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

Carlos Y. Velez Rodríguez
Master in Computer Science
Advisor: Dr. Alfredo Cruz
Electric & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

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 (CTF) competitions. These strategy-based cybersecurity challenges, often hosted by universities, federal agencies, and national laboratories, can serve as an applied learning tool. Three CTFs in particular; 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.*

Key Terms *— CTF, Cryptography, Cybersecurity, Hypervisor.*

INTRODUCTION

Capture the flag events, better known as CTFs, are puzzle-style challenge competitions that are often sponsored and hosted by universities and federal agencies. These competitions 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.

At this time, for CTF training, students can go to CTFtime.org, a CTF advertisement website, to participate in one of the current CTFs. Another approach is to go to VulnHub and download one of the VMs to practice offline. When practicing in the CTFtime.org, the student can only participate in a CTF hosted by an institution or company. Most of the time, these CTFs are very challenging, requiring vast amounts of experience and therefore are not suitable for novices. 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.

While many computer scientists have implemented virtual laboratories [1] [2] [3] and CTF engines [4] [5] [6] in educational curricula, an integration of both techniques as a framework can be of benefit to students. In 2004, Mirkovic deployed a vulnerable stand-alone web-server where red and blue teams created and analyzed various CTF challenges [7]. A disadvantage to this method is that students from the blue team were only able to identify vulnerabilities but were not able to modify the code.

In our research we modify a similar deployment by assigning each participant a unique VM and provide full access to the source code. The advantage is that each participant can now independently identify, modify and execute the code until bugs and patches are corrected. This research tries to answer

the question: Can an integration of VM management with an online CTF engine be implemented to provide real-time cybersecurity training for students?

CAPTURE THE FLAG EVENTS

Undergraduate and graduate student's engagement in CTF competitions improves confidence by providing an opportunity to solve real-life cybersecurity scenarios [1]. In addition, students have benefited from the teamwork and leadership which has resulted in improved soft-skills. At PUPR, professors in cybersecurity courses highly encourage CTF competitions as a means of improving critical thinking, motivating, and improving student's confidence. At the same time, teamwork encourages the participation of in-experienced students who then benefit from adept students in the CTF environment.

In 2017, Alicea studied the effectiveness of CTFs as a cybersecurity teaching tool [8]. According to his study, after participating in CTFs, inexperienced students improved in the areas of cryptography, open source intelligence, and password cracking. While CTFs are generally considered beneficial, in 2014, Chung and Cohen identified problems with participation, quality assurance, and confusing challenges while performing the Cybersecurity Awareness Week (CSAW) CTF [9].

This study builds on findings by Alicea [8], and describes how CTFs improve critical thinking, teamwork and familiarizes students with real life scenarios. Since 2016, a diverse group of undergraduate and graduate students, with varying degrees of CTF experience, have participated in periodical CTFs. In particular, the individualized NCL, CCDC and Cyberfire competitions have served as a setting for: student exposure to challenges based on CompTIA Security+™ and EC-Council Certified Ethical Hacker (CEH)™ certification objectives, management and protection of existing network infrastructure, and learning as you play style challenges, all these have positive results as students are more engaged and eager to continue participating in challenges, regardless of difficulty. This paper focuses on how participation in CTF's allows students to gain knowledge that prepares them for more advanced cybersecurity courses.

CTF competitions emphasize team diversity and also focus on skills and training under pressure, but in a monitored environment [10]. These competitions train students across the nation and provide necessary skills so that they may become qualified for information assurance careers. During the 2016-2018 school year PUPR students took full advantage and participated in many events, including the NCL competition [8].

The NCL, CCDC and Cyberfire competitions are discussed here. The team's name "1nc0gnito", is based on an obfuscation that incorporates binary characters. "1nc0gnito" consists of computer science, computer engineering, and electric engineering undergraduate and graduate students. Students from other departments are welcome to join as well.

FRAMEWORK

Since the 1990s education about information technology has been moving into the online realm as seen in [11]. While traditional methods involving physical hardware can be used, their effectiveness is limited by the high cost of hardware and software in addition to the creation, configuration and maintenance of the laboratory environments [12].

