RULES OF ENGAGEMENT

A physical red team operation should not begin unless the testing team has a dear understanding of the target's threat profile. Identifying the target's exposure factors ultimately enables operators to develop an operation leveraging realistic TTPs and level of sophistication against threats the target will likely face. There is more on this in Chapter 14, Full-Force Red Teaming."

To pause for a moment and state the obvious, threat profiling is not the very first step in an operation. Depending upon if the red team is an internal team or if the team is part of a security firm will ultimately play an important role in what the very first steps in launching an operation truly are. It's not the goal of this book to focus on the front end of the engagement process. But having an agreed-upon scope, objectives, and a prepared plan make up those crucially important pre-engagement requirements.

Overview

Before a physical red team operation can begin, there must be an understanding between the testing team and the client on some very important things; namely, those things that revolve around certain specifics pertaining to TTPs and how they will be carried out For this, we start at the first phase in the REDTEAMOPSEC methodology called, Rules of Engagement (RoE). The RoE is a document that outlines the entire operation from start to finish at a high level. It communicates important information and milestones to the client and much more.

The Rules of Engagement has a few primary functions. Among those functions are to signify which TTPs and targets, from a high level, are fair game. Equally as important, it also signifies which TTPs and targets are prohibited, or out of scope Some TTPs may indirectly or directly cause damage to property. Damage to client property is sometimes considered

out of scope and is often stated as such in the RoE. For example, "Any and all damage to client company property (e.g.: locks, doors, windows) is strictly prohibited."

In contrast, some damage to client property may be permitted by the client because it may be a realistic threat an attacker would use against them. This is precisely where the value of an RoE is realized. A client may be okay with damage to certain locks and windows but not to others. Therefore, it is important to have this understanding clarified and agreed upon in writing. The key here is to be as verbose as possible to avoid confusion.

DAMAGE TO PROPERTY

To step back a moment, I'm not encouraging all-out physical damage to property on each and every operation for the sake of breaking things. The concept of breaking windows during a security test, for example, may seem unconventional to most clients. But what we should remind them of is the fact that bad guys don't play by the rules and we, as red teamers, should push the envelope to mimic their behavior as closely as possible.

We as physical red team operators must propose unconventional test scenarios to clients where it makes sense, and, of course, there has to be some solid reasoning behind the decision to damage property. Finding those situations is not always obvious, so I've put together some guidance to help that process along.

Please see the numbered list below when considering TTPs that involve potential or certain damage to client property.

1. The likelihood that a bad actor would use the same TTPs is significant enough to warrant potential or certain damage.
2. The negative impact a bad actor could incur using the same TTPs is significant enough to warrant potential or certain damage.

3. The use of damaging TTPs will add value and 'realism' to the operation.
4. TTPs utilize the same level of sophistication as a likely bad actor.
5. TTPs utilized are commensurate with the asset's value.
6. The client is aware of the asset's monetary value, business value, and downstream business function should the asset become broken or unavailable.
7. Both you and the client are in full agreement with chosen TTPs, assets, and how the asset will be fixed or reimbursed.

The goal of item #1 is intended to operate as a quick sanity check to ensure the threat is significant enough to test with the expectation of damage and the selected TTP is something a bad actor would actually utilize. We want to avoid overcomplicating TTPs, especially if the bad actor might choose a simpler route.

Item #2 is also a great thought exercise. Here we want to be sure the estimated impact is worthy of the resources it requires to test. For instance, most convenience stores expect kids to steal packs of bubble gum. It is considered a cost of doing business. But unless kids are stealing them by the pallet, the threat isn't impactful enough to install costly security controls or hire red teamers. Test only where the impact, and likelihood, for that matter, a re significant enough to warrant the effort.

A TTP that is likely to cause damage shouldn't be carried out unless the client sees it as valuable to the operation. Breaking a physical control that is inexpensive or easily replaced should not be the sole factor in the decision-making process. Testing newly identified vulnerabilities or retesting old vulnerabilities with updated TTPs is a great way to add value. Doing this gives additional perspective and likely more food for thought.

Item #4 is one of my biggest pet peeves. Over eager red teamers like to over-engineer TTPs to be more like the fictional spy character, Ethan Hunt, than anything. I call this the Mission: Impossible Effect. The term tacticool

also comes to mind. Simply put, physical. security controls should be tested using the same kit and TTPs that a likely bad actor would use. TTPs and kit must be commensurate with the level of sophistication of the bad actor and the physical security control at hand. Any over exaggeration serves only to damage a team's reputation and the value of the operation.

Before making a recommendation to your client to use a damaging TTP, be sure your client has a good handle on the asset's value and any potential downstream impact. Naturally, you won't have these answers, but it is crucially important to walk the client through the brainstorming process. Something as simple as breaking a window may have complicated downstream effects.

I have found it best to raise three important points during these discussions:

- Monetary cost (How much does it cost? Can it be replaced? How long to replace it?)
- Business functionality cost (What are its direct business implications? Loss of availability? Impact to Integrity? Impact to Confidentiality?)
- Downstream impact {Brainstorm potentially unforeseen downstream impact)

If it makes sense to use the TTP and the client gives the green light, the next step is to document this in the RoE. Sometimes an operation changes mid-course and an opportunity to use such a TTP becomes valuable. If so, it's critical to document the details in written format for clarity and non-repudiation purposes.

ROE Outline

The numbered list to follow is an example of a high-level outline of a Rules of Engagement deliverable. I recommend using the existing

components as a bare minimum and to modify as necessary. Again, this is a client-facing document that is presented and discussed at the start of every operation. Since this is one of the very first operational. documents produced, it is probably going to be updated often as the operation progresses. Because of this, the client stakeholders must have complete visibility and be required to review and approve any changes as they happen.

Here are the major components of the RoE:

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. Operation Objective(s)
8. Target Control(s}
9. Out-of-Scope Control(s}
10. Out-of-scope TTP(s}
11. Damage Causing TTP(s)
12. Additional Notes
13. Document Change History Table
    a. Change Description & Date
    b. Client Change Review/Approval Signature & Date

Once again, I recommend readers visit the link published earlier for more information and a modifiable RoE template.

The RoE is a living document and must be updated as often as necessary and shared with client stakeholders and red teamers. Making use of an online client-facing portal to allow for easy document sharing is highly suggested. My team and I use such a portal. that will sends alerts to

all each time the RoE is updated. This gives clients an opportunity to review, ask questions, and provide written approval.

The key to success during any engagement is having a well-documented RoE that keeps clients updated and team members focused. I can't stress this point enough. It will certainly be an exercise in communication and follow through, but it is a necessity that clients will grow to love.