ASSESS & ACCLIMATE

Under the cover of night, the red team leader gives the go-forward signal, and the red team exits the vehicle. As the red team leader drives away from the staging point, a powerful feeling of excitement, nervousness, and a little bit of fear swirls in the bellies of the team. Shaking off some of the butterflies, operators instantly recall. their training, hours of mission planning, and a dash of bravado begins to take hold.

Reams of video and images of reconnaissance intel captured earlier in the engagement fill the team's minds as they situate themselves with the once familiar surrounding air, smells, terrain, buildings, lighting, weather, and security controls. The familiar fit of the ripstop clothing pressing against the skin and the added weight of their gear reminds them of the need to breathe easy and maintain a low profile.

The radio starts to buzz and crackle as the other team members instinctively fall into vee formation, take a knee, and pause. Then the radio begins to crackle into life. Is that a new security camera? Is there a light on inside? Is it busier than normal? Are the guards on a tour? How is this place now different from the Engage in Recon phase and what are we going to do about it? You are now entering into the Assess & Acclimate phase.

The team is preparing to embark on the mission by foot, but before maneuvering operations for an offensive strike agiainst the facility, they must first identify salient changes at the target. In other words, what important differences are there now and do these differences negatively affect the team's ability to reach mission success?

An example of a salient change might be the presence of additional security cameras, fencing, or motion sensors. Because some amount of time can pass between the reconnaissance phase (Engage in Recon) and this phase,. the environment is subject to change without notice. In some cases, the differences could be pretty drastic. Thus, it becomes extremely

important to assess the environment for changes before blindly advancing to the next stage.

Assess

Unless you have somehow uncovered additional intel about recent security improvements inside the targeted facility, you can only assess what you can see in front of you. So the facility's outside may look the same, but security improvements, like biometric scanners, placed internally can throw a wrench into any plan. Lucky for you though, most physical security improvements are placed outside and are typically visible.

You see, unlike the principle of defense in depth common to the information security industry, most physical. security departments have yet to adopt that strategy. So instead we see a lot of physical security controls implemented in only one or two layers, almost always outside the building (fencing, cameras). That said, do not rest on your laurels. Plan for change.

It's worth noting, a great deal of assessing happens initially when boots hit the ground, there's no doubt about that. But as the team advances, the process of assessing and acclimating will be ever present. It's very difficult to plan for the unexpected. After all, that's why it's called the unexpected! There will be disappointing surprises. The best you can do is try to be as prepared and rehearsed as possible.

Now as you might've already guessed, the assessment process is one that needs to happen quickly. To make things even trickier, not all changes to the target environment will affect each team member in reaching their goals. The team must assess environmental changes as a team and communicate them. Then it becomes the responsibility of each team member to know how the change may affect their capability to reach their mission goals and adapt.

Here's a quick breakdown of how this should occur:

- The team performs an eyes-on assessment for any changes in the environment
- Operators communicate any changes over the radio
- Individual operators evaluate how these changes affect their capability for reaching their own mission goals
- Individual operators announce over the radio how these changes affect their capabilities

Consider the sample mission goals below. This is an example of one team member's mission goal to gain unauthorized access through the target's loading dock.

Mission Goals							Recon Results		
	Goal	**Plan**	**Mission Success**	**Estimated Vulnerability**	**Threat**	**Bad Actor**	**Observations**	**Vulnerability**	**Go-Forward?**
1	Gain unauthorized access through a loading dock to capture evidence and leave a business card.	Deploy from area #1, approach from rear van, move west along alley wall. Wear black tactical gear and use under the door tool and air wedge to gain access. Capture video evidence and leave business card.	Gaining access via door exploit, capture evidence, leave business card and exfiltrate without detection.	Inadequate perimeter security.	Moderate to significant service disruption.	Local to regional bad actor. Moderately sophisticated.	Loading dock traffic is moderate by day, non-existent by night. No cameras visible, have motion lights. No RFID badge entry, only door locks. External doors have ADA levers and weather stripping below.	No motion alarms. No security cams. Motion lights can be bypassed on east side. ADA lever handles could be bypassed with under-the-door tool and air wedge. Infiltration to happen at night.	Yes.
2									

Sample Mission Goals

Now, it is not likely that each operator will have a printout of their mission goals with them to reference. So clearly, each and every operator must be able to recall every aspect of their goals from memory. Operators can perform an assessment by recalling the data from the Recon Results columns along with the Goal, Plan, and Mission Success columns (Figure 32). Any recent security changes, upgrades or downgrades, that deviate from gathered recon intelligence have the potential to change the magnitude of the vulnerability or possibly even make the vulnerability disappear.

With guidance from the red team leader and the rest of the team, the team's course of action includes:

- Abort
- Advance as planned
- Acclimate and advance

Acclimate

When something changes at the target environment and it is believed to have an impact on the success of the mission, the team must react accordingly. It isn't all that often that a facility's security posture changes dramatically over a short amount of time. But minor changes can add up, and the team needs to acclimate as a result.

Let's assume the team identified a change in the environment and communicated the issue over the radio. Refer to Figure 32. Let's also assume we confirmed the presence of motion sensing lights at the loading dock where there were not any observed earlier. First of all, kudos to our target for taking steps to increase their perimeter security. After additional examination and collaboration, the team believes they can avoid tripping the sensor by moving slowly far and away from the sensor's focal point. The team also believes that a tripped sensor will not likely attract attention due to the somewhat concealed location of the loading dock.

This is a simple example of how the team can acclimate to changes in the environment. Here are a few things to consider when weighing different strategies:

- Does this strategy put the mission overall in unnecessary jeopardy?
- Does this strategy comply with the rules of engagement?
- Does this hinder or prevent other red teamers from completing their goals?
- Will this hinder or prevent me from completing any other mission goals?
- Do I have red team leader approval to proceed?

Assessing and acclimating to a changing environment is more of an art than a science. With practice, this will become easier.