SecurityTeam@IST

Diogo Miguel Barrinha Barradas

Learnings Report

Abstract—The present report describes what I learned during the execution of my activity, from a soft-skills standpoint. The early concept of student-driven organisation has led me to understand which communication tools were best fit to the team's needs. The exposure to several cybersecurity topics proved to be fundamental to filter those which I was less proficient with, leading to a higher effort in self-learning regarding such topics. Having people in the team with different expertise and interest areas has proved to be useful in brainstorming events. Being both able to express an idea to a teammate and to motivate him were fundamental skills in order to keep the team engaged in it's activities. Ethical issues were also addressed in order to understand where to draw the line between right and wrong when dealing with information systems security. As a whole, the skills I acquired/improved, although not being technical, can help to speed up the integration of a new student in the team and to be a more efficient member in STT.

Index Terms—Communication, Ethics, Organization, Time Management, Teamwork.

1 Introduction

This report has the purpose to present an analysis over the soft-skills acquired and improved during the development of the activity, in the scope of the Independent Studies course at Instituto Superior Técnico (IST). Section 2 explores the way the team organized and proposed meetings or activities, either physically or through a remote channel, featuring a small discussion on the choice of the appropriate one. Section 3 describes the way I dedicated my own time to self-learning activities, so that I could improve the technical skills needed to succeed in a Capture The Flag (CTF) competition. Section 4 describes the way having different minded people with expertise in different topics can be beneficial to achieve better results through more effective brainstorming. In Section 5 I analyze the need for teamwork and in what way it was beneficial to the success of my activity. I discuss the ability to ask for help versus the incapability of progressing through a given challenge. This section also addresses the need to express ideas in a correct manner, adjusting the way to transmit them taking into account our interlocutor expertise. Section 6 explores the idea of ownership of a challenge and in what way can I manage my time in order to remain productive and achieve better results. Section 7 describes the ethical issues of having the necessary technical skills to either act responsibly or wreak havoc with a computer system. Section 8 presents the conclusions of this analysis, where I reflect about the way I can perform better after the execution of my activity.

2 I Think We Should Meet

Security Team at Técnico (STT) employs a student-driven approach in respect to the way and frequency the team can get together. This approach allowed me and other team members to take responsibility about when and why the team should be able to meet. Other than the regular meetings and important CTF competitions which Professor Pedro Adão had the responsibility to schedule on advance, the team has total freedom to schedule meetings or to participate in diverse CTF competitions. Therefore, this approach enables each team member to assume the position of an organizer and to

- *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	LEARNINGS						DOCUMENT						
(0.8) Very Good	Context×2	Skills×1	Reflect×4	Summ×.5	Concl×.5	SCORE	Struct ×.25	Ortog×.25	Exec×4	Form ×.25	Titles ×.5	File ×.5	SCORE
(0.6) Good	1.0	0,8	0.9	1.0	1,0		1,0	1.0	1.0	1,0	1,0	1,0	
(0.4) Fair													
(0.2) Weak													

increase his experience in event organization.

STT meetings usually involved a presentation and a hands-on session. It is respectful to listen to a presentation without importunately interrupt the speaker. Therefore, I have always posed my questions at the end of the presentation, providing that the speaker did not ask for questions in the course of the presentation. These meetings have also fostered collaborative learning since I was able to team up with other colleagues in order to solve some of the exercises proposed in hands-on sessions.

Since the team is composed by several students, it was imperative to make use of distributed platforms which leverage the task of disclosing information or to poll members availability regarding the participation in a non-scheduled CTF. For that matter, the team has set up a Facebook page as well as a Discourse group. While the former is primarily used for meetings and competitions announcements, the latter is used to discuss and share information acquired about challenges during a CTF. The team has also set up a Dropbox account to be used as an information repository regarding techniques and solutions used to solve previous CTF's exercises. The use of these platforms create a good separation between different layers of information the team makes use of, improving the team's productivity.

The team usually met physically on the CTF competitions scheduled by Professor Pedro Adão. However, student-organized participation like Volga CTF are usually scheduled to be performed remotely. Upon participation, it showed that the platforms already being used were insufficient to deal with the inherent information exchange the team performs. To fill that gap, we created an Internet Relay Chat (IRC) channel which can be used for quick chat between team members, demonstrating to be more useful than the aforementioned platforms which would be overflown with extraneous, non-fundamental information.

3 What's all the fuss about?

The skills required to solve a CTF challenge are often highly technical and require a broad grasp over cybersecurity concepts and tools. Since these are not directly approached in the majority of courses attended in Master Degree in Information Systems and Computer Engineering (MEIC), there is the need to develop such skills individually. Even though we are exposed to some of these concepts and tools in the regular STT meetings, there is usually little time to practice on-site and we often just superficially learn about the topic at hand. Although it is better to be aware of a given topic than not, it is difficult to apply that knowledge in a given CTF competition without some practice and deeper understanding about it. Therefore, the ability to be able to practice is fundamental to develop such skills and there is no better way to do that than to tackle a problem alone at our own pace. Self-learning comes of great importance in order to become a better professional. While one can not expect to know every topic in excruciating detail, it is important that one can employ some of his time to specialize in some. Regarding myself, I'm mainly interested in Forensic Analysis and Reverse Engineering. These are the topics I usually find myself studying and practicing on my own. At the end of the day, it is very rewarding to see that I can put those skills to use while helping the team or making some aspects clearer for a more inexperienced team member.

