TRIGGER MOBILIZATION

Many in the physical red teaming industry often overlook the importance of proper team mobilization to the staging site or target site. When is the right time to move out? What time of day makes the best time to infiltrate a facility? Where does the team meet? Do they roll out all together? All of these questions and more will be answered as we examine a better way to mobilize the team for execution purposes.

In the technical penetration testing industry, going from reconnaissance to direct port scanning, for example, marks an important milestone in the penetration test. From that point on, we consider the penetration test itself to have gone from passive mode to active mode. Being in active mode signifies a much more direct assault on the target and thus raises the risk of possibly being caught or compromised significantly. In the physical red teaming industry, we recognize this milestone similarly and refer to it as the Execution Phase. Trigger mobilization and the collective phases to follow in the REDTEAMOPSEC methodology are loosely referred to as the Execution Phase. Let's look deeper into the ever-important aspect of REDTEAMOPSEC we call Trigger Mobilization.

The goal of Trigger Mobilization is to control the movement of red team operators to the target in a controlled and orderly fashion so as not to compromise the mission with their presence. To clarify, the team will mobilize to a staging site near the target site rather than at the target site proper. As I mentioned in Chapters 4 and 5, staging sites allow teams to suit up and test gear while being far enough away from the target proper to go unnoticed yet close enough for the team to deploy in minutes.

In short, Trigger Mobilization is a planning phase that offers us orderly team movement, a staging area for preparation, and quick team deployment.

Here are the important aspects of the Trigger Mobilization phase:

1. Staging, Deployment, and Rally Point Selection

2. Mobilization

Staging, Deployment, and Rally Point Selection

Staging Site Example

Staging Site

Recall from an earlier chapter where we selected a staging area for carrying out reconnaissance {Figure 18). The recon staging site allowed the team to review recon goals, suit up, test gear, and move into deployment point positions quickly. In our example in Figure 18, this site was chosen for its close proximity to the target and its line-of-sight cover from unwanted onlookers. Essentially, the same principles apply when selecting a staging site during this phase but with a slight twist.

From my experience, after the reconnaissance phase is complete, the team generally has a much better understanding of the target site's physical environment and its flow of people, traffic, nuances, etc. Thus, the previously selected site may not be ideal for execution. In fact, simply

having stepped foot on the grounds and having obtained a ground-level perspective first-hand offers team members a chance to feel out the area.

During a recent operation, I recall picking up a very strong sense of tension in the air as my team descended upon the target, and my teammates felt it too. Perhaps it was the giant ominous spotlights blasting the grounds from the guard stations or maybe this location was "too hot," as we Like to say. Something in our gut told us we should do things differently and stage somewhere else.

All in all, a lot can be learned from the initial recon mission. At a minimum, this staging site must wholly support execution purposes and a dose proximity to deployment points. Thus, a different staging site is often selected for this reason. To make staging site selection easier; take the following factors into account when making the new selection.

- Staging site consideration factors:
- Site selection supports execution goals specifically
- Consider lighting conditions (usually performed at night)
- Close proximity to deployment point(s)
- Trust your instincts if the site seems too hot

Deployment Point

Recall from Chapter 4, "Engage in Reconnaissance," where we discussed deployment points and their importance. Deployment points are areas on the map that signify where team members make their final descent upon the target. See Figure 19 for the sample deployment sites we chose in Chapter 4.

Deploying into the field marks an important milestone in the overall REDTEAMOPSEC methodology. What is unique about the Trigger Mobilization phase when compared to recon deployment is that the deployment planning steps aim to enable our entry into the facility. For this reason, there are a few differences in how one should go about selecting deployment points.

Sample Deployment Sites

Deployment site considerations factors:

- On the fringe of being too close to the target
- Consider security camera range, guards, motion lights, etc.
- Consider lighting conditions (too illuminated?)
- Does the site support quick deployment (e.g. exit from vehicle)
- Close proximity to desired entry points (e.g. doors, windows, fence, roof, fire escape, etc.)

Rally Point

Sample Rally Point

See Figure 20 for the sample rally point we chose in our example in a previous chapter. The rally point is where the team will assemble outside the facility and exit the location, usually by vehicle. So once a red team leader deploys her operators in the field, she will likely drive to the rally point and command the team from there. You can think of the red team leader as the getaway driver and the rally point as the getaway spot.

The same criteria that goes into the selection of a rally point is similar to the criteria that goes into selecting a deployment point but with a few differences.

Rally point consideration factors:

- Supports red team leader staying parked for duration of mission
- Considers proximity of personnel from target and bystanders
- Within two-way radio range of the red team
- Supports quick team exfil {e.g. pick up team)
- Considers lighting conditions (too illuminated?)

- What walking route will operators take to reach it? Do their clothes or belongings look especially suspicious?

Mobilization

A successful red teaming mission depends on coordination taking place at many levels. Among the many things central to success is team mobilization. Team mobilization boils down to the controlled movement of red team operators to a target in an efficient, orderly fashion. If effectively completed, the team will arrive intact, on time, and prepared without compromising the mission with their presence.

There have been a handful of occasions where I have experienced missions going sideways as a result of poor team mobilization. Thankfully, they didn't result in total mission failure, but they easily could have. It is important to know when and where the team needs to be extra cautious. Please have a look at the list below pointing out the stages that pose the greatest risk during mobilization. To paint a clearer picture, I will list them in order of risk.

Periods of high-risk during team mobilization:

1. Team member deployment (risk increases for multiple deployments)
2. Waiting for the team at the rally point
3. Team members leaving the target en route to the rally point

Movement to Staging Site

Movement to the staging site is usually done by vehicle. Optimally, this should be done using a single vehicle, like a passenger van. Passenger van windows allow the team to have eyes peeled in several directions and also support space for larger teams when needed. Traveling in one vehicle will aid in preventing unwanted attention.

• Shown below is a quick list of steps during mobilization:
• Circle the staging site

- Reaffirm staging site still meets expectations
- Confirm team is ready for staging
- Approach staging site
- Execute staging procedures

Movement at this phase almost always occurs during the late hours of the night. The dark provides several advantages to the bad guys. The security posture of a facility changes drastic.ally simply by the time of day. Again, this is something the bad guys know, and it is something that they use to their advantage. This is among one of the primary reasons that nearly every physical red team operation I have carried out has been at night. Simply put, it provides a more realistic test. But the cover of night can be blown if improper use of flashlights, for example, give away a team's location through poor light discipline.

On the topic of light discipline, the driver should maintain appropriate light discipline when it comes to the vehicle's headlights, brake lights, and interior lights. Drivers should kill all external lights and mute or turn off interior lighting. Internal light sources emanating from cell phones, laptops, and such must also be kept to a minimum.

Red team operators should maintain appropriate light discipline when outside the vehicle as well. Red lights and low lumen headlamps are ideal here. An important note regarding infrared let use: If the team is using night vision to spot infrared cameras or merely as a visual aid, their equipment will give off a signal visible to others on the same spectrum. Good infrared light discipline means using these tools where appropriate and in limited fashion. It is important to note that light discipline will soon become even more serious when the team reaches their deployment sites and beyond.

Once the vehicle has landed at the staging site, the team should suit up and prepare quickly but thoroughly. Final equipment checks, radio communications tests, and clothing changes should occur at this time.