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. **T**eam 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.

Executing Recon Missions

We have the simplicity of the Recon C3 method to use as a high-level guide during execution. Worth mentioning is, each of the three Cs should be carried out from, at least, two physical vantage points, from afar and up close. Simple, right? I typically refer to this as long-range recon and short-range recon. So, as we step through each of the three Cs, I will divide the action steps into long-range and short-range categories. Let's get started.

1. Contact

Beginning with the first of the three Cs, let's examine the contact phase first.

Long-Range

The first, and arguably the easiest, contact to make is through the internet. Earlier we discussed using open-source intelligence (OSINT) sources to find information about a target. I'll outline several OSINT resources here to help achieve valuable long-range recon. You will conduct this leg of recon from your office.

Company Websites

Scouring your target's website is an obvious first step, and it usually pays off handsomely. Search engine optimization (SEO) experts advise companies to post unique and feature-rich information not only about their business but their culture. In a show of corporate transparency, interior photos,. employee pictures, offices, hobbies, and even musical tastes are shared there.

For all the reasons stated, re con tea ms should scrape the company website in search of a range of topics. I suggest searching and documenting the following information:

- Location address(es)
- Employee names, email addresses, phone numbers
- Technologies used {Careers page)
- Social media accounts

- Photos of exterior and interior spaces

Advanced Google Search

Advanced Google searches are also called "dorks" by those who use them often. What's it all about? Well, it's a way to use Google's advanced search options to find more specific information about something. A dork is a string of text containing advanced search parameters that Google's search engine interprets and displays for you. It's common to use a Google dork to search for Microsoft Word files that contain certain keywords, such as your client's name, for example.

I recommend searching for Microsoft Office file types in conjunction with your target's URL. For a list of Google dork syntax and more, please see the following resource: https://www.exploit-db.com/google-hacking-database

I suggest searching your client's name in Google and then clicking the Images tab. I suggest using your client's name and location as search keywords. This search alone can provide some amazing intel. Google Earth is a great resource for providing an aerial view of the target. There is not a single operation where we have not used Google Earth in some form or another.

Here is what you should be looking for:

- Entrances, parking lots, recon vantage points
- Surrounding structures and businesses
- Any images showing the interior
- Any visible security controls in place (internally, externally)
- Surrounding terrain
- Any metadata to determine the image's age

Job Portals

Job boards can give away a great deal of information about the company's security maturity. You can use sites like Indeed.com and Dic.e.com to gain information about the technologies used by the target.

This would be especially useful if your physical red team operation has an element of technical penetration testing involved.

Here's what you should be looking for:

- Company infrastructure and job roles (Physical security role?)
- Tech stack (Windows versus Mac)
- Security posture/practices
- Contact information (phone, email, names)

LinkedIn

LinkedIn is a great resource to find information about individual targets. At the time of this writing, LinkedIn has an option to upgrade an account with more features. I suggest upgrading so you can view any Linkedln member and so that members won't know you viewed their profile.

Here is what you should be looking for:

- Important staff members, roles, location, and responsibilities
- Staff's previously held jobs
- Peers
- Staff interests, education, and accomplishments Facebook, Twitter, & lnstagram
- Company culture, news, initiatives
- Employee manner of dress (casual, business)
- Emails, phone numbers, staff names
- Interior photos
- Job openings

Short-Range

Short-range contact is made by the recon team making their way to a physical location near, but not at, the target recon areas. This first position is called the staging area.

An ideal staging position should be taken up near the target recon area but far enough away to allow for the team to meet without arousing onlooker's suspicion. In rural and less dense areas with minimal coverage, the staging area may teeter between a short driving distance and walking distance. In more urban areas, the staging area is usually within walking distance and around corners or in alleys .. The recon team should make a few passes around the selected staging area and recon areas to re-evaluate their viability. My personal recommendation is to use a dark-colored passenger van with ample space to stage from.

The staging area should be considered a safe zone, but at least one member should be cognizant of their presence to onlookers and move to another location should suspicions rise.

