INTRODUCTION TO UNDERGROUND OPERATIONS

The computer hacker crouched low in thick brush on a cold December nigh~ just beyond the fence line of his target- a massive U.S. oil refinery. Wearing night-vision goggles and dressed in black, he swung a rubber mallet into the dirt, trying to produce vibrations to distract the plant's ground-penetrating radar system. He swung again and again. Flashlights emerged from a distant building, then disappeared. Soon a train roared by, providing the cover his team needed. Quickly, two more men appeared from the shadows. They threw a wool blanket over a 16-foot barbed wire fence, climbed over and rushed to a small building housing the facility's vital computer controls. The door had an electronic lock, a badge reader, and a plate to thwart lock picking. But the intruders caught a break. The door didn't sit properly in its frame, leaving just enough space to shimmy it open.

Within moments, they had planted a small device, about the size of a credit card, designed to begin penetrating the refinery's controls systems. "Bingo!" crackled from the radio inside a white SUV adorned with a phony logo of the refining company, some 200 yards away. From there, the leader gave the signal to leave - "Rabbit!"

As the other hackers hopped in the van, the driver's nerves calmed. Then a stark reality set in. "We've used a couple hundred dollars in gear, and we were able to break into a refinery without anyone knowing," said the leader.

'The implication is pretty devastating."

He was hired by the refinery to test its defenses against cyberattacks and, like so many others, the mission was way too easy. Despite the refinery's remote location, fencing, high-tech sensors and security team, his team was able to infiltrate its network and potentially wreak havoc.

As this story shows, hackers don't have to limit themselves to the internet to break into computer networks .. With long-range cameras, they

can spend days watching workers entering through front doors, so they can mimic their behavior and exploit weak spots to get inside. Before the team raided the oil refinery in December, they staked out the company's corporate offices.

They watched employees at nearby coffee shops and restaurants, managing to steal and clone badges. The leader said he tries to stay within the bounds of what real hackers can do with a modest investment. In the refinery raid, his team carried only a small amount of gear, including a laptop lock-pick set, and a $35 device to tap the computer systems, all available on Amazon.

They used two 16-foot ladders, which they returned to Home Depot for a full refund, a set of four two-way radios, and lock picks. Such tests have found plenty of security weaknesses, cyber and otherwise, that should worry the energy industry. But the scariest part, he said, is that so much of hacking is low-tech, requiring little expertise. Anyone can do these types of things."

REDTEAMOPSEC METHODOLOGY

I apologize for the dramatic intro, but I believe it illustrates an important point. What this article offers is a small glimpse into the world of Physical Red Teaming and to what extent companies need to take steps to protect themselves from bad actors. Today, bad actors assume many forms, and their malicious plans range far greater than they did even five years ago.

Are you wondering about the security posture of your company or organization right about now? Does this sound like something you should consider for your own organization? Or does it sound like an interesting career path? Well I hope your inner wheels are turning, if only just a tiny bit. In this book, my hope is to provide readers with an understanding of physical. threats and how they seep into other threat domains, cyber and social alike, and have an overall impact on a company. More importantly,

the focus of this book is to provide a comprehensive guide to executing physical red teaming with accuracy and effectiveness.

As a side note, I will use the terms "physical red teaming" and "physical penetration testing" interchangeably.

OVERVIEW

The focus of this chapter is to establish a basic foundation on physical red teaming, whether you have some experience or none.

In short, a physical penetration test is an authorized simulated physical attack on an organization's physical. security in an effort to evaluate their security posture and, ultimately, help improve it. To identify security weaknesses, measure security posture, and offer ways to improve it is a shared goal of just about any penetration test. Governments, companies, and organizations make use of penetration testing in order to improve the effectiveness of their security controls. There are, however, some stark differences between physical. penetration testing and the other variants.

What makes physical red teaming unique is the absence of (most) computing technology as a target. When you hear someone mention penetration testing, most people immediately think technology is the intended target, such as computers, web applications, firewalls, networked devices, and so on. That certainly doesn't mean that computing technology is never used or targeted during physical penetration tests. Instead, we use this simple distinction to convey the things we primarily aim to test. These often include motion detectors, security cameras, employees, access control scanners, security fences, locks, security personnel, and other controls and technologies intended to keep physical assets secure. So to clarify, computer systems and related technologies are utilized and exploited in an effort to further physical security operations.

