SecurityTeam@IST

Diogo Miguel Barrinha Barradas

Activities Report

Abstract—The present report describes the execution of my activity while being a member of STT. This team was created with the objective of improving students' skills regarding cibersecurity topics, in an informal and student-driven manner. During the execution of the activity I attended five team meetings where I was able to listen to presentations about specific cibersecurity topics and to apply the acquired knowledge in brief hands-on sessions. Apart from STT meetings, the real action happened in CTF competitions, where we applied the acquired skills in order to solve cybersecurity challenges. Such competitions are not only a way to improve and learn, but also to help the team climb the ranks and to get recognized.

CTF competitions were a good experience, particularly regarding teamwork. Apart from being able to advance through several challenges myself, teamwork was essential for us to get through more intricate challenges. STT has filled a gap in the actual MEIC curriculum, reinforcing the need for education over the cibersecurity topic.

Index Terms—capture the flag, cybersecurity, information systems, IST, MEIC, STT.

1 Introduction

THIS report describes the activity I performed for the Independent Studies course at Instituto Superior Técnico (IST), while being a member of Security Team at Técnico (STT). Section 2 of the report describes the way the team organized and when meetings took place. In Section 3 I detail what a Capture The Flag (CTF) competition is as well as its different types and what do they entail. Section 4 focus on providing a detailed report on the problems I had to tackle in the CTF competitions that the team attended and Section 5 describes the STT meetings I have attended since the beginning of this activity. Section 6 concludes this document, stating the main difficulties faced and in what way my efforts can be driven to help the team achieve better results in the future.

2 STT Organization

Cybersecurity is a growing concern as an attacker located anywhere in the world can exploit a system vulnerability in order to steal information or disrupt a given type of service. Since its inception, STT aims to improve students' skills on how to address cybersecurity issues through the study and exploitation of vulnerabilities. Related topics such as cryptography and digital forensic analysis are also approached in a very practical fashion. The team has informal meetings once every two weeks, while trying to participate in a CTF competition at least once a month. Students are also encouraged to study and practice their skills at home.

Typically STT meetings pose as a briefing, where the designated session leader presents a type of attack, vulnerability or a step-by-step guide on how to solve a given problem from previous CTFs. Usually these presentations give a theoretical background on the problem being addressed, followed by a hands-on exercise that exposes students to the tools/technology being used.

Currently there are plenty of students connected to STT (about 80). However, this number also takes into account students who were curious about the teams activities and seldom showed up. The number of people that closely follow the team's activities and actively par-

- *Diogo Miguel Barrinha Barradas, nr. 73578,*
  E-mail: diogo.barradas@tecnico.ulisboa.pt,
  Instituto Superior Técnico, Universidade de Lisboa.

Manuscript received June 6, 2015.

(1.0) Excellent	ACTIVITY						DOCUMENT						
(0.8) Very Good	Object×2	Opt×1	Exec×4	Summ×.5	Concl×.5	SCORE	Struct ×.25	Ortog×.25	Exec×4	Form ×.25	Titles ×.5	File ×.5	SCORE
(0.6) Good	1,0	1,0	1,0	1,0	1,0		1,0	1,0	1,0	1,0	1,0	1,0	
(0.4) Fair													
(0.2) Weak													

ticipate in competitions is reduced to about 20 people. Even so, I can state that the active members can cover a wide range of topics related to cybersecurity, managing to form small groups to solve diverse challenge types in CTF competitions.

3 Capture The Flag Competitions

A CTF is a computer security competition where it is expected that participants apply their technical skills in order to secure a machine or to exploit vulnerabilities. CTF competitions can be one of two kinds: Jeopardy or Attack/Defense. The difference among these is described below:

3.1 Jeopardy

The objective in Jeopardy CTFs is to solve as much challenges as possible from those created and put available by the organization. There are several categories of challenges such as forensics, steganography, cryptography, web, reversing, pwning, among others. Each challenge gives a certain number of points to the team that solves it. The proof of completeness of an exercise is given by the submission of a text string that is obtained when one does, in fact, solve the exercise. This string is usually called "flag".

In this kind of competition, teams do not directly attack each other.

3.2 Attack/Defense

In Attack/Defense CTFs each team gets a virtual machine from the organization in which it has to set up several services. The machine has to be configured in order to be detectable by the organization. The goal of this kind of CTF is to analyse the code of such services, to find an exploit and to develop a patch for our own services. Each team may submit exploits which are tested against other teams live services. A team may win points by exploiting unpatched machines and by developing patches to its own machine.

While our team has participated in both kinds of competitions, we prefer the former, being able to achieve better results overall. This is due to the fact that each member can directly focus on the type of exercise where he shows more skill/interest.

