ACCESS PROHIBITED

THE PHYSICAL SECURITY TOOL GUIDE TO HACKS, CRACKS, AND RECON

A RIFT RECON DOSSIER

Access Prohibited
The Physical Security Tool Guide to Hacks, Cracks and Recon

A RIFT RECON DOSSIER

Published in the United States by Rift Recon LLC, 584 Castro Street
Unit 517, San Francisco, California 94114.

Printed in the United States.
Cover design: Rift Recon
Text design: Martin Whitmore
Logo art: Rift Recon
Illustrations: Martin Whitmore
First Edition.
10 9 8 7 6 5 4 3 2 1
ISBN: 978-0-9799019-8-0

CONTENTS

Introduction: ACCESS GRANTED

Combining toughness and sophistication, the skilled, highly intelligent, band-of-outsiders "dream team" has to be one of the most compelling cinema creations ever depicted. Even in its endless combinations, a group of individuals with specialized - usually criminal - skills manages to be both unstoppable and enviable. They're anti-heroes who can go anywhere, and among them is always someone who can fool a security guard, someone who can hack into networks and spy on traffic, someone who can pick locks and open any door, and so on.

Then there are the people who do these things in real life. Usually for a living.
We at Rift Recon are the people who do the real-life versions of these things - more importantly, we outfit and tailor tool kits for the physical security pros who do these things, and we train them, too.

Access Prohibited is our guidebook to the tools you'll find in a physical security penetration tester's "black bag" (also called a "Red Team Kit"). This book is also a fully illustrated, step-by-step how-to guide for the successful use of black bag tools, plus in the field tricks that haven't been shared until now.

The cinema's dream team is a popular formula, and it's one we all know well. But it takes a certain kind of curious mind to venture further than just being merely entertained by this storytelling device, the formula of the thief, the hacker, the driver, the tool specialist (and so on). Someone with this more-curious-than-most mind feels inspired watching the dream team in action, and might identify with one or a few of the characters. Not content to sit still, the curiously inclined wants to be more than just curious; compelled to peel back the layer of artifice, they must find out which of these techniques are real, and how the tricks are done. This person actually wants to do these things.

The person I'm describing is you - and myself, too.

You may have picked up Access Prohibited for a variety of reasons. Those who study bypass techniques, or enjoy the wider interests of the locksport crowd might want to pick through the text and illustrations, seeing which things they already knew and see if we've included anything that surprises them. You may have bought this book because you're a professional physical security penetration tester and want to make sure you add to your knowledge base at every opportunity.

It could be that you're looking through these pages because you enjoy exploring the controversial edges of hacking in the physical realm. Maybe you're inspired by those films and shows that feature smart outsiders who employ dubious - though exciting - talents to complete their tasks and missions. Or, you just want to see the world of locks and security through a different lens, one seen by very few people - perhaps you already do.

You may be reading Access Prohibited because you want to do everything in your power to build a safe home or reinforce a secure business - you want to make sure that what stands between you and losing what's important to you isn't something as simple as a file folder slid between a crack in your door. Some of you are going to pour over these pages because you're an at-risk individual, and want to make sure you have everything possible in your arsenal to ensure you don't wind up as a statistic, such as a woman held against her will.

Perhaps you're just a spy skills aficionado who's ready to soak up some new tricks, or a spy skills fan. But the majority of people picking up this book are physical security professionals on all levels and in all industries. To know how to subvert security is to know how to strengthen it; this is conventional wisdom for security workers and guards at hotels, offices, convention centers, storage facilities, manufacturing plants, and much more.

Access Prohibited is a complete compendium of cracks, hacks and physical bypasses used by the world's top urban infiltrators every day. Many of these clever entry and exit techniques use ordinary, everyday items - though some use specialized tools that require skill and practice, some of which have only been shared among elite security professionals until now.

On these pages you'll lean techniques both basic and advanced about opening most every type of door you'll encounter in everyday urban and office settings, from latch loading (also known as carding a door) and picking locks to fooling heat sensors, magnetic switches and doors that only open from the inside.

See examples of in-person entry tools that support social engineering, such as specialized badges and helpful office equipment with hidden compartments. Find out how to select a multi-tool and headlamp to get for covert urban missions, learn about using LAN Taps for electronic

surveillance, and which endoscope is best when you want to keep a low profile. Read the descriptions and Modus Operandi for each tool and you'll also learn step-by-step how to clone keys, how to defeat padlocks and circular locks, and more.

Every page features a tool or toolset, with full description and tips for the best ones to get, a photo, simple steps to use the tools in the field, and a multi-panel illustration that clearly shows effective use techniques. The entire collection comprises a full infiltration toolkit, while some sections provide examples of basic tools, the reasons you'll need them, and what to look for when you need to select the right one for the job.

The collection of tools and techniques in Access Prohibited are, in fact, the composition of Rift Recon's "Red Team Kit" - a black bag kit used by professional physical security penetration testers worldwide. Everything here is real, and it works.

The knowledge in this book combines that of a locksmith apprentice, a network and physical security penetration tester, a physical security private contractor, and of those involved with law enforcement covert entry teams. The pages of this book are the Red Team Kit's dossier, for field use and reference, and we've adapted them here to provide a guide for everyone interested in what goes into - and happens with - those little black bags.

Most of the techniques described here require familiarity with the tools and how they behave, and plenty of practice. It's a fairly advanced guide that has been boiled down to the basics with a kick; this guide leaves nothing to chance even in its simplest terms, and it's a resource you'll return to for deeper techniques once you've mastered the basics.

Most of what you'll find in Access Prohibited has been hidden or kept secret until now. We strongly feel that this suppression of knowledge about real-life vulnerabilities isn't making anyone safer (though it is making the people guarding those secrets richer). We hope that providing the open access to this information empowers you, teaches you some fun and eye-opening tricks and skills, and helps to make your world a better place.

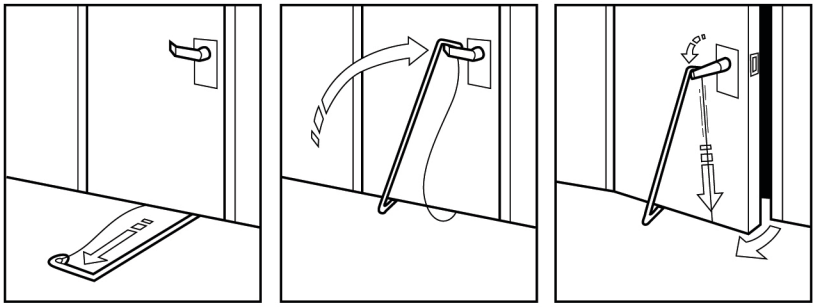
Eric Michaud and the Rift Recon team
San Francisco, California
RiftRecon.com

RIFT RECON

Under the Door Tool

This industry standard tool bypasses some pretty expensive security hardware with a clever mechanism. Rift Recon's Under The Door Tool is comprised of two primary parts: a bent rod (that can be bent further to fit inside the bag) and a wire to control the other side of the rod.

FOR YOUR EYES ONLY



STEP 1:
Slide the L-shaped end of the tool under the door.

