[CHAPTER 9]

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.

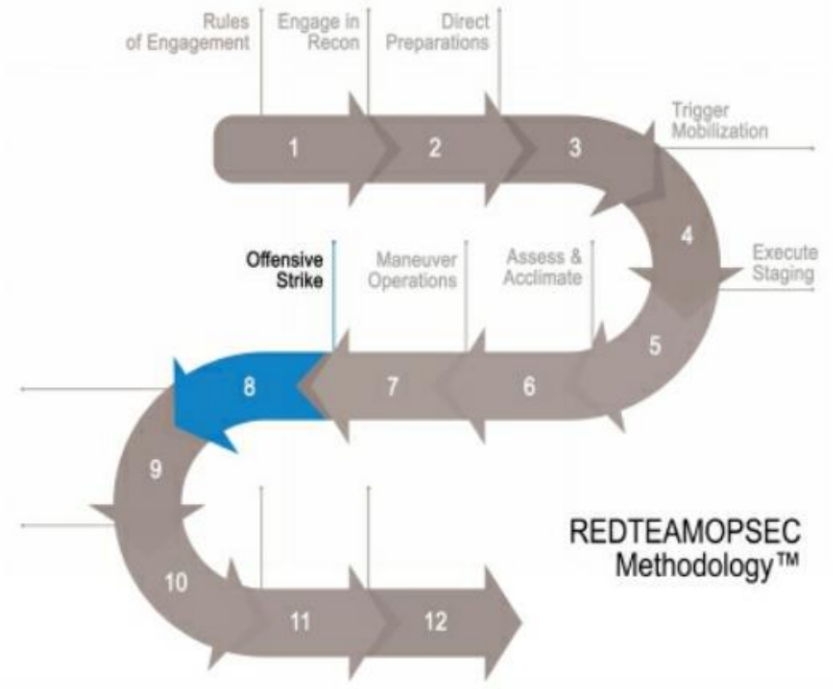

Figure 47. Offensive Strike Phase

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

Figure 48. 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

Figure 49. 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. I describe this false alarm tactic in the first chapter of this book taken from my interview with a reporter with The Houston Chronicle: https://www.houstonchronicle.com/business/article/Put-to-the-test-cybersecurity-experts-easily-10989830.php.

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

Figure 50. 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 ladder which is placed on the opposite side of the fence. You can probably guess what happens next.

Figure 51. 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.

Figure 52. 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

Figure 53. 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 Figure 53, use PIR sensing technology, and have a range of about 15 to

25 feet.

Bypass & Defeat

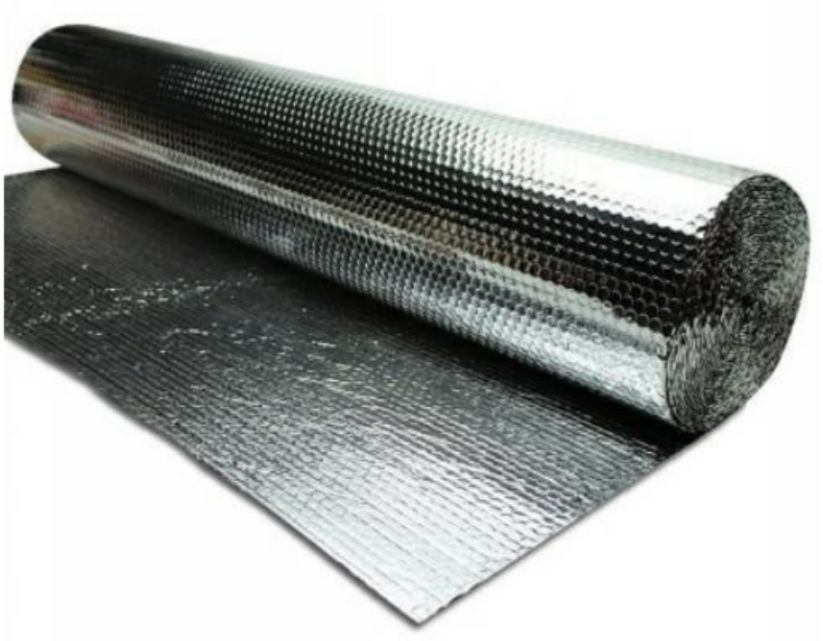

Figure 54. Thermal Radiant Film

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

Figure 55. My team with homemade IR shield (Credit: Paul Szoldra/Tech Insider)

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.

Figure 56. 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

Figure 57. 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-to-exit (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 (see Figure 53) 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 always 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 all sorts of technologies together in various models of alarm solutions 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?

Figure 58. 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, CDM, 3G, LOJACK, 5G 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.

Figure 59. 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.

Figure 60. 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.

Figure 61. 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.

Figure 62. 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.

Figure 63. 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 Figure 63, HID is the dominant RFID access control solution provider in this space.

