OFFENSIVE STRIKE

Both teams, having successfully made it to the exterior wall of the building, radio the red team leader with a SITREP Alpha team states they have reached the loading dock door. Bravo team announces they have reached their position at an employee entrance to the rear of the building. The suspected vulnerabilities: a loading dock door that is believed to be poorly hung and an employee side entrance the cleaning crew usually leaves unlocked during their night shift.

The red team leader replies over the radio, "copy that." A member from alpha team takes a knee and reaches into his tactical bag for a Shove-it tool. Feeling the sweat under his clothes, another shot of nervousness blasts through his body. He can see the silvery reflection of the metal lock in the door frame and pushes the Shove-it in. Also kneeling and facing the opposite direction is the second member of the alpha team keeping watch. Meanwhile, bravo team hides behind bushes just outside the employee entrance door. They are listening for activity and, just then, a cleaning crew worker walks out for a smoke break. Bravo team hits the deck, and they wait. The smoker finishes and re-enters the building--by badging in. Badged entry? On this door? Is this a new security control?

At the other end of the building, alpha team works the loading door lock. Suddenly, the handle gives way and the door opens slowly. They were right about the door. Before them, pitch black darkness, a cavernous sound, a strong smell of diesel, and absolutely no idea what lies just in front of them. Welcome to Offensive Strike.

The Offensive Strike phase is always chock full of surprises. Next to the Evacuate, Evade, & Cover phase, it's one of the most exhilarating. This stage is where the hypothetical becomes reality, where suspected vulnerabilities are either found to be exploitable or not.

Since this chapter is predominately about exploitation, I will concentrate on the physical security controls that I encounter the most and possible ways to defeat them. Note, this is far from an all-inclusive list.

Ground Sensors

Unattended Ground Sensing System

Ground sensing systems, sometimes called Unattended Ground Sensors (UGS), use technology such as seismic, acoustic, and magnetic sensors to automatically detect the presence of people or vehicles. When sensors pick up activity, they usually transmit alarm data to a control hub via radio frequency (RF). Control hubs then transmit to a central control center, often a nearby security operations center (SOC), for incident response teams to manage. Other UGS systems exist with more advanced technology, however this type of system is what we commonly come across.

Ground sensing systems use hardware and cable sensors that are usually buried beneath the surface. Burying the system hardware helps prevent unwanted tampering or disarming and aids in concealment as well. UGS systems are usually placed in key areas of a facility's external perimeter and are often meant to stay there for long periods of time.

Here are a few characteristics of a UGS implementation:

- Difficult to visually detect; relevant in low traffic areas

- Usually intended to "cover" a lot of ground area
- Usually placed a few feet outside a security fence
- Often used as a replacement for guards, guard tours, 24/7 eyes-on cameras, and other motion sensors
- Detection rates can vary greatly according to buried cable depth, cable type, vendor, and implementation tuning
- Extremely prone to false-positives

Cabling Hardware for UGS

Identification

The most common type of systems we encounter are seismic systems that recognize vibrations in the ground. That said, it is very difficult to visually identify UGS systems. Unless red teamers manage to uncover open source intel or first-hand intel about the presence of UGS at a target, the only real way of knowing is by bait testing for it. You can bait test by walking near or on the suspected area with a plausible pretext. During one engagement, my team found a nearby Humane Society and volunteered to walk dogs. They walked a dog very close the suspected area. The dog-walker pretext offered a plausible alibi, if stopped, and enabled the team to have a much closer view of the facility. Later in that engagement, we ran another bait test by fast-walking over the suspected area and back to tree cover. I did this test repeatedly until we were satisfied. Be aware, this kind of bait test involves more risk and should only be performed if there is a pre-established pretext and cover/ concealment is available.

UGS systems are a great physical security control for several. reasons. They are difficult to detect and not easy to hack. You may never know one is in place until it's too late. But don't let that notion fester in the pit of your stomach. UGS systems are not the golden security control that people make them out to be. If they are poorly implemented, not continually tuned to the natural movement of the environment, or not maintained, they are less effective. And their detection success rates vary by vendor solution. UGS systems have one enormous flaw. They rely on people to make them effective. That's right. They only work if people respond the right way every time.

Ask any experienced cyber security person their feelings about working with their company's network intrusion detection system (NIDS), and I would be surprised if you're not met with sighs and eye rolls. UGS systems are no different in principal to NIDS. They require constant care and feeding, and they regularly spew annoying false alarms in the middle of the night. Oftentimes, there are so many false alarms that security people simply begin to ignore them.

BINGO!

Bypass & Defeat

Taking a shovel and pick to a buried UGS system is not the right approach. The most effective tactic toward defeating UGS systems is by way of its responders. My team does this by creating several alarms to fool the responders into thinking there is a glitch in the system, which they later begin to ignore.