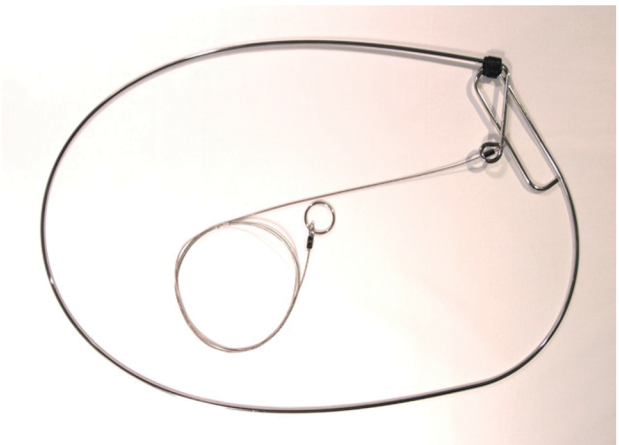
STEP 2:
Twist the tool upright and lean it toward the door handle, and then work the tool over the handle.

STEP 3:
Once you feel it on the handle, pull down on the cable to open the door.

IMPLEMENTATION

Outside of private homes, publicly accessable doors utilize a lever for disabled access, and are left unlocked on the inside - even when the outside lever is locked.

This clever tool slides underneath a door to reach up and pull down on the inside lever. To extend the life of the tool we recommend unbending this tool and storing it hung up or flat on a shelf. When it's time to go, coil the tool to fit in the bag - and you're in.



RIFT RECON

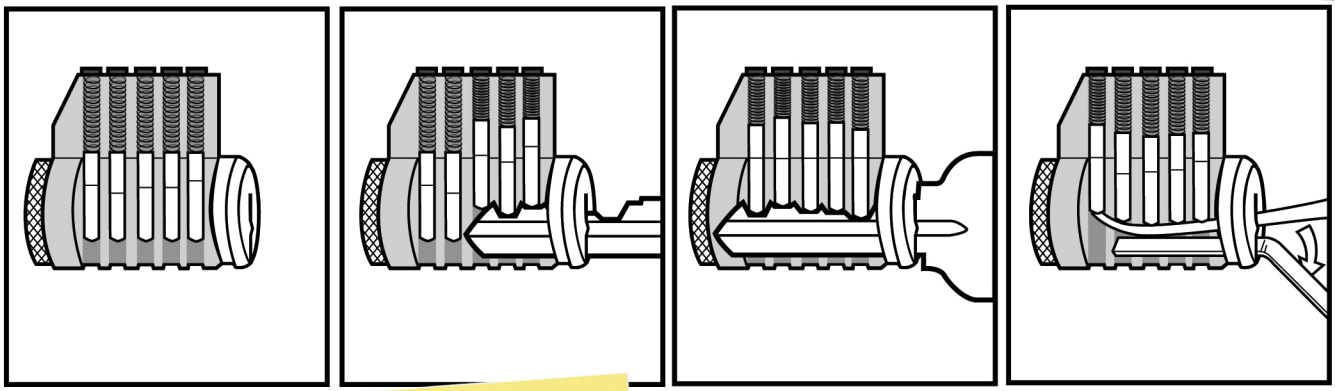
Lockpicks

Lockpicks are often an essential part of every mission and are a classic tool in the physical penetration testers toolkit. You may not use them every time but when you need them you'll be glad they're in your kit.

A standard set of lockpicks will have a short hook, a snake rake, a half diamond, a variety of other picks, and of course, tensioning tools.

Lockpicks made from spring steel or titanium are ideal because they're less prone to cracking and provide good feedback in the hand.

Manipulate



IMPLEMENTATION

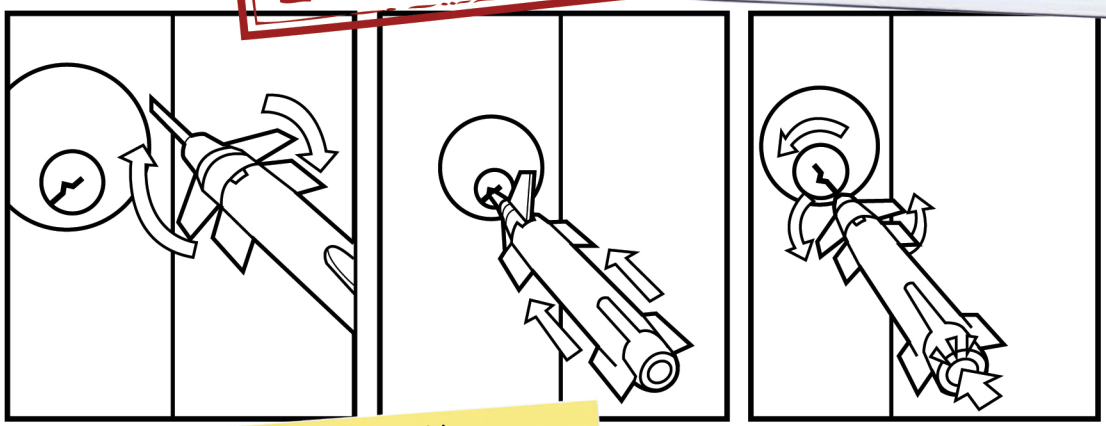
Insert the tension tool into the lock's cylinder plug, leaving room at the keyway top for your second tool. Applying gentle pressure on the tensioner (in the direction you'd turn a key), use a pick tool to reach into the lock, find each binding pin stack and raise each one to the shear line. Repeat until the lock opens. A technique that often works faster on lower-end locks is raking: With Bogota rakes (pictured at right), we find it easiest to jiggle the rake. By varying the angles while inserting and removing the rake quickly, the lock will often open before you know it.

RIFT RECON

Plug Spinner

When you find that a lock is easier to pick to the locked position instead of the unlocked position, a plug spinner generates enough force to disallow pin tumblers from resetting the lock. Our Red Team Kit's selection in a plug spinner tool isn't like the others; ours is exceptionally portable, small, compact and its strength matches its older, clunkier cousins.

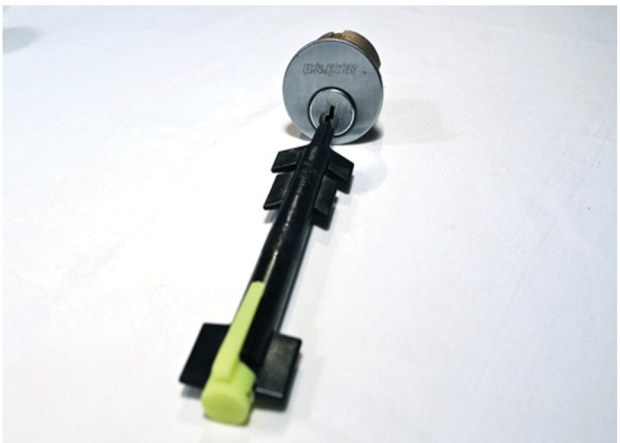
FOR YOUR EYES ONLY



IMPLEMENTATION

Twist the tip of the plug spinner in the direction the lock will allow you to pick it (the opposite direction that you want the lock's plug to spin). Next, push the tip back into the tool to arm the tool, thus locking it and it is ready to use.

Insert the plug spinner's tip into the keyway and turn it carefully until it is as close to re-locking as you can get. You're ready: Press the button to flip the lock. Now you can switch to a regular tension tool to complete your picking (the plug spinner is not rigid enough to use as a tensioner).

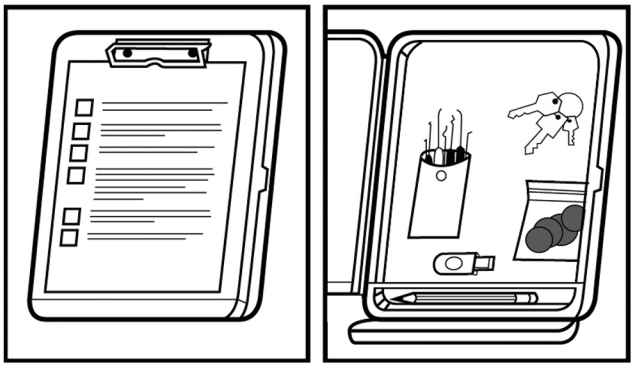


RIFT RECON

Clipboard

Having a clipboard for work is one thing, but using a clipboard for blending in is another thing entirely.

