EVACUATE, EVADE & COVER

A member of the alpha team radios, "Objective #1 reached" into the handset. Now that both teams have communicated that their objectives have been reached, the red team leader gives the order to exit the target. The alpha team, having completed their goal of making entry into an executive's office, quickly blazes a trail back to the warehouse and through the maze of pallets. Just as they exit the loading dock door, a pair of headlights briefly wash over the entrance, and the team runs behind a dumpster. With headlights now squarely positioned on the dumpster, the vehicle isn't moving. They wonder if they've been spotted.

With hard drive in tow, the bravo team resets the server room to its original state and heads back to the employee entrance. Thankfully, the hallways are still dimly lit, and they can see the lights in the same room they entered through. Rushing down the hallway, almost to the room, they hear voices. One bravo team member runs inside the room, meanwhile the street-clothed member circles back to hide in the empty break room. The voices are getting louder near the break room. Thinking quickly, the street-clothed member turns on the break room light. Voices getting even louder, he peeks around the corner to face two night crew cleaners. "Hey, do you have change for a five? This vending machine only takes $1 bills." The workers are startled at first, but believing he is an employee working late, they apologize for not having change and continue down the hall. Waiting a moment, the last member of the bravo team makes his way back down the dimly light hallway, catches up with the other team member, and they exit through the employee entrance.

Evacuate, Evade, & Cover is a small and often overlooked stage. Once a mission objective has been reached, one would think it would be time to just make a run for it On the contrary, there are many things to take into consideration. Where is the team going to exit? Where are they going to rally at? What or who should they avoid on the way out? How should they cover their tracks so no one suspects anything after they leave? Consider

that most physical red team engagements expect operators to exit the facility in order to consider the operation fully executed. Sometimes this means a full covert operation by which none of the operators are to be discovered. Other times, it may call for social engineering tactics, similar to what the bravo team used in our story. Either way, a full and dean exit is usually compulsory. This chapter aims to help explain that better.