It makes no difference if you pound the ground with a rubber mallet or a rubber horsehead. The key to the false alarm tactic is persistence and avoidance. Red team operators must be close enough to be detected and remain unseen when the first responders arrive. The false alarms should continue while the responders are onsite and well after. Personally, I've continued this tactic for nearly two hours straight. Persistence makes the tactic more convincing and increases the likelihood responders will ignore the alarms, providing red teamers an open window for exploitation.

Fencing

Anti-climb Fence

Anti-climb fences are among the most common type of fences, aside from the typical chain-link fence. With substantial space between the links for fingers and toes, chain-link fences are easily climbable. Anti-climb fences, however, have a narrow wire mesh that makes climbing with fingers and toes very difficult. Almost all anti-climb fences have this narrow mesh design, while some also utilize barbed wire or spikes on top.

Identification

Here are a few characteristics of anti-climb fencing:

- Rectangular narrow wire mesh
- Thick vertical iron bar design, often with angled spikes on top
- Angled and irregular patterned wire mesh design
- Chain-link with hard plastic material woven in
- Razor wire, barbed wire, or angled spikes on top
- 8 feet to 18 feet high

Essentially, fences are designed to slow down an attacker's advancement and potentially inflict fear of injury. Anti-climb fences look intimidating because they're supposed to look intimidating. To physical red teamers though, they are merely one of the nominal challenges they are likely to face during a mission.

With the right tactics and tools, just about any security fence can be exploited. Let's examine a few simple ways to bypass anti-climb fences.

Bypass & Defeat

Let's start with the obvious and definitely the most used by my team: Ladders. Operator #1 places a ladder against the fence and climbs up. Operator #2 hands Operator #1 a second I.adder which is placed on the opposite side of the fence. You can probably guess what happens next.

Defeat Security Fencing

But what about the scary barbed wire, razor wire, and spikes? Carpet remnants or thick wool blankets placed over the top will prevent injury. My team uses standard-issue U.S. Army wool blankets, but any pliable yet highly thick fabric will do. Factors to consider when using this tactic:

- Exercise with extreme caution
- Operators must be physically agile
- Have around 4 ft. x 4 ft. of durable fabric to prevent injury
- Wear ripstop clothing, durable boots, and Gloves
- Rehearse this tactic before using in the field

This bypass tactic can be dangerous and should only be carried out with the proper training and safety measures. Another less popular tactic is to utilize specialized climbing gear. Believe it or not, ninja hand and foot claws can make climbing an anti-climb fence possible. I say this with caution though. The hand claws are made of durable steel, as are the foot claws .. However; they can do quite a painful number on unprotected hands. For this to work properly, additional padding absolutely must be added so that your hands do not feel like they are about to separate from your arms. The ninja hand and foot claws are very sharp, and odds of injury are high. This should only be carried out as a last resort and by operators in excellent physical condition.

Climbing Gear

Motion Sensors

An electronic motion detector contains an optical, microwave, or acoustic sensor. However, a passive sensor recognizes a signature only from the moving object via emission or reflection. For example, it can be emitted by the object or by some ambient emitter, such as the sun or a radio station of sufficient strength. Changes in the optical, microwave, or acoustic field in the device's proximity are interpreted by the electronics and can trigger an alarm or series of actions.

Motion detectors have found wide use in domestic and commercial applications. A motion detector may be used to alert a homeowner or security service when it detects the motion of a possible intruder. Such a detector may also trigger a security camera to record the possible intrusion.

Microwave sensors detect motion through the principle of Doppler radar and are similar to a radar speed gun. A continuous wave of microwave radiation is emitted, and phase shifts in the reflected microwaves due to motion of an object toward (or away from} the receiver result in a heterodyne signal (two signals combined into one) at a low audio frequency. In an ultrasonic sensor, a transducer emits an ultrasonic wave (sound at a frequency higher than a human ear can hear) and receives reflections from nearby objects. Exactly as in Doppler radar, heterodyne detection of the received field indicates motion. The detected doppler shift is also at low audio frequencies (for walking speeds) since the ultrasonic wavelength of around a centimeter is similar to the wavelengths used in microwave motion detectors. One potential drawback of ultrasonic sensors is that the sensor can be sensitive to motion in areas where coverage is undesired, for instance, due to reflections of sound waves around corners. Such extended coverage may be desirable for lighting control, where the goal is detection of any occupancy in an area. But for opening an automatic door, for example, a sensor selective to traffic in the path toward the door is superior.

Passive infrared (PIR) sensors are the most common to us and what we will concentrate on here. PIR sensors are sensitive to a person's skin temperature through emitted black-body radiation at mid-infrared wavelengths, in contrast to background objects at room temperature. No energy is emitted from the sensor, thus the name passive infrared. This distinguishes it from the electric eye for instance, in which the crossing of a person or vehicle interrupts a visible or infrared beam.