Most assessors stop at just blending in; our choice in a clipboard puts your game on another level with its discreet storage compartments, and lets you bring tools, surveillance devices and much more to your mission.



FOR YOUR EYES ONLY

IMPLEMENTATION

Be ready for your next phase of entry and use a clipboard that doubles as a tool-kit. Store a variety of entry tools, surveillance items, recording devices and backup tools in the onboard storage space.

This clipboard's generous interior makes you mission-ready with lockpicks, gloves, badges, USB sticks, and even fits a few disguise surprises such as glasses or a hat.

Nothing beats planning ahead, and this ordinary office item with two great storage spaces belies its true purpose.

RIFT RECON

Badge Covers & Lanyards

When your mission calls for assessment that requires in-person ID, having the exact employee badge becomes a make-or-break situation.

Employee badges come in a wide range of shapes and sizes, so it's crucial to have a variety of badge and lanyard options at hand.

(Covers for both horizontal and vertical badge orientations come stock in Rift's Red Team Kit.)

IMPLEMENTATION

Use badges in any combination that best emulates the style you're trying to achieve. To get onsite your should look exactly like the targets.

Be sure to use covers that don't need a lamination machine, and produce the same effect. There are multiple attachment methods: plain clip, badge reel, luggage tag, and neck lanyard.

We've included an RFID card in our Red Team Kit badge pack to increase the wearer's authenticity.

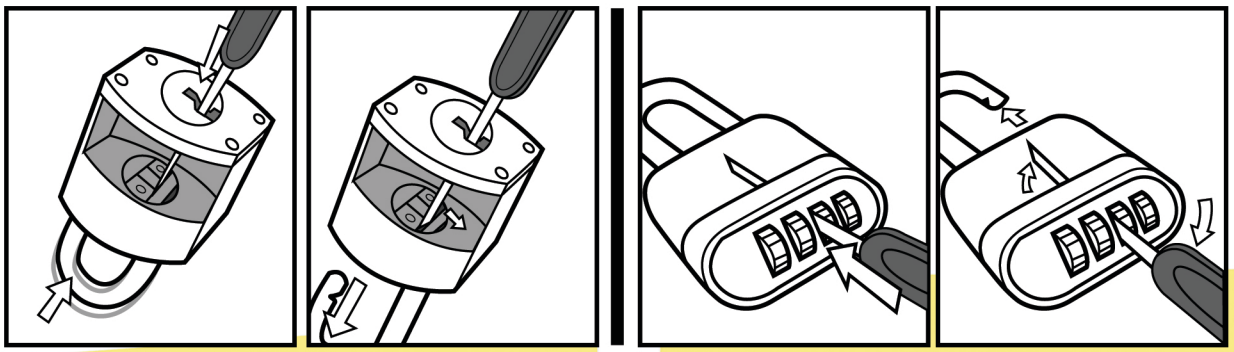
FOR YOUR EYES ONLY

RIFT RECON

Knife Tools

Included in our Red Team Kit are two knife tools: knife tools are ideal for many uses, notably for reaching through lock keyways to act on elements beyond the pins. Knife tools are excellent for opening commonly used padlocks and filing cabinets.

FOR YOUR EYES ONLY



IMPLEMENTATION

Use the thick knife on toe/heel cam padlocks. When you insert the knife tool through the keyway to the back of a vulnerable padlock and seat the tool properly, apply pressure in the opposite direction of the shackle to cause the shackle to spring open.

Some wafer locks have a similar vulnerbility. By pressing the back of a wafer lock, skipping the wafers may allow you to operate the cam in the rear like a light switch.

The Master Lock #175 wheeled combination padlock is vulnerable to overlifting with the thin knife.

Hold the padlock with numbers upright, insert the tool into the top-left gap of the third wheel, then squeeze the shackle down. Slide the knife further under the internal locking plate, and release the shackle.

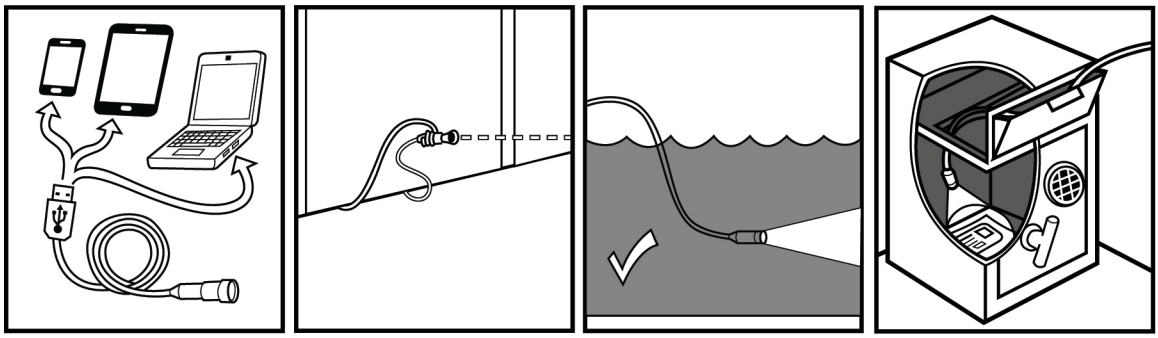
The shackle should open. It may require slight jiggling of the tool while squeezing the shackle again. The knife can also be used to decode some sesame locks.

RIFT RECON

ENDOSCOPE

An endoscope is critical in the recon phase of any assessment - it goes where your eyes can't, and its lighting capability is indispensable in dark environments.

Endoscopes come in a range of sizes and price points, from the small filament with a hefty price tag, to mid-sized and beyond. Be sure to choose an endoscope that works in variable conditions and won't sink your pocketbook if you have to leave it behind. Rift's mid-size waterproof endoscope beat the competition in every test we put it through, and can be utilized with laptops, phones and tablets (using generic drivers).



IMPLEMENTATION

Connect the endoscope to your preferred monitoring or mobile computing device and enjoy clear results.

Look under doors, or over them, through the ceiling plenum. Employ on file cabinets that have a bit of play, or even depository safes.

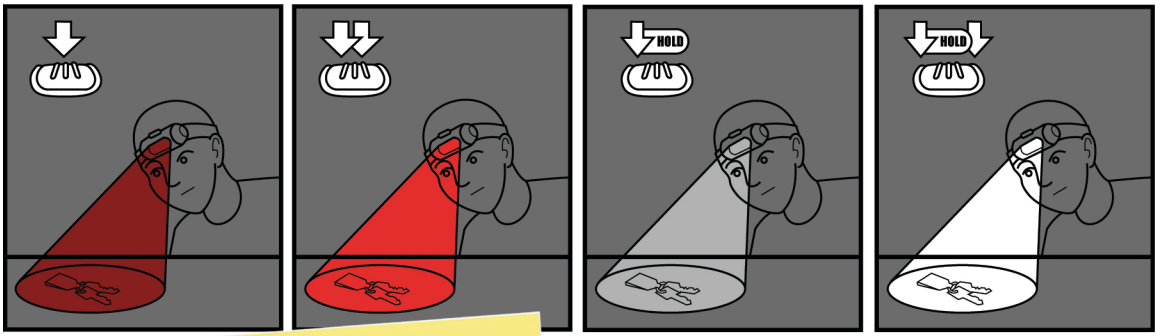
Combine with the copper wire in Rift's Red Team Kit to enhance your control by custom forming bendable shapes.