Presently, students are being provided with the option to take hands-on online courses as part of departmental curriculum [13]. There have been several methods in which hands-on online courses and cybersecurity training have been implemented, including blended learning approaches, virtual environments, and Docker containers [14] [15] [16].

This framework integration focuses on the implementation of a virtual environment and CTF combined with modified "active learning" techniques [17]. It also allows the administrator to build training tailored to a particular course by

including several VMs with operating systems such as Windows 7, Windows 10, Ubuntu Linux, Kali Linux, and CentOS Linux among others.

METHODOLOGY

The CTF Score data was collected from reports generated by administrators after events concluded. For the 2017 and 2018 NCL Spring competitions we received data for the general and individual competencies (cryptography, enumeration and exploitation, log analysis, network graphic analysis, open source intelligence, password cracking, scanning, web application exploitation, and wireless access exploitation), and for brackets, ranks, total score, total flag capture, total flag attempts, and accuracy percentage. For the 2017 Cyberfire competition we received a timeline summary and individual and national score data for base, binary reverse engineering, code breaking, IP and subnetting, JavaScript, no code, ports and protocols, sequence, steganography, and wopr competencies.

For the 2017 and 2018 NCL competitions, data for each category is presented side by side in tables. For the bracket distribution, we will identify 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). To evaluate performance 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 and number of teams participating) that could have contributed to the differences.

To integrate the challenge component some categories were designed within a virtual environment. As an active learning complement, a collaboration between students is required for each challenge; offering students active interaction about each other's selected topic.

The intention is to create 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 will accommodate 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.

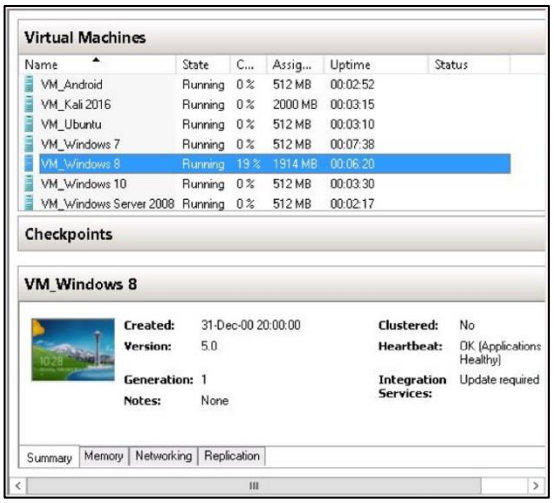

Figure 1
Physical Server with a Virtual Environment Consisting of Seven VMs

FRAMEWORK

In order to accomplish the necessary training and/or practice for the various CTF events, a framework was designed in order to provide reliability, availability, security and room for expansion. There were five components used to construct the framework: deployment (hardware and software), administration (categories, challenges and submissions), Messaging (Mass emails and email scripts), timeline (uses chart.js library), security (captcha, and SSL certificate), server management (VM creation, VM deployment and VM check points) and VM mass script.

The virtual environment will be a self-contained entity able to accommodate previously made

challenges organized in different categories. At the end of each competition, the student will be given an online assessment that will provide metrics. At the same time, the assessment will provide the student with feedback on where to go look for more information and/or tools to facilitate the completion of the challenges in the future. The hardware is capable to maintain more than 30 VMs running for a week to host a typical competition. The system administration is able to reset, stop and start any VM in seconds. In addition, mass scripting is also possible to accomplish, very useful for challenge deployment at a specific time during the event.