Bypass & Defeat

Lever Handles

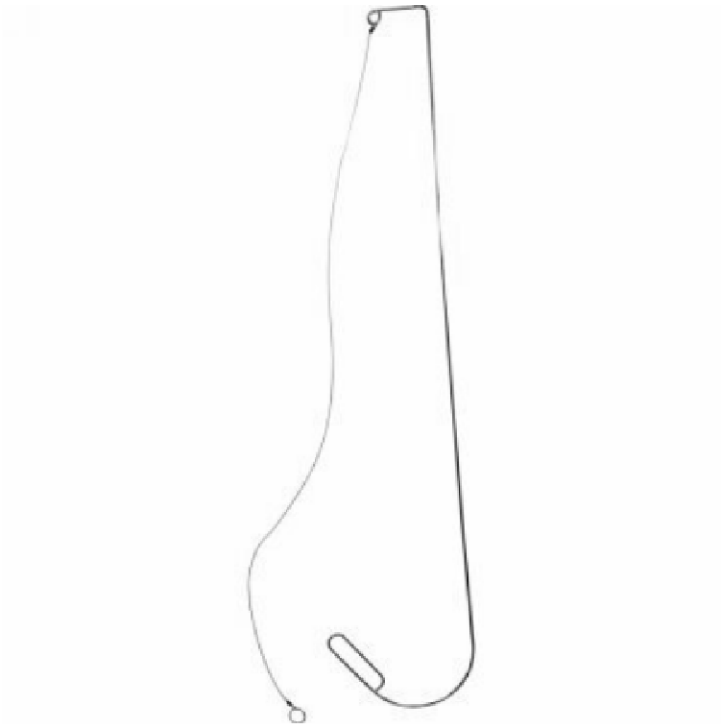

Figure 64. Under The Door Tool

Doors with levers are 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!

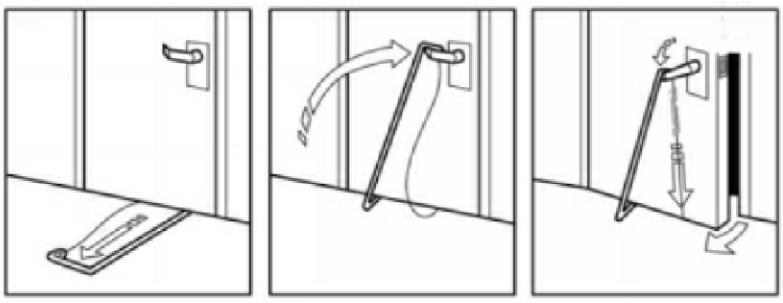

Figure 65. Under The Door Tool Instructions

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.

Figure 66. Double Door Crash Bar Tool (Photo credit: Rift Recon)

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.

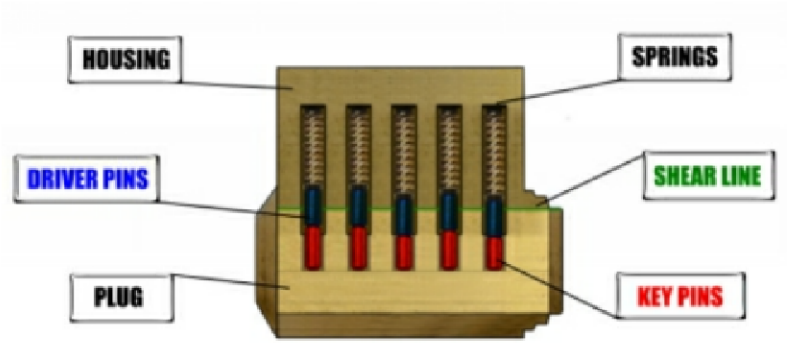

Figure 67. Pin & Tumbler Lock Anatomy (Credit: Art of Lock Picking.com)

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 Figure 67. When the right key is inserted into the keyhole, 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 perfectly to form a straight horizontal shear line. Again, with the correct key, a straight horizontal shear line is created, allow-

ing the key to open the lock.

Figure 68. 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.

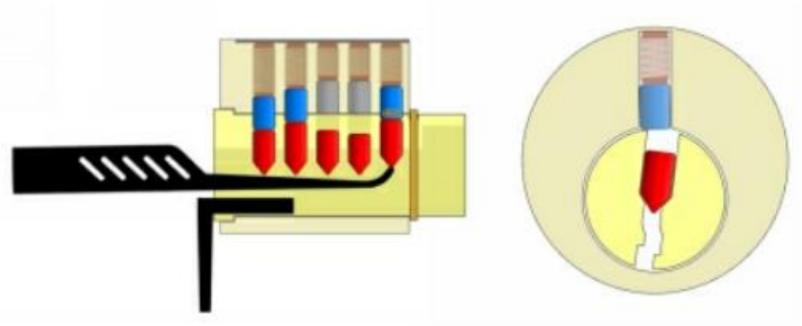

Figure 69. Pick and Tension Tool Causing Pin to Bind

Figure 69 shows how a lock pick is used to agitate a key pin, and the tension tool is used to apply light clockwise torque, causing the driver pin to bind. I highly recommend bookmarking a YouTube channel by 'BosnianBill' for a more in-depth study from basics to advanced lock picking.

