Implementation of Real-Time Cybersecurity Training through the Integration of a Hypervisor and an Online CTF Engine

Author: Carlos Y. Velez
Advisor: Dr. Alfredo Cruz
Electric & Computer Engineering and Computer Science

Abstract

During 2017 and 2018, undergraduate and graduate students from the ECECS Department at the PUPR have seen an academic improvement in cybersecurity from their participation in Capture the Flag competitions. Three CTFs; National Cyber League, Cyberfire, and in-house CTF framework are discussed in this paper. The NCL competitions saw a score percentage increase in Log Analysis and Wireless Application Exploitation. In the 2018 Cyberfire competition, the PUPR team won first place among more than 100 teams including top universities. The recent implementation of the PUPR CTF framework has spiked the interest of students across the campus. To date, an improvement in critical thinking, teamwork, and familiarity with real-life scenarios is benefiting students at our department. Based on these observations, we aim to continue monitoring student development, in addition to incorporating topics covered in the CTFs into the curriculum.

Introduction

Capture the flag events (CTFs) are puzzle-style challenge that provide a platform that mimics current cybersecurity breaches and provide a controlled environment for students and other security professionals to solve cyber threats in a timely manner.

We wanted to measure the progress of students from the ECECS at PUPR in CTF's events; and based on the results provide students with an in-house training framework for practicing real-life cybersecurity scenarios that are tailored to supporting their weakest areas. This research combines an online CTF with a virtual machine monitor (hypervisor) as a self-contained environment.

Background

At this time, for CTF training, students can go to CTFtime.org, a CTF advertisement website or go to VulnHub and download one of the VMs to practice offline. For CTFtime.org, the student can only participate in high difficulty CTFs hosted by an institution or company. The VulnHub website is designed only for offline use and requires downloading one of the VMs and installing it in a host-based virtualization software (e.g., VirtualBox or VMware) in order to run it.

Problem

Can an integration of VM management with an online CTF engine be implemented to provide real-time cybersecurity training for students? In our research we modify a deployment by assigning each participant a unique VM and provide full access to the source code. **Advantage:** each participant can now independently identify, modify and execute the code until bugs and patches are corrected.

Methodology

Category data for 2017 and 2018 NCL competitions, presented side by side (see Table 1 and 2). The bracket distribution identifies where we fall in the national level by dividing the total number of teams between the top 15% (gold), the following 35% (silver) with the remaining 50% (bronze). For performance evaluation across both years, we identified the three categories with lower score percentages of total score for both years. We calculated the mean value of the three lowest score percentages for each year and compare them. Based on the results, we proceeded to analyze by identifying variables (e.g., undergraduate vs graduate participant ratio) that could have contributed to the differences.

We created a virtual environment that consists of a network of several virtual machines with known vulnerabilities (see Figure 1). A main Windows Server 2012 with Hyper-V services accommodates the environment. These will be designed using a metric that will calculate the student's score based on how many challenges were successfully answered. The administrator will have online real-time reports of each student's progress. Challenges will focus on network traffic analysis, web application exploitation, enumeration and exploitation, and password cracking among others.

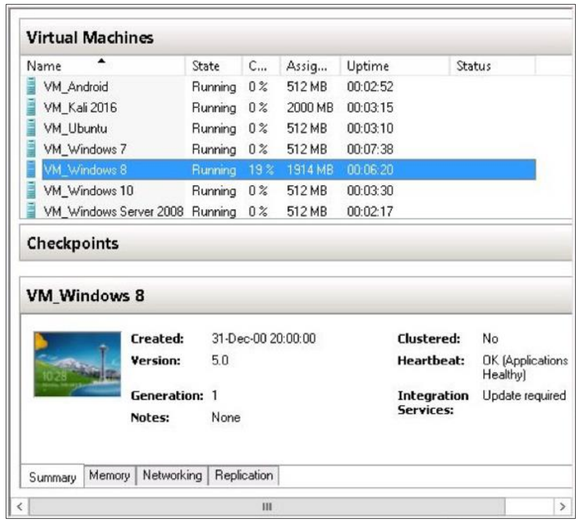

Figure 1 Physical server with a virtual environment consisting of seven VMs.

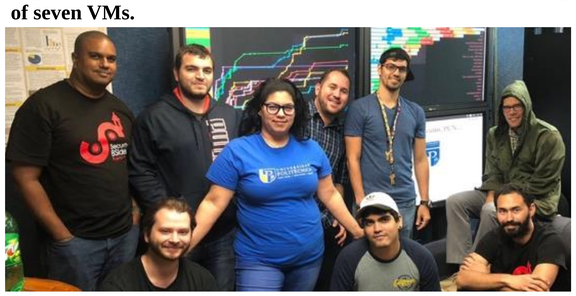

Figure 2 Part of the team (left to right standing: Andre, Jadiel, Nainleen, Luis and Yoshuam; kneeling: Ernesto and Alfredo; sitting: John and Carlos)

Results and Discussion

During the Cyberfire competition in 2018, PUPR team won the first place among more than 100 teams from universities across the US, (see Figure 2 and Figure 3, PUPR highlighted in dark blue).