COMMANDS FOR LINUX AND WINDOWS CATEGORY

To solidify the student's knowledge of basic commands, this category will focus on reviewing and applying the utilization of commands from routine tasks such as navigation, file and folder creation, deletion and naming to more advanced commands that allow network debugging, identification of the computer's IP address, DNS and trace routes in both Linux and Windows systems. Students will be trained on the following tasks for Linux and Windows operating systems:

1. In these challenges the student will learn how to use the Linux man, ls, cd, mkdir, rmdir and cat commands. Students will need to access the General Commands Manual to learn how each command functions. They will then be able to use the commands to navigate between directories, create and delete folders and display file content. In Windows, to access information about a specific command, the student needs to type "/?" after the command. Commands used to navigate files and folders include cd, dir, mkdir, and rd /s /q. The command type is very similar to the cat command in Linux.
2. The second task focuses on manipulation of files and folders through the use of find, locate, grep, sort, and uniq Linux commands while in Windows the commands are find, findstr and sort. These will allow the student to examine strings in multiple files; ideal for log manipulation.
3. Linux network commands such as ifconfig, ping, netstat, traceroute, nslookup and route allow the student to troubleshoot and identify network parameters. In Windows the commands used are ipconfig, ping, tracert, netstat, and nslookup. This new information further permits an administrator to determine how secure is the network to carry out communications with other systems.
4. This task aims to teach the students how to connect to remote systems and services through the use of Linux telnet, ssh and ftp commands. In Windows, only the ftp command is available while Putty (an open source software) will be used for ssh and ftp connections. A successful connection would, in the case of telnet and ssh, provide full access to a remote system. In the case of ftp, files can be transferred securely over the network.

FOOTPRINTING CATEGORY

Students will learn how to scan the source code of a website in search for content written in JavaScript, CSS, and HTML to obtain web cookies. This will be done by using an add-on tool for Mozilla Firefox called Firebug. To do this, students will perform the following challenges:

1. Install the Firebug add-on to Mozilla Firefox.
2. Open the provided website address and scan the source code to retrieve the cookies.
3. Provide specific information about the cookies (e.g., content, amount, and size).

Students will also extract meta tags, emails, phone numbers, faxes and URLs from company web-pages using the Web Data Extractor tool. This information can then be used by students to impersonate someone from one of the company websites. Students will also learn how hackers duplicate entire websites using the HTTrack tool. In addition, the Path Analyzer Pro tool will be used to obtain trace routes, DNS and other routing

information and registries from websites that are not well configured.

To do this, students will perform the following challenges:

1. Install Web Data Extractor, HTTrack and the Path Analyzer Pro tools.
2. Scan a specific website using all the tools.
3. In a new file, save the output from the Web Data Extractor.
4. Duplicate the entire website using the HTTrack tool.
5. Recover the output provided by the Path Analyzer Pro tool.

SCANNING AND ENUMERATION CATEGORY

This category teaches how to monitor data traffic (.pcap file) within a network using the Wireshark packet analyzer. In addition, students will perform Nmap scans on both Windows and Linux machines to spot open ports and identify operating systems in the network. Other scans will include Xmas Scans, ACK Flag Scans, UDP Scans, and IDLE Scans.

To do this, student will perform the following challenges:

1. Install Nmap and Wireshark packet analyzers.
2. Scan single and multiple IP addresses, perform fast scans and detect remote operating systems using Nmap.
3. Analyze a .pcap file to provide host and destination IP addresses, sequence numbers, header length and window size using Wireshark.
4. Duplicate the entire website using the HTTrack tool.
5. Specific to the FTP protocol, the student will analyze a .pcap file for FTP traffic like username, password, names of files transferred and destination folder using Wireshark.

ENCRYPTION CATEGORY

Students will learn basic encryption processes like Caesar, Vigenère and Playfair ciphers. These processes serve as the base for more advanced techniques such as Blowfish and Gost encryption algorithms. In this category, students will apply CryptoForge to solve highly advanced algorithms. A very important part of this challenge is the usage of a web application that shows a step by step encryption/decryption process of the DES algorithm. As a result, students will be able to identify weak encryption keys. Hashes allow students to learn how to detect files that have been modified or corrupted. During a second part of this category, students will learn how to calculate the hash values of files. To accomplish this, on Windows machines they will use the HashCalc tool, while on Linux, they will use built-in commands.

To do this, student will perform the following challenges:

1. Students will access the Caesar, Vigenère and Playfair ciphers online and will answer questions related to this in the assessment.
2. Install the CryptoForge tool.
3. Encrypt and decrypt files by using any of the following algorithms found in CryptoForge: Blowfish, Rijndael, TripleDES or Gost.
4. Identify the weak keys for the DES algorithm using the web application.
5. Install the HashCalc tool.
6. Calculate the ADLER32, MD5, SHA-1 and SHA-512 hashes of a given file using the HashCalc on a Windows machine.
7. Calculate the MD5, SHA-1, SHA-256, SHA-512 hashes of a given file on a Linux machine using commands.