Lock picking resources:

- BosnianBill: https://www.youtube.com/user/bosnianbill
- TOOOL: http://toool.us/resources.html
- Hacker Warehouse: https://hackerwarehouse.com
- Sparrows Lock Picks: https://www.sparrowslockpicks.com

Figure 70. 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 Figure 71.

Figure 71. 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 (see Figure 70).

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 Figure 72).

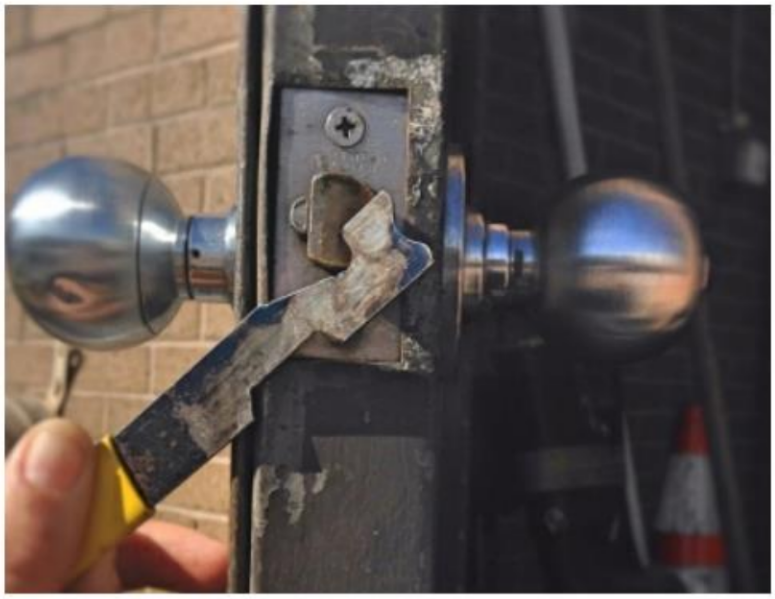

Figure 72. How a Shove-it Tool Bypasses a Latch

Before we assume that all doors are vulnerable, consider that some lock manufacturers have put controls in place to deter shimming. Notice the half-moon 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 pop-

ular with installers. A simple but effective approach is to use a longer Shove-it Tool.

Figure 73. Large Strike Plate Cover Over Large Door Gap

RFID

Figure 74. Tastic RFID Thief by Bishop Fox
(Photo credit: Bishop Fox)

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 in Figure 74 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. Figure 74 shows a modified 12x12 inch HID RFID reader that has undergone massive repurposing for RFID stealing.

Figure 75. My team with RFID in the field (Credit: Paul Szoldra/Tech Insider)

Figure 75 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 cre-

atively 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 below to help those new to the technology get started.

RFID reader and cloner resources:

- https://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/
- https://www.youtube.com/watch?v=W22juSqhJSA
- https://lab401.com/collections/hardware/products/rfid-pentester-pack

Please visit the links below to learn more about how my team used an RFID reader during a real physical red team operation.

https://www.businessinsider.com/red-team-security-hacking-power-company-2016-4

https://www.businessinsider.com/clone-rfid-security-badge-2016-5

[CHAPTER 10]

Penetrate & Control

The alpha team gets ready to make entry through the now shimmed loading dock door. Pulling an infrared borescope from his tactical bag, one operator adjusts the camera fixed to the stiff gooseneck to covertly peer inside and all around the door. Satisfied no immediate risks are present, both operators reach for their night vision monocles, crouch down, and prepare to cross the threshold.

Meanwhile, the door that bravo team planned to compromise has been recently outfitted with an RFID reader. Recognizing the door is ADA regulated, they devise a risky but alternative strategy. One operator, who had planned to change into street clothes after entering, changes now and stands on the sidewalk near the entrance. The other operator moves into a crouched position on the opposite side of the door. Several minutes pass that seem like a lifetime. Then, the loud and unexpected noise of the latch opening nearly scares the team, and a crew worker begins to exit. The street-clothed operator immediately hollers

to the crew worker asking to bum a cigarette as the other operator quietly ducks around the door and inside. The ADA regulated door speed held the door open with just enough time to sneak through.

With the help of night vision, the alpha team winds its way through a maze of pallets stacked eight feet high before seeing a set of double doors. It's dark, and nobody is supposed to be in here. They constantly scan for motion detectors and cameras as they make their way to the doors. It feels like walking through a minefield. Finally, they reach the doors. Posted on the wall is an aerial map of the building's emergency exits. They catch their bearings and advance. This is Penetrate & Control.

