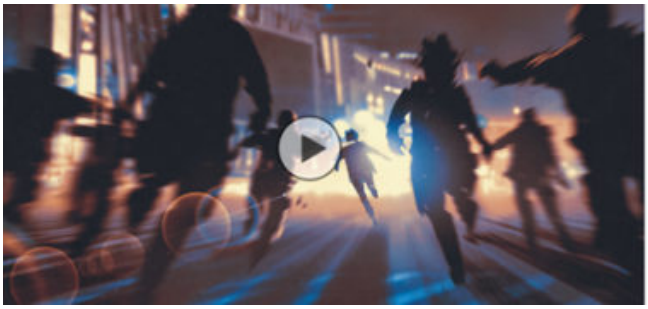
# What Survival Red Teaming Is And How You Can Use It

- *Survival red teaming is a tool to test the security of homes and retreats, plans, & SOP, exposing vulnerabilities, which can then be corrected.*
- *The red team must not get so focused on killing things and breaking stuff that they neglect to record all vulnerabilities exploited. The entire exercise is for not unless vulnerabilities are eliminated.*
- *The end result of red teaming is to improve blue team security. Therefore, the red team should stick around to debrief the blue team and help fix vulnerabilities discovered. Red team expertise aids this process and any adversarial nature tends to evaporate when exercises begin with the end in mind.*
- *While you may not be able to run a red team exercise today, you can get started, which should not be overwhelming. So, take a moment to get started.*

Military, organizations, operations, and plans are challenged by trained, educated, and practiced teams to improve effectiveness.

**"Red Cell members demonstrated the vulnerabilities of military bases and would regularly use false IDs, jump fences, barricade building, take hostages, and kidnap high ranking officers and admirals. Additionally, Red Cell planted bombs near Air Force One, snuck into submarine bases and took them over."** – Wikipedia



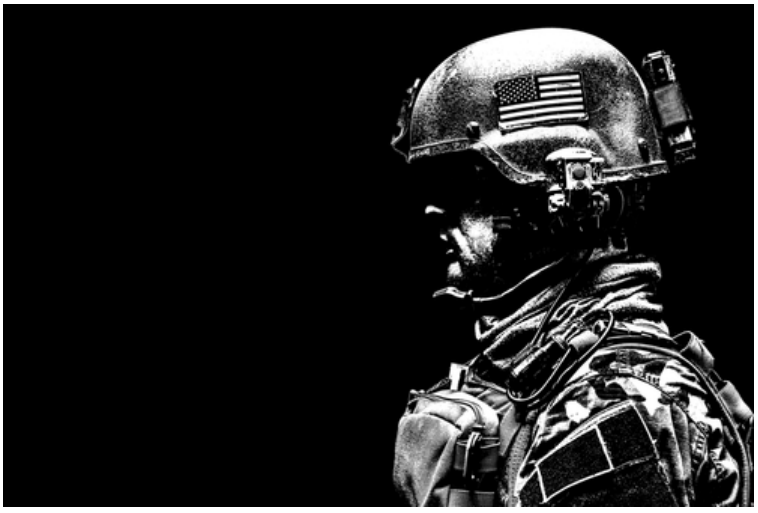


In the context of business, a red team penetration tests test the security of an organization or entity, revealing vulnerabilities and risks and highlighting exposure to that risk (such as costing the company money or making it look bad), to the end of reducing vulnerability.

## Applying Red Teaming to Survivalism

In the context of survivalism, survivalists and survival groups can benefit from the practice of red teaming by revealing susceptibilities in OPSEC, PERSEC, SOP, plans, technology, and the physical security of fixed sites, and then taking steps to reduce vulnerabilities revealed by the exercise. This could take the form of a mock attack on a survival retreat or homestead during a simulated catastrophe or could simulate a home invasion that occurs out of the blue.

## Survival Red Teaming



Survival red teaming exercises should include the following

elements:

- **Define the Scope** – What aspects of security will be tested? The blue team is important to you? I might care about privacy, but another person might not care about it or the scope of a single exercise may be limited to only include physical security due to limitations of time or money.
- **Assemble the Team** – Ideally, the red team should be a trained, practiced OPFOR (Opposing Force) including specialists skilled in the penetration of physical security, the use of social engineering to get what they want (they want blue force personnel to depart from SOP) and technology specialists or PI's skilled in penetrating the compartments of alternate names (callsigns, usernames or pen names of survivalists used to protect their identities) and legal names, tying the two together.
- **Reconnaissance** – The red team recons the fixed site, blue team, and their online footprint collecting intelligence and analyzing it for vulnerabilities.
- **Penetration Test (Kill People & Break Stuff)** – This is the fun part. The highly skilled red team operators get to do what they do best: penetrate the blue force's security by exploiting any vulnerabilities they find. Within the scope of the exercise, the red team should be allowed substantial latitude in achieving their objective.
- **Debrief** – How did the red team penetrate security? To what lengths did red team members have to go to get a member of the blue team to give them a guided tour? The red team's job is usually easier than most people would think because people just don't want to believe others could be bad guys and are averse to challenging them even when they do. IT security usually isn't much harder, not because of shortcomings of the technology, but because of the shortcomings of personnel in sticking