PASSWORD CRACKING CATEGORY

The objective of this category is for students to use the ophcrack tool to determine what is the password used by a specific username in a Windows machine. To do this the students will need to complete two steps: extract the Security Account Manager (SAM) database file from the user's Windows machine using the pwdump7 tool and decrypt hashes from the SAM into readable passwords.

To do this, students will perform the following challenges:

1. Install the pwdump7 tool.
2. Extract the SAM using the pwdump7 tool.
3. Install the ophcrack tool.
4. Load the rainbow table and the SAM file to the ophcrack tool.
5. Run the ophcrack tool (crack) to obtain the possible plaintext passwords for that username.

Web Server Vulnerability Category

This category covers the use of Wpscan and Metasploit tools to find vulnerabilities placed in a local web server. Furthermore, the student will learn how to patch these vulnerabilities until the web server is secured.

To do this, students will perform the following challenges:

1. Launch Wpscan from a Kali machine.
2. Using the Wpscan tool, scan the Wordpress website located inside the local web server to find the PHP and the Wordpress version numbers, installed plugins and usernames.
3. Launch Metasploit and select the "wordpress-login-enum" auxiliary module.
4. Load the PasswordList.txt file to perform a dictionary attack.
5. Login to the Wordpress website using the obtained credentials.

Results

Cyberfire is a highly competitive national-level cybersecurity competition hosted by Lawrence Livermore National Laboratory and Los Alamos National Laboratory. It emphasizes critical thinking and teamwork to solve cybersecurity challenges. In 2018, PUPR team won the first place among more than 100 teams from across universities in the United States (see Figure 2) where PUPR is highlighted in dark blue. This was a virtual online event that began on Friday January 26, 2018 and concluded Sunday January 28.

Puzzles covered in this event included applying various topics of cybersecurity, where critical thinking and teamwork were necessary to solve the challenges. Categories included Base Conversion, Binary Reverse Engineering, Code-Breaking, IPs and Subnetting, JavaScript Obfuscation, No-Code (logic problems), Ports and Protocols, Sequence and Steganography. When teams unlocked a category, other team's score for that specific category decreased until they could score too. In addition, a team that completed 30% of the points in each of five categories, gets a multiplier of 1.5.

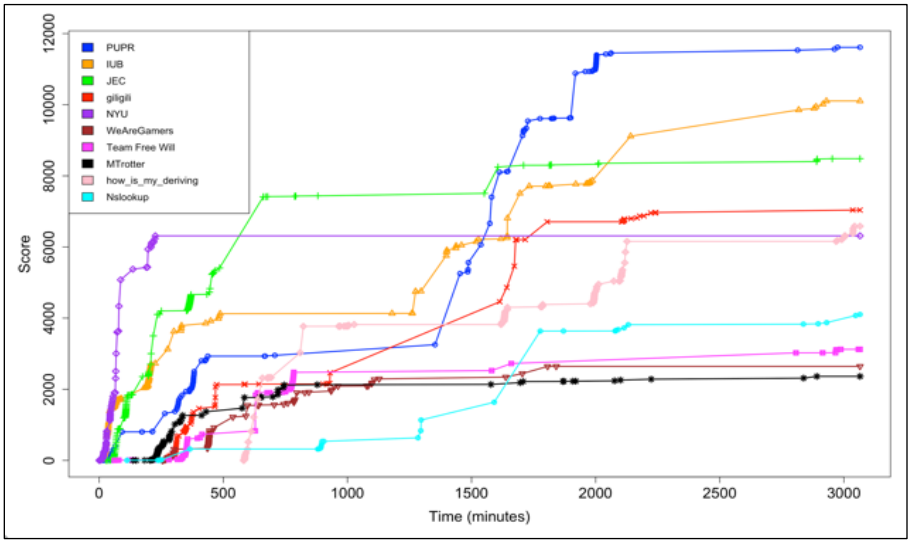

Figure 2
Cyberfire CTF Score (PUPR Team in dark blue)

PUPR team scored 100% in seven categories, while categories for JavaScript, Code Breaking and WOPR scored less than 80%. Students faced a difficult time working through the Code Breaking and WOPR categories, most likely because these topics are not covered in the classroom. As a result, the PUPR team has begun studying and have started talks with the administration to incorporate these in a reverse engineering course.

