, aby dokładnie wiedzieć, co dzieje się wewnątrz cylindra. Brzmi to (i wydaje się) niesamowicie trudne, gdy zaczynasz, ale szybko to zrozumiesz.

• Eksperymentowanie ze skręcaniem - Prawdopodobnie największym błędem popełnianym przez nowicjuszy przy otwieraniu zamków jest umieszczenie niewłaściwej ilości momentu obrotowego na wtyczce podczas próby ustawienia pinów. Tego można się nauczyć tylko poprzez doświadczenie.

• Kołki nastawcze - Jedną z korzyści uczenia się z blokadą treningową jest to, że możesz zobaczyć, jak koło poruszają się i ustawiają, co pozwala poczuć subtelne zmiany oporu, które pojawiają się, gdy tak się dzieje. To dobry sposób na śledzenie postępów. W przeciwnym razie nie jest bardzo jasne, co dzieje się w zamku i bardzo łatwo jest rozwinąć złe nawyki. Musisz również nauczyć się wyczuwać różnice między prawidłowym ustawieniem kołka a uwięzieniem kołka zabezpieczającego w kadłubie.

Techniki zaawansowane

Po zapoznaniu się z podstawowymi tradycyjnymi metodami otwierania zamka z bolcem, możesz poczuć ulgę lub (być może zirytować), że są łatwiejsze sposoby. Puryści zbierający zamki powszechnie rezygnują z tych metod, ale z drugiej strony to nie oni muszą otwierać zamki pod ciśnieniem w nocy, podczas deszczu.

Korzystanie z pistoletu Snap Gun

Snap Gun to automatyczne narzędzie blokujące, które znacznie ułatwia proces otwierania zamków bębnowych. Urządzenie zostało początkowo opracowane dla funkcjonariuszy organów ścigania, którzy nie byli przeszkoleni w zakresie otwierania zamków i którzy musieli szybko otwierać drzwi - tak przynajmniej mówi historia.

Proces otwierania zamka za pomocą Snap Gun jest prosty, ale trochę inny niż użycie wytrycha i klucza dynamometrycznego. W przypadku pistoletu sprężynowego klucz dynamometryczny nadal musi być używany, z wyjątkiem tego, że nie próbujesz ustawiać jednego sworznia na raz. Za każdym razem, gdy spust pistoletu jest naciśnięty, igła zostaje wciągnięta i uderza jednocześnie we wszystkie bolce. Ta czynność (poprzez przekazanie energii) powoduje wyrzucenie wszystkich kołków napędowych do góry. Skutkuje to luką na linii prostej. A więc w praktyce:

1. Włożyć igłę pistoletu sprężynowego do zamka równolegle do kołków.

2. Szybko pociągnij spust pięć razy, cały czas naciskając na klucz dynamometryczny.

3. Jeśli zamek nie otwiera się, zwiększ siłę uderzenia na Snap Gun i powtórz.

Większość zamków (w tym te z kołkami zabezpieczającymi) można otworzyć szybko i łatwo za pomocą Snap Gun. Zwróć uwagę, że wielokrotne użycie tego samego zamka spowoduje (nie może, spowoduje) jego uszkodzenie. Biorąc jednak pod uwagę, że to urządzenie jest tanie, niezawodne i pozwoli Ci zaoszczędzić dużo czasu, powinieneś mieć je w swojej torbie z zestawem.

Bumping

„Wbijanie” zamków jest stosunkowo nową techniką otwierania zamków bębnowych. Wykorzystuje specjalnie wykonane klucze, w których wszystkie rowki są przycięte na jednakową długość. Klucz uderzeniowy, wkłada się do zamka, delikatnie naciskając, aby zapewnić moment obrotowy, a następnie „uderza” lub uderza twardym przedmiotem. Powoduje to jednoczesne przeskakiwanie wszystkich pinów, umożliwiając obrócenie wtyczki. Klucze uderzeniowe muszą być wycinane z półfabrykatów identycznych jak te używane w zamku, który próbujesz otworzyć. Jest to zaskakująco skuteczna technika i tylko kilka zamków nie jest na nią podatnych. Kołki zabezpieczające i podobne środki zaradcze nie mają większego znaczenia podczas uderzania w zamek. Osoby zbierające zamki musiały kiedyś wycinać własne klucze uderzeniowe, ale to już nie jest prawdą. W ciągu ostatnich kilku lat praktycznie wszyscy sprzedawcy internetowi sprzedający wytrychy sprzedają teraz zestawy kluczy uderzeniowych, które otwierają praktycznie każdy zamek pinowy. Podobnie jak karabinek, klucze uderzeniowe są czymś, co chcesz zdobyć, nauczyć się używać i trzymać pod ręką. Jeśli jesteś zainteresowany wpadaniem, gorąco polecam przeczytanie tej białej księgi na ten temat od wspaniałych ludzi z TOOOL http://www.toool.nl/bumping.pdf.