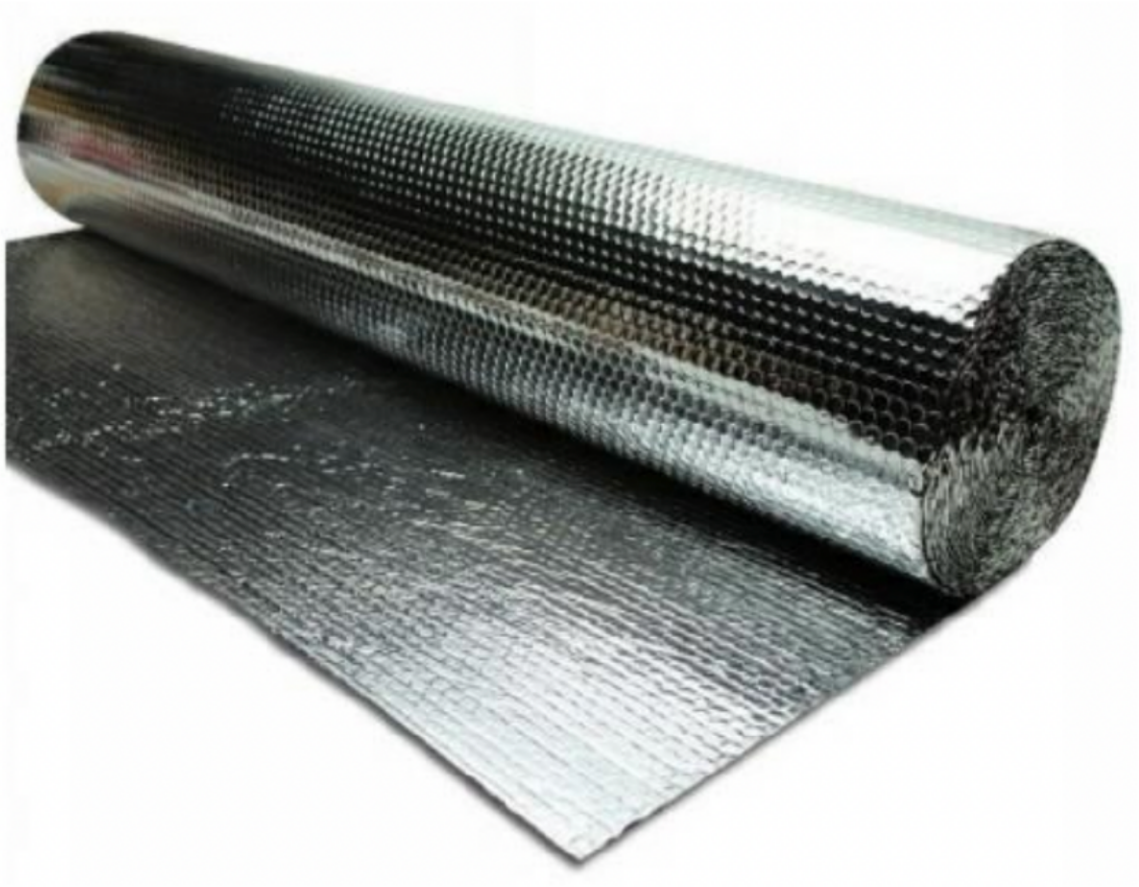
Identification

Motion Detector

Though motion detectors come in all shapes and sizes, they tend to share a common form factor. The "eye," or actual sensor, is identifiable by a spherical shape or behind a window, as shown in the example. Low-cost detectors have a range up to 15 feet while others offer much longer ranges.

Again, from my experience, most of the motion detectors I encounter look like the image above, use PIR sensing technology, and have a range of about 15 to 25 feet.

Bypass & Defeat



Thermal Radiant Film

My team uses a homemade infrared (IR) shield using thermal radiant film stretched over a wooden square frame large enough to hide behind.

Of utmost importance, of course, is to build handles on the hidden side so as not to leak body heat from hands and fingers while holding it up. The IR shield tactic has worked successfully on many occasions and is my team's go-to solution.

On a side note, I have seen a video on YouTube of someone successfully bypassing an IR motion detector by holding up a white sheet instead of

thermal radiant film. Even though it worked in the video demonstration, I recommend using a more robust solution with heat resistant film instead.

High Powered Laser Pointer

Strong laser pointers can be used to essentially blind PIR devices in order to prevent them from triggering. The tactic involves simply directing the laser beam at the center of the PIR device's eye. Carrying out this tactic requires a very steady hand, however. For long distances, a tripod should be used to steady the beam. This tactic is really only useful for blinding one PIR at a time. For these reasons, this tactic is not an option we go with very often.

As a final resort, some PIR motion detectors can be thwarted by simply moving very, very slowly through the detection area. Since most detectors are mounted high, crawling instead of walking can help increase exploitability. But again, an operator must move very slowly to be effective and the mission may not allow for that kind of time.

