

CAPTURE-THE-FLAG: LEARNING COMPUTER SECURITY UNDER FIRE

LCDR Chris Eagle, and John L. Clark

Naval Postgraduate School

Abstract: In this paper, we describe the Capture-the-Flag (CTF) activity and argue that it contributes to a necessary component of the computer security curriculum. This component is the study of software vulnerability investigation. It is currently not properly emphasized in this curriculum. We discuss reasons for this situation and we go on to describe how CTF can be useful for educating students within this focus. CTF helps develop those computer security skills that enable students to identify new vulnerabilities before those with malicious intent find them. It also helps them to hone the core computer security skills.

Key words: “capture the flag”

1. INTRODUCTION

Proactive vulnerability analysis on existing systems is lacking from the modern computer security curriculum. Students do not learn how to locate and fix design, configuration, and application flaws in existing systems. Exercises such as Capture-the-Flag (CTF) teach these skills. As such, CTF fills a critical void in Information Security education.

Our paper is organized as follows. We argue that the vulnerability analysis education problem exists. We describe the current computer security educational approach in the section titled "The InfoSec Educational Environment". There we explore the underlying reasons for the deficiency in this approach and we go on to link these reasons for the educational disconnect with the current approach. We then go on to describe CTF in the section titled "CTF: A Lab to Fill the Gap". There we describe the setup for a CTF exercise and explore why it helps to train students to discover flaws in systems. We summarize our conclusions in the section titled "Conclusions".

We propose that CTF helps to teach those skills that we find to be lacking. CTF fills this niche naturally by providing a safe parallel for the experiences of crackers in the wild. The specifics of a CTF exercise may lead to a general approach to teaching these skills. We focus on these specifics here because they serve as an excellent starting point for two efforts. First, CTF provides immediate educational value. Computer Security departments can participate in CTF exercises to teach a set of valuable skills. In addition, educational researchers can use CTF as an aide and basis to understanding how best to convey these skills.

2. THE INFOSEC EDUCATIONAL ENVIRONMENT

There are a series of challenges that a student of Information Security faces. Educational programs structure themselves in order to meet these challenges. Curricula are also developed to help meet the expectations of potential employers. These expectations present themselves in the course of the day-to-day operation of Information Technology (IT) systems.

Organizations concerned with the security of their IT generally break it down along two lines. The security of an organization's IT flows from that organization's policies, which defines the organization's approach to the problem. The application of the policy is colored, however, by the timing concerns involved. First, these organizations are interested in being able to protect systems that they already have in place. They must do something to deal with known vulnerabilities, or any threats to their operation will have known avenues for doing them harm. Second, they are interested in planning for systems with more capabilities in the future that will better support their mission.

Information Security education has grown to support these concerns. These organizational goals tend to divide a student's education into two categories. We will call these the *protectionist* and *constructionist* approaches to computer security. The protectionist approach focuses on developing students' capabilities to protect existing systems from known vulnerabilities, given known risks. The constructionist approach focuses on developing students' capabilities to build new systems that are free from vulnerabilities to a high degree of assurance.

In his paper *Training the Cyber Warrior*, J.D. Fulp describes this divide using the terms *cyber tacticians* and *cyber strategists*, which correspond to our concepts of protectionists and constructionists, respectively:

Cyber tacticians would focus on reducing the risk of existing fielded systems primarily through the application of appropriate safeguards Cyber strategists would focus on reducing the risk of future systems primarily through the application of structured and formal system design techniques that reduce system vulnerabilities [Ful03].

Teachers use lecture sessions and laboratory work to convey information and experience to their students. Both of these tools tend to support one or the other of the protectionist or constructionist approaches. To illustrate this, we will refer to some generic courses. There are specific counterparts at the Naval Postgraduate School for many of these.

Lecture sections are direct and in Information Security, as elsewhere, are used to convey important baseline facts. Even when there is a lab involved, it typically builds on prerequisite material presented in a lecture. Information Security lectures can cover understanding policy, grasping current threats, and learning how technology (including networking) works. Such lectures are clearly protectionist in nature. Other lectures can discuss the meaning of security and a robust process for developing secure systems. These lectures can include formal modeling and techniques, design approaches, and implementation standards. These are clearly constructionist.

