2011

The Assembly and provisioning of a red team

Daryl Johnson

The Assembly and Provisioning of a Red Team

Daryl G. Johnson
Networking, Security and Systems Administration Department
Rochester Institute of Technology
Rochester, NY   USA

Abstract – *As the value and merit of red team exercises in both academic and corporate settings continues to grow, the need to share experiences with staffing, organizing and supporting the red team becomes increasingly important. This paper documents the Northeast Collegiate Cyber Defense Competition's (NECCDC) Red Team captain's experiences and lessons learned over the past four years. The paper will begin by identifying the skills and attributes needed for a Red Team and a process for selecting and recruiting members. The methods employed to form a cohesive working group from the members in the time available prior to the event will be discussed. The resources necessary for the Red Team to be effective and how they were provided is examined. We will look at how to promote planning and organization within the team focused on specific strategic goals and objectives of the Red Team. There are several duties during the event for a Red Team captain that will be examined and cautions that will be explained. At the end of the competition, the style and delivery of the after-action-report can have a profound effect on the Blue Teams. Experience with different approaches over the years will be examined. Recommendations for Red Team/Blue Team exchanges that can maximize the learning outcome for the students will be provided. Finally this paper will provide a summary of the experiences for others seeking to form and organize a Red Team either for a competition or an internal educational event.*

Keywords: red team, security, education.

1 Introduction

The threats to an organization's information infrastructure today have never been greater as illustrated by the FBI/CSI Computer Crime Survey. From the often quoted Sun Tzu we have "If you know the enemy and know yourself you need not fear the results of a hundred battles."[1] Professor Pascale Carayon describes Red Teaming as "an advanced form of assessment that can be used to identify weaknesses in the security of a variety of systems. The red team approach is based on the premise that an analyst who attempts to model an adversary can find systemic vulnerabilities in a computer and information system that would otherwise go undetected."[2] As the value and merit of Red Team exercises in both academic and commercial settings continues to grow the need to share experiences with staffing, organizing and supporting the red team become vitally important. This paper documents the Northeast Collegiate Cyber Defense Competitions (NCCDC) Red Team captain's experiences over the past four years. The many issues influencing the selection of skills and capabilities, the organization and planning, and the execution of the event from the Red Team perspective will be examined.

2 Assembling the Team

The selection of the individuals for any activity requiring highly skilled members is critical to their combined success. Red Teams are especially sensitive because of the high degree of specialized skills and the pressure of the competition itself.

There are three characteristics that we looked for in recruiting Red Team members. First, *passion* for the security field is the best motivator when a difficult situation or road block presents itself. It pushes the individual to perform above and beyond their limits.

Second, *skill, preparation and dependability*: can they do the job? Are they willing to work long hours for no pay? Can they deliver what they promise? The best indicator I have found is references, recommendations and experience and I rely on all three routinely.

And third, do they exhibit the characteristics of *cooperation, camaraderie, and team focus*? Are they wild horses that cannot or will not pull together for the team but run off by themselves? Do they see themselves as part of something bigger, i.e. the team? Can they see the goals of the team and work towards them? As with the previous set of characteristics, references, recommendations and experience are important but here I call mainly upon the trusted returning members.

2.1 Diversity of Skills

Being an expert is important but having the right mix of skills is critical.[4] Having the right blend of talents and two-deep coverage on the team in vital areas can make all of the difference for red team success.

The skills necessary for a red team member cut across many areas and are changing every year. New languages, OS distros, applications, and networking gear add to the challenge each year. Some of the skills currently on the list are: Windows, Linux and Cisco platforms, vulnerability. Additionally, exploit development, exploit execution, persistence, stealthy techniques, web application exploits, and social engineering are valuable.

In comparison, the blue team must consider in its candidate selection and training the duplication of skill sets across their membership. This goal is primarily driven by the possibility that a member might be lost due to illness or as part of the exercise. Two-deep coverage on the red team is chiefly driven by the benefits derived from the mutual support and greater problem solving capabilities gained from "an extra set of eyes" and "a different point of view" of a difficulty. Therefore selecting at least two red team members focused or at least proficient at every skill area has proven itself a valuable goal.