RIFT RECON

Headlamp

Operating under darkness is often a necessity, making the selection of your headlamp important. Your headlamp needs to fit properly, operate reliably, and function in a way to ensure you don't blind yourself with white light in the field.

In order to find the right unit, Rift tested a surprising number of headlamps. Our headlamp finalist features a very bright white maxbright LED in addition to three smaller LEDs for red lighting, which prevents your dark (or nighttime) visual adaptation from being spoiled - you must hold the button to activate white light so you won't accidentally bump the button on and ruin your night vision.



IMPLEMENTATION

Press once for a dim red light; press again for a bright red light. Hold the button to activate white light, and press again for a brighter white light.

Make sure you have fresh batteries before going into the field and that your headlamp fits snugly.

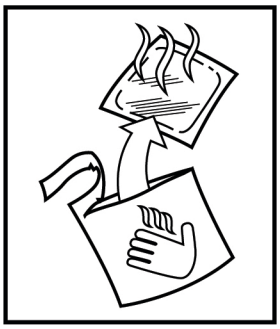
You can also hold the headlamp in your hand as a standard flashlight.

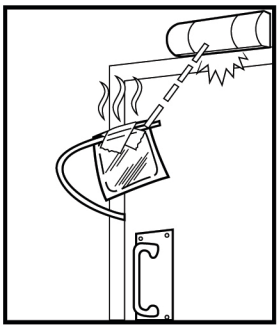
RIFT RECON

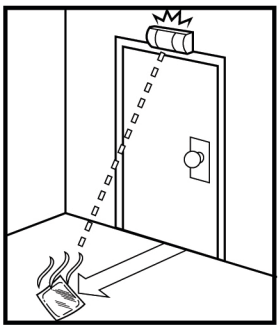
Hand Warmer

Hand warmers can be used for more than their originally intended purpose. When you need to trigger an exit sensor reliant on thermal differentials as well as motion, a well-chosen set of warmers will get you on your way.

FOR YOUR EYES ONLY







STEP 1:
Open package to activate warmer.

STEP 2:
Attach warmer to either a wire and slide it through the gap, or just slide it under the door to activate thermal and motion sensors.

IMPLEMENTATION

Open the package and activate the warmers 5-10 minutes before use.

The best way to trigger heat-activated sensors is to tape a hand warmer to the end of your kit's copper wire, slide it through the gap in the door, and wave the heat-on-a-stick in view of the sensor.

Sliding a hand warmer under the bottom of the door can also work: the motion and heat is often enough to trip the sensor.

RIFT RECON

Elevator Fire Keys

A set of elevator fire keys will ensure that you have full control over most elevators you encounter in the field, can go to whichever floor you want, and can also hold elevators at those floors.

FOR YOUR EYES ONLY

IMPLEMENTATION

Because elevator fire keys radically change the operation of emergency systems, only employ them if you fully understand their actions.

To use, insert a fire key into the key switch at the recall station on the ground floor. Turn the key to set fire service to ON.

The elevator alarm will sound until the elevator reaches your recall station. All elevators will decsend to the recall station floor and all elevator doors will open and remain inoperable.

To reach the target floor, get in the elevator and turn the fire service key switch to the ON setting. Select floor and hold the Close Door button until the door fully closes.

To exit, press the Open Door button until door fully opens. Remember that if you release the door key at any time, the elevator door will go back to its previous state open/closed.

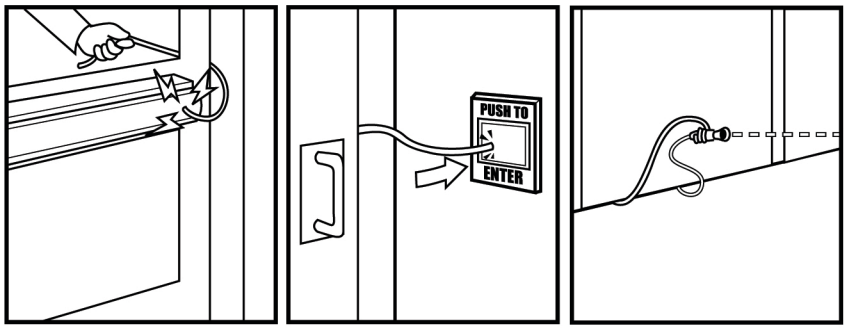
Don't forget to reset each of the key switchs or the elevators may lock out legitmate users who need it.

RIFT RECON

Copper Wire

After much testing, we selected a conductive wire our Red Team customers that has a precise thickness and tensile strength. Too thick, and the wire would be too bulky, heavy and hard to bend and fit into narrow spaces. Too thin, and the wire wouldn't retain its shape.

FOR YOUR EYES ONLY



IMPLEMENTATION

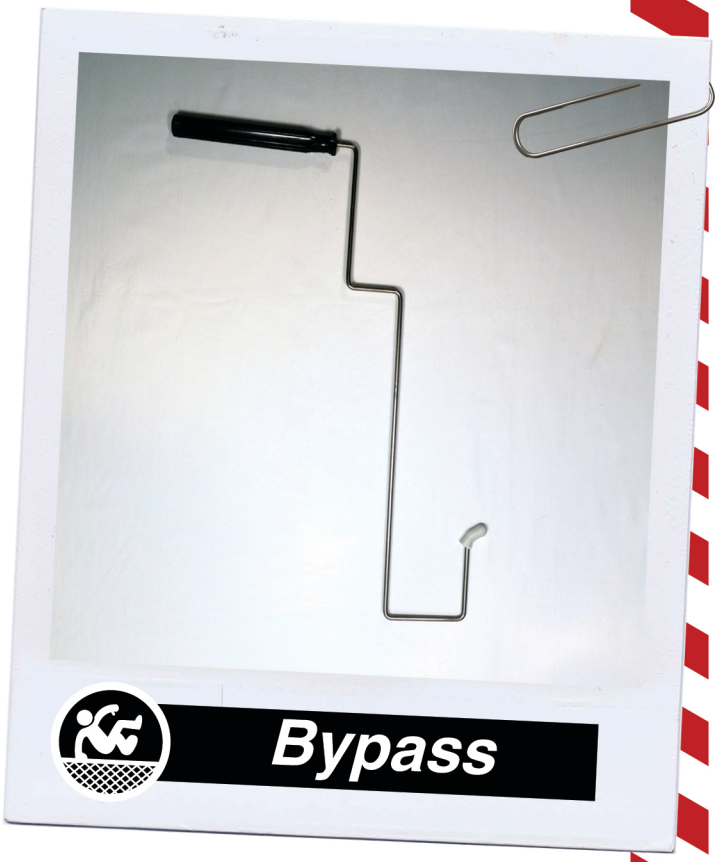
Exit bars based on a capacitive touch system respond to conductive copper wire - by opening up on contact.

Simply grasp the wire with your bare hand and touch the wire to the bar; your body's capacitance is detected by the exit bar, making the door open.

This wire can also be utilized as a custom-bent tool to push request-to-exit buttons; extending straight out underneath doors to trip motion sensors; or securely wrapping around other tools to extend their reach (such as an endoscope).