Alarms

Typical Alarm Control Center

Many of today's commercial alarm systems rely on the same type of underlying technology used to protect residences as well. Albeit, commercial systems typically include PIN pads, RFID readers, request-toexit (RTE) sensors, and much more. What is similar about these systems is the communication medium used to relay data from the sensors to the primary controller and from the controller to an authoritative alarm response center (ADT, law enforcement). Wireless technology, such as Wi-Fi, 4G, 3G, GSM, 433/315/868 MHz RF, has replaced many of the old hardwired systems.

Identification

An operator will see an alarm sensor or ten before ever seeing the alarm control panel and its brand/model. Most commercial control panels, not to be confused with keypads, are installed out of sight in a utility closet or server room.

Thus, alarm system identification isn't allways feasible. In reality, the brand of alarm system is not as important as the technology it uses to detect and communicate. What we are most interested in in this section is the technology it uses to communicate to other sensors/sirens and its alarm response center.

Bypass & Defeat

As I mentioned earlier, most current alarm systems use RF and/or Wi-Fi to communicate locally and a variation of GSM, Wi-Fi, or 4G to alert the authoritative alarm center externally. Vendors will. co-mingle and intermix aU sorts of technologies together in various models of alarm sollutions for their customers. So even if you know the brand of the alarm solution, you may not know the exact communication medium it uses. What is a red teamer to do?

Signal Blocker

Signal blockers are used by attackers to degrade and sometimes completely block alarm signals. The signal blocker pictured here has twelve antennas that can isolate and block GSM, 4G, LTE, Bluetooth, Wi-Fi, 433/315/868 MHz, COM, 3G, LOJACK, SG Wi-Fi, and GPS separately. Many alarm systems and their sensors operate in this very space. Thus, signal blockers are a real threat to alarm systems and prove to be one of the most effective ways in bypassing them.

Signal blockers are illegal in the United States, according to the FCC, and I do not advocate their use where prohibited.

Doors & Locks

Doors and locks make up the majority of the physical. security controls my team confronts. It would take a volume of books to cover the variation in locks, doors, levers, knobs, and their respective vulnerabilities. But in the ongoing spirit of this chapter, I will address the doors and locks my team meets every day.

Identification

When it comes to doors, we do not immediately resort to lock picking. Lock picking takes time, it is noisy, it can give away your position, and it looks nothing like in the movies. So just like it's done on the cyber side, we first look for vulnerabilities. What kind of door is it? Is it old or new? Where are the hinges? What kind of handle does it have? How is it hung? By visually scanning for vulnerabilities or lack thereof, we determine which exploitation route is optimal--to pick or not to pick. Generally speaking, we usually try to bypass it instead.

Levered Handle

The levered handle door is very common in businesses from offices to warehouses. Reason being, its physical configuration is governed by the Americans with Disabilities Act in the U.S. Specifically, the ADA has requirements for the amount of tension applied to activate the door lever, to its height from the floor to the amount of pressure needed to open the door.

Set of Crash Bar Doors

We have all seen these types of doors, particularly in hospitals, shopping malls and large enterprise complexes. They are sometimes referred to as panic bars, push bars, and exit bars. They too, have specifications governed by the ADA ensuring they can be used by all.

Crash bars are more commonly found in the lobbies of buildings to allow for a mass exodus of people in cases of emergency. They will be scattered through the internals of a building, where maintenance workers can open them while pushing big trash bins or crash carts. They are also very popular as designated emergency exit doors.

Commercial French Door

The commercial French door with crash bar activator is a very popular configuration in most businesses. The center gap between the doors is what's most interesting to us red teamers, but more on that later.

Standard Door Knob and Lock

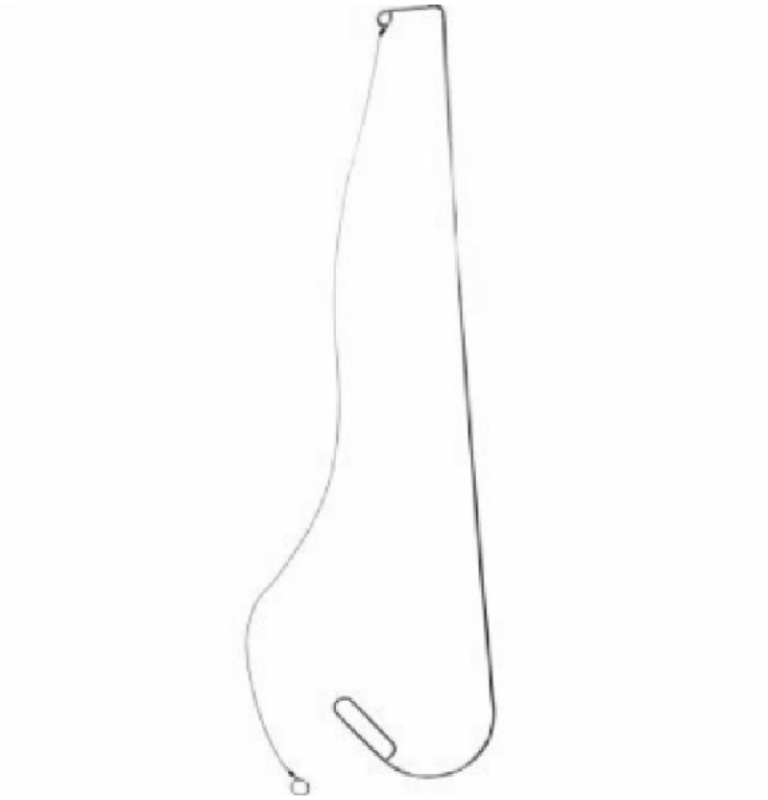
The other type of door handle is the standard knob. In a business setting, you may not run across many standard door knobs because they do not meet ADA compliance. Standard knobs are typically found on utility closets, network closets, storage rooms, special entrances, service doors, etc.