2.2 Camaraderie

Not the most technical characteristic but amity and solidarity are none the less very important to the red team. The members of the team must not only respect each other's technical skills but appreciate the opportunity to red team together. Disrespect or even antagonism can severely impact the performance of the team as a whole.

Since typically the Red Team comes from a wide geographical area, they may not know each other socially. The best indicator is how they worked as a team member during the previous year's exercises. However, with new members that may not be possible. Soliciting feedback from established members is critical. Some of the best indicators come from Twitter and other social networking sites. The tenor of their posts, how others respond, and what other say about the candidates can reveal much about their character and how they might work as a team.

3 Provisioning the Team

Whether you are going camping in the Rocky Mountains or making dinner, you need certain resources and equipment to be successful. A red team has requirements as well that help ensure that they accomplish their goals.

3.1 Resources Required

The most obvious requirement is a computer. The workstation that the red team member works on is their main tool and a very personal one. Typically the red team members are required to prepare and bring their own workstation including any and all software they might require. Frequently they bring more than one and sometimes a server or networking gear as well.

There are more mundane resources needed by the red team. Besides your basic pens, paper, whiteboards, and markers, we have found several other valuable resources. In short lived, fast paced exercises, intra-team communication is crucial to getting the most out of the team. A bag of USB sticks helps quickly move data and tools around. A networked printer in the red team room for documentation and reports is useful. Keeping track of who has what IP address within the red team, what is known about the blue teams, who is focusing on what aspect of which blue team, and a host of other information can be facilitated by whiteboards, poster boards on the walls and lots of duct tape (lots). But this year, the best tools utilized by the red team for organizing and keeping track of both the blue and red teams was Armitage.[5] This GUI interface for Metasploit with its team collaboration support provided a great platform for intra-team documentation and coordination of effort. Armitage facilitated the coordination of members skilled at target acquisition, exploitation, persistence and score-able information harvesting.

3.2 Support Structure

In addition to the resources mentioned, the 2011 red team was supported by an individual on the red team dedicated to system support. This was one of the improvements requested by several of last year's red team. With the compressed time frame of the exercise it was felt that an individual who could maintain support services such as a red team web, DNS, DHCP and other services as identified for the rest of the red team would aid in keeping the red team members focused on the attacks.

One of the time consuming and distracting tasks for the red team was recording and submitting score-able accomplishments. The system support individual prepared and managed a system to make it easier for the red team members to construct a report of a new exploit or duplicate a similar existing report and modify it. This system also helped to sure that all required information and evidence was included in the report to make sure that it was grade-able by the white team.

4 Team Planning

Six to nine months before the event, the recruiting of red team members begins. It has to start this early to get on peoples calendars before other commitments. Even then their commitment can be superseded by employer priorities or family demands (new additions to a family do take priority). In four years of planning, there has always been at least one member whose plans get thwarted. Therefore, it is advisable to recruit at least one extra member for the red team.

The security community is a relatively small and remarkably close society. Coupled with the need for camaraderie and that the group will be working very closely and intensely for three long days, soliciting suggestions from returning members for new recruits is a big plus. They can also provide feedback on potential new members. This activity solidifies the members ownership of responsibility for the teams overall success and provides the red team captain with a much broader view of the perspective market place for new members.

4.1 "…Know thyself"

As the membership in the red team is incrementally established, team building activities can begin.
Several mechanisms for intra-team communication have been tried: wikis, Google groups and docs, etc. Everyone's life is busy and you are asking these folks to volunteer a nice chunk of their time (much of it personal) with no remuneration other than some fame and bragging rights. Communication has to be easy. It has to be normal. None of the tools mentioned was used by a large enough segment of the team to become adopted. Plain old email has year after year ended up being the communication platform of choice that everyone could live with.

The first item of business is to introduce all of the members to each other. The captain typically starts with a short bio, background and skills. The rest of the team follows with their contribution. The captain should collect all of these as late joining members will need to be brought up to speed.

The next phase is planning a strategy for the event. The captain might start with some questions for the team such as: Do we assign red team members to each blue team or to each target type? Much of the planning is only instigated by the red team captain. Once started often the red team members direct the planning themselves with minimal steerage from the captain.