One obviously needs to be exposed to different topics and concepts in order to understand which he is more interested in. STT meetings and CTFs participation naturally contribute to this exposure. I've always found Cryptography to be a fascinating topic but had no more knowledge about it other than the one acquired during the Distributed Systems or Network and Security courses. I could attest that my knowledge about the topic was manifestly insufficient to even understand CTF's cryptography challenges, let alone to solve them. I realized this on the first CTF STT has participated since it's inception, back in October 2014. Taking this into account, I am currently enrolled in the Cryptography and Security Protocols course offered by the Master Degree in Mathematics and Applications. I am now able to understand the concepts behind such challenges and actively try to solve them.

4 Split just a bit

CTF competitions have different types of challenges. By the time of STT's inception and first CTF participation, members directly flocked to the kind of challenges related to their skills and interests. Back then, the team posed much more fragmented than it is today as there was a different group dealing with each class of problems. While teamwork happened inside of each group, a disconnection among groups was noticeable. Along with this disconnection it was possible to check the difficulty of thinking ”outside of the box”, as people were more equally minded regarding the way to solve a given exercise. Today, each member now has a broader understanding over the several types of challenges. The team is not as fragmented as before and brainstorms among the whole team are frequent. This enables a faster and more creative development of solutions which in turn enhance the overall results obtained in CTF competitions.

5 Can you give me a hand?

Teamwork is fundamental to endure a CTF competition, since no single member of the team is an expert in every topic. At first, relating to the first competitions STT has participated in, it was difficult to guarantee that the full group focused in a given challenge type was present in the CTF at a given time. This gradually pushed team members to ask for help among each other, even if their interlocutor was not as comfortable with that kind of problem. I've been in both sides of this situation, having both asked and being asked for help in topics I was or, respectively, I was not comfortable with. The former situation asks for the need of being able to express the problem to someone who may not be comfortable with the topic. This requires a certain care since I must walk the other person through the several steps that lead me to a certain conclusion. This kind of concern could be avoided when speaking to someone who immediately understands what I'm talking about. Therefore, it is fundamental to adjust the speech taking into account the degree of expertise of whom we are talking to. The latter situation is all about adaptability, once one may need to rapidly grasp seemingly unrecognized concepts and still be able to help a teammate in a reduced amount of time.

6 Pet Challenge

It is often difficult to think of the right approach to solve a challenge right off the bat. It usually takes some time until one is able to correctly analyse the problem at hand and to gather enough information to picture a possible solution.

I felt that the initial enthusiasm can start to fade after several hours trying to solve a single challenge. When facing such problems I think it was imperative to manage my efforts, allowing me to get some rest by performing quick breaks. In this process, I approached other teammates, trying to understand which problems they were tackling and try to come up with some idea that might help them. This process allowed me to drift away from my problem while remaining productive regarding the team's objectives. When going back to the challenge at hand, one can continue to explore a certain idea in order to solve it or to explore a different approach. In either case, persistence is fundamental. After all, up to that point, one surely is the team member with more experience in that particular challenge.

Teammates shall be encouraged often, so that they can feel they are still an important part in play, despite not being able to solve a challenge at a given time. They may eventually succeed.

7 With great power comes great responsibility

Participating in STT nurtured my skills in complex cybersecurity topics. In particular, to be trained to spot vulnerabilities and to explore them is of great importance. It is fundamental to be able to think like an attacker in order to devise systems which are both more secure and reliable. However, this knowledge can be put to use either in responsible and legitimate activities or in malicious activities, aiming to corrupt or to destroy information systems.

It is ethical to refrain to use such skills for malicious purposes, limiting their use for professional activities. Even if one is unable to be employed to perform penetration testing, there are several places where such skills can be put to good use. As an example, there are ”Bug Bounty” programs set up by tech-savvy companies where one can be monetarily rewarded by finding vulnerabilities and responsibly disclosing them. This enables both the company to fix their systems (so that they can provide a safer and more reliable service) and the cybersecurity enthusiast/professional to continue exercising his abilities in a responsible and useful fashion.

STT enforces the following of a good conduct, not being held responsible by any wrong doing any team member may perform with the acquired knowledge.

8 Conclusion

The activity I developed throughout the semester has been a way to improve some soft-skills that are useful to one’s personal development. Other than acquiring both theoretical and practical cybersecurity skills I had the opportunity to improve soft skills like teamwork, communication, time management and persistence. These skills, although not being technical can help to maximize the work progress and output throughout the activity’s execution. The activity I performed has also demanded a lot of discipline in order to be able to autonomously study and practice the concepts I have been exposed to, for the duration of my participation in STT.

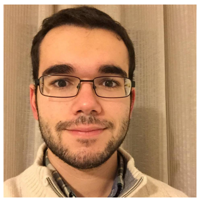
Ethical issues were addressed in STT and I considered this discussion to be of great relevance. It is important to understand where to draw the line between right and wrong, something particularly hard to do when dealing with intangible resources such as pure information.

As far as teamwork goes, I think the enthusiasm and willingness to help teammates exceeded all my expectations. I was able to attest that when people are motivated to pursue one collective goal they can achieve very good results.

To conclude this report I must state that the opportunity to learn and work as a team gave me the chance to improve my organisation and communication skills, giving me the ability to coach new students that may join STT.

Acknowledgments

The author would like to thank all the people with whom he has teamed up for their endless support and enthusiasm throughout every CTF competition.



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.