Security Team

Frederico Miguel Reis Sabino

Activities Report

Abstract—Nowadays, the security and privacy of each user is a big concern. No system is completely secure and confidential information leaks may very well happen. The Security Team of Instituto Superior Técnico (IST) is a team where its goal is to learn more about those security issues and the problems that they may bring. We do so in a completely controlled environment without disrupting any real service.

Index Terms—security, cyber, exploits, ctf, challenge.

1 Introduction

Sensitive information exists since mankind is capable of storing and transmitting it. Its access was often solved by a simple physical lock-down and, for the most part, the problem was solved. Entering the age where data can be stored digitally (and often) in a machine that is connected to the world can be problematic – physical restrictions no longer have the intended protection effect.

As the mechanisms to protect digital information evolved so the attacks to breach it. The attacks and defenses can benefit mutually from each other – if an attack is possible then it means that the defense mechanism needs to be improved to counter measure it (making it an overly better system). The objective of the Security Team of IST is to teach its participants the importance of a secured system by showing what are the possible attacks (to that same system) and respective consequences.

This is done in a completely controlled environment without any implication to any real-life service/business.

2 Building blocks

In order to fulfill the main objectives for the Security Team, we enrolled in various competitions/challenges that required expertise in the big area of security. So we needed a team composed of elements that were eager to learn more about security by solving those same challenges in a controlled environment. We also organized meetings in order to synchronize our goals and skills. These are the main "blocks" that are part of the Security Team and will be explained in detail in this section.

2.1 The Team

The Security Team of IST (STT), was created in October 2014. Its main objectives are learning cyber-security by exploiting vulnerabilities in a controlled environment. The main organizer is professor Pedro Adão.

Anyone in IST could enter the team – it is not exclusively for people taking the computer science/information systems degree but, initially, what happened indeed was that the majority of the members were indeed from the computer science field... but, as the team grew, more and more members from other degrees joined. The only requirement to enter the team was to sign a document that states that any activity done in the context of the Security Team is done legally in a controlled environment and be part of the IST's community.

I can not say exactly the number of members in the team because it is seen like an open community where people come and go but I can say that the team structure is very flexible because its members have different schedules

• *Frederico Miguel Reis Sabino, nr. 73239, E-mail: frederico.sabino@tecnico.ulisboa.pt, Instituto Superior Técnico, Universidade de Lisboa.*

Manuscript received 6 June, 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	0.8	0.8	0.6	0.8	0.8		1.0	0.8	0.8	1.0	1.0	1.0	
(0.4) Fair													
(0.2) Weak													

and we can have a considerable team size present in the challenges (that will be explained in detail in section 3).

2.2 Controlled Environment

As of now I have mentioned that everything done was in a "controlled environment" without really explaining what it really is.

The controlled environment is an environment created by some group or organization that is made of services with vulnerabilities to be breached. It is a set of machines that can be seen as a sandbox where we attempt to breach a given service running on that machine. This sandbox allows us to run activities that would otherwise be considered a threat to a real system (finding exploits).

Those challenges most of the times had a theme associated with it (as will be explained in section 3). In those environments there were also other teams competing and we had a leaderboard. The more challenges we completed the more points we obtained towards the leaderboard.

2.3 Meetings

It was decided on the first meeting that we should carry other meetings every 2 weeks. These meetings served mainly as a checkpoint to know in which challenges we should participate in. They then evolved to a lecture style meeting where members of the team (or guests) would explain different attack scenarios, possible breaches, exploits and the state of the art in the security field.

In those meetings we learned about (but not only): buffer overflows, Cross-site scripting (XSS), how to use sqlmap and practice exercises from previous challenges.

3 The Challenges

The challenges that the team participated in were Capture the Flag (CTF) style challenges. Within the CTF style we have two major types: Jeopardy and Attack-Defense. Those challenges could be completed either at IST or remotely. Professor Pedro Adão reserved a room in Pavilhão de Informática 2 that would be open while the challenge was in progress. This room had all the requirements to build our workstation (our laptops), and also food and water for the whole event.

Figure 1. CTFtime available at ctftime.org

With different events from different organizers how could we keep track of our progress and what were the future events? Fortunately the CTF community created a service called CTFtime that not only keeps track of the global leaderboard but also stores information about each team progress, in what competitions they participated in, what were the results, past events and more importantly future ones.

