Capture-The-Flag Framework and Virtual Environment for Cyber Security Education

Author: Jadiel A. Colón Pérez
Advisor: Jeffrey Duffany, Ph.D.
Electrical and Computer Engineering & Computer Science Department

Abstract

When studying cybersecurity or other computer-related technical careers, a problem among the students is the lack of hands-on experience. This can be solved by participating in internships, conferences, and competitions. Internship opportunities and local conferences are limited, and not every student has the flexibility to leave their homes, families, and even day jobs for a prolonged period. The solution that is being proposed is to incorporate a virtual environment that includes exercises like a Capture-The-Flag competition. These are designed to serve as an educational exercise used for experience in securing a machine, as well as conducting and reacting to attacks found in the real world. This environment will be coupled with a framework that allows students to submit the found flags and be evaluated instantly.

Introduction

Many competitions are organized around the world as capture the flag (CTF) events. They require students and/or participants to solve problems, earn points, and thus demonstrate their skills in different areas of cybersecurity [1]. They consist of a series of challenges that vary in their degree of difficulty and require participants to apply different sets of skills. The development of a learning environment framework in the form of a CTF competition is what is being discussed in this project. As part of the creation and validation of the framework, three CTF frameworks were analyzed and one was chosen. The frameworks that were considered were: Facebook capture the Flag, CTFd, and Mellivora. A CTF based on the Mellivora framework was chosen for several reasons: simple to use, light, very fast, and fits our required needs. For a long time, competitions have driven economies, research, and knowledge itself. The same could apply to education [1]-[2]. Its incorporation into an environment that is directly related to what students are learning in class could prove to be beneficial. The challenges include: network traffic analysis, steganography, open source intelligence, cryptography, among others.

Problem

The lack of hands-on experience when studying cybersecurity and computer science related disciplines is a serious problem that must be solved [3]. The proposed framework and virtual environment will fill in that gap by fulfilling the following goals:

- Assist participants in developing a solid foundation of cybersecurity related threats and concepts.
- Assist participants in developing a high level of proficiency in several cybersecurity software tools.
- Provide participants from diverse backgrounds and experience with an adequate difficulty level.
- Encourage participants to enroll into regional and international Capture-The-Flag competitions.
- Help students familiarize with the linux terminal and other non-Windows-related tools and software.

Background

Although the concept of CTF (Capture-The-Flag) competitions has existed for a long time now [4], these events came to prominence in 1996, when it was announced that one would be hosted at Defcon 4, one of the largest hacker conferences in the world [5]. Back then, the events were not as organized as we know them today. As an example, in Defcon 5 and 6, participants could choose between providing targets or attacking targets provided by others to earn points [6]. Since then, the game has advanced and grown into something almost completely different. The point scoring structures have become mostly automated, and organizers for the different competitions are named early as to give them time to arrange the necessary infrastructure. Furthermore, there are different types of CTF challenges, the main ones being the attack-defense CTFs, Jeopardy-style CTFs, and a mixture between the previous [7]. The basic principle of attack-defense CTFs is that each team is given the same set of vulnerable server software. Teams configure and analyze the software they are given before the actual competition starts [8]. Points are awarded for attacking other team's vulnerabilities and for defending your own systems. Jeopardy CTFs are the most common kind of CTFs. These usually involve certain challenges which are provided for the competitors by the people that are in charge of organizing the event [5]. The challenges usually range from very easy, to hard. Because of this, the points awarded are typically based on the set difficulty for the exercises.

Methodology

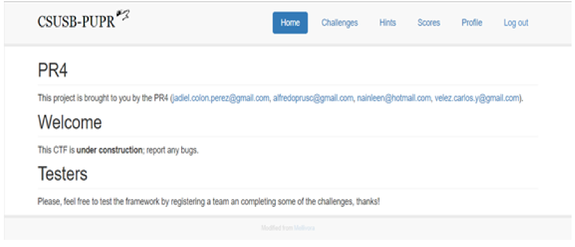

Figure 1
Finished Framework Layout

Because of the different needs and requirements of the environment, a custom CTF framework had to be built by using existent ones as reference. For this purpose, different CTF frameworks were evaluated. Some of these frameworks were the Facebook CTF framework, CTFd framework, and the Mellivora framework. In the end, it was decided that the best choice was the Mellivora framework. This decision was made for several reasons, like the fact that the Mellivora framework is written in PHP which is a simple language. It also works with a MySQL database, and the project itself is easy to deploy in an Apache Webserver. No public scoreboard was available for it, but it was added after the framework was implemented.