Once at the staging area, the team should meet and finalize details before taking up their next recon positions. This is often an opportune time to review recon goals.

Staging Area

The image above depicts a large building, our fictional target, and illustrates one possible staging area behind several long rows of cold storage buildings. This staging area is ideal for its vehicle cover and less visible approach from the rear of the targeted building. Recon of all locations should happen during the day and at night in an effort to capture the most comprehensive intelligence possible. Most often, the same staging area position can be used during both nighttime and daytime.

2. Conceal

At this step, the recon team must stage for concealment. Operators must adapt their clothing according to:

- Time of day
- Weather/terrain
- Recon goals

Time of day matters in rural areas where there is less lighting and less structural cover .. At night, black tactical or dark camouflage may be better here. This type of clothing at any hour in an urban setting around people should be avoided unless the team feels highly confident they can avoid bystanders. In areas of rough terrain, combat boots by 5.11 Tactical are essential. A wide array of ripstop clothing can be found in tactical and everyday fashion form as well.

Ultimately, recon goals are the largest predictor of clothing requirements. What is the information you're after and how will you get it? Sometimes it means walking right up to somebody and talking with them. Occasionally my team will engage in conversation with bystanders or even target employees. In every single one of these situations, we wear street clothes. So again, the goal will make the garb.

Naturally, team members use tools to capture recon intel. Sometimes they use discreet cameras hidden on their body while other times they use a video camera hidden in a shoulder bag. In every situation, the goal is to get close enough to make the determination that a vulnerability exists.

Having video footage to study later helps tremendously in making that determination.

Bag containing hidden camera.

The photo above shows a shoulder bag that was built to conceal a hidden camera inside. Concealment tools and tactics like this enable operators to capture recon intel in open areas without drawing unwanted attention.

Figure 9 shows another team member using an everyday laptop bag to conceal a portable RFID reader. As he made his way through the office, he managed to capture and later clone the RFID badges of individuals with high-level building privileges. These badges were later used to make entry into the facilities at night.

How and what to conceal depends upon the recon goals defined earlier in this process. The options are endless and are limited only by your

imagination and creativity. That said, I want to provide some concealment tactics and tools that my team uses on a regular basis.

Vehicle Hide

Your team should take photos of the location from a distance. My team almost always does this from the recon vehicle. Earlier I recommended a passenger van. Passenger vans have many windows providing multiple vantage points and space to move around.

A vehicle hide consists of window coverings that prevent outside light from coming in that could potentially expose the photographer while providing just enough space for the camera I.ens to poke through. You've seen these in spy movies, I'm sure. They can be fashioned with scissors, a black bed sheet and some double-sided tape. Cut the black sheet into sections large enough to cover all rear windows and use the double-sided tape to attach the top and bottom areas of the sheet to the interior. A hole can be cut into the sheet just big enough to poke the camera lens through. Vehicle hides help tremendously in avoiding detection.

Bag Hide

Figure 8 illustrates a great example of using a bag hide to conceal a camera inside. In this example, we cut out a nickel sized hole in a shoulder bag and poked the lens of a Go Pro camera through it.

Phone Hide

If your coat or shirt has a breast pocket, simply put your smartphone in video record mode and use it to capture video evidence. Most smartphones come equipped with a camera at the top of the device making it an easy way to record video from your shirt pocket without drawing attention.

Hand Hide

On several occasions, I have covertly cupped a GoPro camera in my hand as I made my way past a facility. These small form factor cameras make it super easy to take video, and quickly stash it in your pants pocket.

Pen Hide, Button Hide, Glasses Hide & Other Discreet Cameras

There are online marketplaces, such as Amazon. com, that are full of discreet cameras too numerous to be listed here. Some of the cameras I've used include pen cameras, button cameras, and eye-glass cameras. These cameras are generally useful only in good lighting and within dose proximity to the target. Consider investing in at least three discreet cameras in various form factors. Each has their advantages and disadvantages and should be used in appropriate situations.