RIFT RECON

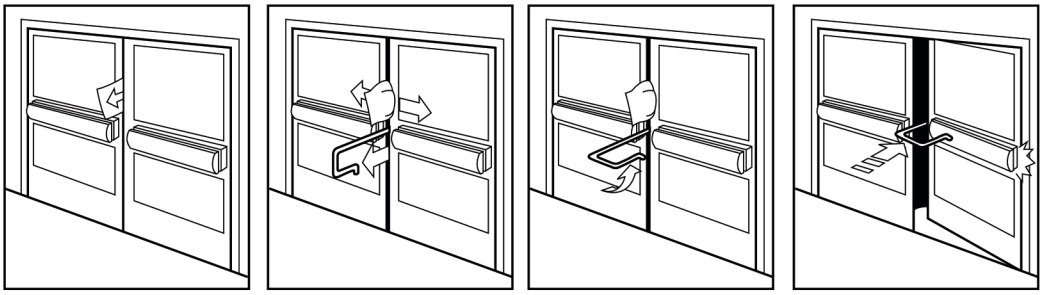
Push To Exit Bar Tool



When you come up against a door, and the push-to-exit bar is on the other side, you dont need to figure out plan B when you have the right tool at hand.

Theres no need to improvise a way to pull back on push-to-exit bars from the outside: tried, tested and true, this tool is perfect.

Our Push To Exit Bar Tool has it all: a firm handle, a rubber tip for grip (and to prevent leaving marks), plus strong steel fabrication set to last many uses and several years.



Implementation

Look for a gap between the doors and vertically insert the pushbar tool through the gap.

Keep the tool even with the push-to-exit bar, inserting it until you reach the large bend just past the midway point of the tool.

Rotate the tool 90 degrees in the direction of the push-to-exit bar. Pull back on the tool so that the tip is pulling on the pushbar. Apply force to engage the pushbar and the door will open.

If you have difficulty getting the tool through the gap, use an airbag as a wedge to enlarge the space.

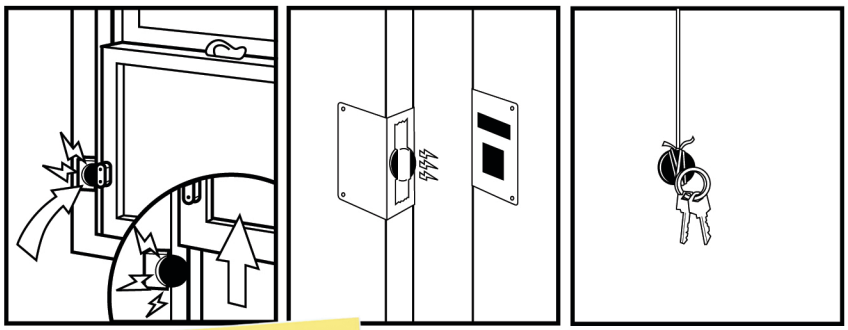
RIFT RECON

Magnets

Many sensors rely on (or are disturbed by) magnetic fields - so they're easily manipulated with small magnets.

For these examples we'll describe the magnets in our Red Team Kit. The first is a round disc magnet half a millimeter thick with a surprising pull force of more than 6 pounds. The second magnet is also a disc, but much thicker.

Covered in teflon, it can be used underwater, in salt water or even in weak acids. Teflon makes it non-marring, so its easy to remove and you dont have to worry about using it on easily-scratched surfaces.



IMPLEMENTATION

Magnets are great at fooling reed switches (which detect if a door or window has been opened). Slide the thin disc magnet into a door or window's thin gap, and either can be opened without triggering the alarm.

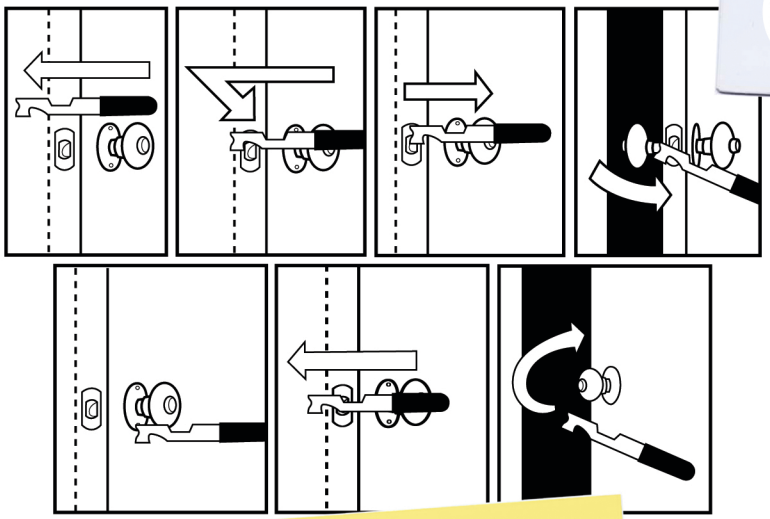
Be sure to tape the magnet to the side where the hall-effect sensor is, rather than the mating magnet. (This is often the side of the sensor that is not on the moving part.) The magnets can also be used as impromptu magnetic pick-up tools, and for many other on-the-fly tasks.

RIFT RECON

Latch Loiding

Loiding is also known as carding a door. Our Red Team Kit features a variety of tools that can be used for loiding: house numbers, a shove knife, a shrum tool, and our handpicked file folder.

The house numbers are discreet, unsuspicious and provide plenty of leverage. The shove knife is a pro tool featuring different tips. The shrum tool is very strong. When you need an odd shape, our file folder can be trimmed to spec.



STEP 1:
Insert tool into the door jam above or below the latch.

STEP 2:
Slide tool over the latch.

STEP 3:
Apply pressure to the latch and pull the tool back, opening the latch.

From the opposite side:
Push the tool straight into the latch, popping it open.

IMPLEMENTATION

With a little practice, loiding can be done very quickly. Push your loiding tool into the gap above or below the latch, slide the tool toward the latch. You may have to wiggle it a bit, and then pull it back to depress the latch.

When you encounter improperly installed hardware, or you approach from the door's opposite side, just push the tool straight into the latch. Spring loaded latches with a deadlatch will not open if the dead-latch is properly engaged.

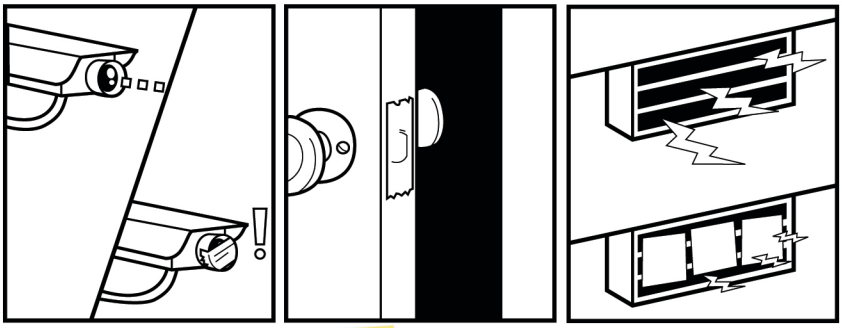
RIFT RECON

Tape

Three specific tape products are chosen for our Red Team Kit; each is selected for uses specific to physical penetration assessment activities, strength, and lack of evidence.

The mini-roll of gaffer's tape - the beefier cousin of duct tape - is stronger than duct tape, easier to rip by hand, and doesn't leave behind a sticky residue. The double-sided masking tape is strong, the thinnest in its class, and won't leave any remnants.

Finally, we always include double-sided foam tape squares, which also leave little trace.



IMPLEMENTATION

Gaffer's tape will secure items, or envelop anything that requires a black cover (such as latches, cameras, sensors, or more).

Use masking tape is when you need a thin amount of clearance between objects or to envelop anything that requires a whiter cover, such as motion detectors.