Atakowanie innych mechanizmów

Nie wszystkie zamki zawierają kołki rozporowe. W tej sekcji omówię inne mechanizmy blokowania, z którymi prawdopodobnie się spotkasz. Omówione już systemy zamków są bez wątpienia najczęściej stosowaną formą zamków. Otwieranie takich zamków wymaga pewnych umiejętności i wytrwałej praktyki. Większość innych form zamków wymaga od atakującego jedynie automatycznej znajomości konkretnych technik wymaganych do ich pokonania. Wiele mechanizmów blokujących można łatwo pokonać bez żadnych umiejętności, jeśli wiesz, jak działa mechanizm. Stanowiło to mniejszy problem przed pojawieniem się Internetu i łatwym rozpowszechnianiem związanych z nim informacji. Ale Internet udostępnia każdemu informacje o otwieraniu zamków.

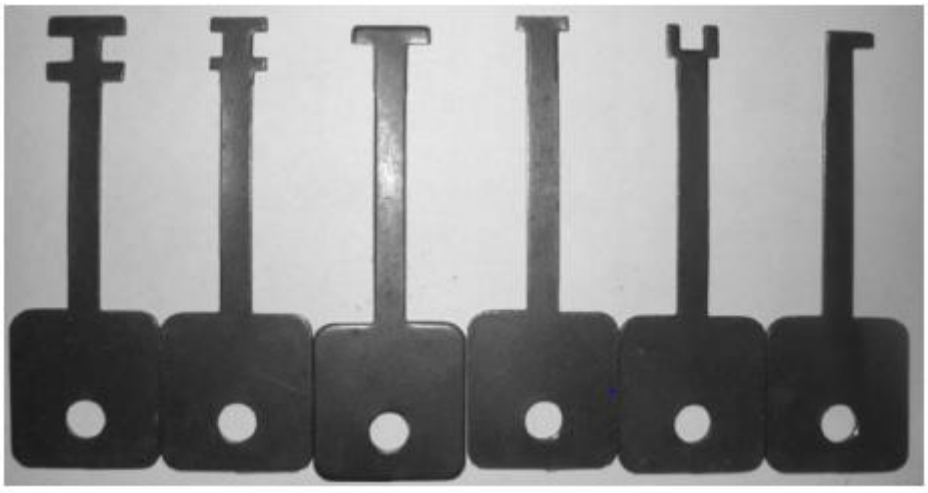
Pokonanie kłódek

Kłódki służą do zabezpieczania różnych aktywów, przede wszystkim tam, gdzie wymagana jest przenośność - na przykład łańcuchów rowerów. Jednak kłódki są często używane do łańcuchów bram

i ogrodzeń i często są używane jako dodatkowy mechanizm blokujący drzwi. Kłódki są zwykle oparte na bolcach (choć ze zmniejszoną liczbą szpilek. Prawie nigdy nie obejmują one szczegółowo omówionych środków bezpieczeństwa i w związku z tym można je atakować za pomocą tradycyjnych wytrychów. Często jest to jednak niepotrzebne, ponieważ w mechanizmie blokującym występują dodatkowe słabości). W przeciwieństwie do zapadki z bolcami znajdujące się na drzwiach, kłódki (z konieczności) odsłaniają kluczową część mechanizmu, samą klamrę. Wiele kłódek wychwala zalety ich dodatkowych bezpiecznych pałąków (mówiąc, że nie można ich łatwo przeciąć). Nie jest konieczne. Wewnętrznie, niezależnie od tego, czy kłódka jest zamkiem trzpieniowym, czy zamkiem szyfrowym, relacja między pałąkiem a mechanizmem blokującym jest bardzo prosta. Aby otworzyć kłódkę potrzebujesz specjalnych wytrychów zwanych podkładkami, które możesz kupić w sklepie z otwieraniem do zamków lub wykonać samodzielnie. Podkładki to małe cienkie kawałki metalu, które można włożyć między szeklę a kadłub i przekręcić, co powoduje odłączenie mechanizmu blokującego i otwarcie zamka. Nawet kłódki, które reklamują się jako „dowód wytrychu" lub „wysoki poziom bezpieczeństwa", można zwykle otworzyć za pomocą metody podkładek. Podkładki można zrobić z kilku rzeczy (w tym puszek po coli). Zapoznaj się z instrukcjami znajdującymi się w tej witrynie internetowej http://www.instructables.com/id/Open-Any-Padlock/.

