DIRECT PREPARATIONS

Successful physical red team operations would not be possible without a strong game plan. Goals sourced from the RoE and raw recon intelligence power the operation and are vital to the preparations phase of the REDTEAMOPSEC methodology.

In this chapter, we will cover the preparations and analysis necessary to further the red team operation. We will analyze the recon intel and align the action steps to follow in support of the RoE .. This step is critical and paramount to the success of the operation as a result of the decisions made here. Some of the decisions made at this step will be made as a team. However, most of the heavy lifting in this phase will fall upon the shoulders of the red team leader.

Here are the primary areas of concentration for this chapter:

- Recon Intel Review
- Vulnerability Analysis
- Additional Needs & Resource Planning
- Operational Plan Development

Recon Intel Review

Immediately following a reconnaissance mission, the recon team should meet to debrief. To prepare for the meeting, the red team leader should gather all notes, footage, and photos from each of the team members. Once all recon artifacts have been collected, the red team leader should begin creating a timeline of events. Oftentimes, the timeline of events is a client-facing document that summarizes the mission's beginning, end, and milestones in between. I've found that clients like to use these timelines to better understand why their current security controls did not detect or trigger an incident when reviewing security camera footage, guard tours, etc.

When reviewing recon artifacts, each recon member should provide their recollection of events including times, captured footage/photos, and observations. This verbal walkthrough should be detailed, in chronological order, and align with previously defined recon goals. Every artifact (video, photo) should be reviewed by the team. Any observations unable to be captured by video or photo should be entered into record by the red team leader. By now, the red team leader should have a more complete timeline of events to be shared with the client. If so desired, the red team leader could upload the timeline to the document repository for client review.

Having discussed the observations and outcomes of each recon goal together, the team must analyze the results.

Vulnerability Analysis

Vulnerability analysis is a critical part of the preparations step. At this point, the team must analyze each outcome to answer the following:

Given the recon observations, does the team believe there is a vulnerability present?

Is there a security control in place to defend against exploitation of this vulnerability? If so, how sophisticated is it?

Is the likely bad actor more sophisticated and/or better resourced than the in-place security control?

Recon Goals			Results		
#	Goal	Plan	Observations	Vulnerability	Go-Forward
1	Surveil loading dock area, search for insecure doors and possible entry ways. Also take note of any security cameras and motion lights.	Deploy from area #1, approach from near on foot and walk along alley way. Wear blue-collar clothing and fake a phone call while pausing in front of entrances. Capture footage and take every opportunity to video door locks up close.	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					

Finalized Recon Goals Table

Please see the Results columns above. This shows the completed version of the Recon Goals table presented earlier in this book. Some columns have been hidden for space. The red team leader should complete each recon goal with a summary of the observations, vulnerability, and decision to move forward with testing or not.

As stated earlier, the team must analyze each recon goal's observations to determine if there is a vulnerability present and if testing is applicable. In some cases, recon intel may indicate adequate protection or better. In most cases, this determination is usually not so apparent. The decision to go forward with testing is one that should be made as a team. Most importantly, if a vulnerability is present, would the likely bad actor be sophisticated enough to exploit it? How weH resourced would he need to be? Is this a vulnerability that is worth testing? These are all important questions to be considered. Remember, vulnerabilities should be tested in a commensurate fashion with the level of sophistication of would-be perpetrators.

Additional Needs & Resource Planning

As the vulnerability analysis portion comes to a dose, the team has decided which security controls pose issues significant enough to be tested. The team should also have a clear idea of how to test those issues. As a result of all this, there will likely be changes. They might find a need for additional tools and maybe even more team members. It is important at this step to ensure the team makes, purchases, or sets aside these extra necessities. This is a pivotal point in the process as we prepare for execution down the road.

From my years of experience, this phase almost always involves changes to the RoE. So now would be a good time to revisit the RoE and update as necessary. Any RoE changes must be shared and approved by the client before moving forward.

All in all, a lot of this planning can occur without involving the client. But this marks an important point at which operation dates and times should be finalized. This will need to be coordinated with the client and must be done as far in advance as possible.

To prepare for immediate next steps in the REDTEAMOPSEC phase, such as Trigger Mobilization, a second staging site should be chosen at this time. If you recall from Chapter 4, the staging site is where the team suits up, tests gear, and makes final preparations minutes before deploying into the field. The next staging site should be ideal for specific execution purposes. You may find that your previously used staging site during reconnaissance is still an ideal spot. However, understand that most operations take place at night and could involve wearing dark clothing, carrying strange tools, or behaving suspiciously. Be sure the next staging site is conducive to those activities.

Here is a short list of preparation items that should be covered here:

- ✓ Finalize TTP strategies and adapt plans and resources appropriately
- ✓ Acquire additional tools and equipment before moving forward, if necessary
- ✓ Add additional red teamers to the operation, if necessary
- ✓ Finalize operational dates and times with client
- ✓ Coordinate travel plans for the execution of the operation
- ✓ Determine the ideal Staging Site (see "Execute Staging")

✓ Update the RoE and obtain approval from the client

✓ Operational Plan Development

Before going any further, I will link to an editable Microsoft Word template of an Operational Plan below.

OPERATIONAL PLAN TEMPLATE

I will provide a brief outline of the same Operational Plan to follow.

The list to follow is an example of a high-level outline of an operational plan. I recommend using the existing components at a bare minimum. You will need to modify as necessary. Again, this is a client facing document that is presented and discussed following the Engage Reconnaissance phase. The plan is subject to change. Therefore, client stakeholders must have complete visibility and be required to review and approve any salient changes as they happen.

Plan development is where most of the effort will be concentrated during this phase. You'll notice the operational plan provides the client with some of the same information as the RoE, but with more meat, particularly number 11, titled Operation & TTPs. Operation & TTPs aligns perfectly with the REDTEAMOPSEC methodology and aims to summarize to the client what will happen at each point. Items A to Kare what we will be covering in detail in the chapters to follow, so don't be alarmed if you don't know their meaning right now.

Operational Plan Outline

Here are the major components of the Operational Plan:

1. Client Name
2. Client Contacts
3. Project Contacts
4. Red Team Members & Roles
5. Target Location Address(es)
6. GPS Coordinates (Each location)
7. Photos of Location{s)

8. Operation Dates & Times
9. Operation Objective(s)
10. Target Control(s)
11. Operation & TTPs
    a. Reconnaissance
    b. Preparation
    c. Mobilization
    d. Staging
    e. Assess & Acclimate
    f. Maneuver Operations
    g. Strike
    h. Penetration & Control
    i. Execute Operational Orders (OPORD)
    j. Evacuate, Evade, & Cover
    k. Collect & Exfil
12. Out-of-Scope Control(s)
13. Out-of-scope TTP(s)
14. Damage Causing TTP(s}
15. Additional Notes
16. Document Change History Table
    a. Change Description & Date
    b. Client Change Review/Approval Signature & Date