3. Capture

The capture phase marks the last step in the Recon C3 method. To add clarity to this critical phase, please consider the following process diagram.

Figure 10. EDECE Process for Recon Capture

Figure 10 shows the five-step EDECE Methodology (pronounced "ED-eh-see"} for the capture phase of recon missions. Let's unpack the EDECE method as we step through our recon mission.

Long-Range

Establish Rally Point

A rally point is a physical location where the recon team will go to once their recon mission is completed or aborted. In the case of multiple operators, there may be several rally points depending upon the location of the operators. In our example, there will be only one rally point.

The red team leader is almost always positioned inside the recon vehicle at the rally point. This is where she will command the team and communicate with the client throughout the mission. A good rally point is one that places the vehicle close enough to provide eyes-on surveillance of the target, yet far enough away to go unnoticed. Operators should be able to walk to the rally point without difficulty and without arousing suspicion.

Selected Rally Point

The red team leader must then communicate the location of the rally point to the rest of the team and to the client. Next, the team should get ready for deployment into the field.

Deploy Team

Before making the trip to deployment locations, an equipment check and a communications check should be performed. Radio communication is recommended for night deployments, while smartphones and Bluetooth

earbuds are recommended for daytime deployments when around people. In daytime situations, it helps for the entire team to hop on a conference call.

Deployment Areas

Team mobilization is made toward each deployment area in numeric order. Operators should be deployed in a staggered timeframe with at least five to ten minutes in between. See Figure 12 for ideal deployment positions in our example. Deployment positions should be selected for their close proximity to the target while providing cover for the operator's exit from the vehicle. All operators should exit from the passenger doors as opposed to the van's rear doors. Rear door exits often look suspicious to onlookers.

Deployment positions should be selected so that their vantage points offer the most physical. coverage of the target. Notice in Figure 12, each operator is deployed from opposite ends of the building. Immediately before exiting from the recon vehicle, the operators should:

- Have their authorization letter and ID present
- Perform a communications check (phone or radio)
- Perform a gear/tools check
- Switch their video capture gear to record
- Communicate to the client that recon is about to start
- Take a deep breath and try to relax

Short-Range

Engage Target

Each operator should have at least one hands-free discreet camera or body-worn camera in record mode to capture the target's exterior as they approach the target. The footage from these vantage points gives additional visibility and oftentimes helps uncover security controls not previously noticed from afar.