Otwieranie zamków chronionych

Jeśli dorastałeś w Wielkiej Brytanii, prawdopodobnie miałeś zamki zabezpieczone na tylnych drzwiach. Są to bardzo proste urządzenia i zapewniają jedynie minimalne zabezpieczenia. Jedyną rzeczą, która powstrzymuje zamek przed otwarciem, jest szereg przeszkód (zwanych wardami), które uniemożliwiają przekręcenie klucza. Odpowiedni klucz bezpośrednio odpowiada tym przeszkodom. Zły po prostu się nie zmieni. Jest jednak duży problem. Wykonanie klucza (lub małego zestawu kluczy), który może ominąć wszelkie osłony i nadal zapewniać wystarczający moment obrotowy do podniesienia zatrzasku, jest trywialne. Prawdopodobnie słyszałeś termin klucz do szkieletu. Stąd pochodzi. Klucz do szkieletu miałby z natury wygląd szkieletowy, aby pasował do dowolnego zestawu zabezpieczeń. Zamki chronione są również popularne w niektórych markach kłódek (ale metoda podkładek jest nadal najłatwiejsza). Tworzenie lub pozyskiwanie kluczy szkieletowych jest banalne. Są dostępne w każdym sklepie, w którym można otwierać zamki, lub można je wyciąć z półfabrykatów, jak pokazano na rysunku



Otwieranie zamków rurowych

Jak już wspomniano, jest mało prawdopodobne, aby zamki te odegrały dużą rolę w karierze testera penetracji, ale warto wiedzieć, jak je otwierać. Są one najczęściej widoczne w świecie IT na zamkach zabezpieczających laptopa. W rzeczywistości są to zamki bębnowe. Jednak kołki są ułożone raczej w okrąg niż w jednej linii. Istnieją różne podejścia do atakowania tych zamków; ponieważ kołki są odsłonięte, możliwe jest ręczne manipulowanie nimi do linii wzniosu. Problem polega na tym, że podczas obracania wtyczki musisz trzymać wszystkie szpilki na miejscu lub szpilki po prostu wpadają w następny sąsiedni rowek, co wymaga jednego kompletnego wybrania na szpilkę. Trwa to zbyt długo i jest łatwiejszy sposób. Najpierw musisz zdobyć wytrych rurowy - bestię bardzo różną od twoich tradycyjnych wytrychów i stosunkowo drogi. To narzędzie jest wkładane do zamka i obracane. Gdy jest wsuwany do zamka, każdy z wytrychów jest wciskany do oporu; wiązanie kołków zabierakowych następuje za linią ścinania zamka. Kiedy ostatni kołek jest wciśnięty, płaszczyzna ścinania jest wolna i zamek otwiera się. Można to zrobić w ciągu kilku sekund.

Otwieranie zamków waflowych

Zamki waflowe to najtańsze na rynku zamki, które faktycznie wymagają klucza. Są powszechnie spotykane w szafkach na dokumenty i szufladach, a zamki w wielu samochodach są również formą zamka waflowego. Zamki waflowe występują w dwóch głównych formach; jednostronne i dwustronne. Jednostronny zamek waflowy jest łatwy do otwarciaa; podwójny wymaga trochę więcej wysiłku, ponieważ efektywnie zamek trzeba otworzyć dwa razy, a za drugim razem trzeba utrzymać na miejscu początkowe płytki. Te zamki działają zasadniczo w ten sam sposób, co zamek bębenkowy, w którym właściwy klucz popycha płytki do punktu ścinania, umożliwiając obracanie się wtyczki. Różnica polega na tym, że jest tylko jeden „szpilka", nie ma oddzielnego sterownika ani szpilek do kluczy. To sprawia, że są niezwykle łatwe do wybrania, ponieważ po prostu napinasz i popychasz płytki za pomocą podnośnika, aż usłyszysz, jak klikają pojedynczo. W przeciwieństwie do zamka pinowego, nie można ich wcisnąć zbyt wysoko. Ergo, skręcanie i podnoszenie to wszystko, czego potrzebujesz. Jeśli jesteś choćby trochę kompetentny w wybieraniu zapadek z pinami, zamki waflowe otworzysz w mgnieniu oka.