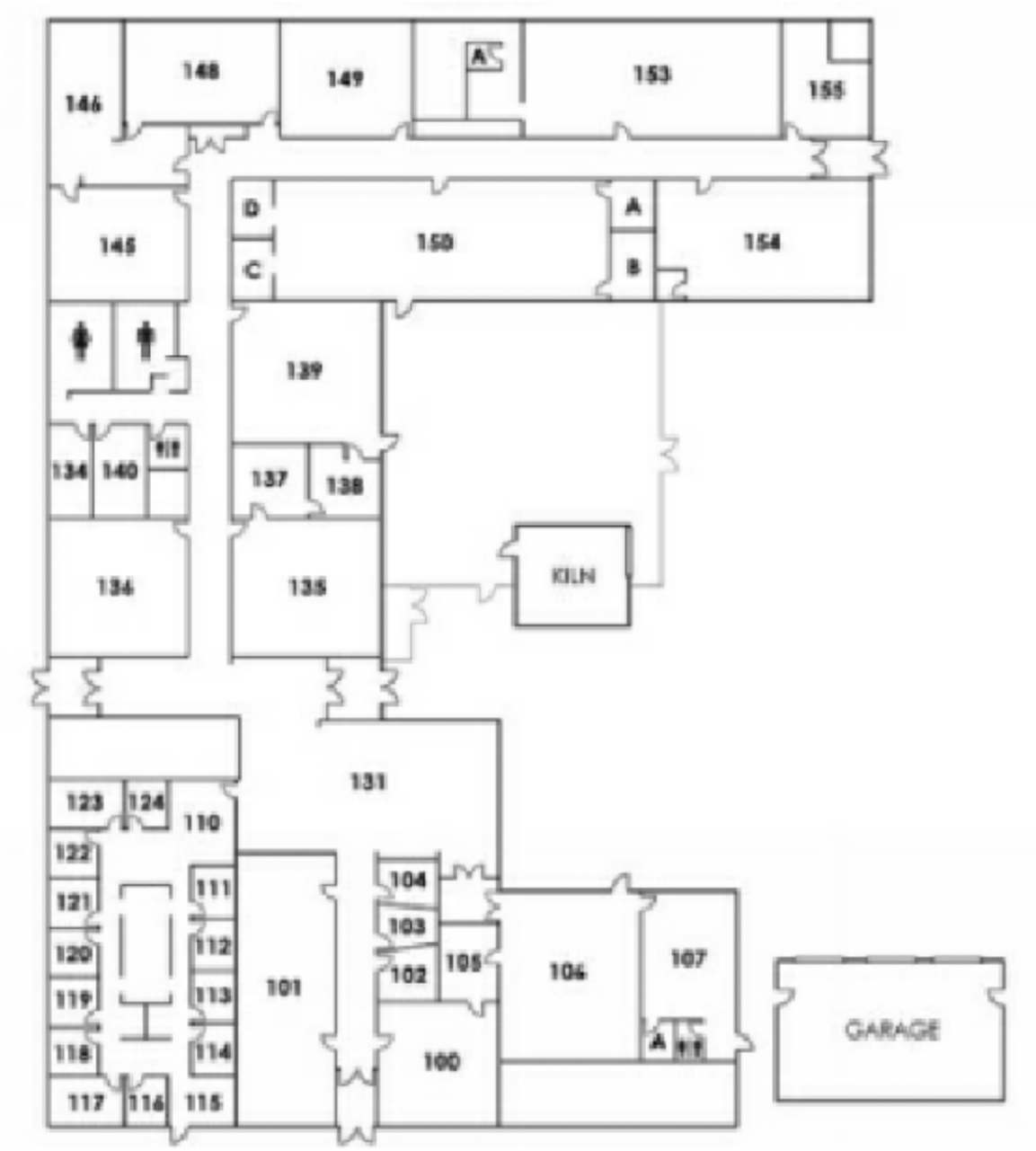
Evacuate

First off, let me explain why the term evacuate was used to describe this step when it could have simply been titled exit. Think of an evacuation as more of an orderly exit from a facility. I want to underscore the significance of an orderly exit.

Once the bravo team nabbed the external hard drive and reset the server room, they made like a wild banshee and rushed for the door. It's natural to want to flee precariously after having done something "bad." However, just as carefully as you infiltrate a facility, you must evacuate it just as carefully.

It's easy to expect hallways and rooms to remain unchanged, even if you just passed them seconds ago. Expect the environment to change. Constantly. Otherwise, the lapse in situational. awareness will surely lead to grave mistakes.

Building Layout



Building Map

Identifying building maps to help navigate in and around a facility are often discovered during the Penetrate & Control stage. Then, the goal was to find certain rooms to gain access into. At this stage, operators should use information in building maps with the intent of looking for alternate exits and additional areas to avoid. There is no hard requirement that a team has to exit the same way they entered. Though most operations involve exiting

through the same entrance, finding an alternate exit closer to the rally point may be ideal .. In any situation, building maps should be sought out at this stage in order to enable an orderly exit from the facility.

Rally Point

Rally Point

Critical to the next step of the evacuation stage is the rally point. The rally point is the designated location outside the facility where red teamers will meet once ordered by the red team leader. Recall from our earlier chapters that the red team leader gives the order to rally once all mission goals are met. The rally point is where the red team leader waits at a nearby location, usually in a vehicle, during the execution process. All red teamers must know exactly where to find the rally point. As stated earlier, it is their sole destination once their mission goals have been met.

Staging, Deployment, and Rally Points

A thorough study of the operation's staging, deployment, and rally points is necessary during the operation. Optionally, an additional rally point called an emergency rally point could be created. If the facility is hot with lots of personnel onsite or the operation involves several mission goals, an emergency rally point could provide a temporary safe haven during the engagement.