Physical security operations require an appreciation for complex puzzles and out-of-the-box problem-solving. Fortunately for many traditional penetration testers and hackers, this is an easy transition. It's becoming familiar with physical security methodologies, threats,

vulnerabilities, and tools that become the crux. I can speak from experience; this was one of the most trying aspects for me. In this book, I hope to build upon your hacker mindset and bridge the gap of know-how by showing how to execute physical penetration tests professionally.

The REDTEAMOPSEC methodology provides a quick glance at my approach for conducting physical red team operations and will serve as the chapter outline for the remainder of this book. I developed this methodology in response to a lack of any real and relevant framework on the subject of physical red teaming. As you might have already noticed, REDTEAMOPSEC is an acronym for each of the twelve crucial and distinct steps in the physical red teaming process.

Here are the 12 steps in the REDTEAMOPSEC methodology:

1. **R**ules of Engagement
2. **E**ngage in Reconnaissance
3. **D**irect Preparations
4. **T**rigger Mobilization
5. **E**xecute Staging
6. **A**ssess & Acclimate
7. **M**aneuver Operations
8. **O**ffensive Strike
9. **P**enetration & Control
10. **S**ecure OPORD
11. **E**vacuate, Evade, & Cover
12. **C**ollect & Exfiltrate

The components of the REDTEAMOPSEC methodology won't make much sense right now, and that's okay. A chapter will be devoted detailing each of the following twelve steps in chronological order.

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.

ENGAGE IN RECONNAISANCE

In this chapter, I will provide a quick overview of the concept of reconnaissance (recon) and how it should be carried out during physical. red team operations. I will propose a couple of high-level, tactical approaches to take toward reconnaissance that I believe make the process more systematic, effective, and repeatable. Finally, I will close out the chapter by providing a list of must-have tactical surveillance gear my team and I use every day.

Overview

Reconnaissance is a mission to obtain information by visual observation or other detection methods, about the activities and resources of an enemy or potential enemy, or about the meteorological, hydrographic, or geographic characteristics of a particular area (Reconnaissance (US Army FM 7-92; Chap. 4). A successful red team operation would not be possible without a solid foundation of actionable intel about the target or targets. What kind of intelligence? The location of security cameras, entrances, checkpoints, guard huts, and motion sensors are just a small example. Engaging in planned reconnaissance missions aimed at discovering these items is what this chapter is all about.

As you've probably already realized, reconnaissance is a military tactic heavily used during any number of military operations. It is extremely useful in exploring areas across enemy lines in an attempt to gain useful

information about an enemy's position, combat strength, terrain, weapons, etc.

Obviously, we are not engaging in military warfare here, but incorporating military TTPs during our physical red team operations has been paramount to the success of my team's operations. Therefore, this book will be heavy on military-themed concepts for their added benefits.

In this chapter, we will make use of an adapted version of military-themed reconnaissance tactics to help us obtain information about our targets in the same way bad actors might.

Before Getting Started

A few things must be in place prior to the start of a recon engagement. Some of these practices, such as inter-team communication during recon, might be altogether new to readers and may require some level of introduction. As a result, the subsections to follow aim to shed light on these critical components.

Red Team Leader

The hierarchy for small red teams is usually very flat. However, every team should be made up of two or more red team operators and at least one red team leader. Here are some of the basic responsibilities of a red team leader:

- Knows the mission at-hand completely and thoroughly
- Serves as primary communicator with client
- Serves as primary communicator between team operators
- Certifies team readiness
- Responsible for the actions of the operators
- Commands the operators in the field
- Determines mission success

Generally, the red team leader is the most experienced on the team. She must possess excellent communication, organizational, and tactical skills.

Project Repository

Critical to any engagement are project documents, spreadsheets, project notes, evidence, and so on. By now, we already have the Rules of Engagement and a fairly good understanding of the operation as a whole. As we progress through the REDTEAMOPSEC methodology chain, additional project artifacts will be created, shared, and updated. Therefore, it is imperative to establish a centralized and secure repository for disseminating and communicating in writing.

