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.

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.

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.

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.

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

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. 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

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 critic.ally 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.

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 comers 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 rs 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 time line, 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.

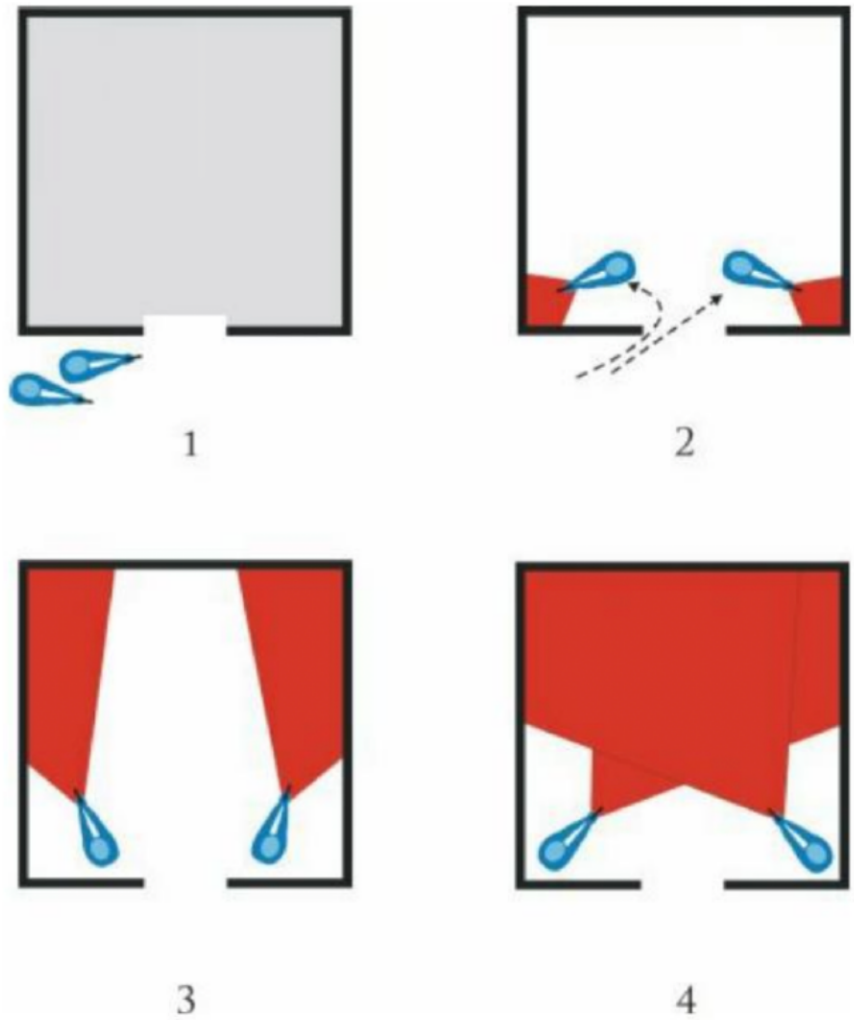
The trick to discovering these coverage gaps is not easy though. Sensors and cameras installed at sharp angles create vertical zones of exploitation. The same internal sensors and cameras are almost always installed too high far above head heigiht, creating a horizontal zone of exploitation. Operators 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.



Clearing a Room (guns not necessary)

A great way to split up clearing a room is depicted above. 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 checking 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.