CTF: Alternative Training for Offensive Security

Chung-Kuan Chen
National Chiao Tung University
ckchen@cs.nctu.edu.tw

Shiuhpyng Shieh, Fellow of the IEEE
National Chiao Tung University
ssp@cs.nctu.edu.tw

***Abstract*—Offensive security is a concept of defense based on adversary's mindset. Traditional security education is insufficient for offensive security. Most security courses are designed from the defender's perspective, and have a big gap from the real world problems in practice. The emerging contest Catch-The Flag (CTF) can complement the traditional education for security training. In a CTF contest, competitors will try to solve security problems that are verisimilar to real world problems. The CTF infrastructure also provides the platform to sharpen competitors' security skills. There are three types of CTF competition: Jeopardy, Attack and Defense, and King of the Hill. While Jeopardy can cover a wide range of knowledge of skills, such as pwn, reverse engineering, web, forensics, and cryptography. Attack and Defense competition focuses on the entire vulnerability life cycle. In this type of competition, competitors are given green light to attack each other. As a typical example, the target program is first analyzed. If vulnerabilities are discovered, an attacker can develop exploits to compromise other teams' machines. Meanwhile, to counter the same attack, the vulnerabilities of their own system should be patched. King of the Hill is the variant of Attack and Defense. The longer the competitors can take over the system, the more score they can get. With these different types of CTF competition, the offensive security skills can thus be polished. To encourage automating generation of the defensive system, the DARPA recently launched the Cyber Grand Challenge aimed for the first CTF competition played solely by machines.**

***Keywords*—Security training, Jeopardy, Attack and Defense, King of The Hill, Catch The Flag**

I. Offensive Security Training

Offensive security, complementary to the traditional defensive security, is the concept of defense based on the comprehension of adversary's mindset. Consequently, security experts can identify the weaknesses for potential compromise in the whole system, and then accordingly proper defense mechanisms can be chosen and deployed. Offensive security awareness is important even for system and network administrator. Every administrator should learn the concept of offensive security to certain degree. In the software development cycle, programmers should understand common weaknesses that are easy to attack by an adversary. Software programmers should avoid writing programs with weaknesses, such as, buffer overflow, and SQL injection. Similarly, these weaknesses can also be avoided in the code review step if the reviewer understands the intrusive approach taken by the adversary.

For security experts, the importance of offensive security drastically increases in recent years. For penetration testing of a software program, there may exist hundreds of entries potentially vulnerable to attacks. Testing these entries individually is very time consuming, and without the knowledge of adversary's method the test itself may fail. To effectively discover system vulnerabilities, the penetration testers should be familiar with adversary's penetration methods.

To achieve offensive security, education for offensive thinking is the first step. However, adversary's thinking is difficult to learn through traditional courses and education. The thinking of an attacker is opposite to that of a traditional software developer. For the developer, the software construct process starts from software design, followed by program development, and then software testing. In contrast, the adversary hacking starts from software testing to discover vulnerabilities, followed by reverse engineering to understand the software, and finally development of exploits. As a result,

traditional education in compliance with the software construct process fails to cover offensive security. Furthermore, security-related courses only focus on defense rather than offensive security.

The other issue is practice. Similar to traditional software development, practice makes perfect. Adversary skills also require significant effort in practicing. Different skills may be adopted in different situations. The traditional security education often focuses on basic concepts and theory. Little practice is involved in the course. Therefore, the gap between the course and real world problems exists. In addition, the lack of practice is also a problem for offensive security education. Due to the intrusive behavior of hacking skills, it is not a good idea to conduct exercises online in a public network where real systems may be corrupted and malicious behavior is forbidden.

II. CTF: THE WORLD WIDE GAME FOR HACKERS

Capture the Flag (CTF) is a promising solution to offensive security education and talent discovery. In a CTF contest, competitors should think as a hacker and break security problems. Security-related problems are designed and announced to competitors by CTF organizers. The competitors' goal is to find the flag, a string crafted in a specific format, hidden in the problems via some security exercise.

