Red Team Activities in the Virtual World

The art of delivering opposing force activity in the closed loop environments of the modeling and simulation world of Cyber Ranges

Thoughts from a leader in the Field

J D Lovett

Creator of the DoD Cyber Security Range (CSR)

Technical Director (2009 – 2017) of the DoD CSR and MCCR

Consulting SME, Labs & Ranges, STAHL Consulting LLC

So, you have made the decision to build your own cyber range and now you want to determine how you will add the red team activities to it to increase realism or to simply support events where red effect is needed. There is a myriad of challenges to overcome and most labs/ranges across the country still don't do it very well.

Simply adding a technical professional with hacking skills is not the answer, but it is a good step in the right direction. More important though is building red teaming into the range design, not trying to bolt it on after-the-fact. Ranges that do this end up with a poorly architected system that barely deliver red effects and often does it so poorly the Warfighters can see it coming a mile away.

System design is the single most important aspect of creating a range as it affects every aspect of the coming events; it affects the ability to deliver services, implement changes, run concurrent activities and it greatly affects how you staff the operation. I share this with you to give you pause – now take that time to re-consider what you are planning and put a new perspective in place to allow a thoughtful review of the current plan.

Virtual World

Creating an expansive virtual world to mimic a chunk of the real Internet is one of the most fun undertakings a technical professional can perform. Why? It feeds several key aspects of their professional minds; their desire to learn everything about networks, the ability to build a perfect system, their desire to learn new things (all things network) and their desire to be a well-rounded professional, though we all have a different perspective on that focus. Building a virtual world is so fun as it can always be expanded upon to increase the level of realism. It could be a life-long task in a professional's home lab, just like some people create scale models of their favorite places.

As I mentioned above though, it's very important to understand the scope of the build before you begin. That's not to say don't build everything; instead, I'm saying don't build everything in this stage of the build. Keep each build phase focused on specific achievable goals and as you achieve them, wrap up this stage and then consider what should be included in the next phase. With this in mind, begin to focus on your red teaming and the planned activities for the build. Identify which parts of the red need to come first and then what should follow in each additional build phase.

Internet is built in regions

Now if you are building a huge virtual world to mimic activities that come from different regions of the world, it's important to remember the Internet is built in regions. Yes, there is a backbone and root services but in terms of red teaming – the activities we see as a Warfighter are a function of the professionals within specific regions of the globe. The activities have styles that

are unique to them as much as the regions have inherent tools and architectures; and these too are used by those red professionals to achieve their goals.

Remember, IP addresses are registered to companies, organizations and governments by where they are in the world. It's always good to be able to replicate a little of the transport aspect of the IP schema by creating even a simplistic regional structure. And if you are doing a lot of training with high-level professionals it's the only way to allow them to maintain training value; anything to simplistic will be a waste of their time. Consider whether you need to craft an ASP/ISP architecture to provide the appropriate training value. You know that ISPs give network access to companies and such. Well, ASPs provide backbone to ISPs so they can use it for their customers.

This is where a high-level red practitioner is needed to assist the design team in the manner of tools that need to be portrayed as well as corresponding architectures. Remember, not everything has to be included. Also remember that some items are more critical than others and should come first. Secondary items can be part of following phases. Take the long-view as you prepare the system build but don't short-change the system at the start.

Limited build

Ok, you've been asked to build a red team function but you're only authorized to build a simplistic red architecture inside a simple virtual world. This is not uncommon; it happens every day across the world as IT and Cyber departments decide how to respond to a specific event. The answer invariably is to build a simple model to better understand what happened and how it can be prevented. My advice in this instance is build a simple model, bring in the "live" attack and let it run. You'll need to feed it what it needs; DNS, default gateway, specific IPs, specific protocols. And capture everything that occurs and begin the deconstruction of the activity and the attack.

This is actually a great first activity to accomplish to better understand how red activity works and what needs to be built to re-introduce it into a virtual world to actually leverage it for training purposes. You'll be surprised by the number of services you have to create to allow the attack to progress. This will feed your desire to learn how better address models in the future. Which makes it a great learning activity.