4 CTF Competitions Entered

Departamento de Engenharia Informática (DEI) has given permission so that the team can use the meeting room in Pavilhão de Informática II in order to get together when participating in CTFs. Tipically, a Jeopardy style competitions lasts for about 48 hours. Below I describe my participation in the CTFs that I attended during the execution of my activity. I also describe the Boston Key Party (BKP) CTF, which took place by the end of February, as well as some of its challenges that were discussed during the first STT meeting, after the official activity submission.

4.1 Boston Key Party

- Start date: Friday, February 27th at 10pm
- Duration: 43 hours
- Place: Pavilhão de Informática II - DEI's meeting room

This competition's format was Jeopardy and the distribution of challenges was based on the subway map of Massachusetts Bay Transportation Authority, where each line corresponded to a given type of challenge. The challenge types were the following: Reversing, Cryptography, Pwning and Miscellaneous (named School-Bus).

At the start of the competition I teamed up with Tiago Brito in order to tackle the first challenges that spawned. In the first few hours we managed to solve several Miscellaneous challenges for a total of 125 poins, namely Symphony, Brigham Circle, Prudential, Northeastern Univ and Museum Of Fine Arts. The solutions for these challenges focused in taking advantage of vulnerabilities in HyperText Markup Language (HTML) forms GET parameters or PHP language particularities, proving to be fairly simple to solve.

Another Miscellaneous challenge we tackled was Heath Street, which proved to be a forensic style challenge. At this point we had the help of Valmiky Arquissandas, who found out the provided file was a file system that could be mounted and explored. We ran into a red herring, being led to believe the flag we were looking for was inside a password protected zipped file. The flag ended up to be in an erased file which we had to recover. This was discovered by another team member in the following day.

After reaching a dead end in Heath Street, I teamed up with João Cardoso in order to solve Haymarket, a reversing type of challenge. In this challenge we were provided with images of thirty punch cards where a game was programmed. João found out a guide that explained how to read the punch cards. We then split the cards and began to write down the code of the program. Around 8am I discovered the flag in a string that was supposed to be displayed by the program. At this moment, I left so that I could get some sleep, having returned Saturday at around 2pm.

I spent some time of the afternoon looking at several challenges, having spent some time dealing with Central Square with the help of João Godinho and Filipe Casal. This was a Pwning type of challenge, where it was possible to send an image to a web page in order for it to be processed at the server and downloaded in another format. We managed to understand that it was possible to inject arbitrary code into the server, but we ended up not being able to solve the challenge.

Saturday night I teamed up with Professor Pedro Adão and David Duarte in order to analyse Riverside, a reversing type of problem. We were provided a Universal Serial Bus (USB) packet capture, from which we would need to derive the flag. This challenge demanded some time for research, namely discovering the model of the USB device (a Logitech mouse) in use and studying the USB protocol. Our hunch was that the capture represented a mouse movement over a virtual keyboard. We had some errors when extracting the coordinates and the plots we constructed were fuzzy. We worked on reconstructing the mouse movement until around 3am, time by which we left. In the following day I had little availability to work on the challenges. At around 4pm, I've contacted João Godinho who was working in Central Square. We were unable to solve it until the competition ended.

STT ranked 87 out of 828.

4.2 UCSB iCTF

- Start date: Friday, April 10th at 4pm
- Duration: 9 hours
- Place: Pavilhão de Informática II - DEI's meeting room

This competition's format was Attack/Defense. The team had some trouble on connecting our virtual machine services and they only ended up being online a few moments after I met up with the team at 9pm. Up until that time we were low on the scoreboard, having lost some points over the unavailability of our services. I teamed up with Filipe Casal and we were able to launch a successful exploit, earning some points for the team. We spent the remaining time trying to develop patches for our own services, without great results.

Although the team is not very experienced in Attack/Defense CTFs, we found this one not to be particularly well set up. Apart from having a total of 40 services to exploit and patch (plenty for a 9 hour long competition), many of them were modifications of services used in past editions, giving advantage to teams that had already participated.

STT ranked 56 out of 88.

4.3 Plaid CTF

- Start date: Friday, April 17th at 10pm
- Duration: 48 hours
- Place: Pavilhão de Informática II - DEI's meeting room

This competition's format was Jeopardy and it was organized by Plaid Parliament of Pwning (PPP), which occupies the top position in teams ranking. The challenge types were the following: Reversing, Pwnable, Cryptography, Web, Forensics and Miscellaneous. I met with Filipe Casal at DEI's meeting room at the start time of the competition. Some of the first challenges to be released were Pwnable and Reversing type of exercises. In this competition, Pwnable exercises mixed several areas of expertise. We tackled *qttpd*, which was divided in three parts and was the first Pwnable challenge. It involved crawling in a website in order to find a binary file and configuration file related to the HyperText Transfer Protocol (HTTP) server that was serving it. We thought that the binary file would need to be reverse engineered and we took a look at PNG Uncorrupt, which was a Forensics challenge. The objective of this exercise was to recover a Portable Network Graphics (PNG) image which had, arguably, problems in its transmission. We spent some time looking at the content of the file in a hex editor and we understood we would need a better understanding of the inner structure of PNG files. We spent some time gathering information, concluding that the file is structured in meaningful blocks of metadata, apart from the image data itself. Looking at the file again I detected discrepancies in checksums and data block lengths. We left at 1am.