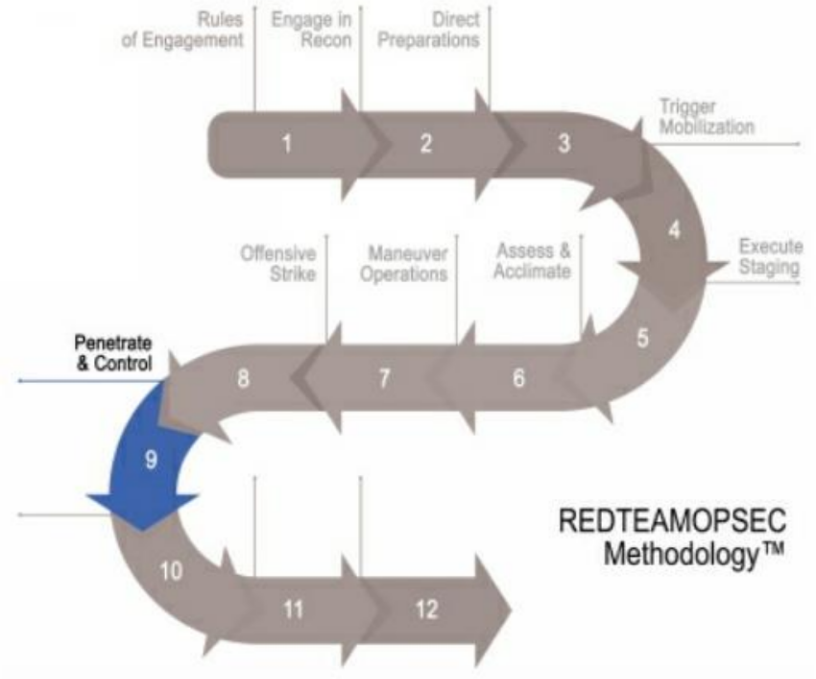

Figure 76. Penetrate & Control Phase

There's nothing like breaking into a building in

the middle of the night not knowing who or what is around the next corner. Even though these are lawful engagements, the feeling isn't any less nerve-wracking and adrenaline-charged. How do I go unnoticed? Are there people in here right now? Where am I and which way should I go? What is around that corner? What if someone sees me? As physical red teamers, we've all asked ourselves the same questions. Days upon days of planning has led up to this and any little mistake could be devastating to the operation.

This phase offers much needed guidance on how to penetrate and control access to a facility.

CHARACTER CHANGE

Changing clothes and character from a red team operator to an office cleaner or employee persona, for example, is not uncommon once building penetration has been reached. Once inside the building, switching from black tactical clothes to a business casual employee costume can be a great pretext to fall back on if spotted. In fact, some operations may require a character change.

Here are some situations that may warrant such a change:

- If the facility will be occupied during Penetrate & Control
- If the potential for occupancy is not known
- If the facility's internal layout is large and not known
- The operation will take place overtly or during the daytime

Precisely which character to change to is entirely dependent upon plausibility and which persona (office cleaner, employee) is likely to occupy the facility at the given time.

Figure 77. Cleaning Smock

A character change almost always involves changing clothes and developing a pretext. The complexity of both depends on the level of security awareness of its staff, who may stop and question the team. For offices, the most common persona is the commercial cleaning worker. It can be pulled off with relatively simple clothing and props. Jeans, a smock, and some latex gloves. Add a cleaning tray to store your pick set, flashlight and spray bottle or two.

Figure 78. Cleaning tray as a prop

I recommend using a clothing change and pretext as a backup plan to nearly every operation.

ESTABLISH YOUR POSITION

Operational orders (OPORD) almost always require red teamers to reach a destination, like a server room, and perform a number of tasks once inside a facility. But how do you get to that destination when you don't know where it is? This is often the case with me and my team. Sometimes we catch a break and find the building layout ahead of time through reconnaissance. Sometimes the building's external layout makes it evident. But generally speaking, we never know the facility's floorplan until we are physically in the midst of it.

Cardinal Direction

First and foremost, every red teamer must understand their four cardinal directions and how to find their position with a compass. The four cardinal directions, or cardinal points, are the directions north, east, south, and west, commonly denoted by their initials N, E, S, and W. Points between the cardinal directions form the points of the compass.

Most smartphones and smartwatches can do this pretty easily with the help of GPS. However, I always caution the use of these devices because they usually need to be activated and emit a bright light, which may give away your position in a dark area. Instead, I

recommend using a wrist compass with night glow. I highly recommend this for those of us who are abnormally directionally-challenged, like my wife. Bless her heart.