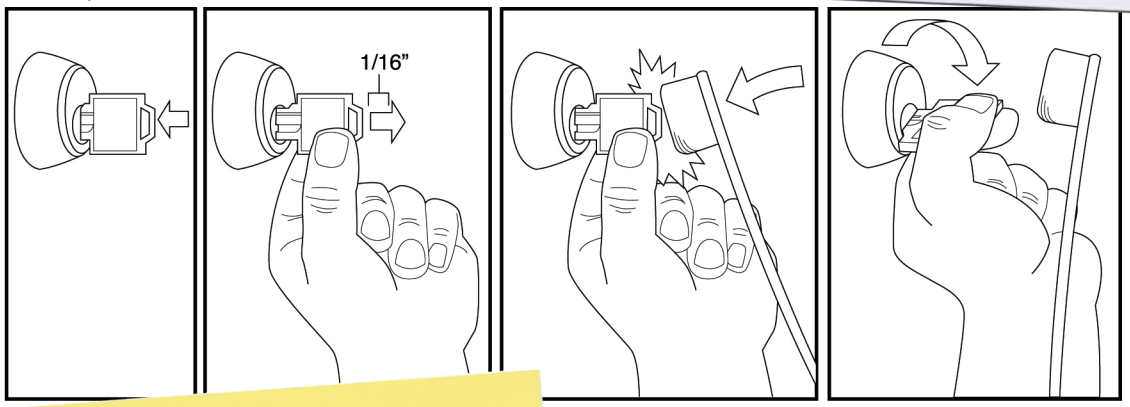
Foam tape squares can be used on electromagnetic locks (the big magnets found at the top of door frames). Prior to mission execution, you can casually apply a few squares on the magnet to increase the distance from the metal contact plate which makes it easier to open later.

RIFT RECON

Bump Keys

A bump key is a modified key blank with the lowest key bitting allowed by code. When inserted into the right lock and struck with a bump hammer, the bump key will cause the driver pins to leap above the shear line, thus making the lock ready to open.

When timed with a quick turn, the lock opens. Locksmiths have known this technique for decades but it wasnt shared publicly until recently. A bump hammer is a tool that applies force to the key. Alternatively, any light weighted object can be used, like the handle of a screwdriver.



IMPLEMENTATION

When a bump key is hit, the small "ramps" drive into the key pins with force. This force transfers through the key pins to the driver pins, which fly up past the shear line; the pins align.

When the pins align the lock is free to turn open. Imagine Newton's cradle or pool-balls, and you get the basic idea. Reminder: lock bumping damages the lock cylinder and pins, so avoid bumping a lock that can't be ruined.

STEP 1:
Slide bump key into lock, pull it out one pin-length.

STEP 2:
Put slight pressure in the direction it should turn.

STEP 3:
Give the key a light tap with the bump hammer. Lock opens.

STEP 4:
If the lock doesn't open, pull key back one pin-length, repeat steps 1 and 2.

RIFT RECON

Lubricant

The wrong lubricant can tank your entire mission. That's why we recommend a lubricant that is a PTFE in a solvent base for phyiscal security assessments.

WD-40 is a great lubricant in many cases, but terrible for locks - it dries and parts re-freeze. Graphite is messy and can clog lock cylinders when moisture enters. Wet lubricants can be ideal but most will attract dirt and dust into clean environments.

We make sure to outfit our Red Team customers with a PTFE based lube, which can do what other lubes can without their drawbacks.

FOR YOUR EYES ONLY

IMPLEMENTATION

When you're out on a physical security assessment just a few sprays of a PTFE based lube will free up stubborn locks for easy, quiet manipulation - spritz into sticky or old, dirty locks that have been outside.

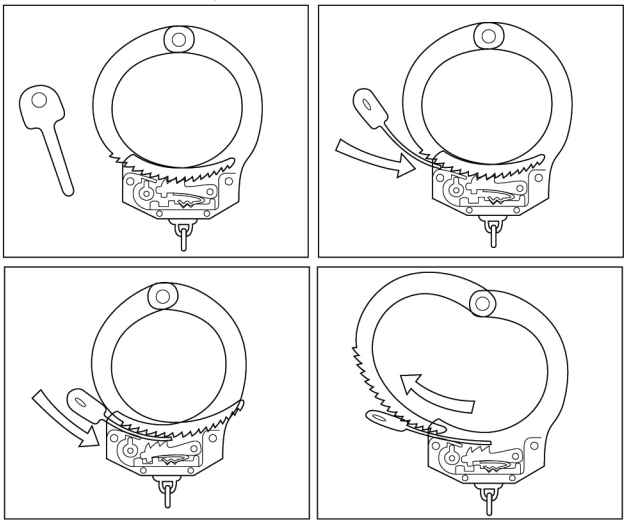
This lubricant can also be used with many other tools in your kit (for sliding in and out of tight spots), or applied on stuck screws, hinges, frozen, or stubborn file cabinet sliders, and much more.

Lubricant can also be sprayed on file folders to get them through tight door jams to trigger REX (Request to Exit) sensors.

RIFT RECON

Handcuff Shim

Small, concealable, covert: a good handcuff shim is made of strong spring steel, and primed for use many times over. Reliably strong, it's also thin enough to use on police-issue handcuffs that are made with tighter tolerances.



FOR YOUR EYES ONLY

IMPLEMENTATION

A handcuff shim is used to slip past the ratchets in handcuff bracelets, and is the fastest, most reliable way to open handcuffs when you don't have a key.

With handcuffs on, feel around with your fingers to find the side of the bracelet with a single metal bar (the part of the bracelet with teeth, which make the bracelets tighter). Use your thumb to guide the shim into the hole below where the teeth (the pawl arm) enter the hole. Push the shim into the hole on the side with the teeth as far as it will go.

Maintain pressure on the shim and over-tighten the handcuff to pull the shim down into the housing further.

It almost feels like you're using the shim to press the teeth deeper and tighten the cuff. (It can help to use a table or edge of a chair.)

Once the shim inserts fully into the housing, rotate your wrist out of the cuff.

After one wrist is free, repeat the process on the other wrist with both hands in front.

RIFT RECON

Multi-tool

Muti-tools are essential, and allow you to perform a multitude of actions with a minimal carry.

Full-size multi-tools are all typically about 100mm long when folded, and ones with a serrated knife will make the knives on other multi-tools seem like a nail file in comparison. A multi-tool with a longer and thinner Phillips head screwdriver than other multi-tools are suited for computers and server racks. And believe it or not, read the manual that comes with your multi-tool; few people do, and many miss out on less obvious features within the tool.

The pentester's multi-tool must meet a number of very specific requirements. Namely, a Red Teamer's multi-tool should be specifically tested and selected for high stress and high performance in-the-field actions.

FOR YOUR EYES ONLY

IMPLEMENTATION

Pocket-sized multi-tools are not ideal for most pentester's uses. A full-sized multi-tool is better because it is less likely to slip or offer imprecise application, which can damage screws and other surfaces. Because nothing should be left to chance, make sure the knife has both a serrated and smooth portion, and locks down for safety and usability.

The scissors can cut out custom shims from a plastic file folder - or even nearby soda cans. A suitable multi-tool should also feature screwdriver bits, full-size wire cutter pliers (jaws that provide leverage), a wire stripper, and needle nose pliers.

RIFT RECON

Waterproof Notebook, Pen, & Pencil

Despite electronic recon tools, a standard notepad is a required piece for a stealthy and efficient mission. A standard-issue item in Rift Recon's Red Team Kit, the Field Notes notepad is made of resilient, high quality Yupo Synthetic Paper - the same as the print edition of this dossier. This material is uniquely waterproof and extremely tear-resistant.

With a pen you can take notes on the notepad underneath a full-flowing stream of water. Go ahead - try it. Our selection of grid-layout paper makes sketching out floorplans, recon notes, and mission schematics a snap.