RFID Controlled Door

Many companies these days use Radio Frequency Identification (RFID) technology to control access into their facilities. RFID uses electromagnetic fields to automatically identify and track tags (RFID card as shown in Figure 63) attached to objects. The RFID card contains electronically stored information, much like a unique serial number. In an RFID access control system, this unique serial number is linked to an individual or group of individuals. From there, access into areas of a facility can be managed electronically for that individual for all doors that are RFID-enabled. As seen in above, HID is the dominant RFID access control solution provider in this space.

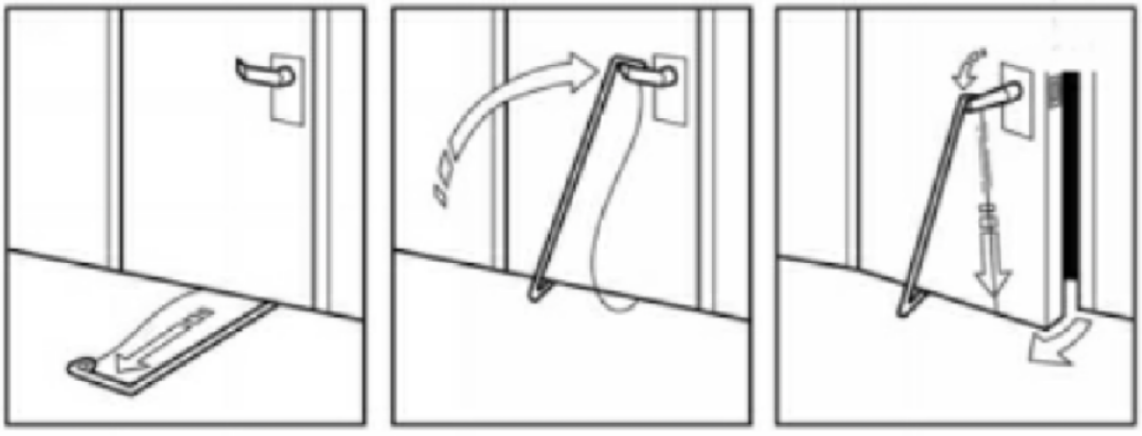
Bypass & Defeat

Lever Handles



Under The Door Tool

Doors with levers a re susceptible to bypass using a tool appropriately named the Under The Door Tool (UTDT). My team has used this on countless engagements with great success. This tool is a must-have!