Figure 79. Glow in the dark wrist compass

A wrist compass keeps an operator's hands free, doesn't require activation, and doesn't emit any light in the process. Using a compass to orient oneself and obtain their bearings using a memorized aerial photo of the building is very effective. If necessary, a small aerial printout could be carried by the operator if the

building happens to be a sprawling complex.

Emergency Maps

Figure 80. Emergency evacuation map

Safety administrations, like OSHA in the U.S., mandate certain safety requirements for businesses. For example, OSHA requires organizations to develop an emergency action plan for the goal of protecting lives and property during an emergency; an evacuation policy that provides posted signs and placards concerning emergency exits, fire extinguishers, first aid kits, and so on. While floor maps are not specifically identified, many businesses choose to convey this information using a posted floor map. I have some good news and some bad news. First, the bad news. Not all businesses are required to convey emergency

information using building maps, and when they do, the amount of detail can vary greatly. Now for the good news. It's much easier to convey information visually using a building map, and we see that most businesses do.

Feel free to jump for joy when you spot one of these little gems! Generally, no matter how little information it may provide, it is usually better than nothing. Use what information you are able to glean from posted signs to support establishing your position and direct you where to go

MOVEMENT

Take another lesson from the previous chapter, Maneuver Operations. Movement through a facility, under covert conditions, should be done using the rushing technique, just as movement should be done outside a facility.

Rushing is carried out by slightly crouching at the waist, bending at the knee while keeping the head facing forward (see Figure 81). This makes an operator's profile smaller than walking upright, yet it enables quickly dashing from one position to another. I have found that rushing enables me to hide the sound of my footsteps a little better. But again, rushing should only be used during covert movement and in areas where there is little to no chance of the area being occupied. It would be hard to smooth talk your way out of being seen creeping around suspiciously like that.

Hazards

Figure 81. Avoiding hazards while rushing

There are all sorts of hazards that could potentially give away the position of a red teamer and make their task harder. If I had to list the most critical hazard when it comes to penetration and control, I would say windows. In the throes of an infiltration, it is difficult to be situationally aware of 360° around your body, and it's easy to walk right past a window that could give you away. Unless an office lobby is the objective, they should be avoided for these reasons. But there is more than just one hazard to be aware of.

Here is a list of the most common hazards:

- Windows

- Doors, corners, and stairs
- Cameras and motion detectors
- Lighting (internal lights or poor operator light discipline)

Let's briefly talk about lighting. Earlier in this book, I stated that red teamers should use flashlights only when necessary. Light usage must be directed only at the area of concern, should be colored red, and have low lumen output. However, internal lighting is a different animal altogether. An office, for example, is almost always partially illuminated. It is important not to mess with internal lights, but it is critically important to know where these illuminated areas exist.

Avoidance is the best tactic for lit areas. If traversing through it is inevitable, operators must crawl or rush while using surrounding objects for cover. It is strongly advised to refrain from turning off the lights. The sudden change in environment setting could alert someone.

Figure 82. Wi-Fi Borescope

When it comes to doors and corners, a borescope (also called an endoscope) can be used to peer under doors and around corners. In the spirit of light discipline, the model that we use connects to a smartphone via Wi-Fi. This means the light emitting from the phone could compromise our position. But this is one instance where I'm fine with the risk, given the reward. Though I have not used a blue light filter to cover the smartphone screen, I'll bet this, along with turning down the brightness, is enough to mitigate the risk.

It should also be noted that the image a borescope gives is far from high quality and it doesn't do well

seeing long distances. However, there's nothing like being able to see inside a room before trying to make entry, even if the image is grainy. A borescope is an ideal tool to check under doors and around corners for security controls (cameras, motion detectors) and avoiding people.

When confronted by an area secured with motion detectors, the first course of action should be avoidance. Find a less secure route. When avoidance is not an option, however, motion detection evasion inside a facility becomes trickier. There is less room to move around and sensors can be, and often are, tuned to levels of higher sensitivity.

Here are three go-to tactics for evading motion detectors:

- Conceal body heat (from PIR)
- Very slow movement
- Angle concealment

I've mentioned how to evade most of today's motion sensors earlier in this book by using a mylar blanket to deflect body heat. The tactic I provided involved fixing the mylar to a wooden frame and building in a handle to prevent hand/finger heat from contaminating the mylar. The idea is no different here, except the wooden frame part.

Evading PIR motion sensors during the Penetrate & Control phase has to be done with a more limited toolset. Carrying a big mylar blanket and frame isn't

going to cut it. Instead, an operator should carry a pair of gloves and fold-up mylar in their tactical bag. The gloves should be used to shield finger heat from contaminating the mylar while the operator holds it in front and away from her body.