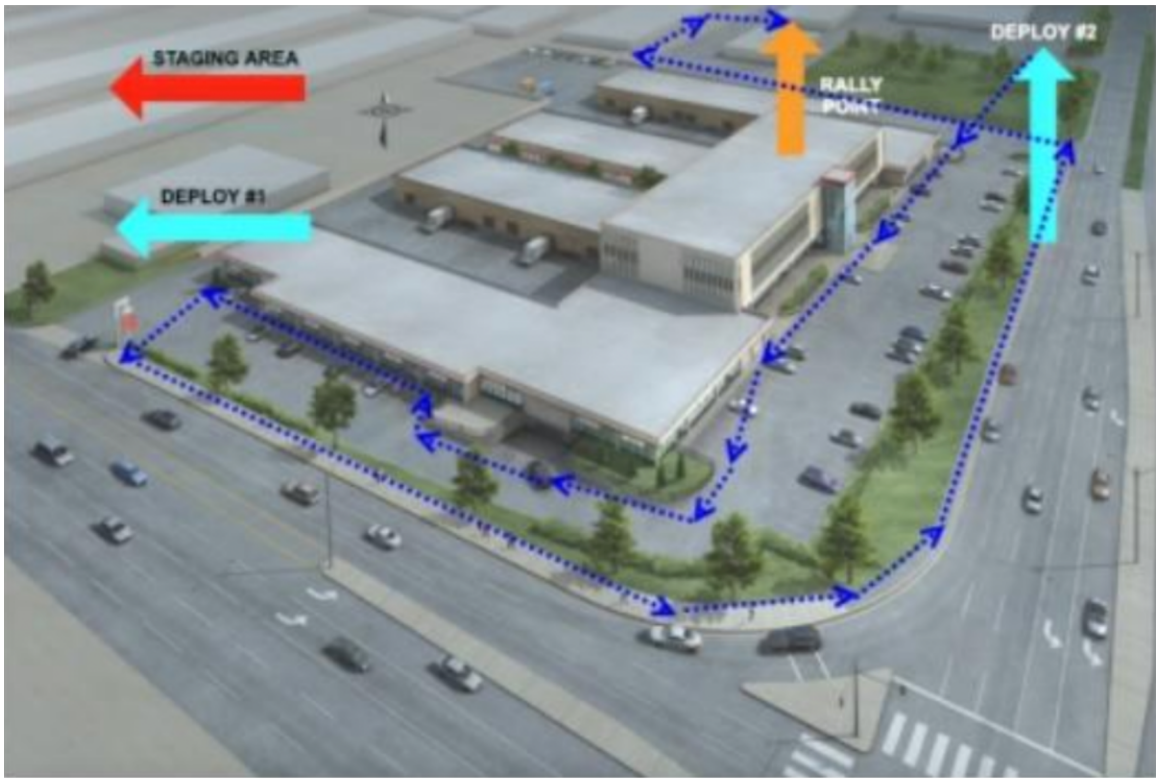
A second camera should be available and aimed at fulfilling their recon goal. From my experience, this second camera is typically a GoPro stashed away in a pocket, an iPhone, or a pen camera. You want a device you can quickly grab to capture intel and then stow it away as necessary.

In our example, let's refer to the operator deployed at location #1 as operator #1 and so on. Operator #1 should make her way along the designated route. Refer to the dotted pink line shown below.

Operator #1 Recon Route

Operator #1 's goals are to capture physical security controls installed to the rear of the building. The loading docks are of significant importance since very few access controls are present there. A large sweep of the rear with a hands-free camera will provide useful footage to review at a later date.

Operator #1 must maintain contact with the team and alert them of any onlookers taking an interest. She should also indicate whether the scene is clear to deploy operator #2.



Operator #2 Recon Route

Operator #2's route shown above has her hugging the front and west sides of the target. She will then travel along the sidewalk along the highway then veer north to capture the east side before reaching the rally point.

Capture Intel

Each operator will have one or more areas of interest that she will likely pause to observe and record. These recon goals will vary from operation to operation. That said, here is a viable list of recon goals the team in this example would likely try to capture.

Operator #1 (Refer to Figure 13)

- ✓ Loading dock doors, trucks, dock entrances
- ✓ External lights and their focal points
- ✓ Cameras, motion sensors, motion activated lights
- ✓ Barriers, fences, walls

✓ Entrances and signage
✓ Entrance locks
✓ Surrounding activity (foot traffic, vehicle traffic)

Operator #2 (Refer to Figure 14)

✓ Lobby, lobby doors, lobby security controls
✓ Lobby activity and personnel (receptionist)
✓ Office activity, employees, manner of dress, roles
✓ Vacant offices to the west
✓ West side office doors, locks, physical security controls
✓ External lights, internal lighting, and their focal points
✓ Cameras, motion sensors, motion activated lights
✓ Alternate entrances, locks and signage
✓ Surrounding activity (foot traffic, vehicle traffic)

Some of the goals here can be captured by simply walking past the area with a camera. Yet other goals, such as examining locks, often require the operator to stop and record. For these stop-and-record situations, I recommend faking a phone call while walking slowly near office windows and while you walk up to video record door locks. The more distracted you appear, the more likely you will not be called out by an onlooker.