to SOP and information security best practices. Finally, physical security is also often easily penetrated because people leave doors unlocked, installers install locks improperly and manufacturers design flaws into security products. This is all about disclosing the discovered vulnerabilities to the blue force, so effectiveness can be improved.

- **Implement Changes** – Fix the vulnerabilities.

In 1932, Rear Admiral Harry E. Yarnell read teamed Pearl Harbor, demonstrating basically the same tactics the Japanese would use to attack it in 1941. The US Navy's assessment?

"It is doubtful if air attacks can be launched against Oahu in the face of strong defensive aviation without subjecting the attacking carriers to the danger of material damage and consequent great losses in the attack air force."

The rest is history. I hope your assessment isn't like the US Navy's assessment because, if you're happy with your defenses, so is the enemy. When red teaming reveals the chinks in your armor, don't pat yourself on the back and say you're good. Fix them! Unless you shore up the vulnerabilities that a red teaming session reveals, the exercise is for naught.

Therefore, survival consultants and coaches engaging in red teaming exercises with clients would do well to stick around for a few days to help implement solutions to the vulnerabilities the exercises reveal. Without that follow up, the clients may not get their money's worth.

- **Rise & Repeat** – Even one red teaming exercise is sure to reveal many vulnerabilities and correct them, but you won't know for sure that they are corrected unless you run another exercise and the red team fails to exploit them, but in most cases, the red team will still succeed by exploiting less obvious vulnerabilities which should also be eliminated. The more red team exercises you

complete, the more vulnerabilities you will eliminate and the wider the scope of the exercises can become.

## Benefits to Physical Security

Nothing is going to beef up your home or retreat's physical security like having a bunch of your ex-Special Forces buddies attacks it. If you don't have ex-special forces buddies, make a deal with a nearby survival group. Depending on the level of trust they deserve, you might even enter into a mutual aid agreement to reinforce each other if called upon to do so and help each other test security. You will need a basic understanding of one another's security to do this, so why not red team each other?

## Importance of Scope

The scope of the red teaming exercise sets limitations and the scenario to avoid mission creep and keep the exercise realistic on schedule. If the object of the exercise is to test a household's plan to deal with a peacetime home invasion and the red team attacks it with a tank-mounted flamethrower, they missed the scope and the exercise won't be of any use to the blue team. The objective is to improve the defenses within specified budgetary and time constraints. Due to the creative and proactive nature of red teams and their passion for playing their role, inexperienced red team members sometimes

lose sight of the objective. If the scope is for the team to infiltrate a military installation, the latitude will be substantially greater.

## Recon Phase

If the scope of the exercise includes testing the physical security of the fixed site during the absence of rule of law, the reconnaissance phase will involve the red team finding the most effective routes of approach and locations for hides, so they can count the number of retreat members, observe their schedules and take stock of defenses, carefully documenting details with notes, photos and video for the attack, debriefing, and follow-up phases.

If the scope includes OPSEC/PERSEC in the presence of rule of law, the recon may be more along the lines of hacking, social engineering, and covert entry techniques to perpetrate a home invasion, kidnapping or to steal firearms and emergency preparedness gear the blue team has displayed on social media.

They will find the best places to conceal cameras to observe the retreat or security patrols and patterns. They will listen to analyze radio communications. Given enough time, they would eventually be able to learn a great deal about a group that uses radios for routine communications. They will watch for the changing of the guard and whether the approach of guards to their observation posts are visible and note the positions of the posts themselves. They will note the condition, equipment, bearing, and level of training of personnel and try to determine their functions. They may well be able to pick out who leaders are by their body language such as pointing or placing hands on hips as they direct others or because they are shadowed by an aid or radio operator. They will try to see whether fighting positions incorporate aiming posts and look for dead areas protected from direct fire from those positions where they can make a safe approach.

In a presence of rule of law OPSEC/PERSEC exercise, if a blue team member has uploaded unredacted photos of pocket dumps to social media, the red team may simply make their own copies of keys in the photos for the attack phase which they will use to let themselves in because, thanks to lax PERSEC, they now own the place.