In the next morning there were some more exercises available. I resumed my work in PNG Uncorrupt and found out there was a known problem regarding newline conversion from DOS 0x0D 0x0A == \r \n to Unix 0x0A == \n, where a byte is dropped. However, I approached the solution in a wrong way, replacing all 0x0A bytes by 0x0D 0x0A, adjusting the data blocks length and checksum. Although I could now distinguish elements in the image, it was still too noisy to be read. This challenge would ultimately be solved by Afonso dos Santos on sunday, following the suggestion of Professor Pedro Adão to try a bruteforce approach, replacing the 0x0A bytes by 0x0D 0x0A so that it matched the original length and checksum value of each data block.

During the afternoon of saturday I split my work on PNG Uncorrupt with a Miscellaneous type of challenge, Kolmogorov. This exercise had a very vague hint(”How did his pet snake learned to play golf??”) and provided us with a seemingly fuzzy text file with a few lines. It took us a lot of time until we connected Kolmogorov’s Complexity to code golf, a kind of programming competition where a player aims to write a correct program in the fewest lines of code as possible. I came up with of the idea of finding a Python dialect used in code golf. However, I did not find any. We were not able to complete this exercise, but my hunch was, in fact, correct. The provided text file was a program written in Pyth, an esoteric language designed to be compiled into Python, which main purpose is conciseness.

Around 11pm the organization launched a new Forensics challenge. I teamed up with David Duarte and we analysed the code that was provided. It could apparently be interpreted in order to generate an image. I found out it was a raster image encoded in Andrew’s ToolKit (ATK) format. David Duarte was able to open the image in XnView, a program that can read such files and recovered the flag.

In the final day of the competition I met with the team around 6pm. I tackled radhos (the Web challenge) with David Duarte, where it was supposed to recover the flag from a given hashed key in a distributed key-value store. We found out that the solution was related to how Python’s basic hash implementation works on 32 or 64 bits systems. 64-bit hashes are truncated in order to be able to be compatible in 32-bit machines, rendering it open for collisions. While we tried to find a collision in the remaining time, we were unable to find any until the end of the competition. Known write-ups solve this problem by studying the internal code of Python’s hash function and finding a way to diminish the search space.

STT ranked 74 out of 895.

4.4 Volga CTF Quals

- Start date: Friday, May 1st at 4pm
- Duration: 48 hours
- Place: Remote

This competition’s format was Jeopardy. I was only able to play in this CTF until 6pm of May 1st. I focused in two Steganography challenges available, namely poem and captcha. The former was a pdf file with several sonnets, while the latter was a PNG image. I dwelled with the first one by comparing the full text of the sonnets with several versions available in the internet, as some letters could have been changed throughout the text. This was not the way to go and I turned my attention to captcha.

In captcha, the provided PNG file was badly formatted, as it contained several new PNG headers inside. I teamed up with Filipe Casal and we were able to extract thousands of different images from within the original one. Each image represented a single character that could be repeated in several images. Afonso dos Santos was able to complete the challenge by developing a program that could distinguish each character by its image file size and used them as data in the PNG's data block.

STT ranked 59 out of 250.

4.5 DEFCON Quals

- Start date: Friday, May 16th at 1am
- Duration: 48 hours
- Place: Pavilhão de Informática II - DEI's meeting room

This competition's format was Jeopardy and it was organized by Legitimate Business Syndicate. This competition was a direct access qualification round for the most famous CTF in the world, DEFCON (known as the World Series of Hacking). The challenge types were the following: Reversing, Pwnable, Web, and Miscellaneous. I met with the team at 16pm of May 17th and teamed up with Tiago Brito. Up until that point, the team had only solved one exercise, revealing the high standards of the competition. There were available challenges from all of the above categories, with the exception of Web. We tried to help other teammates in some of the challenges they had already explored. We observed that nearly all of them provided a binary file which we would need to reverse engineer at some point in time to advance through the exercise.

This competition blatantly confirmed that one of the main difficulties of the team resides in binary reverse engineering. This kind of challenges forces one to analyse a program at a very low level. While this task can be tedious by itself, there is often additional complexity as the binaries can be obfuscated. This was an opportunity to explore the capabilities of Hopper, an OS X disassembler and debugger. This tool is also able to provide pseudo-code of low level routines in order to ease binary analysis.