There are unfortunate situations where the red team leader orders the team to the rally point when things go sour. The reasons are varied, but usually, because an operator gave it their best, but for some reason couldn't complete their goal successfully. Difficulty exploiting vulnerabilities are the usual suspect. This does happen and should not be frowned upon. Unless there is language in the SOW that says otherwise, a team could make another attempt where it seems reasonable and realistic.

Evade

Evasion is defined as an act of escaping, avoiding, or a trick to get around something. We accomplished this during infiltration, but we were equally focused on trying to find unknown security controls. During evacuation, we are keenly focused on evading those security controls and people. To our benefit, we now have a better sense of the in-place security controls and how to avoid them and the movement of people, if any. As a result, this usually enables us to move quickly during the evacuation.

Movement during the evacuation involves at least two positions. The first is a crouched walking position enabling moderate movement inside a target. The second is the dash. Dashing is utilized once the red team is outside the facility and en route to the rally point.

Dash Movement

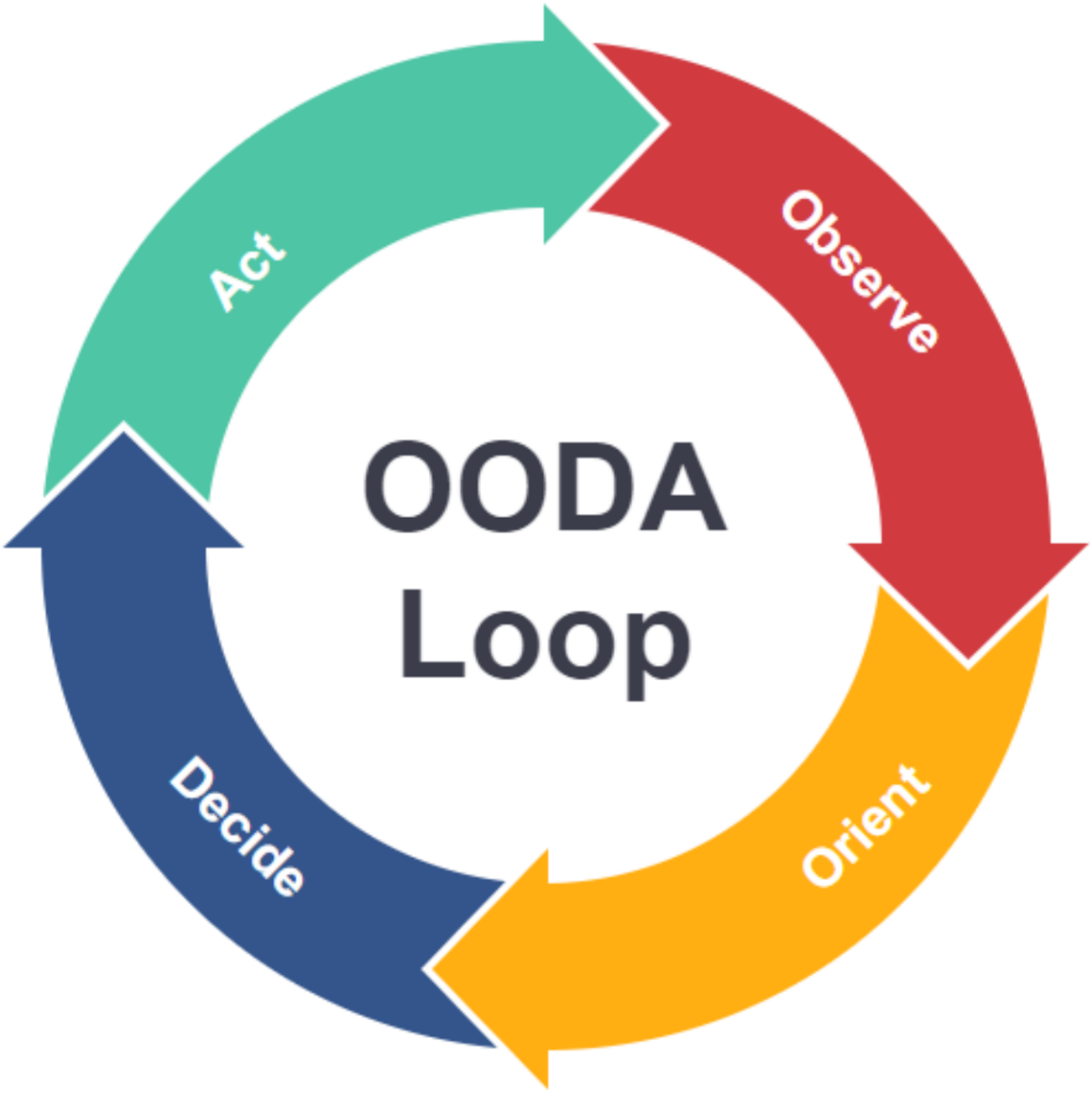
Example of the dash movement

Similar to the rush movement in the Maneuver Operations chapter, the dash is the fastest method to get from one point to another. Similar to rushing, dashing starts from a dropped position and moves to a crouched sprint. Sprinting is what makes this movement different from rushing.

Dashing about every five seconds is ideal since it makes it difficult for potential bystanders to fully track movement.

Just as with rushing, each dash must have a designated drop destination. In other words, an operator should not drop to the ground simply because five seconds have passed. A drop destination providing some level of cover or concealment should be sought out in conjunction. Optimally, the drop should include the time to cycle through an OODA loop.

OODA



OODA Loop

Recall from our earlier chapter, "Maneuver Operations," a description of an OODA loop. It stands for Observe-Orient-Decide-Act and is a decision-making framework used to train soldiers to make decisions when there's little to no time to assemble all the data. The OODA loop framework enables red teamers to filter available information, establish context, and quickly make the best decision using the information available at the time.