Laboratory exercises (labs) are a more interactive teaching tool. They have the benefit that they can provide experience in a subject. They are often more appealing to students than other types of work. It is difficult, however, to convey abstractions and theories through labs, as complex material can be challenging to model in a lab. Many of the labs in existence parallel the class lectures described previously. Teachers have also experimented with more comprehensive labs that exercise a variety of skills and the coordination of those skills. A Cyberdefense Exercise (CDX) is a lab that is focused on network security from a defense point of view. The converse of this is a Red Team Exercise, which attempts to take advantage of known vulnerabilities to test an installation's defenses. Labs such as these are protectionist in their approach. They encourage using known processes to achieve some well-defined goal using established technology and procedures.

For example, in his paper *Teaching Network Security Through Live Exercises*, Giovanni Vigna gives an overview of several configurations of interactive teaching techniques. One of the experiments that he describes is a lab called Capture The Flag. As Vigna describes it, though, this form of CTF exercise continues to contribute to the protectionist educational approach.

The team's goal was not to prevent the other team from breaking into the host. Instead, the priority was to detect the attacks of the opponents. In addition, each team had to attack the other team's hosts and retrieve the flags for each of the attacked hosts [Vig03].

Here, the priority is learning about intrusion detection. Intrusion detection is a tool that is helpful for identifying when attacks may be taking place on IT resources. It is often taught to students as a component of a network security framework, and as such it is part of the protectionist educational focus.

In contrast to such labs, there are other labs that provide interactive experience to students who are developing systems. These labs include training using the development tools. They can also expose students to experimentation with computing system components that can help students reason about future systems. These labs are clearly constructionist in their focus.

There are important skills that are overlooked in these approaches to teaching Information Security. The protectionist focus has students learn what policies need to be enforced, and how to enforce them. With this focus, students harden systems and react to problems based upon known vulnerabilities. Once these students become practitioners, they must keep up to date in order to keep their systems up to date. Looking to the future, the constructionist focus has students learn the design skills needed to put together systems that are robust in the face of threats. The constructionists incorporate policy from the beginning to ensure that systems conform to policy. The nature of vulnerabilities is a vital input to both of these areas. Who is trained to discover new vulnerabilities?

3. CTF: A LAB TO FILL THE GAP

We propose that Capture-the-Flag serves as an example of the type of material that needs to be included in Information Security education. Capture-the-Flag is a team-based sport that is essentially an exercise in controlled, time-sensitive system subversion (also known as cracking). Aside from a set of artificial goals that give the sport a measuring stick and a set of artificial boundaries that keep the sport contained, participants have an extraordinary amount of freedom. This freedom motivates students to experiment and forces those students to hone skills that are not normally covered in a standard Information Security curriculum. CTF is one component of an educational focus that is currently missing from institutional Information Security education.

One of the potential drawbacks to CTF is the amount of setup required. CTF is based on the concept of running one's own—and subverting others'—services. A service is any application that can be utilized remotely over a network. Many services, for example, make use of a common web server. There are a plethora of potential services that can be used. In fact, many CTF configurations have tried to mix some common services with some that are more arcane.

The CTF setup introduces the concept of a flag in order to monitor whether each of a particular team's services is available, and if so, who controls it. If a service is controlled by a team other than the team who owns that service, then it has been remotely compromised. A flag is some small string of data that identifies a particular team. In order to assign scores to teams, service flags are cryptographically "rotated" in an unpredictable way in order to monitor the duration for which a service is controlled continuously by a given team. There must be an automated way to perform this scoring. This "scoring server" accesses each team's services in much the same way that the participating teams access each others' services, but it may also have additional privileged access mechanisms for performing flag rotation that must be communicated

to the teams in advance. The development of the scoring server is the primary source of the complexity in the preparation for the exercise.

Game play is also quite complex, although given a correct setup it is straightforward. Each team is given space within the network topology. Each team is also given media, typically optical, such as a CD or DVD, containing working images of the systems sufficient for running the services. How the team organizes itself to satisfy the exercise's requirements is left entirely to that team.