Since binary analysis did not result in a good outcome, we focused on the Web challenge once the organization has made it available. This challenge did not have an accompanying hint whatsoever, which made us oblivious at first about what we were supposed to do on the exercise. About half an hour to the end of the competition, Professor Pedro Adão noticed a commented piece of code in one of the pages of the provided website. That proved to be the main point to exploit the exercise. Tiago manipulated that piece of code to inject an update on the server, after which he retrieved the flag. Unfortunately, he obtained the flag too close to the end of the competition and was unable to submit it on time.

STT ranked 113 out of 284.

5 STT Meetings

The meetings between the members of STT usually take place every two weeks in Laboratory 14 at Rede das Novas Licenciaturas (RNL), taking about one to one and a half hours. As already stated in section 2, there is usually a session leader scheduled for each meeting. It is presented below the content of each meeting that I attended since the submission of my activity in March 9th.

5.1 6th Meeting

The 6th STT meeting took place on Tuesday, March 10th. This session was specially interesting as we had Luís Grangeia as session leader. Luís Grangeia is an information security professional working in the field for about 10 years, who kindly volunteered to talk about Cross-Site Scripting (XSS) vulnerabilities. XSS consists in a type of computer security vulnerability found in web applications, enabling the injection of a client-side script into web pages visited by a third party.

Luís started his presentation by giving an overview over the theme and theoretical aspects related to XSS. When everyone was comfortable with the topic, Luís introduced a purposely vulnerable website designed to enable people to test XSS vulnerabilities.

5.2 7th Meeting

The 7th STT meeting took place on Tuesday, March 24th. This session's objective was to wrap-up our participation in the BKP CTF, by looking at write-ups for some problems we tackled.

Professor Pedro Adão presented the solution for Airport, a cryptography type of challenge. In the remaining time each one of the people in the room browsed through the BKP CTF available write-ups in order to understand how a particular problem was solved. In this process, I studied the solutions for Riverside and Central Square. We could see that we have been very close to the solution of Riverside while in Central Square we would have needed to make use of pre-processing directives in the code injected into the server.

5.3 8th Meeting

The 8th STT meeting took place on Tuesday, April 14th. This session leader was João Godinho, who presented Buffer overflow vulnerabilities (both stack and heap based). Such vulnerabilities allow an attacker to execute arbitrary code by overrunning a buffer's boundary and overwriting adjacent memory positions.

As usual, João started the presentation by giving an overview of the vulnerability and in which ways can it be exploited. Then he moved to manage an hands-on session. Each attendant had downloaded a virtual machine (Protostar from Exploit Exercises) where there were programs that could be subverted by using the above techniques.

5.4 9th Meeting

The 9th STT meeting took place on Tuesday, April 28th. This session leader was Afonso dos Santos, a student from Integrated Master Degree in Aerospace Engineering (MEAer) who presented web-exploits, in particular SQL-Injection.

5.5 11th Meeting

The 11th STT meeting took place on Thursday, May 27th. In this session we performed a wrap-up of the semester's activities. Members were encouraged to continue participating in eventual competitions that happen during the summer, even if remotely. We were also encouraged to practice our skills, be it on specific reversing tools or develop our abilities in writing exploit code.

Finally, we were able to verify that the team currently stands in position 142 out of 4075 teams registered on CTFtime, for the present year, aiming for a place in the top 100 teams until the end of 2015.

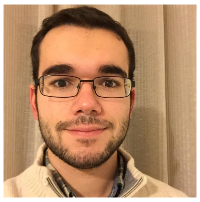
6 Conclusion

Making part of STT gave me the chance to study cybersecurity problems and the possibility to exchange know-how with several members of the team. While the main goal of the team is to enhance the skill set of its members in cybersecurity issues, we were able to obtain good results in diverse CTF competitions. These results are directly implied by the effort shown by each of the team members who participated in such competitions. I think that the commitment I employed while executing this activity has paid off as I was able to learn how to tackle a large range of cybersecurity issues in a fairly small amount of time.

Lastly, I think STT has filled a gap in the actual Master Degree in Information Systems and Computer Engineering (MEIC) curriculum, which lacked a broader education over the transversal cibersecurity topic (In fact, MEIC restructuring will present cybersecurity as a possible specialization). Since the team now has several people with some expertise on the topic, I hope more interested students will join STT in the future, not only to learn but also to have some fun while participating in CTF competitions.

Acknowledgments

The author would like to thank Professor Pedro Adão for the creation of STT and the ability to gather equally minded people regarding the information security topic. He would also like to thank everyone with whom he has teamed up during CTF competitions over the unmeasurable experience sharing.



Diogo Barradas is a 21 years old student at IST. He has completed his Bachelor's degree in Information Systems and Computer Engineering and is currently pursuing a Master's Degree in Information Systems and Computer Engineering, majoring in Distributed Systems and Enterprise Information Systems. He has a keen interest in information security and digital privacy.