If the site is a hard target, the red team may probe defenses with a “false alarm” to gauge response times and to observe whether QRFs (Quick Reaction Forces) muster and their numbers.

## Attack Phase

The attack will ruthlessly exploit any vulnerabilities discovered in the recon phase and put the SOP, planning, and training of the blue team to the test. If dead zones were discovered in fields of fire, they will approach unmolested. If the red team was able to identify the leader, they may create a ruse to draw him and shoot him at the outset. If the retreat lacks night vision, the attack may come during the night when most of the group is asleep and it will take longer for them to respond.

In the presence of a rule of law scenario, the red team may exploit stolen phone bills from mail or email to spoof phone numbers and impersonate members of the organization to gain entry. If mail or packages are delivered to the home address,

a red team member may dress as a delivery worker with a package and a scanner to get a naïve household member to open the door for them. They may pretext a mother by calling her while her child is at school, tell her there has been a school shooting, and ask her to identify her child to throw her off balance to get needed information such as a phone number or SSN.

## Debriefing, Follow-up & Repetition

While it is easy to focus on the attack of the red team, the objective of red team exercises is to improve the effectiveness of the physical security of the blue site, its technology, leadership, planning, SOP, and the execution of that SOP by blue team personnel. One of the first payoffs is learning where an enemy will most likely attempt to recon your site from, thus enabling you to deny them access to that area by installing obstacles, booby traps or sensors, removing cover or concealment, modifying observation posts and fighting positions to cover them with overlapping fields of fire or by aggressively patrolling those areas. The exercise may also reveal methods an enemy may use to conduct reconnaissance, enabling you to take countermeasures. You may learn that your locks aren’t installed properly or that unless alarm keypads are cleaned, and codes changed regularly, it is easy to see which keys are pressed, greatly reducing the time needed to find your code.

Whatever vulnerabilities are discovered, they must be corrected, and the exercise should be repeated to verify that the vulnerabilities have been eliminated and to expose new susceptibilities, so they can also be corrected. The effectiveness of security measures improves as it is put through more cycles.

# Technology OPSEC & PERSEC

Technology has advanced so quickly that PERSEC (Personal Security) and privacy are violated so routinely and thoroughly that I'm sad to say that many survivalists don't even believe they are still universal human rights and won't lift a finger to protect their own privacy. The truth is usually simply that they're addicted to convenience, just like the millions of other sheeple in the "Land of the Not Quite so Free as it Used to Be."

If you value convenience over privacy in the extreme, why prepare at all? It's more convenient to just roll over and die than to engage in inconvenient and responsible pursuits like being prepared or striving to become more antifragile. If this sounds like a rebuke, it's because most survivalists could benefit from a little "tough love" regarding the measures they take to protect their personal privacy.

Survival PERSEC and OPSEC are mostly about compartments your legal identity from your identity as a survivalist and conceal the extent of your wealth and preparedness. True, you could bear your teeth and fangs straightaway in the hopes that you're too hard a target for anyone else to take on, but you're throwing Sun Tzu out the window. There's always a bigger fish out there somewhere.

Taking reasonable precautions to limit your online and physical profiles makes you more effective at surviving because it gives you options. It is the versatile and adaptable that survive and you need options to adapt. If you must reveal your teeth and fangs to protect yourself someday, you still have that option, even if you normally choose to conceal them.

## People & SOP

Red teaming exercises find lapses in SOP and the execution of SOP by personnel. In the world of security, it's seldom necessary to use brute force to pluck the low-hanging fruit because we are creatures of habit. We evolved to feed ourselves expending the least amount of energy necessary. When we pick a trail, it's nearly always the path of least resistance, which makes us very predictable unless we choose not to be. It isn't necessary to crack encryption when people are careless about information security and a home invader doesn't need to kick in your door if he can get someone to open it for him. Most often than not, a criminal with mediocre social engineering skills and a clipboard can talk someone into opening a door. Properly done, red team exercises bring SOP vulnerabilities like these homes with gravity and then fix them.

## Planning & Execution

Does everyone in your household or retreat know the plans? Are your plans simple enough to succeed? Are they adaptable to the types of tactics real enemies would likely use? Is your communication effective enough to implement changes on the fly? Do you have backup plans in case you come out on the losing end? Is the tradecraft of your operators adequate to execute plans and not get followed to rally point if everything goes sideways? While it's probably going to be

tough to answer some of those questions without the benefit of experience, realistic war gaming exercises will give you an idea and a starting point.