The first CTF contest, Defcon CTF, started in 1996. Until now, Defcon CTF is still the most important contest in the world. Every year, hundreds of teams participate in the Defcon qualification for the chance to be part of the final contest in Las Vegas. In the Defcon final, a few qualified elite teams compete in the live, face-to-face environment to pursue the championship.

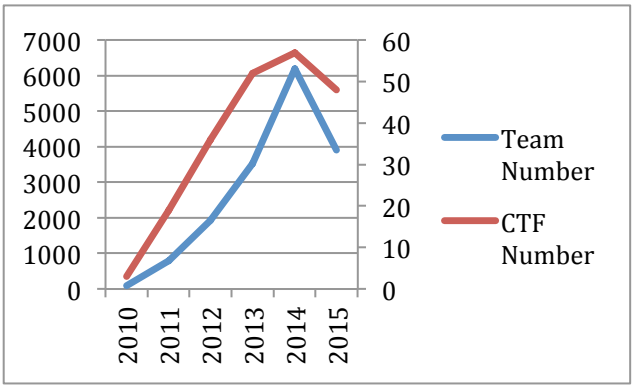


Figure 1 *Trend of CTF and Teams*

Besides Defcon CTF, there are many other CTFs [1-20] held around the world, such as SECCOM held in Japan, CodeGate in Korea, RuCTF in Russia, HITCON in Taiwan, and 0CTF in China.. This indicates that CTF gradually becomes a critical platform for offensive security training. All of these CTFs attract hundreds of teams to participate.

XCTF is the CTF tournament organized in China. In the tournament, a number of CTFs are held at different universities. The front-runners with higher overall ranking are qualified to compete in the XCTF final contest. Among all the CTFs in China, 0CTF and BCTF are the world-class competitions. Other CTFs in XCTF are mainly for students in China. CTF teams around the world can still participate in these CTFs. With this high frequency of CTF contests, both experts and students have remarkable opportunities to learn and polish their security skills.

CTF contests are not solely designed for security experts. Different CTFs may target at competitors at different levels. As a beginner of CTF, Backdoor CTF, ASIS CTF, Hack.lu CTF are good choices to enter the world of hacking. On the other hand, DEFCON, PlaidCTF, CodeGate and Ghost in the Shellcode CTF give more advanced and challenging problems to the competitors. Due to the wide range of difficulty, one can find the CTFs suitable for them to learn security skills.

To attract more students to learn security, some CTFs are dedicated to students. Among them, CSAW CTF is designed for undergraduate students to learn skills during the contest. It was the biggest contest in 2014, and more than 18,000 competitors from 75 countries around the world attended. In addition, picoCTF and HSCTF further reach out to high school students. These CTFs help high school students get exposed in the exciting new area.

Even though all the CTF contests aim for security education, each CTF may have its individual goal. For example, PHDays (Positive Hack Days) CTF is designed to mimic the real-life conditions where the contemporary vulnerabilities of information system are adopted as the contest problems. Moreover, depending on the contest scenario, the underlying infrastructure may change over time. In this way, competitors can practice to solve real-world problems for a variety of infrastructures. iCTF, the UCSB International Capture The Flag, targets on building a distributed, world-wide security contest for more students to join and learn attack and defense skills. The iCTF framework is also published for others to establish their own CTF contest. Thus, it may ease the difficulty to hold a CTF contest.

One important feature of CTF is gamification which makes the contests more interesting and attractive to students. Some CTFs try to make their contests more fun. PlaidCTF 2012 constructs the contest as the RPG (Role-Playing Game) game, shown in Figure 2, where competitors play the role as an adventurer to execute a mission that is indeed a security problem. Ghost in the shellcode CTF includes problems hosted on Pwnie Island since 2014. Pwnie Island is the first personal, open-world MMORPG (Massively Multiplayer Online Role-Playing Game). In the game, a competitor should complete the missions impossible unless game hacking techniques are used.