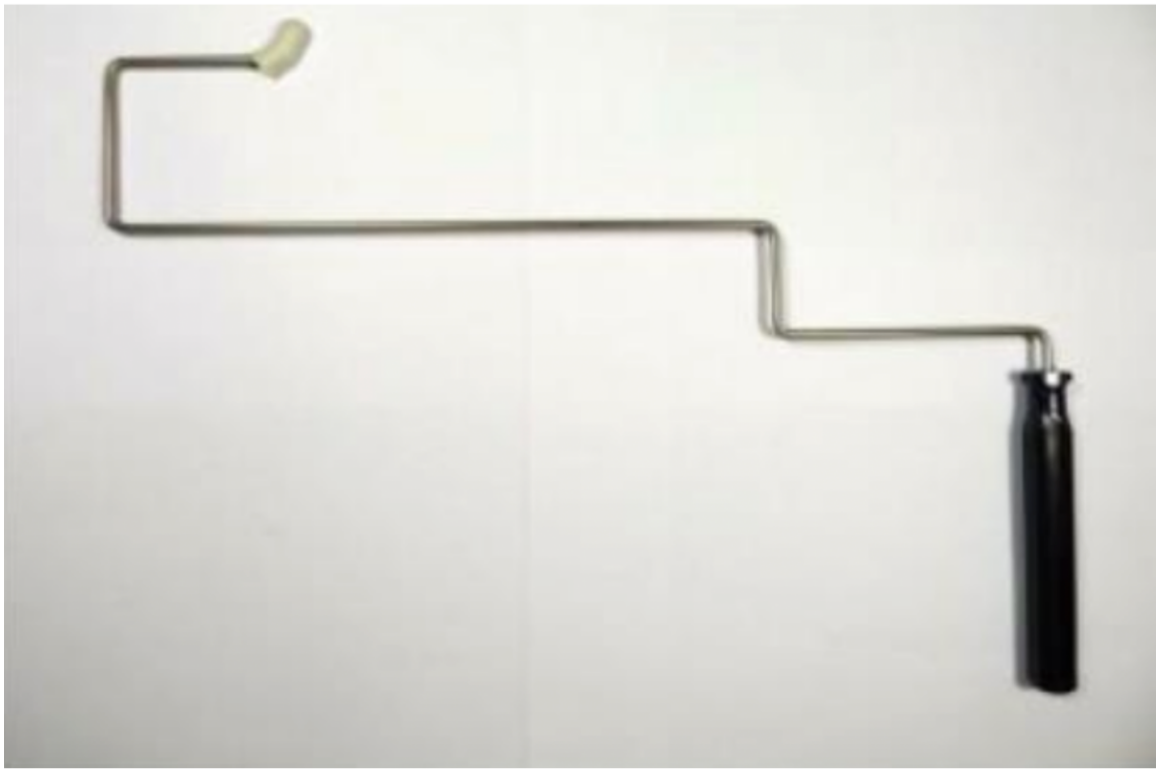


Under The Door Tool Instructions

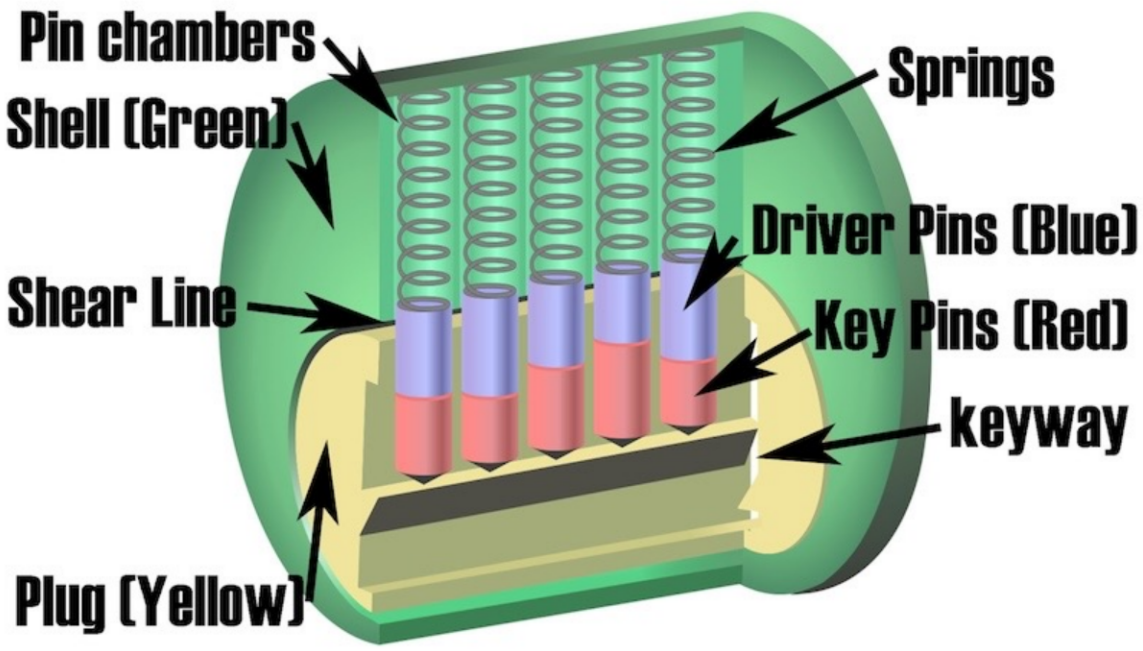
It is an odd-looking piece of equipment that not only takes a little getting used to, but it takes a minute to wrap your head around how it works. To help, I recommend a quick search on YouTube for a visual demonstration.

Crash Bar

Just like the standard lever handle, a tool exists aimed at exploiting the flaw inherent in crash bars. The double door bypass tool exploits the gap between French doors equipped with crash bars on the inside of the doors. See Figure 60. First, the bypass tool is inserted in the gap between the two doors. Most doors will have rubber weather stripping or brush material in between. Once most of the tool is through the gap, the operator turns the tool 90 degrees and lines the tool. up with the crash bar on the opposite side. Then, she pulls the tool inward, thereby depressing the crash bar and opening the door.



Double Door Crash Bar Tool



Pin & Tumblr Lock Anatomy

To better understand how this tool works, I recommend a quick search on YouTube for a visual demonstration. On a side note, crash bar tools can be made on the cheap with moderately gauged wire and a vice. Otherwise, visit your local Home Depot. Door Knob (Lock) Door knobs like the one pictured earlier in this chapter are pretty common in the workplace. While the knob itself can be vulnerable to lock picking, there are other vulnerabilities as well. Before we get to that, let's cover the lock picking aspect first.