4.2 Clarifying the Goals of the Red Team

Red teaming is thrilling. The hunt and capture aspect is exhilarating. One problem that has been seen in previous red team exercises is the loss of focus on what is the red team's actual goal. That question is often answered with "Well, breaking into the blue teams systems of course!" The problem with that answer is that it is neither accurate nor realistic. An attacker in the wild would break into a system but that would not be their goal. Their goal is to secure a reward. That reward might come in the form of compensation for items acquired after breaking in such as credit card numbers, PII or trade secrets. Their goal is something on the other side of the door they forced open.

For the red team the goal is to score points. Those points come can come from breaking in but it does not stop there. Often the red team can become focused on the exploit and lose sight of the more realistic goal of obtaining database contents, credentials, PII and confidential documents. The exploit is professionally satisfying and therefore can itself become the focus. The red team needs to be encouraged to look beyond the exploit and focus on scoring as many points as possible.

Part of the planning of the red team is answering the question: "Now that we are in do we pillage or burn?" There is a part of most folks that want to "rm –rf /" when they get privileges. And although that does score points because you could do it and the blue team loses more points because they are down and miss service checks, is it the best approach if the goal of the red team is to score as many points as possible? The red team has tossed around this question many times and evolved an heuristic approach to the issue which will undoubtedly change again. Using the law of diminishing returns, once the score-able points gleaned from a system nears zero and no additional avenues of attack present themselves, plant as many backdoors as possible and bring the system down. Nearing the end of a day when it is no longer possible to recover, burn the system. The mental and morale strike of having a system down over night is a tough hit. At the beginning of the last day wipe all systems possible so that recovery is futile.

5 Challenges Faced

Probably the greatest challenge to the red team is time. Realistically an attacker would be able to perform reconnaissance stealthily over a long period. The time compression of the event makes stealth difficult. It also makes recovery of lost persistence within the blue team costly in terms of points scored. The best defense against time for the red team is planning and preparation.

5.1 The Unknown

Time is not the only challenge to the red team. Typically few facts are known about the target infrastructure and nothing is known about the business injects that will be employed. The inclusion of injects that involve forensics on boxes, VoIP, SCADA, non-typical network devices or OSs, or other unusual services become difficult to exploit without time to overcome the often steep learning curve.

6 Duties of the Red Team Captain

Besides the recruiting, organizing, and provisioning responsibilities already mentioned, the red team captain works with the white team before the event to develop a working relationship and provide input on competition development.

It is helpful to red team morale if they can all stay at the same hotel. The red team often worked late into the night on exploit development and planning. Last year we were able to procure a meeting room at the hotel for part of the time to facilitate this after hours work.

Even with the scoring system, the red team captain must read and validate all of the scoring reports before they are forwarded to the white team. Last year we thought that the new red team scoring system would eliminate the captain validation step but it did not and likely cannot. Mistakes will be made and issues of misunderstanding of score-able events and reporting consistency between members of the red team will continue to require the captain's scrutiny.

Relative to scoring, the red team captain should work with the white team to clarify how the scoring will work. The red team members need to know what are considered score-able items or activities. The scoring function should emulate the relative value of various assets and difficulty of acquiring them. Without this knowledge the red team must rely on guesses and assumptions.

One of the duties that keep the red team captain constantly busy throughout the event is taking questions from the red team to the white team for clarification and ruling. Is it allowed to do ...? Can we get points for …? Does this rule mean …? About a third of the red team captain's time during the event is spent resolving red team questions.

Another third of the red team captain's time is spent answering questions from the white team. Explaining what a scoring reports means is frequent but other white team questions come up as well. Is this alarmed event because of a red team action? Did the red team do …? Did you folks brick …? We are seeing … - is that you folks?

6.1 Cautions for the Red Team Captain

The red team captain is typically going to be as much of a "techie" as the rest of the red team members. The attraction to "join in the fun" and perform exploits and dig for score-able things is magnetic. My experience is that when the red team's captain "plays" the duties that fall solely on the red team captain's shoulders do not get the attention necessary and both the red team and the competition can suffer. The caution is "even if you think you can wear two hats at once, your head is not really that big!" If you accept the role of red team captain, also accept that you will not be performing exploits.