I encourage using an online portal system expressly designated for document sharing coupled with advanced features to notify users and provide a means to comment and calla borate. If this isn't immediately available, one could make do by using Google Drive, Google Sheets, and Google Docs.

Communication

It goes without saying, but ineffective communication will ruin any and every engagement. So to start on the topic of communication, we will focus on two types:

- Client Communication
- Inter-team Communication

Client Communication

Expectations should be set in advance on what kind of information the client might expect to receive, approve, or collaborate on. In the beginning, this will likely be the RoE. However, clients should have a basic understanding of the many different types of documents that could be shared and what actions they should take in response, if any. For example, updates to formal documents or agreements, such as an RoE, will require review and approvals. Intel the red team uncovers on targets may only

require a client's review. Photos the red team takes during recon missions may not require any action on behalf of the client. In any event, we don't want our client to become confused about what to do and how to respond to the many pieces of information they find in their possession.

A cadence of communication should be established and understood between client and red teamers. This becomes more important when a red team is actively engaged while deployed onsite during a recon mission, for example. This type of communication is most often conducted by phone, text, email and radio respectively. Therefore, the client should be informed and expect to receive and respond to a high volume of communication from the red team during reconnaissance missions.

There should also be a designated list of contacts the red team communicates with during such recon missions. This communication happens during au hours of the day. Thus, these designated contacts must be available by phone, at a minimum, in the event something important is discovered or if something goes sideways during the recon mission. Generally, if something goes awry during recon, it usually means the recon team was compromised. In other words, an employee, bystander, or third party may have seen the recon team doing something suspicious, preventing the team from continuing.

To aid in client communications, a section in the RoE is often designated to define who the client assigns as its contacts along with their contact information and role. An additional piece of documentation called an Authorization Letter (aka: Get Out of Jail Free Card) will further describe the contact/ escalation list along with additional information. The Authorization Letter is something we will cover in greater detail later in this chapter.

Inter-team Communication

Information designated as client-facing should be communicated through the red team's document repository. But much of the inter-team communication can and should happen in a team meeting or series of team meetings. Any output from those meetings should be uploaded to a

document repository for internal. use. On that note, let it be known that not every piece of documentation needs to be reviewed or shared with the client. This usually amounts to internal strategizing sessions and team planning estimates. That information can be limited to internal use only.

Inter-team communication, from resource planning to strategizing, will be gathered throughout the REDTEAMOPSEC phases. That said, a great deal of that work often occurs in the early phases of recon planning and during the execution phase. Whenever a team meeting or discussion occurs, I highly recommend taking notes. I have found myself in many situations where my team rehashes topics that were previously discussed. Taking notes and sharing them with the team will keep them informed and more focused.

Here are some key points to capture during inter-team meetings, strategizing sessions, and discussions:

- Strategy ideas
- TTP planning
- Time constraints and travel
- Resource planning considerations
- Reconnaissance vantage points
- Risk areas for bystander detection
- Staying in alignment with objectives
- Recon equipment needs

Equipment

Equipment requirements will change from one recon mission to another. Even during the same engagement. Unfortunately, there is no one-size-fits-all solution. But what I wiU offer here is a list of equipment that my team and I tend to use on nearly every recon mission.

Most recon missions boil down to these important steps: Contact, Conceal, and Capture, what I call the Recon C.3 Method. We will talk more about the Recon C3 method later in this chapter.

For now, here is a list of essential equipment my team uses on nearly every recon mission:

Reconnaissance Equipment List

This is a curated list of equipment me and my team use during social engineering operations. It doesn't include every piece of equipment we own but will definitely serve as a great place to get started. Happy hunting!