FOR YOUR EYES ONLY

IMPLEMENTATION

The key to your mission's success is thorough recon and documentation - and this kind of prep is key to effective risk management.

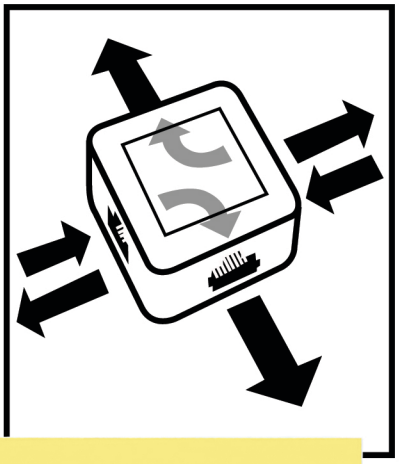
Every detail counts; entries and exits, layout, staff timing, everything - and unless you have a perfect memory, take notes.

Use the waterproof grid-layout notebook to document everything - even in the rain. Use your multitool when you need to sharpen your pencil on the go.

RIFT RECON

LAN Tap

Use the LAN Tap to sniff traffic over the wire. With this tap, there's no need for wire splicing and cutting, or messing with bulky powered switches. Plug an ethernet cable into one side and make the other connection to the device and use the other two ports to passively sniff all traffic. Our LAN Tap has the requisite capacitors to negotiate a gigabit connection down to a 100 megabit so that it can still be passively tapped without any external power. On the monitoring ports, the transmit lines are disabled so that it is impossible to transmit information out - perfect for staying hidden.



STEP 1:
Remove ethernet cable from host, and plug it into the A port.

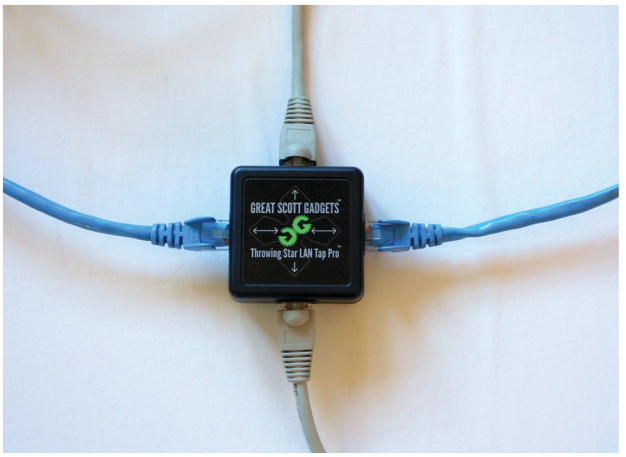
STEP 2:
Plug a second cable into the B port, then plug the other end into the host you removed the first cable from.

STEP 3:
Use monitoring ports to capture traffic.

IMPLEMENTATION

So small you can carry this in your pocket - and make sure you bring three ethernet cables. Plug your target's ethernet cable into port "A". Then plug one of your ethernet cables into port "B". Take the free cable end and plug it into the target port.

Now you're able to use the monitoring ports to capture the traffic that you need with a device running TCPdump, Wireshark, or a similar program. Note that each port captures traffic flowing in a single direction.



RIFT RECON

Clamshell Kit

The central player in the key cloning Clamshell Kit is the clamshell itself: the kit is portable and includes overflow channels. The low-temp melt alloy in the kit is non-toxic and melts below 200F; it's a eutectic alloy, which makes it much easier to pour and form a key. We prefer an adjustable butane lighter, which burns hotter than non-butane, and its kickstand lets you work hands-free. Also included: a sharp scraper and Plasticine.

IMPLEMENTATION

Step 1: Prep

Squish the Plasticine into each half of the clamshell mold.

Sandwich the key you want to clone between the two halves of the clamshell.

Only part of the key handle should be sticking out. Press the clamshell together, and then gently separate the halves and remove the key.

Step 2: Cloning

Use a thin tool (like a lockpick) to scribe thin, shallow lines from the key impression toward the front of the clamshell, exiting out one of the side channels. Dust talc lightly over the Plasticine to prevent sticking.

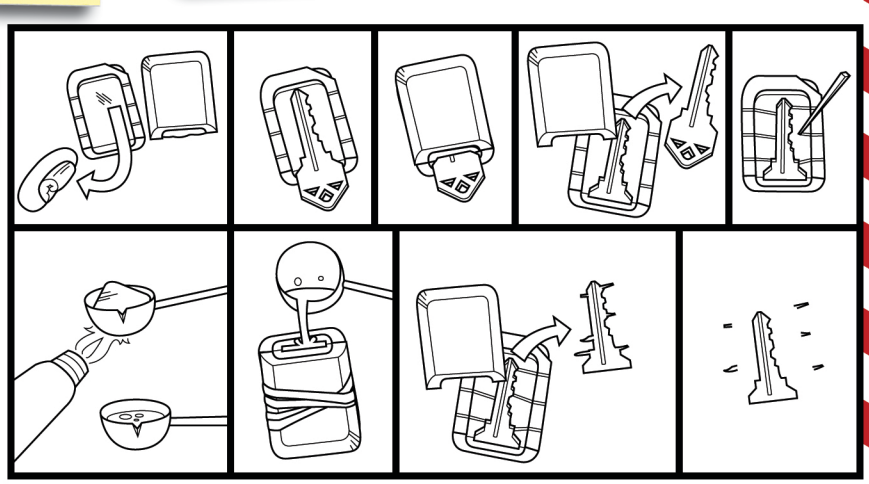
Compress the halves again and use the rubber bands to hold the clamshell shut. Next, put some of the low-melt metal into the ladle. Use the lighter to melt the metal until fully liquid. Pour the liquid metal into the closed clamshell. Try periodically tapping the shell on a hard surface to avoid air bubbles.

Step 3: Use

Wait 5-15 minutes for the metal to cool and solidify.

Separate the clamshell to remove the cloned key.

Check for imperfections, snap off protrusions and you have a key that's good for 5-10 uses.

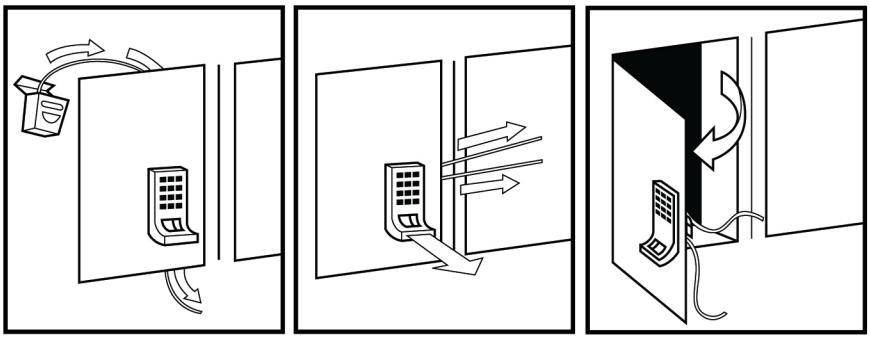


RIFT RECON

Dental Floss

Dental floss is ideal for a surprising multitude of uses. It's strong (especially when doubled-up or braided), and waxed floss will squeeze and slip through tight spaces in a way that few other materials can.

FOR YOUR EYES ONLY



STEP 1:
Thread floss in the top and through the bottom of the door.

STEP 2:
Pull through the side with the spring-loaded latch.