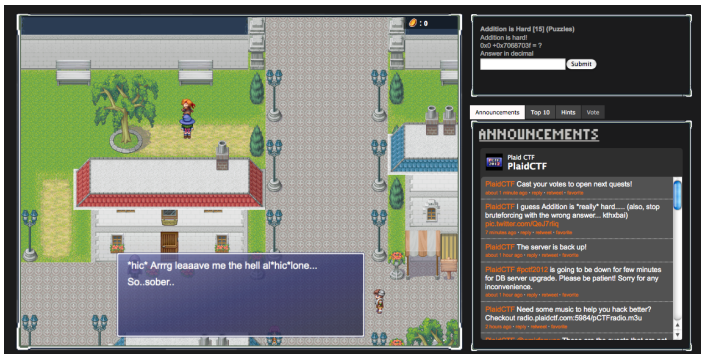


Figure 2 *RPG Style CTF in PlaidCTF 2012*

According to the authoritative CTF ranking site CTFtime, about 100 CTF contests are recorded and 16335 teams has registered till 2015. These CTF teams come from 64 different countries around the world. The trend of growing number of teams and CTFs is demonstrated in Figure 1. The blue line in the figure denotes the total number of teams registered to

CTFTime over the years. And the red line indicates the total number of CTFs held each year. As the figure demonstrates, the total number of teams participated in CTF grows from 90 in 2010 to 6197 in 2014, while the total number of CTFs also increases from 3 in 2010 to 57 in 2014. Note that, the data collected for 2015 is only up to August, and therefore the decrease in 2015 does not indicate the actual number.

III. Different Types of CTF

There are three types of CTF contests, Jeopardy, Attack and Defense, and King of the Hill. Consider the last two CTF types with the requirement of a stable network. They are mostly held in a closed environment and only a limited number of teams can join. Therefore, many CTFs hold Jeopardy-style CTF in the qualification round. Only the best teams can participate in the finial round of CTF that is either in Attack and Defense or in King of the Hill style.

A. Jeopardy

Jeopardy shown in Figure 3 is the most common CTF type. Just like the TV shows with the same name, competitors will encounter several problems in different disciplines. In general, Jeopardy CTF includes the problems on pwn, reverse engineering, web security, forensics, and cryptography. Each problem has a score that indicates its difficulty. Once a competitor solves the problem, the associated score is earned. As a proof of problem solving, the flag hidden in the problem is discovered and submitted to the organizer as evidence.

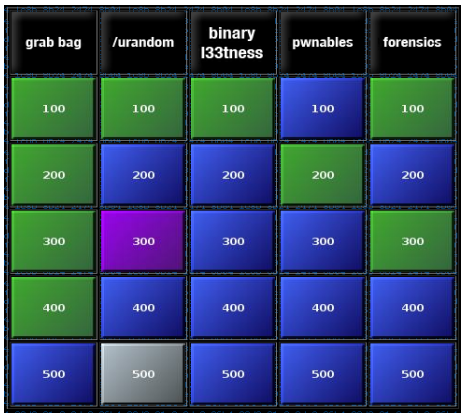


Figure 3 *Scoreboard of Jeopardy CTF, Defcon CTF*

1) Pwn

In the pwn discipline, a vulnerable executable and the information of a remote server are given. With the executable, a competitor can analyze the executable offline and discover vulnerabilities such as buffer overflow, use-after-free, and format string. The exploit—an attack program based on the vulnerability—can be developed to steal the flag from the remote server.

2) Reverse

The reverse engineering problem often provides an executable with the flag hidden by the designed algorithm. With disassembly and decompiler tools, competitors need to understand the algorithm's logic and unveil the key. For example, given the user validation program with unknown registration code, to generate registration code, the final flag can be unveiled after understanding the algorithm.

3) Web

Similar to the pwn problem, a remote web server with vulnerabilities is given. The difference is that the program is not given in most cases. Therefore, the black box analysis is needed to discover web vulnerabilities such as, SQL injection, cross-site scripting (XSS), and command injection.