3.1 Jeopardy

The Jeopardy style competitions were the ones that our team most participated in. They have a set of challenges/tasks that are arranged in different categories. Those categories include Web, Forensic, Crypto, Bynary Reverse, among others...

Those competition have a time schedule (that usually spans for 1 or 2 days). Starting the event a list of challenges is published to all the teams registered and the objective is simple: solve the challenges as quick as we can! Those challenges are solved in a controlled environment (as already explained).

By solving a task, the team accumulates the points from that task. When the competition is over, the team with more points wins the challenge.

This kind of competition required active work from its team members since we were competing within a time frame against many other teams from all over the world. Also, many times, not all the challenges were immediately available to solve! Some of them required another tasks to be completed first (in a chain style) while others would only appear later in the competition.

Many of those competitions had a background theme associated with it. For instance,

Figure 2. HACK.LU CTF Challenge

in Figure 2 the background theme for the competition was in the old Wild West (here named Wild Wild Web). Many times the themes presented in the challenges, provided not only clues but facts about different science fields (so we were not only learning about how to exploit a given vulnerability!).

A given task in this kind of competition had always a flag associated with it. The flag is just a sequence of characters (we can see the input field on the bottom of Figure 2). Submitting the correct sequence of characters would grant the team the points associated with that given challenge.

The objective of all the tasks in this competition is to obtain that given set of characters through solving the task.

3.2 Attack-Defense

An Attack-Defense competition gives each team a network or host with services that are vulnerable to attacks. As in Jeopardy, these competitions have a time schedule but we can say that the time is divided into 2 main events. The first one is when the event starts - it is given time for the teams to patch (fix the security issues) their host/network; the second event is when the organizers connect each team and so the virtual war begins (literally).

Each team attacks one another, trying to break through the patched services (usually using exploits) for winning attack points while actively defending their services (defense points).

4 Results

Given that the team is very recent and the objective is primarily learning about security vulnerabilities, not all the members had the expertise to immediately tackle the tasks proposed. Even so we obtained very good results , for instance, in the first CTF that we participated in, we have finished in position 52 out of 396 teams globally. I consider this a really good position for a team that had just been formed.

To help in future competitions we organized a Dropbox repository that contained tips and previous challenges to help in future occasions. This repository was also used for ongoing challenges so all team members could check the latest advances on a given task (either locally or remotely).

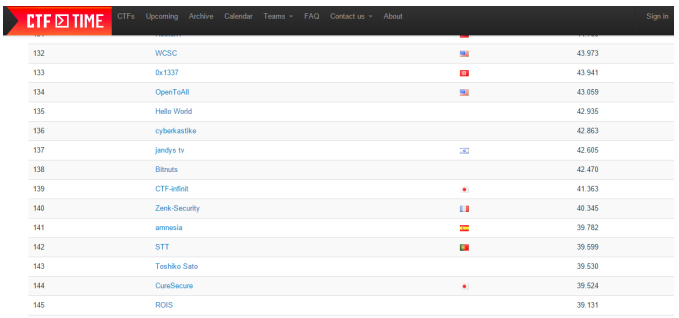


Figure 3. STT's current global position as of June 2015 - 142

In Figure 3) we have the current global position for our team that as of June 2015 is position 142 out of 4075 teams globally.

5 Conclusion

I can say the main objectives of the team were accomplished and continue to do so. I have learned many new concepts and tools and how I can apply them to make a system more secure.

It also allowed me to explore the world of CTF's that I didn't know that existed in such a large scale.

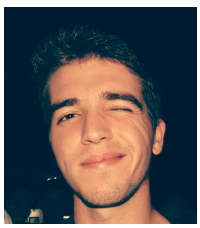
The team also provided everything needed to begin "hacking"! Many coffees were drank and many flags captured. We climbed the leaderboard fast and we are happy with the results.

ACKNOWLEDGMENTS

I would like to thank professors Pedro Adão and Miguel Correia for taking the initiative to start the team and to provide the resources that the team needed. I also would like to thank all the members involved in the competitions because I have learned a lot with them.

REFERENCES

[1] https://ctftime.org/ (visited on 6th June 2015)
[2] https://wildwildweb.fluxfingers.net/2014/scoreboard (visited on 6th June 2015)



Me My name is Frederico Sabino and I am a master student at IST in Information Systems and Computer Engineering. I am also currently working at Direcção de Serviços de Informática (DSI) and I am a member of STT.