Red teamers must continually observe, orient, decide, and act as they encounter and evade new obstacles during the evac process. A facility's environment is always changing, and operators must know how to conduct OODA loops to support their operation.

There are all sorts of obstacles that could potentially give away the position of a red teamer and make it difficult to reach the rally point smoothly. This stage is all about evasion, and evasion is all about being covert. That means going unseen and unheard wherever you are. However, in the thick of an operation, it is difficult to be situationally aware within 360 degrees of your body, and it's easy to walk into a hairy situation. When evacuating and evading, here are a few key strategies to use:

- Chart an exit path to the rally point with the most shadows
- Be mindful how your profile casts shadows dynamically as you pass different perspectives of light
- Become situationally aware of the sound of your movement (i.e., footsteps, radio chatter; tools)
- Make heavy use of cover (i.e., hug shadowed walls and avoid lit areas) • Tune in to the sounds of the environment (Le., traffic, voices)
- Peek before moving through doors, around corners, and using stairs
- Radio your teammates and warn them of any obstacles

Leveraging these key evasion strategies will help enable a smooth evacuation. Remember, evasion is all about quick dash movements, OODA loops, and becoming hyper aware of your surroundings and your body profile.

Cover

Covering tracks is an effort to hide or destroy evidence of the physical red team's actions and presence. There are usually many physical targets to a single operation and failing to adequately cover physical evidence may put the target on high alert. You wind up contaminating the test environment since employees react much differently if they become highly suspicious. Unless this is the intent, red teamers must carefully cover their tracks.

Let's start by further defining what it means to cover your tracks. Yes, to a certain degree it does involve actually obscuring your footprints in applicable environments in dirty and rugged terrain.

Office

Red team operations that require operators to scrub offices and cubicles for sensitive documents are fairly common. These areas must be treated with the utmost care so as not to leave a trace. I'm always careful when I need to move keyboards, chairs, mice, phones, coffee mugs, monitors, and laptops. Anything the user touches throughout their daily routine that is even slightly out of place will certainly raise an alarm. These personal workspaces and objects are sacred ground to many office workers, and they can tell when something is wrong.

