Topics

Using *Capture the Flag* Events as Training Opportunities

INTRODUCTION

Capture the flag (CTF) is a traditional children's outdoor game in which two teams attempt to protect their own flag, while at the same time trying to locate their opponent's flag, capture it, and return it to their own home base in order to win the game. An increasingly popular adaptation of this game has spawned an entire subculture within the computer security community. At Defcon[1], the capture the flag competition is one of the longest running of many well-known competitions, having been introduced in 1996 at Defcon 4.

CAPTURE THE FLAG VARIATIONS

There are two primary variations of CTF as played in computer security circles. Each offers competitors a chance to put into practice skills from all facets of the computer security field with the ultimate goal of retrieving "flags" that may be delivered to the contest organizers in order to demonstrate that a particular challenged has been solved or a particular goal met.

Perhaps the most well-known version of CTF is the version that has come to be known as the "Defcon-style" CTF. The Defcon CTF is a *full-spectrum* CTF played by a limited number of teams in a live, head-to-head event. At Defcon, the scale of this game has grown from eight teams to its current size of 20 teams that compete at a live event over the course of three days in Las Vegas, Nevada every summer. In a full-spectrum CTF, the event organizers provide each team with identical server images pre-configured with custom software developed by the organizers. Each team's server is connected into an isolated game network dedicated to the competition. Each team is required to simultaneously administer and defend their own server while attempting to penetrate the defenses crafted by each of the other teams in order to capture flags which are turned in to the organizers in exchange for points.

The rules for a full-spectrum CTF are intentionally unrestrictive in order not to limit the creativity of each team in building novel defenses. In order to prevent teams from shutting down vulnerable software as a means of defending it, teams are typically graded on their ability to continue providing these "services" to the public, which includes the organizers who periodically test whether each team's software remains accessible both to the organizers and to other teams. There is an expectation that teams patch any flaws that they find in their assigned software rather than simply shutting the software down.

As teams find flaws in their own software and come to understand how they may themselves be vulnerable to attack, they also understand that every other team playing the game is also vulnerable to the same attack. Consequently, teams attempt to use each flaw to penetrate their opponent's servers and, following each successful penetration, retrieve a flag from their opponent. Flags are placed on each team's server by the organizers and are periodically replaced in order to provide new flags to capture throughout the game. This periodic rotation of flags forces teams to repeatedly demonstrate that they can maintain access into their opponent's servers and allows for the gradual evolution of both defenses and offenses as the game progresses.

The Defcon CTF has become so popular that hundreds of teams attempt to qualify to play in the Defcon CTF every year with many of these teams spending months of preparation time in the hopes of earning a trip to Las Vegas. Increasingly the Defcon CTF is becoming an international event. Prior to

2006 competitors at Defcon consisted solely of American teams. In 2006, the first international team, from South Korea, qualified and participated in the Defcon CTF. In 2013, two-thirds of the participating teams at the Defcon CTF were international teams including teams from Japan, South Korea, China, Russia, and mixed European teams.

A number of other full-spectrum CTFs have developed since the first Defcon CTF. Most of these are open primarily to academic institutions with the most well-known of these being the University of California, Santa Barbara's iCTF (International CTF) competition which has become the largest scale full-spectrum CTF in existence. In 2013, the iCTF hosted 90 teams from around the world in an eight-hour live event.

The second variation of CTF is based on the concept of solving puzzles in order to be awarded points. In a puzzle CTF, organizers develop a number of security-related challenges and make them available to participants for solving. Participants do not interact with one another; instead teams race to be the first to solve puzzles and to gather the most points.

The infrastructure to host a puzzle CTF resembles a traditional web site on which the puzzles are posted more than a live network battle ground. This makes it somewhat easier to host puzzle CTFs and allows far more teams to participate in a live puzzle-style event. In many cases 500 or more teams may be competing simultaneously to see who can win the event. A puzzle-style event is used as a qualifying event for the Defcon CTF, allowing hundreds of teams the opportunity to compete for a chance to compete in the live Defcon event.