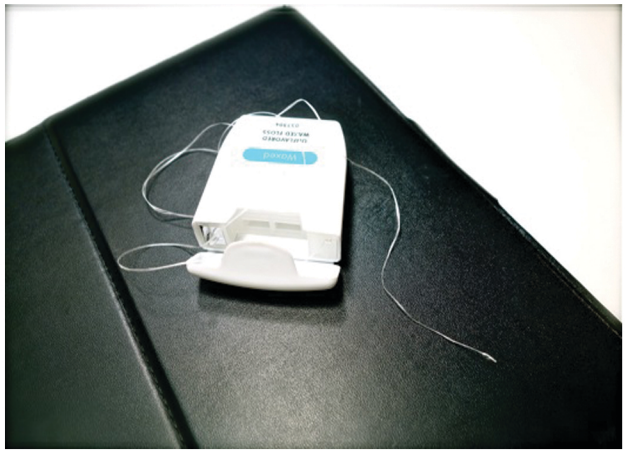
STEP 3:
The floss will retract the latch and the door will open.

IMPLEMENTATION

Floss can be used as a type of twine or string for light uses; tie floss to a magnet to create a pickup tool.

This technique is great for defeating locker cabinets with spring-loaded latches; insert floss into the locker's top to thread it through the bottom of the cabinet.

Then pull the floss from both ends over to the side where the latch is - while you pull, the floss retracts the latch to pop open the door.

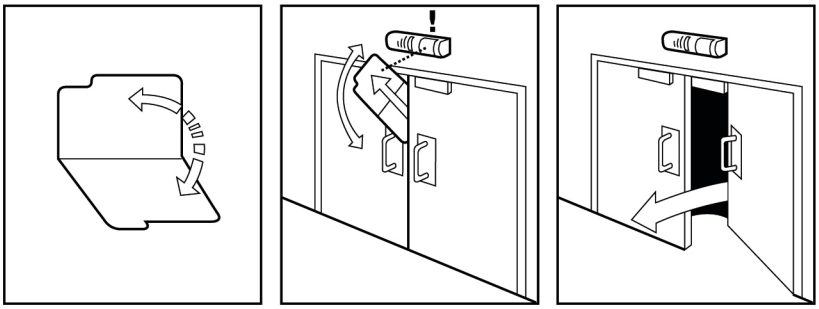


RIFT RECON

File folder

Although it's an ordinary, everyday item, the file folder is a bypass tool in disguise - which is why you'll find a file folder in every expert physical security penetration tester's toolkit. Yet while some use the old, familiar beige folders we're all familiar with, any old paper file folder simply isn't tough enough to go the distance.

About the same thickness as a standard manila file folder, a polypropylene file folder can handle all sorts of abuse - and will definitely take you where no paper folder has gone before. This attack works best on double-door entrances/exits with a motion detector placed right in the middle.



Step 1:
Open the folder so it's one long piece of plastic.

Step 2:
Slide most of the folder through the gap between the two doors while leaving a bit for your hand to hold the folder. If it feels too tight, use some spray lube.

Step 3:
Wave the folder near the motion detector. This should trip the sensor and unlock the door.

Implementation

The file folder's primary implementation is for insertion through openings near the top of a door to trigger motion sensors. (Motion sensors are commonly used to detect people trying to exit; their articulation is to send a signal to the system to unlock the doors.) For tight doors, prime the folder with your Red Team Kit's dry lubricant. Our tough folder can also be used in place of a shim, to maneuver pesky latches out of the way.

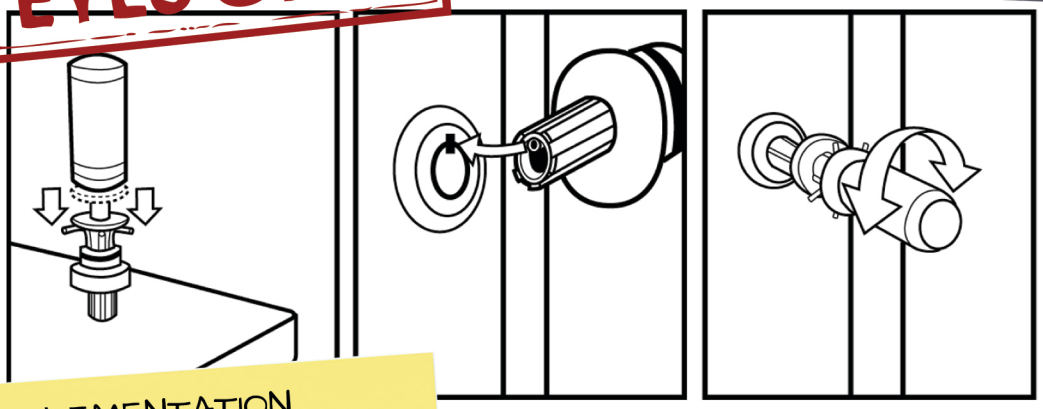
RIFT RECON

Tubular Lock Pick

Circular locks - the kind you'll see on file cabinets, lockers and bike locks - are called tubular locks, and this breed of security hardware has evolved its own specialized opening tool. A tubular lockpick makes most of these locks surprisingly easy to open; our choice is one that converts for use with both 7-pin and 8-pin tubular locks, and comes with extra parts so youre covered if parts break in the field.

Manipulate

FOR YOUR EYES ONLY



IMPLEMENTATION

Use a tubular lockpick as a key, or use its tubular key gauge to measure a lock's depths and get a key made at a later time. This isn't a tool to use without practice - you need to feel the appropriate amount of tension set by the threaded collar. Convert it to an 8-pin tubular lock: remove its threaded collar and compression ring, loosen the set screw (hold its shaft inside the handle); remove the feeler covering the rolled index pin. Use a nail to push the pin out; insert it the other way so the tool aligns with an 8-pin tubular lock. When you put it back together, only hand-tighten the set screw to avoid over-tightening.

STEP 1:
Remove cap and press the tool's tip down on a flat surface.

STEP 2:
Use the washer to press all of the feelers down flush against the tip. Index the rolled index pin with the notch in the tubular lock.

STEP 3:
Put the tool into the lock, rotate it back and forth lightly, repeat until the lock opens.

STEP 4:
When the lock opens, tighten the threaded collar down so you dont lose the bitting of the lock.

ABOUT RIFT RECON

RIFT RECON (riftrecon.com) tailors its clients from a suite of exclusive physical security services to meet specialized needs in hardware, assessment reports, tool creation and team outfitting, specialized trainings, and expert referrals. Rift operates across varied security industries, including product security, physical security, hardware research and development (including gadgets and kits), and caters to professionals striving to meet their own clients' various physical security needs.

Rift works with a range of clients from independent trainers to high net worth individuals, as well as red teams, indie physical security contractors, product security teams and companies requiring exacting hardware assessment reports. Discreet and methodical, Rift stands as the company in the world positioned to expertly source, secure, or innovate and manufacture hardware to meet the exacting, often critical, hardware security needs of its clients.

ABOUT RIFT RECON CEO ERIC MICHAUD

ERIC MICHAUD (@EricMichaud) is Founder and CEO of Rift Recon and Director of Hardware Curation at ExploitHub. He has advised on physical security, lockpicking, and hackerspaces for over a decade. Michaud is a professional physical security advisor; an R&D, test and analysis expert; and specializes in forecast and strategy. He started HacDC and Pumping Station: One, is the author of the How To Start A Hackerspace Series, and advises hackerspaces - bringing the movement to over 900 locations worldwide.

Michaud's skill opening impossible-to-pick locks earned him a place in locksport history with the "Michaud Attack." He co-founded and served on the Board of Directors for TOOOL US and is referenced widely in academic papers, talks and books including Open In Thirty Seconds.