Optics (Long/Short Range)

Headlamp: http://amzn.to/2EW7EYL
Nikon P900 Camera: http://amzn.to/2HuKGX0
GoPro Hero 6: http://amzn.to/2Hww6OR
Night Optics: http://amzn.to/2HwFIJj
Binoculars: http://amzn.to/2ETJwpx
GoPro Chesty Mount: http://amzn.to/2Hz9JZ5
Tactical Flashlight: http://amzn.to/2CyGwtL
Thermal Cam Add-on (iPhone): http://amzn.to/2HzadhR
GoPro Head Strap: http://amzn.to/2BFoKIm
Low Profile Tripod (Camera): http://amzn.to/2HtyeHf
Standard Tripod (Camera): http://amzn.to/2EH7QMl

Discreet Recon (Short Range)

Pen Camera: http://amzn.to/2EHClSf
Button Camera: http://amzn.to/2Gw12NM
Glasses Camera: http://amzn.to/2EU8lBH

Clothing

Tactical Pants (Night Covert): http://amzn.to/2CyUnzW
Tactical Top (Night Covert): http://amzn.to/2C9HmkW

Tactical Boots (Night Covert): http://amzn.to/2GuiSRm
Balaclava (Night Covert): http://amzn.to/2CyVqjB
Tactical Rucksack: http://amzn.to/2GtjyGQ
Coveralls (Dumpster Diving): http://amzn.to/2Hvs9Ke
BDU Top (Non-urban Terrain): http://amzn.to/2EH5WLy
BDU Pants (Non-urban Terrain): http://amzn.to/2sHwAOF
Gloves: http://amzn.to/2EKdvAY

Accessories

All Weather Notebook: http://amzn.to/2GvGipC
All Weather Pen: http://amzn.to/2sIODnH
Compass: http://amzn.to/2BFS1m5
Climbing Claws, Hands: http://amzn.to/2BFEFGv
Climbing Claws, Feet: http://amzn.to/2EG9Q7f
Two Way Radios & Earpiece: http://amzn.to/2CCMb1L

Counter Surveillance

Bug Sweep/RF Hidden Cam Detector: http://amzn.to/2BDwryC

Contact (equipment for movement, comms, carrying gear)

- MOLLE tactical vest — load-bearing vest to carry essential gear on the body.
- Handheld radios — short-range field radios for team voice communications.
- In-ear headset (2-pin covert style) — single-ear/headset for hands-free comms.
- Tactical ripstop pants — durable pants (various colors) for terrain protection.
- Tactical ripstop shirt — durable shirt (various colors).
- Tactical daypack — compact pack for carrying mission equipment.
- Compass — basic magnetic navigation for open-area navigation.

- Timekeepers — wrist/field watches or timers for reconnaissance timing.
- Multitool (compact) — pliers/knife/screwdrivers for field tasks.

Conceal (equipment to reduce signature and protect when breaching obstacles)

- Balaclava — face/neck concealment.
- Rugged tactical boots — all-terrain boots for mobility and protection.
- Durable gloves — cut/abrasion resistant gloves for handling rough obstacles.
- Thick wool blanket — robust blanket useful for climbing over barbed wire or insulation.
- Mylar (space) blankets — low-signature thermal blankets (can reduce IR signature).
- Headlamp with red light mode — hands-free illumination using red to preserve night vision.
- Compact red-beam torch (tactical) — portable red flashlight for covert work.
- Wireless endoscope (flexible borescope) — remote visual inspection around corners and tight spaces.

- *Capture (equipment for observation, evidence collection, and signals capture)*
- Rugged laptop (Mac or Windows) — field workstation for capture, processing, and storage.
- Camera with long optical zoom — for distant visual reconnaissance.
- Tripod (stable) — support for long-zoom shots.
- Night-vision binoculars — image-intensifier binoculars for low-light observation.
- Small body-worn action camera (GoPro or equivalent) — helmet/body mount for hands-free video.
- Head-worn camera mount — supports head/helmet camera for hands-free recording.
- Binoculars (standard) — visual magnification for mid-range spotting.

- Thermal imaging attachment (phone compatible) — thermal camera for smartphone.
- Eyeglass / discrete wearable camera — covert head-mounted camera.
- Wi-Fi capture antenna / adapter — external antenna for Wi-Fi signal monitoring.
- Miniature pen camera — ultra-discreet camera for close-range capture.
- All-weather field notebook — waterproof notebook for field notes.
- All-weather pen — writes in wet/cold conditions.