Alternatively, a riskier approach is to evade detection simply by moving slowly. Most detectors use heat signatures to baseline a given area's environment. When a sudden change in the heat baseline occurs, the sensor triggers an alarm. Motion detectors are tuned with tolerances for gradual changes that do not abruptly interfere with the heat baseline. Therefore, evasion is possible given the operator moves very, very slowly. Taking 25 minutes to move 15 feet may not jive well with the mission timeline, however.

While this evasive technique is possible, it should probably be used as an option of last resort. I recommend practicing this tactic before considering using it.

A tactic for evading motion detectors and security cameras involves exploiting coverage areas, or lack thereof. Inexperienced security equipment installers mistakenly install security controls too high or create zones of exploitation due to gaps in coverage. As a result, it is possible to evade motion detectors and cameras by slipping through these coverage gaps.

The trick to discovering these coverage gaps is not easy though. Sensors and cameras installed at sharp angles create vertical zones of exploitation.

The same internal sensors and cameras are almost always installed too high far above head height, creating a horizontal zone of exploitation. Operators can successfully exploit these vulnerabilities by crawling, crouch-walking or hugging the wall tightly within the zone of exploitation.

It is difficult to know precisely where exploitation zones exist. For this reason, my team does not leverage this very often. Instead, we would combine this tactic with mylar shielding and slow movement to put better odds in our favor.

Clearing a Room

As the team advances through the facility, they will need to make entry into a room or rooms to reach their mission objective. Sometimes simply making entry into a room, like a server room, satisfies the objective while most of the time they will need to perform a set of tasks like retrieve a piece of equipment, find documents, and so on. Whatever their OPORD might be, the team must do so in an efficient and coordinated fashion.

In physical red teaming, the process of securing the room is called "clearing a room." Unlike law enforcement and the military's use of the phrase, we are not gunning for hostiles. Instead, we are first ensuring the room is suitable for entry. Then we are carrying out our OPORD. As I mentioned earlier, OPORD usually consists of a set of tasks the team needs to perform to successfully complete the mission.

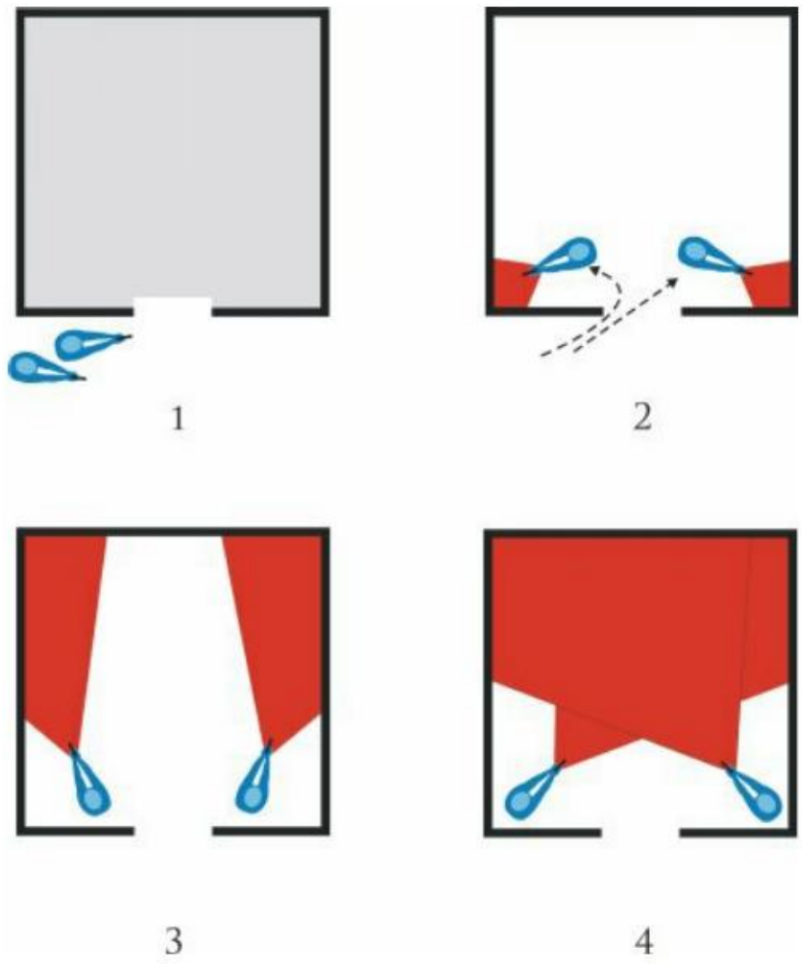

Figure 83. Clearing a Room (guns not necessary!)

A great way to split up clearing a room is depicted in Figure 83. Please excuse the show of guns in the diagram.

Step #1

The team should stack up in a line outside the door. An operator should first ensure entry will not compromise the mission. This usually means check-

ing for security controls and making sure the room isn't occupied. A borescope under the door or other tactic can help with this.