In the case of JavaScript, the last puzzle left had a maximum score of 2,000 points. The complexity required the analysis of an obfuscated script that used a key string presented in the HTML source code, something the team did not realize at the time. For the Code Breaking and the WOPR categories, the team did not have enough experience or knowledge to solve the puzzles in a timely manner. For Steganography only 16 teams were able to complete at least one point. For a previous competition, PUPR team created a repository with steganography tools that became essential to solve the puzzles.

The team consisted of 12 undergraduate and graduate students (see Figure 3) were 5 of them are junior undergraduate students who are eager to continue the legacy of this unique Cybersecurity team. More than half of the team had taken courses in advanced cryptography and were able to pull resources together to identify the hidden messages.

Figure 3
Part of the Team at the End of the Competition (from left to right standing: Andre, Jadiel, Nainleen, Luis and Yoshuam; kneeling: Ernesto and Alfredo; sitting: John and Carlos)

The NCL team participation saw an increase in bracket distribution from 152 in 2017 to 256 in 2018, with a difference of 104. For the 2017 competition, the PUPR team ranked Silver, signifying values between the top 15% to 50% range, while in 2018, the PUPR team ranked Bronze, signifying values on the lower 50%.

For the 2017 NCL Spring competition, PUPR ranked 15 in the whole nation. In addition, the PUPR managed to get number 5 within the bracket (see Table 1) for the whole distribution by categories. The next year, in the 2018, a new team was formed to participate once again. This year, the PUPR team improved in the categories: Log Analysis and Wireless Exploitation (see Table 2) for the Total Score Percentage.

In general, for the total score percentage, an increase of 10% and 15% were observed for the Log Analysis and Wireless Access Exploitation categories, respectively between 2017 and 2018. The remaining seven categories showed a decrease of 11% in Enumeration and Exploitation, 14% in Web Application Exploitation, 18% in Open Source Intelligence, 23% in Cryptography, 35% in Network Traffic Analysis, 37% in Password Cracking, and 50% in Scanning.

In particular, the categories with the lowest scores in 2017 were: Web Application Exploitation (35%), Network Traffic Analysis (51%), and Enumeration and Exploitation (61%). In 2018, these categories scored 22%, 16%, and 50%, respectively (see Tables 1-2).

For the CTF framework, a total of 3 competitions has been successfully hosted where a participant managed to solve all the challenges scoring the maximum possible score of 3000 points (see Figure 4) for the timeline graph showing all scores in the vertical axis and the time in the horizontal axis. During these competitions, students were able to use their assigned virtual machines for various challenges in cryptography, password cracking, web analysis exploitation, log analysis and web exploitation. Some of them required installation, configuration and deployment of hacking tools.