Because they lack a head-to-head component, puzzle-style events often offer a wider variety of challenges across a larger number of security-related skills than full-spectrum events. Categories present in puzzle-style events often include reverse engineering, cryptography, forensics, packet analysis, web security, network reconnaissance, and many others.

Between these two types of events, CTF has become so popular that it is possible to find a CTF of one type or the other taking place almost every week of the year. In fact an entire online community has emerged and is tracked by sites such as ctftime.org[3], which offers both a comprehensive calendar of events as well as results tracking and team ranking. The ranking system in particular highlights both the popularity of CTF and the increasingly competitive nature of the events.

BEYOND THE COMPETITIONS

While CTF events themselves are great fun for all participants, there is much more to CTF than just solving challenges. CTF offers a small window into the computer security field and the games and the excitement surrounding the games are both a great way to introduce new people to the computer security field, identifying talented individuals within specific security disciplines, and a way for established security professionals to showcase their skills.

One of the great opportunities available through CTF is to be able to introduce computer security to young students as a non-traditional introduction to the computer science field. When appropriately packaged, a CTF for young students can both demonstrate the dynamic nature of the computer security field and gently introduce young people to the security problems they are faced with through their everyday interaction with technology. In particular, the media often speaks of the dangers

that are present when using social media. Younger users often see social media as a convenience, a necessity, and an expectation without understanding the risk they may be exposing themselves to through reckless use of such technologies. A well designed CTF can go a long way towards raising awareness and increasing interest in computer security at ages where traditional computer programming may be too difficult to introduce.

As CTF evolves, or more specifically as organizers consider how they might evolve their games, one of the most important ways that CTF can become even more useful is to package CTF as a complete training opportunity in which the organizers provide training in CTF-specific skills, which mirror the skills of everyday security practitioners, leading up to an actual CTF event. Since the organizers typically have complete visibility into their CTF infrastructure, they are uniquely situated to utilize the data they collect, to include packet capture and event timelines, in order to conduct after-event training with participants in which feedback on procedures may be provided along with addressing any shortcomings noted during the event. Used in such a manner, CTF can be a valuable tool both in the workplace as a training opportunity and for the general public as a recruiting tool.

CONCLUSIONS

Japan like many nations faces a critical shortfall in the workplace for skilled computer professionals. Many studies show that it is increasingly difficult to reach younger students and motivate them to pursue education and jobs in the computer field and more specifically in the computer security field. CTF is used in many organizations as a motivational tool as well as a great source of pride when an organization's teams perform particularly well in large competitions. In the United States, companies boast of successful participation in CTF and individuals proudly list CTF on their resumes when applying for jobs in the security field.

As a means of introducing anyone to the computer security field CTF provides a highly interactive way to generate both involvement and interest. While CTF alone is certainly not going to solve the personnel shortage faced by many companies and nations, in a field that lacks innovative ideas for stimulating interest, CTF certainly looks like a good place to start.

REFERENCES

(1) Defcon Computer Security Conference, http://www.defcon.org.
(2) University of California, Santa Barbara iCTF, http://ictf.cs.ucsb.edu/
(3) CTF Time, https://ctftime.org/

ABOUT THE AUTHOR

Christopher Eagle

Christopher Eagle (Chris Eagle) is a Senior Lecturer of Computer Science at the Naval Postgraduate School (NPS) in Monterey, CA. A computer engineer/scientist for 28+ years, his research interests include computer network operations, forensics and reverse engineering. He has been a speaker at conferences such as Black Hat, Defcon, Infiltrate, and Shmoocon and is the author of "The IDA Pro Book," the definitive guide to IDA Pro. He is a multiple winner of the Defcon Capture the Flag Competition and was the organizer of that competition from 2009-2012. He is currently working with DARPA to build their Cyber Grand Challenge competition.