There are entire books devoted toward mastering lock picking. This book will barely scratch the surface. Instead, I hope to introduce some fundamentals to spur further learning on the subject.

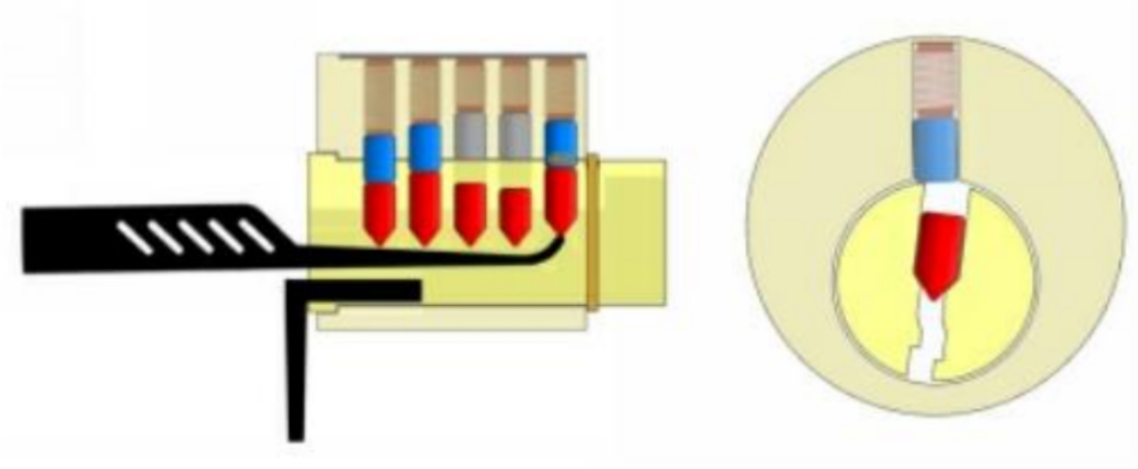
In a pin and tumbler lock, the most common lock my team faces, the springs maintain a downward tension on the driver and key pins. This ensures the driver pins are always blocking the shear line, which prevents the lock from opening. See Fig1ure6 7. When the right key is inserted into the keyhol.e, the key pushes the spring-loaded key pins higher up in the housing. The correct key's peaks and valleys (bitting cuts) match with the irregularly-sized key pins to lift the driver pins up and align perfect:ty to

form a straight horizontal shear line. Again, with the correct key, a straight horizontal shear line is created, allowing the key to open the lock.

Sample Lock Pick Set

Picking a lock, however, is made possible by exploiting manufacturing defects in the machining of the lock so that the pins can be agitated and torqued enough with a pick and tension tool to make the driver pins sit

askew inside the housing. Clearly, this is not the manufacturer's intent, and some manufacturers go through extreme lengths to prevent picking. Additional pins, security pins, and different shaped pins are a few examples of mitigating controls manufacturers use.



Pick and Tension Tool Causing Pin to Bind

The figure above shows how a lock pick is used to agitate a key pin, and the tension tool ls used to apply light clockwise torque, causing the driver pin to bind. I highly recommend searching YouTube channel for a more in-depth study from basics to advanced lock picking.

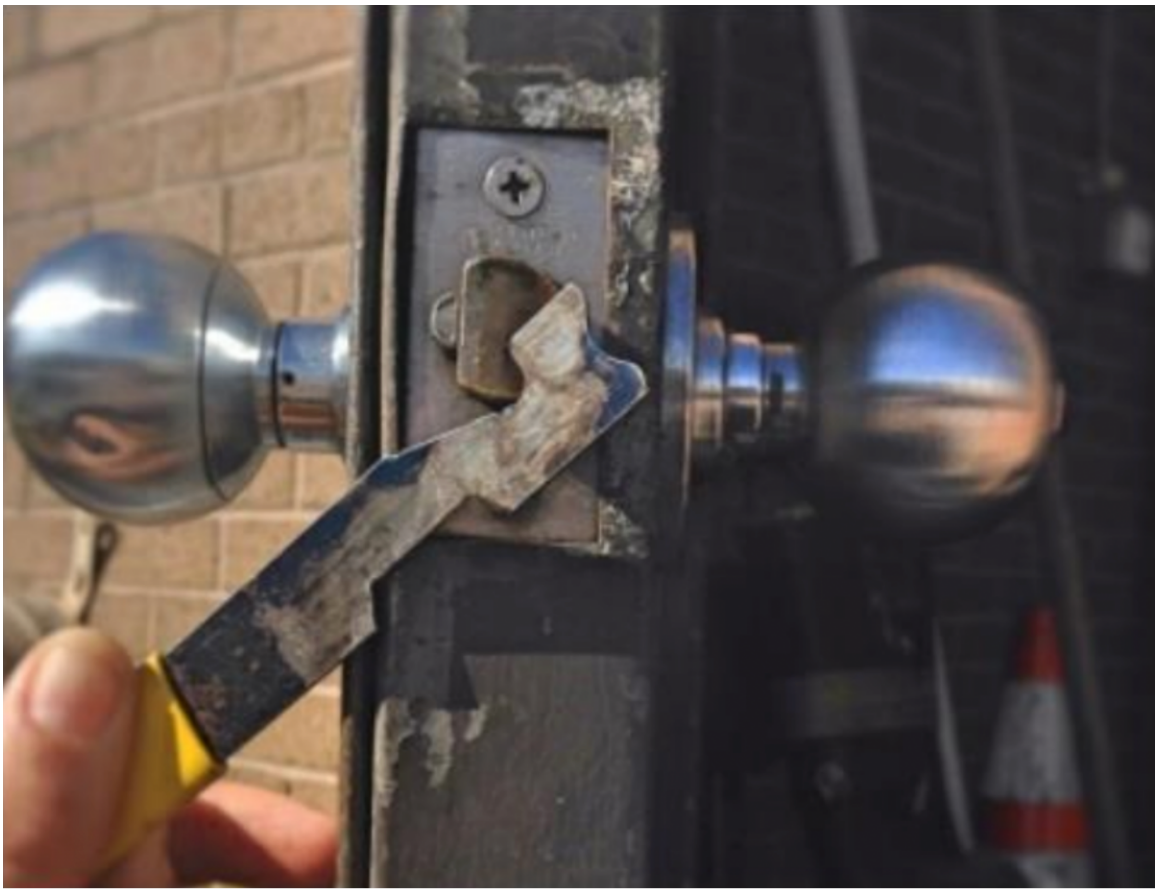
Lock picking resources:
TOOOL: http://toool.us/resources.html
Hacker Warehouse: https://hackerwarehouse.com
Sparrows Lock Picks: https://www.sparrowslockpicks.com