The most important characteristic of a CTF exercise is its focus on the 0-day exploit. A 0-day exploit is a software system vulnerability that has not been previously disclosed. 0-day exploits include both vulnerabilities that have not yet been discovered as well as those about which certain groups may know but choose not to reveal. In contrast to Vigna's approach to CTF exercises described earlier, the ones in which we have been involved require the development of new exploits. This is a CTF exercise's primary benefit. In order to be competitive, teams must harden their systems as much as possible. In turn, this means that other teams must find new, previously unknown and hence innovative ways to undermine their competitors' systems.

We have broken down the important educational targets for developing 0-day exploits into eight areas. These areas are:

1. Consistently secure programming practices
2. Compiler theory
3. Assembly language
4. Operating system theory
5. Reverse engineering theory
6. Networking and practical protocol analysis
7. Exploit methodology, and
8. Ethics and disclosure

Many of these topics are traditional computer science areas of study. In an Information Security educational environment, these topics would all be taught with a concentration on learning where flaws could exist and discovering where flaws actually exist. These skills border on both protectionist and constructionist domains, but they are largely overlooked in modern Information Security curricula.

While the 0-day exploit is of paramount importance to a CTF exercise, these exercises develop a wide assortment of additional skills. Building up a picture of how the exercise has been constructed and finding targets to analyze develops computer forensics skills. Defending the systems requires a combination of network security and system administration skills. This defense must be responsive to new attacks, and it requires extensive knowledge of a wide array of system components, including various (and potentially arcane) operating systems. Participating effectively in a CTF exercise requires preparation. This preparation is targeted towards enabling the team to cooperate. It requires some technical work, such as network engineering, but it also requires proper team management. CTF is a thorough information security exercise. It integrates well with other Information Security educational targets and so it can be used effectively to train Cybersecurity professionals.

4. CONCLUSIONS

In response to the IT environment and the security needs of that environment, an educational program of protection and construction has developed. We suggest that these categories are very useful educational foci, but that they require additional support. We need to be training people to act like crackers and find new vulnerabilities in existing systems. Exercises such as Capture-the-Flag develop these needed skills in students.

We conclude that we need a third focus for students. We will call this focus the *destructionist* focus; its primary goal is to learn how to break software and computer systems and thereby expose the vulnerabilities in those systems. Destructionists complement both protectionists and constructionists. Destructionists work to uncover new vulnerabilities. This information naturally supports the protectionists, who specifically work to counter known vulnerabilities. Destructionists also work to expose new models of risk and to better understand the weaknesses in system composition. This information is useful to the constructionists in that it will provide them with a better foundation on which to base their design decisions.

In our observation, CTF has helped students understand the security relevancy of system details in a way not previously covered. Students participating in our formulation of a CTF exercise are forced to deeply and thoroughly inspect and understand the operating environment of IT systems. They must then be able to assemble this knowledge into a viable threat. Our description of the CTF architecture gives students almost free reign in their manipulation of the game systems. Students are forced to take everything into consideration as a possible avenue of attack.

There is still a good deal of work that needs to be done to incorporate CTF neatly into an educational environment. In our experience, evaluating students based upon their participating in one of these exercises can be challenging. Individual students are likely to have very different aptitudes, and a CTF exercise tends to draw out specific skill sets. A CTF exercise is unavoidably a team exercise. As a result, we have typically used CTF exercises as extra-curricular activities, although this is also due to the fact that we are still working to integrate CTF-related material into the curriculum. This has the side benefit that as an extra-curricular activity, CTF provides an avenue for students to interact with the hacker community.

5. REFERENCES

- [Ful03] Fulp, J.D. Training the Cyber Warrior. Security Education and Critical Infrastructures; June 26-28, 2003; Monterey, California, USA; The International Federation for Information Processing. Kluwer Academic Publishers, Boston, Massachusetts, USA. 2003.
- [Vig03] Vigna, Giovanni. Teaching Network Security Through Live Exercises. Security Education and Critical Infrastructures; June 26-28, 2003; Monterey, California, USA; The International Federation for Information Processing. Kluwer Academic Publishers, Boston, Massachusetts, USA. 2003.