Dark web

The phrase "dark web" means different things to different people or players. Some professionals style themselves Ninjas hiding in the shadows to catch an enemy unawares. To them it's just another set of shadows to hide in. Others consider it a "dark" place where evil gathers to spring upon the righteous (I kid you not). Still others simply consider it an unlit room where the owners have simply decided to not turn on the lights to illuminate the space. As you'd expect they don't want people just wandering in and browsing their stuff.

In Internet-speak, it's architecture that is not listed in the domain name servers (DNS), so it is not reachable via the web browser using a search engine. Instead, the owners and users of this space keep their IP addresses in their mind or written in notes they keep hidden. The goal is simply to keep it from being advertised; how the Internet normally works. Dark space owners have to share their addresses with anyone they wish to support, usually after money is exchanged. It should also be noted that some things that are commonplace now, started on the dark web and won some sort of wider acceptance, so they became part of the normal Internet; Internet funds (like Bitcoins) and VPN architectures (the Onion) are good examples.

The dark web can be a key component of your virtual model if you planned to do wide-ranging red and/or will be supporting the training of high-level defenders. The dark web is a whole uncharted architecture within the Internet where people, companies, organizations and also governments have stashed millions of specialized tools, servers and capabilities to keep it out of plain view. And not just the bad guys use the dark web.

The "good guys" have known about it for decades and place tools and capabilities there as well. In fact, many older Internet professionals will tell you stories of "dark web" use during the 70s and 80s before the Internet became a known thing. That would make some of those good guys the original users of the "dark web". Of course, the phrase "good guys" isn't very helpful as perspective typically determines whether you consider them as good or bad. I'm sure that as of right now the content of the dark web isn't so lopsided a split as most folks would think.

If you plan on building a model where the red team acts widely across the system, you will need to create some dark web of your own. Partly, to hide the tools of the red team out-of-plain-sight and partly to make the users search for the goods. Additionally, you will want to determine how many dark web activities need to be replicated to support planned event types and styles. My advice is simple here – don't build more than you need, but build enough framework to allow for regional flair. Also remember a vast model isn't built overnight. There will be more build potential later, to extend your dark web needs.

You cannot forecast your punch

A common problem across the cyber range community is forecasting your punch; not properly disguising activities which allows high-level defenders to quickly identify the red effects. This is also a common problem with new hackers; they don't know enough technique to operate without being quickly recognized. Before I built the DoD Cyber Security Range (CSR) I would attend different cyber exercises (sometimes as a visitor and sometimes as a Warfighter) and the common refrain was the event was over on day 1. Why? Because the defenders turned on their tools and captured packets for analysis. They quickly determined that the traffic being generated (to make the system look like it has hundreds of users) all looked the same. Every regular packet was the same size. A quick filter was then added to the tool to only show traffic that wasn't that size. What wasn't that size – the red traffic.

Ok, so not every defender knows how to Analyse traffic and create a filter to highlight it, true. So, if the low-level players don't have access to a higher-level professional to help them with problem escalation, they could still have some meaningful time inside this virtual world. That's a pretty poor way at looking at a cyber range or any type of model...And when you consider most defense teams have team leaders with wide experience, the argument falls apart pretty quickly. Sadly, there are still ranges that operate this way today – and it's 2021.

I should also note that is a tremendous number of new tools bringing better "user" automation to lab environments (and to cyber training systems) to better mimic user behaviors; these new tools are being called "digital workforce" and they allow much more realistic behaviors which immediately increases the training value for high-level practitioners.

Between digital workforce and improved traffic generation, I see a brighter future for our cyber labs and much better training for more experienced users. So don't just use the free-to-government tools when they lower the expectations and reduce the training value. Your Warfighters deserve a better training experience.

Red team as part of operations

Let's shift gears now and discuss the red team professionals and how they can fit into your staffing model. As a guy with a ton of experience supporting events, I will tell you that any range revolves around the operations staff. You may only have one event ongoing any week but many more are in some stage of planning. At the CSR we usually had multiple events underway and dozens in planning phases, meaning we had to be very efficient; in implementation (build), in event execution (use) and in tear-down (reset). I will also share that almost all of my customers wanted some type of red effect in their event, even when they didn't need it. Why? Range customers find red teams and their work "sexy" and want it in their event too.