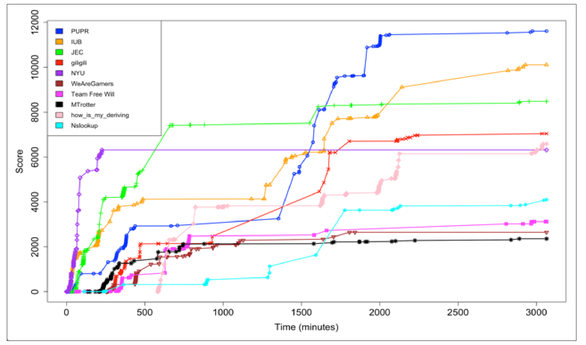

Figure 3 Cyberfire CTF score (PUPR Team in dark blue). Time line graph with scores in the vertical axis and the time in the horizontal axis.

For the 2017 NCL Spring competition, PUPR ranked 15 in the whole nation. In addition, the PUPR managed to score 5th place within the bracket for the whole distribution by categories. In 2018, a new team was formed to participate once again, where PUPR team improved their Total Score Percentage for the Log Analysis and Wireless Exploitation categories.

For the CTF framework, a total of 3 competitions have been hosted successfully, with a participant managing to solve all the challenges and scoring the maximum possible score of 3000 points (see Figure 4).

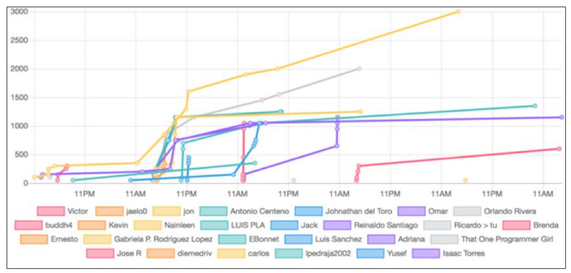

Figure 4 PUPR CTF framework Time line graph with scores in the vertical axis and the time in the horizontal axis.

Table 1 Results from NCL Spring 2017

Categories	Bracket Rank	National Rank	Total Score	Total Possible Score in Game	Total Flag Capture	Total Flag in Game	Total Flag Attempts	Accuracy (%)
Cryptography	5	10	580	680	17	19	22	77
Enumeration and Expl.	1	3	310	510	4	5	4	100
Log Analysis	3	9	450	500	15	16	19	79
Network Traffic Analysis	13	28	310	610	17	22	23	74
Open Source Intelligence	8	13	185	185	22	22	27	81
Password Cracking	9	26	515	750	24	28	24	100
Scanning	5	17	330	350	17	18	25	68
Web App. Exploitation	6	13	85	240	2	7	2	100
Wireless Access Exploitation	17	43	235	375	12	14	12	100
Total	5	15	3150	4150	131	148	159	82

Table 2 Results from NCL Spring 2018

Categories	Bracket Rank	National Rank	Total Score	Total Possible Score in Game	Total Flag Capture	Total Flag in Game	Total Flag Attempts	Accuracy (%)
Cryptography	19	79	235	375	13	18	14	93
Enumeration and Expl.	10	50	100	200	5	6	5	100
Log Analysis	3	7	400	400	25	25	26	96
Network Traffic Analysis	49	159	85	525	7	32	10	70
Open Source Intelligence	14	54	185	225	15	16	15	100
Password Cracking	25	106	125	400	10	24	11	91
Scanning	21	99	110	250	9	15	11	82
Web App. Exploitation	26	92	65	300	3	10	4	75
Wireless Access Exploitation	15	71	175	225	13	14	17	76
Total	19	93	1580	3000	101	161	114	89

Conclusions

A decrease in score percentage during the NCL 2017 and NCL 2018 appears to be related to an increase in difficulty level in challenges and increase in team participation. In addition, PUPR team experience level was less in 2018, due to higher number of participants with an undergraduate level. Ongoing CTF development has peaked student's interest in the cybersecurity field, with 27 students participating. Better metrics such as score by category, percentage of completion by student and team scores would allow the administrator to have the ability to design a better cybersecurity training based on outcome analysis. In addition, a self-participant's assessment pre-challenge would provide a base for further metrics.

Acknowledgements

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

Alicea, Y. (2017, April). Cybersecurity Competitions as Effective Cybersecurity Teaching Tools. *In the Annual Information Institute Conference, eds. g. Dhillon and s. Samonas*.

Chothia, T., & Novakovic, C. (2015). An Offline Capture the Flag-Style Virtual Machine and an Assessment of its Value for Cybersecurity Education. *In Summit on Gaming, Games, and Gamification in Security Education.*

Chung, K., & Cohen, J. (2014). Learning Obstacles in the Capture the Flag Model. *In Summit on Gaming, Games, and Gamification in Security Education.*

Duffany, J. (2015, July). Active Learning Applied to Introductory Programming. *In XIII Latin American and Caribbean Conference for Engineering and Technology*.

Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017, March). Capture the Flag Unplugged: An Offline Cyber Competition. *In the ACM Technical Symposium on Computer Science Education*.

Gavas, E., Memon, N., & Britton, D. (2012). Winning Cybersecurity One Challenge at a Time. IEEE Security Privacy, 10(4), 75-79.