Stosowanie niszczących technik wejścia

Jeśli zasady zaangażowania pozwalają na stosowanie niszczących metod omijania zamków, masz szczęście. Do Twojej dyspozycji są różnorodne techniki. Niektórzy powiedzieliby, że uciekanie się do nich jest oznaką amatora, ale destrukcyjne wejście ma swoje miejsce; niezaliczenie zlecenia, ponieważ nie można było otworzyć zamka, byłoby niefortunne i zapewniłoby klientowi fałszywe poczucie bezpieczeństwa, gdy dane drzwi prawdopodobnie otworzyłyby się z dobrym kopnięciem. . . . Ponieważ jednak „korzystanie ze stopy" prawdopodobnie mówi samo za siebie, omówię następujące kwestie:

• Wiercenie - Jest to najczęściej stosowana technika, z której korzysta ślusarz, jeśli z jakiegoś powodu nie można otworzyć zamka za pomocą tradycyjnego otwierania. Będziesz potrzebować akumulatorowej wiertarki i mocnej wiertarki (idealnie nadaje się do muru 5,5 mm). Umieść wiertło w zamku tuż nad rowkiem i przewierć wszystkie kołki zabierakowe. Czasami trzeba wziąć nieco duży

kawałek i poszerzyć otwór. Kiedy otwór jest zrobiony, weź płaski śrubokręt i wciśnij go w rowek, obróć go dobrze, a zamek się otworzy. Przećwicz to, zanim spróbujesz w terenie, ponieważ bardzo łatwo jest zepsuć i spektakularnie bałaganić, kiedy to zrobisz. Upewnij się, że nosisz rękawice i okulary robocze, aby chronić oczy.

• Ciągnięcie - jest to technika używana przez straż pożarną, aby szybko dostać się do domu, chyba że masz wyjątkowo słabe drzwi wejściowe, w których wolą używać siekiery (i kto może ich winić?). Potrzebujesz urządzenie zwane „Cylinder Lock Cracker". Po raz kolejny jest dostępny u ślusarza lub w sklepie z wytrychami. To urządzenie może być używane tylko na zamki z lekko wystającą wtyczką. Cracker pasuje do przedniej części wtyczki i jest dokręcony. Następnie użyj dźwigni, aby wypchnąć wtyczkę kadłuba pozwalając na wejście.

Podsumowanie

Omówiliśmy podstawy otwierania zamków. Jeśli nie wiesz czegoś, kiedy zaczynałeś czytać, powinieneś wiedzieć przynajmniej coś! Omówiliśmy następujące kwestie:

• Otwieranie zamków jako hobby - zbieranie wytrychów i dobra zabawa to najlepszy sposób na nauczenie się przedstawionych tutaj pomysłów. Istnieją kluby otwierania zamków, do których możesz dołączyć, gdzie możesz dzielić się pomysłami i uczyć się wskazówek od profesjonalistów.

• Otwieranie zamków - nauczyłeś się podstaw techniki otwierania zamków, a także typów dostępnego sprzętu i sposobu jego użycia. Teraz powinieneś wiedzieć, czym różni się podnośnik, klucz dynamometryczny i grabie.

• Mechanizmy odporności na wybieranie - powinieneś mieć już dobry pomysł na sposoby, w jakie wytwórcy zamków starają się utrudniać otwieranie zamków i powinien wiedzieć, że te mechanizmy są dalekie od doskonałości.

• Sugerowane ćwiczenia - nie za bardzo nauczysz się otwierania z książki. Weź trochę sprzętu i poćwicz - ćwiczenia tutaj to dobry początek.

• Snap Gun - to bardzo przydatne narzędzie może być Twoim najlepszym przyjacielem w przypisaniu testów generacyjnych, gdy czas jest czynnikiem krytycznym. Nie nauczy Cię czegokolwiek o klasycznym otwieraniu, ale dzięki temu Twoje życie stanie się lepsze i dużo łatwiejsze.

• Inne mechanizmy blokujące - powinieneś już wiedzieć, jak otwierać kłódki i zamki rurowe. Powinieneś wiedzieć, że zamki waflowe są bardzo podobne do zamków szpilkowych, a zamki z wkładkami zapewniają najmniej bezpieczeństwa ze wszystkich.

• Niszczycielskie wejście - jest mało prawdopodobne, że podczas testu penetracyjnego będziesz miał dużo ochoty na te metody. To powiedziawszy, niektórzy klienci są otwarci na bardziej realistyczne scenariusze intruzów.

Otwieranie zamków to sztuka, której nie możesz się spodziewać w ciągu nocy. Cierpliwość! Jest to niezwykle przydatna umiejętność dla testera penetracji, którą możesz ćwiczyć w dowolnym miejscu - jest również bardzo satysfakcjonująca i daje dużo radości.