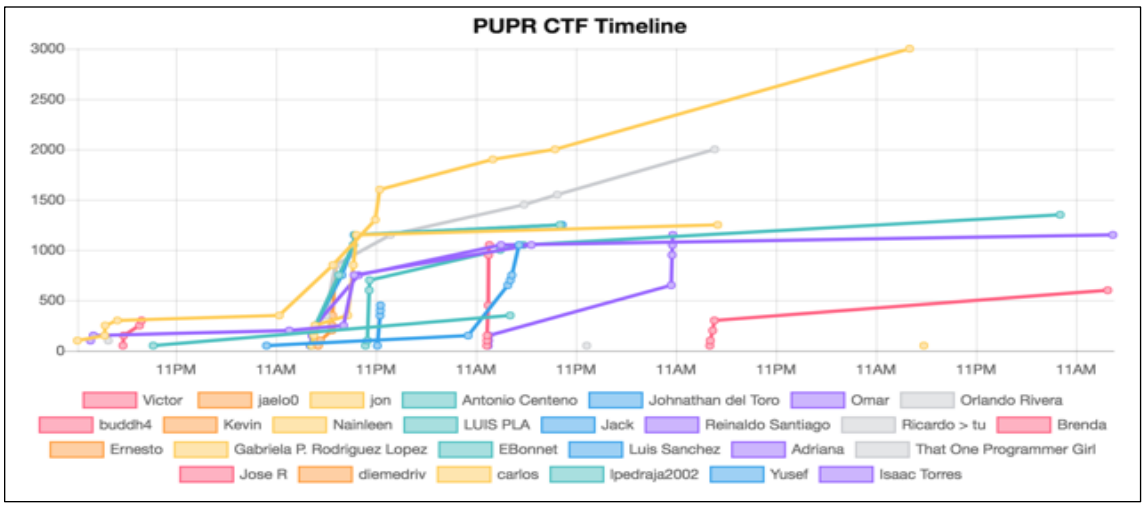

Figure 4
PUPR CTF Score

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
Enu & Expl.	1	3	310	510	4	5	4	100
Log Analysis	3	9	450	500	15	16	19	79
Net. Tra Ana.	13	28	310	610	17	22	23	74
Open S. Intel	8	13	185	185	22	22	27	81
Pass Crack	9	26	515	750	24	28	24	100
Scanning	5	17	330	350	17	18	25	68
Web App. Ex	6	13	85	240	2	7	2	100
Wir Acc Expl.	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
Enu & Expl.	10	50	100	200	5	6	5	100
Log Analysis	3	7	400	400	25	25	26	96
Net. Tra Ana.	49	159	85	525	7	32	10	70
Open S. Intel	14	54	185	225	15	16	15	100
Pass Crack	25	106	125	400	10	24	11	91
Scanning	21	99	110	250	9	15	11	82
Web App. Ex	26	92	65	300	3	10	4	75
Wir Acc Expl.	15	71	175	225	13	14	17	76
Total	19	93	1580	3000	101	161	114	89

DISCUSSION

For the NCL, a decrease in ranking from silver to bronze appears to be related to an increase in competitiveness of 104 teams for the 2018 with respect to the 2017 competition.

An effort was made to practice challenges that dealt with Log Analyses, Wireless Access Exploitation, Cryptography, and Web Application Exploitation, but only Log Analyses and Wireless Access Exploitation saw a score increase. In 2017, a total of 10 students, 6 graduates (only 4 had experience) and 4 (only 3 had experience) undergraduates. In 2018, a total of 5 students, 3 graduates (experienced) and 2 undergraduates (no experience). For 2017, the ratio of experienced vs inexperienced participants was 2.3 while in 2018 the ratio was 1.5, which could have resulted in the observed decrease in performance. According to participants, they observed an overall increase in challenge complexity which made it difficult to answer the challenges on time, resulting in many unanswered questions.

The three lowest categories for 2017, Web Application Exploitation, Network Traffic Analysis, and Enumeration and Exploitation saw a decline in score percentage of 13%, 35%, and 11%. In the case of Web Application Exploitation one of the difficulties experienced by the participants scores was the unfamiliarity with the implementation of new software tools. For the other two categories, the difficulty appeared to have increased which might have resulted in partial answers to challenges.

A total of 44 challenges covering 7 categories were created with a participation of 27 students from PUPR. Seven of those students were not able to complete any of the challenges (see Figure 4 shown above). For the Password Cracking category, out of the 3000 possible points, the average was 681 points, representing a 23% completeness.

Because the CTF was open to all students of the PUPR community, not all of them were experienced in these types of competitions or had the necessary programming skills. This possibly resulted in 7 students performing very poorly and unable to complete any of the challenges.

This was an astonishing success from the PUPR team among recognized teams including universities such as New York University, Indiana University, Western Carolina University, California State University, University of North Carolina and the University of Puerto Rico. The competition was intended to last for 48 hours but due to some server downtime it was extended to 53 hours. The puzzles covered in this event included various topics of cybersecurity where critical thinking and teamwork are necessary to solve them. The categories included base conversion, binary reverse engineering, code-breaking, IPs and subnetting, JavaScript obfuscation, no-code (logic problems), ports and protocols, sequence problems and steganography.