Before embarking on a recon mission, the team should use a Load Out List to list and keep track of necessary equipment.

Environmental situations, such as urban settings vs. rural settings and day vs. night, will ultimately determine the extent to which these tools are relevant. Keep in mind this is not a full and complete list, however this is good enough to prepare any recon team from the get-go.

PLANNING RECON MISSIONS

Though the specifics of a reconnaissance mission always vary, performing them can and should be carried out in a systematic process. No set of unique recon goals or objectives should completely deviate from a solid methodology. From a high level, the C.O.V.E.R.T. Recon Method (COVERT) is a system that enables the recon mission process to happen repeatedly with consistency and confidence.

COVERT Reconnaissance Method

1. **C**onsume RoE
2. **O**btain Targets
3. **V**erify Goals
4. **E**stimate Resources
5. **R**eady Team

6. Team Executes

As you can see in Figure 4, the COVERT recon methodology is a very straightforward six-step process. Its best use case might be to use it as a high-level operational guide to red teams.

Later in this chapter, we will cover another method called the Recon C3 method, whose intent is to help tactically guide red teams during the execution phase of a recon mission. But for now, the COVERT recon methodology can be used as a valuable tool to distill the sometimes complex process of carrying out reconnaissance missions.

In previous years, I struggled to produce consistent results from operation to operation. Eventually, I discovered one of the primary reasons was due to a fickle process I was using to gather information. COVERT recon helps smooth those edges.

Consider COVERT as a basic plan for operationally stepping through the reconnaissance phase of a physical. red team operation. Let's start by studying each of the six steps.

Consume RoE

By now, the RoE should be in hand and contain, at a minimum, enough information to begin planning reconnaissance. Remember, the RoE is a living document and may not contain much detail just yet. However, it should contain enough information to launch a recon mission of substance.

To get things rolling, the information consumed and analyzed should at least amount to the following:

- Target locations (addresses and GPS
- coordinates)
- Targeted people (specific individuals and/or
- employee roles)
- Google Earth photos
- Targeted controls
- Out-of-scope controls
- Operational objectives
- General idea of the complexity of TTPs

The team should not move onto the next phase until this basic information is acquired and understood. In fact, it might be helpful to copy and paste this information from the RoE into a separate internal document that can be easily reviewed by the team. It could prove useful as a quick reference cheat sheet as the team goes through the COVERT process.

Since the recon team will soon be going onsite to conduct recon, authorization from the client must be obtained from everyone but the recon team and a few client stakeholders. Employees, civilians, security forces, and bystanders may think the recon team's actions look like anything from a burglary in process, to terrorists in action, to a swat team raid, to trespassers, to plain old creepy dudes. As a result, each recon team operator must have a legitimate reason for their presence, as well as explanations for everything you have on your person.

Obtain Targets

The RoE will have some basic information about targets, but certainly not exhaustive amounts. In this step of the COVERT process, we want to dive deeper into where and who our targets are and what might be around them.

Open-source Intelligence (OSINT)

At this point, we will have physical addresses, GPS coordinates, maybe some aerial photos from Google Earth, and perhaps a handful of staff names we are targeting. Using addresses, we should be searching open sources like Google to find images and information relevant to our targets, etc. This leg of recon is what most folks refer to as Open-source Intelligence (OSINT). OSINT is data collected from publicly available sources to be used in an intelligence context.

When the team becomes aware of a target name our goal is to turn that name from a 'John Doe' into a persona. What do I mean by that? Searching my name in Google will turn up other people that share my name, who you'll find you can quickly dismiss. However, you may find some other interesting information about my career, schools I've attended, businesses I own, and other personal interests. Slowly my name evolves from merely a name into a fuU-fledged persona. This intel may serve to be valuable in targeting me later, or it may not. But the principal points I am making here are to personify the raw information we have in the RoE using OSINT tactics and turning it into something of value to the operation.