Step #2

An invisible line straight down the middle of the room should act as a dividing line. This is crucial to avoiding doubling up on efforts and wasting time scouring over an area that's already been looked through. Great care should be taken to avoid contaminating the room by pushing papers aside, moving chairs, etc.

Once inside, the team should turn to their immediate corners and begin to clear the room there.

Step #3

As the team continues to clear the room, per the OPORD, it is critical at this point to communicate with each other concerning their findings. It is likely that one (or more) of the operators will have carried out OPORD and this information should be communicated to each other and back to the red team leader.

Step #4

During covert operations, it is vitally important to not leave a trace. Operators must be aware of their body profile at all times to avoid contaminating the room with their presence. So it is important in this

step to collect tools and re-situate objects to their original location to reset the environment.

Penetrate & Control sets the pace for movement through a target via controlled entry and progression. Mission objectives are not reachable without considerable protocol, efficiency, and communication at this phase.

[CHAPTER 11]

Secure OPORD

Several minutes have passed after the crew worker finished his smoke break. The bravo team member who bummed a cigarette from him earlier rapped three times on the external door and the other bravo team member lets him in. The area is partially lit, but free of the cleaning crew. Operational orders in the RoE say they must reach the server room and retrieve an external hard drive left for them by the client stakeholders.

Hugging the darkened wall, the bravo team makes their way toward a pair of French doors they believe leads into the main office corridor. Upon reaching the doors, they rush the hallway stopping every few seconds, still not knowing where they are until one of the team notices a sign saying, IT Department. All enclosed offices and room are centered in the middle of the building. Bravo team rushes each enclosed office/room until one operator notices a room protected by a PIN pad. One operator inserts the borescope under the door. It looks like the right room, but it's dark. The

other operator removes the curled up under-the-door tool from his bag and moves it into position. Quietly the operator pops the door latch! They move in quietly, switching to NVGs. It's the server room. Sitting on a server in an open rack is the external hard drive. Kneeling on the raised computer room floor, server fans whirring loudly, cool air circulating and LED lights flashing everywhere, the bravo team radios the red team leader, "Red team leader, this is bravo team. Objective 2 reached!"

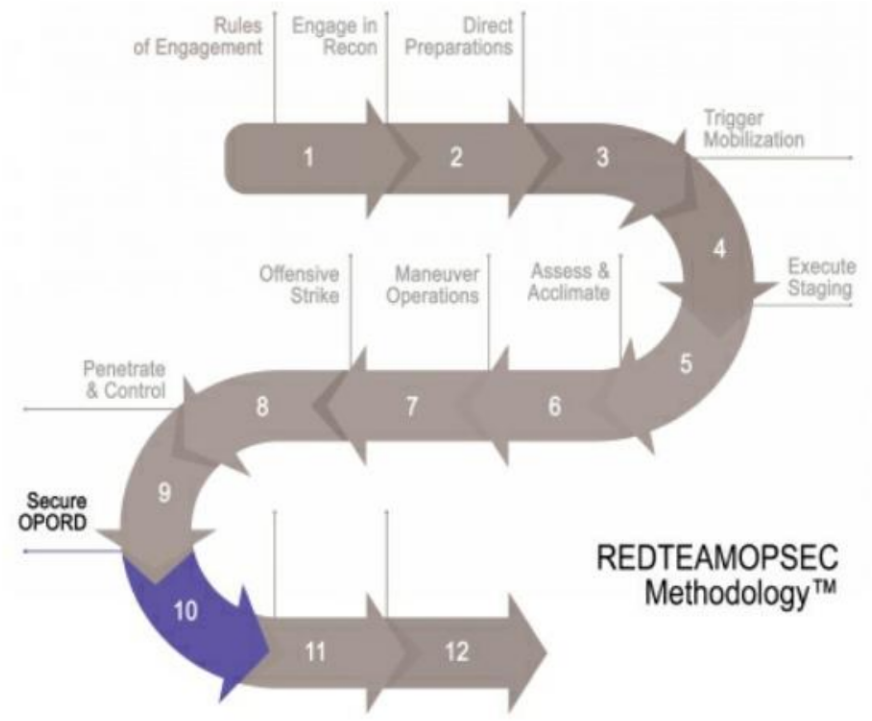

Figure 84. Secure OPORD Phase

Secure OPORD is a significant phase, if not the

most significant phase, of the REDTEAMOPSEC methodology, or any given physical red team operation for that matter. It is at this point where the red team carries out the intended actions on objective.

By this time, quite a bit of activity has occurred. Reconnaissance has been performed, the team has staged, moved into offensive position, exploited physical weaknesses, and gained access into the facility. Now comes the time where the all-important objectives are carried out. It's all led up to this.