Shove-it Tool

Stepping away from lock picking, there are many doors that are vulnerable to shimming. Have you have ever seen someone crack open a locked door with a credit card in a movie? Technically, that's shimming. Doors that have small to large gaps between the door and the frame could be vulnerable. You stand a good chance of being able to shim a door if you can see the slight metallic reflection of the locking mechanism through the door and frame. See below.

Shim Exploitable Door

There are several tools designed specifically for shimming, ranging from plastic to metal to wires. In reality, they all do pretty much the same thing. My tool of choice is the Shove-it Tool. The Shove-it Tool is a simple lock bypass tool that works on many types of locks. The shape of the tip allows for pushing, pulling, or sliding latches. A red team operator would simply slide the device into the gap between the door and the frame to activate the latch and open the door (see below).



How a Shove-it Tool Bypasses a Latch

Before we assume that all doors are vulnerable, consider that some lock manufacturers have put controls in place to deter shimming. Notice the halfmoon shaped metal piece to the left of the latch. That is sometimes referred to as a tamper pin. When the door is installed properly, only the latch should go into the hole in the metal plate on the frame (keeper) and the tamper pin should be depressed. When the latch sits inside the keeper and the tamper pin is depressed, shimming becomes more difficult. Yet we see most latches with tamper pins installed to allow the tamper pin to go inside the keeper, making shimming much easier. Metal shields designed to cover a door latch (strike plate cover) to deter from shimming a door are popular with installers. A simple but effective approach is to use a longer Shove-it Tool.

Large Strike Plate Cover Over Large Door Gap

RFID

Tastic RFID Thief

As I mentioned earlier, organizations make heavy use of RFID readers on doors and issue RFID cards to employees to electronically manage access in and out of their facilities. These systems make access control very efficient and secure for businesses when implemented properly. However, many of today's organizations are unaware of the risks of using an insecure RFID implementation. Tools like the Tastic RFID Thief make stealing RFID access from employee badges trivial. My team has built several readers like this one using parts and schematics available widely on the Internet.

An RFID reader tool is a must-have in every red teamer's kit. The figure above shows a modified 12x12 inch HID RFID reader that has undergone massive repurposing for RFID stealing.

RFID reader in the field.

The photo above shows my team member using an RFID reader hidden inside a laptop bag. The red teamer scheduled a meeting, under false pretenses, with an employee known to have an RFID badge with elevated building access privileges. The red teamer got close enough to the target's badge to later make a duplicate copy which was used to gain access into the building later that night.

Stealing and cloning RFID employee badges is a real and rampant risk. Nearly all of my team's physical red team engagements have involved use of our RFID tools to some extent. Operation of the RFID reader is fairly straightforward if you are somewhat technically savvy. Where the real rubber hits the road is how creatively an operator can use and covertly disguise one to achieve their goal.

Acquiring an RFID reader like the one depicted here is not always easy. So I've provided a few resources bellow to help those new to the technology get started.

RFID reader and cloner resources:

- https://www.bishopfox.com/resources/tools/rfid-hackinq/attack-tools/
- https://www.youtube.com/watch?V=W22juSghJSA
- https://lab401.com/collections/hardware/products/rftd-pentester-pack