4) Forensics

In forensic problems, the flag is hidden in the object given. The target objects vary from network packets, document files to disk images. Realizing the principle of system can help solve the problems. For example, a disk image is given, but the flag is inside a deleted file. Therefore, knowledge of the file system should be understood, and some forensic tools can be used to recover the deleted file.

5) Cryptography

Cryptographic problems usually contain the encrypted flag. While encryption, some weaknesses are involved in the cryptographic system. Competitors can therefore break the encryption algorithm and find the flag. Weak cryptographic algorithms, such as Vigenere cipher, can be broken by frequency analysis and brute force. Short key encryption and insecurely chosen small prime numbers in RSA are some examples of the cryptographic problems.

B. Attack and Defense

Attack and Defense CTF is a verisimilar contest in contrast to Jeopardy. The competitors are put into a closed environment, trying to attack each other. The server, a k.a. gamebox, is given to each team. Just like the real environment, several vulnerable services are deployed in the gamebox. The service can be any kind of network services, such as vulnerable website, and socket program. Therefore, the basic requirement for a competitor is to maintain service availability and at the same time to compromise other team's service.

To exercise the attack and defense skills, the whole life cycle of vulnerability, from vulnerability discovery to exploit development and service patch, is involved in the contest. Due to the identical environment given to each team, competitors need to analyze their service to discover the vulnerabilities. Then, the exploit code can be developed to steal the flag associated with each service as the evidence of successful compromise. At the same time, a competitor should protect his service from being compromised. Hence, patching the vulnerability is also an urgent task.

Attack and Defense CTF is a zero-sum game. If a team gains some score, the other team will lose the same score. Each service has three statuses: service alive, service down and service compromised. The minus points will be given for service down or service compromised. In the situation of service compromised, the losing score will be evenly given to the teams that successfully compromise this service. If a service is down, the score will be also evenly distributed to other teams whose service are still alive. Hence, the overall score remains the same during the contest.

As the real world, time is an important factor for the Attack and Defense CTF. The duration of competition is divided into several rounds, e.g. 5 minutes a round. In each round, the flag of each service is updated. Only the flag of current round is worth the score. Therefore, the earlier an exploit is developed, the more flags and higher score will be received. On the other

hand, patching the service earlier can mitigate the score loss in the early phase.

Not only the security skills can be trained in the Attack and Defense CTF, the system administration skill also plays an important role. Permission setting is the basic skill needed. With misconfiguration, the adversary can compromise the service. Monitoring system status to discover hidden backdoors and cleanup backdoor process is another important administrative work. Network packet analysis is not only used for defense but also used for attack. After understanding the attack method via network packet analysis, replay attacks may be possible by constructing other teams' attack exploits.

In contrast to the Jeopardy CTF held online for competitors around the world to participate, the Attack and Defense CTF is often held in a designed and controllable environment due to its complexity. Therefore, only a limited number of teams can participate in the contest.

C. *King of the Hill*

King of the Hill is the CTF type derived from the Attack and Defense CTF. King of The Hill is also held in the closed environment. Each team also needs to attack other teams and patch vulnerable services. The key concept of King of the Hill is keeping the control over the system as long as possible. The limited number of services will be provided to competitors. All the competitors can access each service and discover its vulnerabilities. After competitors get control of the service, they can try to patch the service and prevent other teams to take it over. The longer a competitor controls the service, the higher score will he receive.

King of the Hill CTF is verisimilar to the real world situation where only one team can take control of a service. Just like website defacement, each team should put their identity in the service to prove the successful compromise. Different from the Attack and Defense CTF where every team successfully compromising the service can get score, only the team remains in control of the service can gain the score. Other team does not get any score even if they compromised the service.

To reflect the real situation, the infrastructure in the King of the Hill consists of services widely used in the real world, such as LAMP server, AD server, database server and web server. Therefore, an attacker should polish his attack method for each service and at the same time gets familiar with operations to patch the service.