Here are some OSINT resources you can use to personify an individual, a company, and/or its facility:

- Google Images and Google Earth
- Google Dorking (https://www.exploit-db.com/google-hackingdatabase)
- Twitter, LinkedIn, Crunchbase, Indeed,
- Monster

- Recon-NG, Maltego

Verify Goals

Given the information obtained during the previous steps in the COVERT process, now is the time to set reconnaissance goals and ensure they align with the RoE as a whole. One way to do this is by reviewing the RoE's objectives and targeted security controls. Then ask yourself, what is the operation's overall objective? What are the client's most critical assets? What controls are we testing, who are the likely bad actors, and how sophisticated are they? Answering these fundamental questions will enable the development of reconnaissance goals that, in the end, will feed the latter phases of the operation.

Let's take a look at an example. Let's assume our client is a critical infrastructure power company that owns substation facilities that have small huts providing network connections into its SCADA and internal network. The client has nearly 100 of these small housing structures in substations spread across a wide geographic footprint. As the red team, we suspect their physical security posture might not be adequate and likely pose significant threat by likely bad actors through these substation structures.

During this step of the COVERT process, we need to set recon goals that enable u.s to find out whether our suspicions of these small huts is correct. We might set a goal to covertly recon a few substations in an attempt to learn what cameras, motion detectors, and personnel are present. In every physical. red team operation, there will likely be several recon goals just like this all serving different purposes but unified in support of the RoE and the operation in its entirety. Make a list of the recon goals and share them with the team. Feel free to use and adapt the sample recon goals shown in Figure 5.

#	Goal	Plan	Est. Vulnerabilit	Threat	Bad Actor

1	Monitor personnel traffic at substation A to H. Identify physical security controls (cameras, motion-detection, locks, RFID)	[PROVIDE DETAILS ABOUT HOW THE TEAM WILL EXECUTE THIS GOAL]	Inadequate perimeter security	Moderate to Significant Service Disruption	Nation-state, moderately sophisticated

Estimate Resources

Among the most essential parts of estimating resources are time, travel, and tools. Estimating resources is a breeze if you follow those simple steps.

Time

Time consists of both operation time and red team operator time. To begin, we need to understand the client's needs and relevant deadlines. Of course, that will vary from client to client.

It is in everyone's best interest, however, to carve out as close to a finalized project timeline as possible as early as possible. It's especially critical when it comes to both the recon and the execution phase since this usually involves travel. Poorly coordinated travel is one of the biggest reasons operations fail Some red teams will conduct their initial recon and then immediately go into the execution phase during the same trip to the site. The REDTEAMOPSEC method separates these two occurrences for this very reason. As a result, each red team operation will require a recon team and an execution team, both involving separate trips to the site. Oftentimes, the recon team consists of the very same execution team, minus an operator or two.

When considering how long it may take onsite, I always ensure there are at least three days for onsite recon. This gives time to capture intel during the day and night on more than one occasion as opposed to a single day and night. Some recon goals may be accomplished by one operator, while the rest of the recon team achieves a different goal. Good planning will help the team use the time onsite more efficiently.

Travel

Once a project timeline is established, it now becomes essential to estimate team resources. How many red team operators will it take for recon? Which operator will do what? How long do we need to be onsite? Some of this information will become evident once recon goals are defined. Most recon missions can be done with three operators, occasionally only two. It's a good rule of thumb to adopt at least three operators for every recon mission.

Travel plans should be made early for at least three operators. In order for the team to get acclimated, the travel plan should include at least one full travel day. The team could use the extra time on a travel day to review the recon goal list one more time and prep tools or other equipment.

Tools

By now, the recon goals list is widely known, a project timeline is there, and the recon team may be assembled. A big part of the necessary tools can be sourced from the recon goals list. The team should take the time to ensure each of the tools are in working order and make efforts to purchase or make any others.

Let's not forget that clothing is also part of this step as well. Terrain and weather considerations may force the team to bulk up and make new purchases as a result.

Ready Team

This step assumes the team has well-defined recon goals, is fully equipped, and has arrived onsite. You could consider this step a mini version of step five in the REDTEAMOPSEC method called, Execute Staging. This is the staging phase, one of the last steps before the team switches from passive recon to active recon.