Methodology (Continued)

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

Figure 2
Partial Scan of The Vulnerable Services

For the virtual environment that was to accompany the CTF framework, it was important to include exercises and vulnerabilities that still represented real threats, even if they did so in a different way than presented in the project. A common problem that still affects developers and users alike is when hackers hijack an applications code and insert backdoors or malicious code into them. To demonstrate this vulnerability, the vsftpd includes an unintentional backdoor that can be exploited both manually, and by using a Metasploit module. Misconfigured services are also a security risk that plagues many businesses even today. In the TCP ports 512, 513, and 514, there are services known as "r" services. These have been purposely misconfigured to allow access to any remote host. Another common problem is the use of weak passwords [4]. Some of the accounts, including the root account, have a very weak password that can be broken by a simple brute force attack or a simple password list. Some of these passwords are "user", "batman", "123456789", and "service". The database services, like the PostgreSQL, can be accessed with the username "postgres", and the password "postgres", while the MySQL service can be accessed by "root" with a blank password. The attacking machine that would be used in the virtual environment was chosen to be Kali linux from the very beginning. This was determined taking into account that most of the tools that would be needed in order to solve the challenges already come preinstalled in Kali. Also, knowledge of Kali linux and the penetration testing tools that it contains is essential for any cyber security professional.

Results and Discussion

The environment and framework were initially developed by and for the NSF Scholarship for Service students as a means of practicing for other CTF competitions. Faculty and student training was later identified as another opportunity. There are several college courses that could benefit from a hands-on laboratory in the form of a CTF competition, but the ones that could fit best with what has currently been developed are Network Security (CECS 7230), Computer Forensics (CECS 7235), and Computer Security (CECS 7570). All of these courses belong to the Master Program in Computer Science, IT Management and Information Assurance area of interest, which is Approved by the NSA. Preliminary testing of the virtual environment demonstrates that the total amount of machines per each user still requires a lot of resources. Around 3 to 4 GB of RAM are necessary to keep each user's subnet functioning properly. Agreements are being made in order to host the virtual environment externally.

Future Work

In the future, the virtual environment should be adapted to handle NCL and CCDC type competitions. Online compilation is also in the process of being added to the framework, so that coding challenges can be included. The challenges also need to be modified so that they can resemble real-world scenarios. Vulnerabilities are in the process of being added and updated. The new machines should be deployed and tested inside the environment. Once the environment reaches a larger scale, a regional CTF competition should be hosted in order to get people interested in the topics related to cyber security.

Acknowledgements

I would like to thank Dr. Jeffrey Duffany for his support, not only as my project advisor, but also as a great mentor.

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract/award #1563978

References

[1] Leune, K, & Petrilli, S. J. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. Proceedings of the 18th Annual Conference on Information Technology Education – SIGITE '17. doi:10.1145/3125659.3125686
[2] Ford, V. et al. (2017). Capture the Flag Unplugged. Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education - SIGCSE '17. doi:10.1145/3017680.3017783
[3] Idika, N. C, et al. (2009). Maximizing network security given a limited budget. The Fifth Richard Tapia Celebration of Diversity in Computing Conference on Intellect, Initiatives, Insight, and Innovations - TAPIA '09. doi:10.1145/1565799.1565803
[4] Venter, H., & Eloff, J. (2003). Assessment Of Vulnerability Scanners. Network Security, 2003(2), 11-16. doi:10.1016/s1353-4858(03)00211-3
[5] About NCL. (n.d.). Retrieved May 17, 2018, https://www.nationalcyberleague.org/about
[6] Wargames. (n.d.). Retrieved May 18, 2018, from http://overthewire.org/wargames/
[7] Cobb, S. (2016). Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis. Retrieved from https://www.virusbulletin.com/uploads/pdf/magazin e/2016/VB2016-Cobb.pdf.
[8] National Collegiate Cyber Defense Competition. (n.d.). Retrieved May 19, 2018, from http://www.nationalccdc.org/