CONCLUSION

A decrease in score percentage during the NCL 2017 and NCL 2018 appears to be related to an increase in difficulty level of challenges and increase in team participation. In addition, PUPR team experience decreased from 2017 to 2018, due to encouragement for undergraduate students' participation. 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 the outcome. In addition, a self-participant's assessment pre-challenge would provide a base for further metrics.

ACKNOWLEDGEMENTS

I would like to thank Dr. Alfredo Cruz for his tremendous support, as an advisor in this research and as a true mentor during my entire degree.

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] M. Lehrfeld and P. Guest, "Building an ethical hacking site for learning and student engagement," in *SoutheastCon 2016*, Norfolk, VA, 2016, pp. 1-6.

[2] S. Roschke, C. Willems and C. Meinel, "A security laboratory for CTF scenarios and teaching IDS," in *2010 2nd International Conference on Education Technology and Computer*, Shanghai, 2010, pp. V1-433-V1-437.

[3] J. Son, C. Irrechukwu and P. Fitzgibbons, "A Comparison of Virtual Lab Solutions for Online Cyber Security Education," vol. 12, no. 4, 2012, pp. 173-179.

[4] T. Chothia and C. Novakovic, "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*, 2015.

[5] V. Ford, A. Siraj, A. Haynes and E. Brown, "Capture the Flag Unplugged: An Offline Cyber Competition," in *The ACM Technical Symposium on Computer Science Education*, 2017, pp. 225-230.

[6] E. Nunes, N. Kulkarni, P. Shakarian, A. Ruef and J. Little, "Cyber-Deception and Attribution in Capture-The-Flag Exercises," in *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2015.

[7] J. Mirkovic and P. Peterson, "Class Capture-The-Flag Exercises," in *Summit on Gaming, Games, and Gamification in Security Education*, 2014.

[8] Y. Alicea, "Cybersecurity Competitions as Effective Cybersecurity Teaching Tools," in *The Annual Information Institute Conference*, April, 2017.

[9] K. Chung and J. Cohen, "Learning Obstacles in the Capture the Flag Model," in *Summit on Gaming, Games, and Gamification in Security Education, 2014*.

[10] E. Gavas, N. Memon and D. Britton, "Winning Cybersecurity One Challenge at a Time," in *IEEE Security & Privacy*, vol. 10, no. 4, July-Aug., 2012, pp. 75-79.

[11] A. Smeaton, "Using Hypertext for Computer Based Learning," in *Computers & Education*, vol. 17 no. 3, 1991, pp.173-179.

[12] C. Willems, W. Dawoud, T. Klingbeil and C. Meinel, "Security in Tele-Lab — Protecting an online virtual lab for security training", in *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, London, 2009, pp. 1-7.

[13] D. Wu, J. Fulmer, and S. Johnson "Teaching Information Security with Virtual Laboratories," in *Innovative Practices in Teaching Information Sciences and Technology: Experience Reports and Reflections*, 2014, pp. 179-192.

[14] J. Wang, W. Cheng, H. Chen and H. Chien, "Benefit of construct information security environment based on lightweight virtualization technology," in *2015 International Carnahan Conference on Security Technology (ICCST)*, Taipei, 2015, pp. 1-4.

[15] C. Willems, T. Klingbeil, L. Radvilavicius, A. Cenys and C. Meinel, "A distributed virtual laboratory architecture for cybersecurity training," in *2011 International Conference for Internet Technology and Secured Transactions*, Abu Dhabi, 2011, pp. 408-415.

[16] T. Zlateva, L. Burstein, A. Temkin, A. MacNeil and L. Chitkushev, "Virtual Laboratories for Learning Real World Security," in *Colloquium for Information System Security Education*, June, 2008.

[17] J. Duffany, "Active Learning Applied to Introductory Programming," in *XIII Latin American and Caribbean Conference for Engineering and Technology*, July, 2015.