7 After Action Report

Besides the competition aspect, the CCDC events are a powerful and unique learning experience for the students. Attending blue teams come with all levels of preparation and skill. Part of the value of the red team is to give the blue teams both encouragement to continue in the security field and comeback next year as well as feedback on what they did well and how they can improve in the future.

Traditionally the red team has conducted an after action debriefing to all of the blue teams at once at the end of the event. The report has been part introduction to the red team members and a general overview of what the red team has accomplished and observed. The problem was that the presentation was limited in time and could only be very general. Also new teams can get overwhelmed and possibly discouraged because of inadequate preparation and experience. These teams need encouragement and support to not give up.

Last year at the 2011 NECCDC, we tried something different with two teams that struggled during the competition. Their coaches asked us to stop in and talk to them giving some pointers and specific feedback. We then conducted our typical all team debriefing. Our experience with the two teams meeting with them individually was an epiphany. The change in their attitude and morale was striking. We spent 15 minutes with each of the two teams. We were able to provide specific feedback about their team. We also answered lots of their specific questions about what we did and what they could do to better prepare. At the end there was no question that they had benefitted from the competition and were coming back next year.

8 Conclusions

Our experience with assigning red team members to skill and application specific areas, instead of to a blue team, has served us well. It made the most effective use of our skills and attention.

It is imperative that the red team through the red team captain be involved with the white team before the event, consulting on the design and development of the exercise. A blind red team mainly tests the red team's skills not the blue team's skills and preparation.[6]

Our experience with the one-on-one debriefings with the blue teams has convinced us of their value to the students. We are recommending next year that time be allocated after the event to allow the red team to meet individually for 15 minutes with each of the blue teams. It is our experience that this provides better feedback and more values to the students.

9 Acknowledgments

This paper could not have been written without the shared experiences of many people. I would like to acknowledge the work of the 2011 NECCD Red Team: Jonathan Claudius from Trustwave, Laura Guay from SecureWorks, Raphael Mudge from Delaware Air National Guard, TJ OConnor from US Army, Ryan Reynolds from Crowe Horwath, Jason Nehrboss from CSC/Bath Iron Works, Joshua Abraham from Rapid7, Will Vandevanter from Rapid7, Gerry Brunelle from Boeing, Todd Leetham from EMC, and Silas Cutler from RIT. I also need to thank Tom Vachon from Kayak as the white team captain and Themis Papageorge from Northeastern University who organized and hosted the competition and many others.

10 References

[1] Sun Tzu, *The Art of War* (Tribeca Books, 2011).

[2] P. Carayon and S. Kraemer, "Red Team Performance: Summary of Findings University of Wisconsin-Madison & IDART: Sandia National Laboratories" (2004).

[3] Furtună, et al, "A structured approach for implementing cyber security exercises", 2010 8th International Conference on Communications (COMM),

[4] Dodge, R.C., Jr.; Ragsdale, D.J.; Reynolds, C., "Organization and training of a cyber security team," *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance*, 2003.

[5] Raphael Mudge, "Armitage - Cyber Attack Management for Metasploit." [Online]. Available: http://fastandeasyhacking.com/. [Accessed: 18-May-2011].

[6] P. Herzog, "OSSTMM 3 – The Open Source Security Testing Methodology Manual" [Online]. Available: http://www.isecom.org/mirror/OSSTMM.3.pdf. [Accessed: 18-May-2011].

[7] G. B White and D. Williams, "The collegiate cyber defense competition,", *Proceedings of the 9th Colloquium for Information Systems Security Education*, 2005.

[8] P. Sroufe, S. R. Tate, R. Dantu, E. Celikel, "Experiences During a Collegiate Cyber Defense Competition," *Journal of Applied Security Research*, Vol. 5, No. 3, 2010, pp. 382–396.

[9] J. Mattson, "Cyber Defense Exercise: A Service Provider Model," in *Fifth World Conference on Information Security Education*, 2007, 81–86.