Knowing how many events you plan for a month, the quarter and for the year is really important to your staffing model. Knowing the types of events and how many will require red effect is also tremendously important for the red team staffing. Types of events; some events are led by an instructor so they require less red team support. At the CSR we would provision a capability the instructor could trigger when they were ready. We called this the easy button, because the instructor could trigger it and watch as the students respond. It wasn't necessarily easy for my staff though, as a lot of work often went into creating that script/tool for the instructor and if often had to run many times during the event. Free-form events required the red team to stand by and engage a specific "attack" when the event leader was ready for it. Of course, many hours of preparation may be needed for the delivery of each attack.

It's probably time for a discussion on red team expertise. There are many different levels of red team experts, ranging from someone who recently completed an ethical hacker course, to someone who completed the NSA red team level 2 course. Most fall somewhere between these two ends. And just completing a hacker course is not a great indication of actual expertise (well completing the NSA level 2 course in record time is), but some people new to red teaming

become amazing professionals in very short order. There is an expectation that red team professionals understand the method of operation and someone who just got their ethical hacker certification will not be.

That doesn't mean there will not be a role for them. I believe the mentoring process used across the industry is great. Pairing a new practitioner with a senior practitioner is something I learned early on as a young Marine. The senior would not only teach technical detail to the junior but also operational aspects as well as expectations. Juniors could not move into critical roles (operate individually) until the expected overall understanding had been achieved, as verified by the mentor.

I should discuss the special nature of red teamers like other high-level professionals across the cyber community. Many have few social skills or verbal communication ability so they don't fit a traditional role model. They also tend to be very private people and keep their own counsel. They do not typically fit into the wider IT department and do not like being the center of attention. In fact, they like to be in their own space with limited access to it; they do not want visitors popping by to say hi or to be a stop on the facility tour. They do not want to meet VIPs or other guests unless they are of a similar bent (high-level technical practitioner). They tend to not want to speak with company management (executives), the PM or the customers. When you find the occasional red teamer, who does and also excels in this difficult field, keep them – they are worth everything you pay them and should be cherished.

Summary

It is possible to create a cyber range with widely available red effect, both live-action and pre-canned. A thoughtful approach to system design is the best path to success. Focus the time and attention needed to identify the types of events, the planned schedule and the staffing model before you begin the process of ordering hardware and software and hiring the operations team. Spending time up front to properly gauge the scope of the project will ensure a better result is achieved. It's also critical that you conduct the design review with an experienced red teamer who can help you prepare the non-standard Internet sub-systems that will efficiently and effectively deliver your red effects. Just like we preach "baking" security into the start of your system design, make sure red teaming is part of the complete design process, to ensure you achieve your goals and deliver a sustainable system.

About J D Lovett

JD is a Marine veteran with wide experience across the IT and cyber community (Lead Engineer, Firewall Engineer, Computer Repair, Server Administrator, Network Assessor, NOC Manager, Base Network Manager) and the creator of the DoD Cyber Security Range (CSR). JD pitched the Range idea to STRATCOM in 2008, during an update session for the 8570 series, while working on a team of network auditors. The pitch was successful and the CSR pilot began the next year (2009).

After designing the CSR, JD served as the Technical Director through 2017 and during this time developed an unmatched understanding of cyber range operations, having personally led over 100 events. The CSR design was the first DoD cyber lab/range to be certified by the Joint Interoperability Test Command (JITC) to support developmental and operational test (DT/OT) for IT and cyber systems. It also became the De Facto design for Ranges across the country. More importantly, it allowed the Military community to advance cyber training from a very basic capability in 2008 to a much more advanced capability today. A capability that supports the Defense Secretary's vision of building training that supports our warfighters in their true warfare space often referred to in the motto "train-as-you-fight".

JD was the thought leader inside the DECRE technical working group that pushed the Range community to enhance the portfolio and create standards. He was a principal contributor to the DECRE document library; DECRE Range Interface Standards Guide (2015), the DECRE Cyber Range Framework Vision (2017) and the DECRE Enterprise Reference Architecture (DRAFT)(2017).

His efforts through DECRE won funding for the Army-led PCTE pilot, which is now the biggest cyber training endeavor ever undertaken by the DoD. JD is a plank-holder in the PCTE pilot, joining the project in 2017 and departing once success was proclaimed (2019). The PCTE's private-cloud moves to full production this year to support DoD's cyber mission teams. JD is also the co-creator of the Marine Corps Cyber Range (MCCR)(2014).