COLLECT

There are so many opportunities to accidentally leave behind equipment at the target and misplace or forget evidence altogether during an operation. I should know. I've made these mistakes myself, and it nearly cost me the operation. I was gloating a little back at the hotel after completing what I thought was a successful mission inside a secure substation yard. Then a shockwave hit me when I realized I didn't have my Shove-it tool. I looked everywhere for it. After some thought, I was pretty certain I dropped it after climbing over one of four barbed-wire fences. In fact, I was even more certain it was probably inside the inner-most fence closest to the building we broke into, along a path heavily used by its employees. It was not a proud moment.

In this stage, I hope to provide guidance on how to properly collect evidence, equipment, and rally with fellow operators for a successful mission.

Evidence

Figure 104. An example of a bag to collect evidence

A fair percentage of physical red team operations I have been privy to have included the capture of physical evidence. This is unlike a flag, which is a designated object an operator sets out to acquire.

Figure 105. Red teamer capturing evidence during an infiltration

Evidence might be a sticky note with root credentials, a document with confidential information, or sometimes an untethered laptop. Evidence is a security risk an operator happens upon by chance that she finds during execution and is found to be relevant to the nature of the mission objective. For example, an untethered laptop would be taken as evidence if the company's concern is theft. Confidential documents would be taken if the company is concerned with unauthorized data disclosure. Of course, how this evidence is captured is entirely dependent upon the RoE. But it is fair to say that most often the evidence will be physically taken with the operator as opposed to only being photographed.

In short, red teamers in an operation that allows for the physical acquisition of evidence must plan for it by having adequate storage on their person to accommodate the evidence they find.

Equipment

My story about losing a piece of equipment is a real threat to red teamers, and it has dire consequences. Recall from the "Execute Staging" chapter where I advised red teamers to securely pack their gear to prevent it from falling out. This advice applies to every time an operator pulls a tool from their pack and replaces it.

An equipment check should be conducted at this point to prevent leaving something behind and raising alarms by anyone who sees it. In my previous example, I left behind a Shove-it tool. This piece of equipment looks a lot like a Slim Jim used in years past to break into cars. A giant wrench would have been thrown into our entire operation had anyone noticed it laying around near the entrance.

To reduce the chances of accidentally leaving equipment behind, I recommend making a cheat sheet of packed gear and where each piece of equipment is held.

PACKED GEAR							
BAG	Tactical Backpack	Large Comparment	Front Pouch	Left Pouch	Right Pouch	Bottom	Top Zipper
		Under-the-door-tool	Laptop	LED headlamp	PlugBot, Shove-it, pick set	Small torch,	USB drive

Figure 106. Packed gear cheat sheet

I almost always use the same tactical backpack and almost always put the same pieces of gear into the same compartments. But even as a seasoned red teamer, I know the anxiety that comes about in the midst of an operation, and that will cause mistakes. A small printed copy of the cheat sheet is useful in ensuring pieces of equipment are not accidentally left behind.

Operators

This brief but necessary step is more about communication than anything. It's imperative all operators know it is time to make for the rally point, to what location if it has changed, and if there are any hazards to consider. From the story earlier in this chapter, the red team leader gave the authorization for the alpha team to head to the rally point. Later in the story, the red team leader communicated concerns about a crowd gathering near the rally point. As a result, a slight deviation from the original plan was necessary in order to make a clean exit.

Essentially, this step is here to ensure the operators are able to collect at the rally point safely and make a clean exit. The onus for this step falls mostly on the red team leader. But it is important for the red teamers to communicate and coordinate similarly to support a fully executed operation.

EXFILTRATE

The term exfiltrate is defined as the process of withdrawing from a place or stealing sensitive information from a computer. As you might've already guessed, the REDTEAMOPSEC methodology applies directly to the physical withdraw from a place. But there is a fuzzy line between physical red teaming and the exfiltration of electronic data.

Unfortunately, many physical red team operations today do not cross into the cyber realm to also include ethical hacking tactics. Testing is often compartmentalized to physical security without regard for how physical security vulnerabilities also impact cyber vulnerabilities and personnel vulnerabilities. To combat this, my company RedTeam Security created an approach called Full-Force Red Teaming. This is a more complex issue to be covered in this chapter. For the sake of brevity, please refer to the final section of this book titled, "Full-Force Red Teaming."

Flags

I've used the term flag throughout this book. Let me take a moment to expand on it some. The term

flag is derived from a game called Capture the Flag (CTF). It is a traditional outdoor game where two teams each have a flag (or another marker), and the objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base.

As you can see, our use of the term flag is loosely based upon capturing an object from our client and the similarities tend to end there. A flag can be anything and usually ranges from a piece of old equipment to a physical document and everything in between.

Figure 107. Capturing a flag in a data center

Operators will certainly know which flags need to be captured and must plan for it accordingly. Keeping track of them during an operation is usually not difficult since there are generally only one to three flags per target. Operators can create a cheat sheet, similar to one used for packed equipment, to better manage flags captured if necessary.