I always look under keyboards for passwords and other sensitive information. More often than not, I am rewarded with something useful. When peering under keyboards, I use two hands to lift up the side that is closest to me giving just barely enough room to look under. It's as if the keyboard is attached to the desk with a hinge on one side. You should never lift a keyboard or any object completely off the desk, unless absolutely necessary. Peer under it instead. This one tactic alone will go a long way in minimizing your physical presence.

If keyboards are the most common object I handle in an office, the second object would be the office chair. When office workers leave for the day, they usually swivel. around and get up from their chair to exit. This

position places the seat of the chair outward, ready for the worker to sit down. An office worker's chair that is out of place is one of the first things they notice. They will know someone has been there. When re-positioning a chair, take a mental picture to be certain it is put back in its original place.

During some of my previous covert military training, the instructor recommended taking a before and after photo as an insurance policy. There are smartphone apps on the market that make before and after comparisons even easier. Offices are chock full of disasters waiting to happen, such as accidently knocking over a pile of papers, etc. So there is reasonable cause to resort to taking before and after photos. Although I have never done this in the field, I do see the benefits. However, I cannot caution those considering this tactic enough to turn off the camera's flash and volume.

Lights

There is a general rule about lights in the world of physical red teaming. If the lights are on, leave them on. If the lights are off, leave them off. That said, my team has violated this rule in the field under very specific circumstances. However, let it be known that altering the environment in such a drastic and visible way, such as turning on the lights, is a very risky move; a decision to be made after carefully weighing the circumstances. But because so many of the red teams I train fail in this department, I felt it should be covered here. Stick to the general rule and leave the lights where they are.

Locks

If your physical red team operation involves lock picking, you could be leaving behind one very significant clue. So you picked a lock open to the networking closet, achieved your mission goal, shut the door behind you and evacuated. If you didn't pick the lock closed, you could be in big trouble.

By exploiting the manufacturing defects in the lock itself, you've managed to pick it open with your pick set, not a key. The lock will remain

in its open state until you pick it closed, aka locked. Remember, you don't have the key, so you'll need to use your pick set to re-lock it. If the lock is protecting something critical, like access to a restricted area, this may result in the filing of a formal incident report and could put the target on high alert.

Terrain

During red team operations, our goal is to become covert, and hiding footprints in various forms of terrain and weather is very challenging. One of the best ways to cover physical tracks, like shoeprints, is to use overshoes. In fact, one of the most effective ways to obscure boot prints is to use overshoes made of carpet. The thick fabric obfuscates the tread and, in some cases, hides the foot impression altogether. You won't find these at the store, you'll have to fashion these by hand from carpet remnants. I highly recommend these for use in dry to moderately wet ground.

Overshoes big enough to fit over boots

A different set of overshoes is needed to cover up prints inside a facility.

High top overshoes, like those pictured here, are ideal to avoid leaving a trail of moisture or mud from the rough terrain to sidewalks, entrances, and hallways of a facility. Some facilities have surrounding terrain that would make a very noticeable mess, not to mention leaving a telling trail of evidence. Rubber overshoes work the best in keeping what's underneath dry.

A pair that can be swapped out quickly and stored inside a tactical bag is even better.

Moist and muddy ground is the antithesis of what you should be traversing. Avoidance is the best tactic, but this is not always possible. You want to seek out terrain of hard-packed soil or rocks and pebbles. This terrain is the best to use so as not to leave any visible tracks.

Snowy ground is another animal altogether. I find this the most difficult environment to traverse covertly. I suppose operators could use snowshoes for more sophisticated operations, but that isn't realistic for most operations. Covering the tracks for a team of operators is nearly impossible. The best tactic in this situation is to obscure the size of the team to look like one individual, instead of multiple. This is done by having the entire team walk in single file while stepping into each other's snow prints. The idea is that anyone noticing the prints won't be as concerned since it merely looks like one person was walking about instead of a multitude of people.