To help certify readiness, here is a quick checklist of must-haves:

- Every operator is carrying an authorization letter and a federal or state identification
- Every operator is carrying the necessary gear

- Every operator's gear has been checked and is in working order • Every operator has a means of effectively communicating situation reports (SITREP) to the team during execution
- Every operator has an assigned recon goal and knows their role in accomplishing that goal
- Every operator knows what signifies mission success for each recon goal
- Every operator knows what to do in the event of a compromise by an employee, a bystander, law enforcement, or security force
- Every operator knows where the rally point is located

Team Executes

Go Red Team! This is the most exciting part of running recon missions. Tensions are high, the adrenaline is flowing, the team puts their planning into action and actively moves into position. This marks the point at which an operation could go sideways if compromised. It is critical that the team stays on task and follows the plan closely.

Truth be told, no amount of planning will guarantee that the mission will go off perfectly. Expect hiccups along the way and take time to play out what you would do in potential and unfortunate scenarios. Some say reconnaissance is far more of an art than a science, and, to some degree, that's not entirely untrue. I have found success in operationalizing it with the COVERT method, as we've seen here, and the Recon C3 Method as you'll see next.

Recon C3 Method

I developed the Recon C3 method to enable recon teams to stay on task and approach reconnaissance missions uniformly and clearly.

The Recon C3 method includes three critical execution phases of recon missions: Contact, Conceal, and Capture. Despite the simplicity of the C3 method, reconnaissance missions can and do sometimes go off the rails if

not managed properly. As stated earlier, this method offers a quick and easily digestible way for recon teams to stay on course. So, l.et's take a moment to unpack each of these phases and examine a little further.

Contact

The primary step during the execution phase of a recon mission is to make contact with the target or targets. Contact can happen in several ways depending upon the objective. However, most missions start out through surveillance from afar. This could amount to the team watching the movement of people as they come and go from a targeted building. It could mean using Google Earth to capture aerial photos of the target. Making contact, in another example, could mean engaging in conversation with a targeted person with the goal of surreptitiously obtaining information from them.

Alternatively, making contact could mean using covert methods of entry to break into a building under the cover of night. Essentially, making contact is the first step in what we caU active reconnaissance and marks an important delineation between recon planning and recon execution.

The contact phase is important for another primary reason. If the recon team is seen doing something suspicious by an onlooker or an employee, the recon mission could be compromised. Depending upon the circumstances, the entire operation could be compromised in a manner significant enough to warrant aborting it altogether. So, the introduction of this significant risk should not be taken lightly, and the team should proceed with caution.

We will discuss how teams should exercise caution during the contact phase later in this chapter.

Conceal

Next in the Recon C3 method is the conceal phase. It is important to note this can mean many things depending upon the recon objective. However, in most scenarios red teams quite often hide their physical presence under the cover of darkness while taking photos and video of a

target from a distance, for example. Yet in other situations, operators may make their presence known to human targets, but might be concealing discreet recording devices in order to capture recon intelligence of importance.

As I stated earlier, it is very common to conduct recon missions in hiding. This can happen from outside a building, incognito in front of people, and so on. In nearly all situations, clothing becomes among the most valuable concealment tools. Wearing camouflage outside an industrial building is no different, in principle, than wearing a business suit in a corporate environment. In both situations, the objective is to blend in without drawing attention. The same concept is applied to discreet tools, such as a pen camera or an eye-glasses camera. Thus, the concept of concealment often relates both to the red team operator herself and the tools used to acquire intel.

Capture

The capture phase is fairly straightforward and is the end goal in any recon mission. No, we're not capturing hostages. We are capturing information, by video and photo, that will. allow us to analyze and make predictions about where there might be vulnerabilities.

The information we capture almost always includes the following:

- Physical security controls (fences, barriers, cameras, entrances)
- People (attire, traffic patterns, civilians vs. employees, roles)
- Places (surrounding businesses, cafes, restaurants, traffic)
- Terrain/Weather (urban, rural, sunny, snowy, desert, rocky)

Analysis performed at the capture phase feeds the rest of the REDTEAMOPSEC process and gives light into the operation's specifics such as: how, who, what, when, and where.

With that brief introduction of the C3 methodology, let's strap in and dig into the heart of recon mission execution.