Here are a few false scenarios you can use for stop-and- record situations:

- Distracted telephone conversation. Use this scenario to walk slowly and occasionally stop to capture recon. Be animated as you talk and use your hands to gesture.
- Walk, Stop, Text. Stop and position your camera to record the desired area while you pretend to type out a long text message.
- Enter the office and ask for directions. Ask directions to a nearby restaurant or cafe and capture footage of internal spaces. Be careful

whenever approaching targets face-to- face this early in the operation.

- Mistaken delivery. Fake a pizza delivery to the office while you capture footage of internal spaces. This usually provides more time on the inside as employees hunt for the owner of the pizza. Select an independent pizza restaurant and be sure to dress appropriately. Again, be careful whenever approaching targets face-to-face this early in the operation.

These fake scenarios, or pretexts, can be adapted to fit many different recon goals. They can certainly become more aggressive depending upon the need to penetrate deeper into the facility.

As I have mentioned previously, a second tour of recon capture should be made during nighttime hours. Since most business offices are closed around the midnight hour, this second tour will have a slightly different focus.

Here are some common nighttime recon goals:

- Target activity (cleaning crew, overnight security), if any
- Surrounding activity (foot traffic, vehicle traffic)
- How well-lit is the target and where are the unlit areas?
- Locations of motion-activated lighting, if any
- Viable infiltration points based on these Factors

The security posture of a facility can drop significantly simply by the time of day. As a direct result, most red team infiltrations are attempted during the wee hours and thus it become increasingly critical to estimate just how much the environment changes.

Exit to Rally Point

Things can sometimes go sideways during recon execution. To prepare for the unexpected a backstory, or pretext, is necessary. Each recon operation must have a plausible explanation in the event of a compromise.

For believability, each operator must rehearse and become comfortable reciting their backstory with confidence.

Communication amongst the team is important, Largely when a team member has been or is about to become compromised. The red team Leader must make a snap decision in response. Usually, the red team leader will give the other team members the command to exit quickly and gracefully. This is done to minimize the likelihood of further compromise leading to complete mission failure. The uncompromised team members should then make their way to the pre-determined rally point unless directed otherwise.

In contrast, upon successful completion of the recon goals by the team, each operator should communicate to the red team leader accordingly. If the red team leader feels the recon goal has been met, she should give the command to exit to the rally point. For large recon coverage areas, there may be several rally points but, in most cases, there will be only one pre-determined rally point.

When the exit order has been given, the red team leader should stagger exfiltrate procedures so that the entire team is not seen leaving all at once. As a rule of thumb, the operator who faces the highest likelihood of being compromised should be exfiltrated first and so on. Each operator should follow the pre-determined exfil route as planned, unless conveyed otherwise by the red team leader.

Before leaving their position, each operator should perform a quick equipment and tools check to ensure nothing is l.eft behind that might indicate their presence. If necessary, steps should be taken to cover any physical tracks. That said, our ground coverage at this point is considered light and non-intrusive when compared to the operational execution. We will discuss covering tracks in greater detail Later in the REDTEAMOPSEC method.

The team should make their way to the rally point calmly and in the same manner as their initial approach. The team should enter the vehicle through the passenger door and move to the rear allowing any following

team members to enter similarly. Once all members have returned to the recon vehicle, the team should perform a more detailed equipment/ tools check to be sure nothing was left behind. As the vehicle departs the rally point, all team members should immediately document their findings and observations while they are still fresh in memory. Some of my team's most telling observations were incapable of being caught on camera, so it's very important to have note-taking supplies, paper tablets, or laptops handy. By now, the red team leader should communicate to the client that the team has completed the mission and has departed the target location.

A recon debrief session should be held once the team is able to meet and discuss their observations, photos, and video. Each operator should provide an overview of their recon goals and go over their related recon findings in detail with the team. The red team leader should compile all of the recon footage, photos, and notes as each operator presents their findings. This data will feed into the next phase in the REDTEAMOPSEC method as deep-dive analysis takes place and preparations are made for progressing through the operation.

The next phase of the REDTEAMOPSEC methodology is called Direct Preparations and is central to transforming raw data from the recon mission into valuable information.