IV. CTF as Education for Practical Offensive Security Skill

To complement traditional security courses, CTF can educate students with verisimilar practices and real world problems. For the Jeopardy style CTF, competitors can learn a wide range of security problems, from web security to reverse engineering and software exploitation. In contrast, the Attack and Defense CTF focuses on the life cycle of vulnerability, thereby learning skills from vulnerability discovery to exploit development and software patching.

It takes time and effort to deploy new techniques, such as SDN and IoT, in the real world. However, CTF is based on the emulated environment, hence new techniques and platforms can be introduced more easily. For example, DEFCON final already used ARM architecture instead of x86 as the attack and defense architecture for several years. In Boston Key Party CTF, problems about SDN are given. Hence, not only practical but also advanced techniques can be exercised in the contests.

CTF can also be the playground for new attack methods. While solving the problems, competitor can adopt advanced attack to bypass some defense mechanism. Several advanced attack methods already appeared in CTF contests. For example, SROP (SigReturn Oriented Programming) is the attack method proposed in S&P 2014. And several problems related to research topics, such as symbolic execution and sandbox breaking, are designed as problems in CTFs.

Moreover, experience and skills learned from CTF can help competitors realize and deepen their research. DARPA recently launched a project called CGC (Cyber Grand Challenge). CGC is aimed to be the first CTF played solely by machines. In the contest, competitors have to automate the process of vulnerability discovery and software patching. This is just one of the examples that shows the impact of CTF experience to the future research.

In summary, CTF can complement traditional security education to enhance offensive security training. Putting the competitors into the CTF and facing real problems can bridge the theory and the practice. While solving the problems, both offense and defense skills can be practiced. The infrastructure used in the CTF contest can be the best playground for competitors to exercise their security skills.

Acknowledgements

This work is supported in part by Ministry of Science and Technology, Ministry of Education, TWISC, ITRI, III, iCAST, TTC, HTC, D-Link, Trend Micro Inc., Promise Inc., Chungshan Institute of Science and Technology, Bureau of Investigation, and Chunghwa Telecomm.

References

[1] DECON CTF, https://www.defcon.org/html/links/dc-ctf html

[2] SECCON CTF, http://ctf.seccon.jp/

[3] CodeGate CTF, http://ctf.codegate.org/

[4] RuCTF, http://www ructf.org/

[5] 0CTF, https://ctf.0ops.sjtu.cn/

[6] HITCON CTF, http://hitcon.org/2015/

[7] XCTF, https://time.xctf.org.cn/

[8] BCTF, https://bctf.cn/

[9] Backdoor CTF https://backdoor.sdslabs.co/

[10] ASIS CTF http://asis-ctf.ir/home/

[11] Hack.lu CTF http://2015.hack.lu/

[12] PlaidCTF http://play.plaidctf.com/

[13] Ghost in the Shellcode http://ghostintheshellcode.com/

[14] CSAW CTF https://ctf.isis.poly.edu/

[15] picoCTF https://picoctf.com/

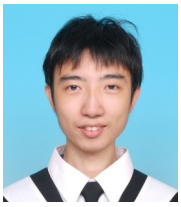
[16] HSCTF http://hsctf.com/

[17] PHDays CTF http://www.phdays.com/program/contests/

[18] iCTF http://ictf.cs.ucsb.edu/

[19] Pwnie Island http://pwnadventure.com/

[20] CTFTime https://ctftime.org/



Chung-Kuan Chen is a PhD Candidate in the Department of Computer Science, National Chiao Tung University (NCTU), Hsinchu, Taiwan. Contact him at ckchen@cs nctu.edu.tw.

Shiuhpyng Winston Shieh is a distinguished professor and past chair of the Department of Computer Science, NCTU; and the Director the Taiwan Information Security Center at NCTU. He is an IEEE fellow and ACM Distinguished Scientist. Contact him at ssp@cs.nctu.edu.tw.