# Security Team Técnico

António Lopes

*Relatório de Actividades*

**Resumo**—Neste relatório é descrita a actividade na qual participei, "Security Team Técnico", e, por conseguinte, no que consistiu. Assim, são descritas as diversas reuniões e as múltiplas participações em competições internacionais de "Capture The Flag" nas vertentes "Jeopardy" e "Attack-Defense". São também definidos os conceitos de "Capture The Flag", "Jeopardy" e "Attack-Defense".

**Palavras Chave**—"Capture The Flag", Segurança, Security Team, Competições Internacionais.

## 1 Introdução

A participação na actividade Security Team Técnico (STT) divide-se em duas partes fundamentais para poder integrar-me na equipa e trabalhar com a equipa. Neste sentido, a actividade consistiu em reuniões onde a equipa se reunia para discutir tópicos como a importância da ética na engenharia informática focando-se nos conhecimentos adquiridos, quais as competições em que se iria participar, etc, e para falar sobre tópicos relacionados com a segurança em sistemas informáticos. Esta última, consistiu em quer professores, quer alunos, abordarem um tópico sobre segurança em sistemas informáticos e apresentar o mesmo para toda a equipa que estivesse presente. Estas reuniões serviam não só para partilhar conhecimentos como também para proporcionar um espírito de equipa e trabalho.

A segunda parte da participação consiste na participação em diversas competições internacionais de segurança de Capture the Flag (CTF), nos formatos "Jeopardy" e "Attack-Defense".

• *António Lopes, nr. 73721,*
*E-mail: antoniovilarinholopes@tecnico.ulisboa.pt,*
*Instituto Superior Técnico, Universidade de Lisboa.*

*Manuscript received 06 01, 2015.*

## 2 Motivação

A realização desta actividade teve como motivação, por um lado, os conhecimentos que podem ser adquiridos com esta experiência e, por outro, poder trabalhar em equipa para resolver os vários problemas. Neste contexto, a motivação surge em dois pontos, primeiro, trabalhar os conhecimentos já adquiridos com novos conhecimentos é essencial para a minha formação como futuro engenheiro e,segundo , trabalhar em equipa é também algo essencial para a formação de qualquer pessoa na sociedade, contribuíndo para a adaptação a uma realidade perto da que se enfrenta no mundo laboral onde as equipas são de várias pessoas com diferentes "backgrounds".

## 3 Reuniões

Ao longo do semestre ocorreram 6 sessões de encontro da equipa. Em cada uma destas foram discutidos diferentes tópicos e feitas diferentes apresentações. Para além destes assuntos, os membros da equipa, por norma, a seguir a uma competição procuram as soluções de outras equipas para um dado problema não resolvido e são depois discutidas nas reuniões entre todos.

As reuniões foram feitas num dos laboratórios do edifício "Redes e Novas Licenciaturas"e tinham uma duração de cerca de uma hora e 30 minutos.

Em seguida, as reuniões são enumeradas assim como alguns dos seus tópicos:

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

1) 10/03/2015 Apresentação: ”XSS vulnerabilities- Luís Grangeia
2) 24/03/2015 - ”Boston Key Party write ups analysis”
3) 14/04/2015 - Apresentação: ”Buffer Overflows- João Godinho
4) 28/04/2015 - Apresentação: ”Web Exploits- Afonso
5) 12/05/2015 - ”Preparation for DEF CON - write up analysis”
6) 27/05/2015 - ”Wrap up of STT activities and competitions”

# 4 Competições Internacionais

Como já mencionado ao longo deste relatório, nas secções 1 e 3, houve várias reuniões para a equipa discutir problemas e as soluções. Está inerente às reuniões a preparação para algo mais, comprovar a teoria com a prática. Assim, ao longo do semestre participei activamente em mútliplas competições de CTF. Antes de mais, é necessário definir o que é uma CTF.

## 4.1 CTF, o que é?

Um desafio de ”Capture The Flag” consiste numa série de problemas relacionados com segurança informática onde é necessário aplicar conhecimentos técnicos em múltiplas áreas da informática, e senso comum, de maneira a conseguir explorar as vulnerabilidades que o sistema apresenta para capturar a ”Flag”e pontuar. Logicamente, quantos mais serviços forem explorados, mais pontos a equipa consegue e melhor classificada fica.

Algumas das competências necessárias são a interpretação de código nas diferentes linguagens e sobretudo assembly, conhecimentos acerca dos diferentes protocolos existentes, criptografia, estenografia, etc. Estas competências são também desenvolvidas tanto durante as reuniões e competição como fora quando cada elemento procura soluções de problemas de outras competições.

Este tipo de competições pode ser do tipo ”Jeopardy” ou ”Attack-Defense”que são descritos em seguida. Por fim, cada um dos desafios tem uma categoria associada, desde estonografia, a ”pwn”, entre outros.

### 4.1.1 *Jeopardy*

Este tipo de CTF consiste em serem disponibilizados serviços para toda a equipa, quer sejam executáveis, quer sejam serviços a correr num servidor, entre outros, e usar os conhecimentos, ou procurar acerca do assunto, e explorar o serviço.

Quando um serviço é explorado e é obtida a ”Flag”, esta é submetida no servidor de quem organiza a competição e a pontuação associada é obtida.

### 4.1.2 *Attack-Defense*

Este tipo de CTF consiste em serem disponibilizados serviços que estão associados a cada uma das equipas, iguais para todos, e explorar os serviços em todas as equipas. Isto é, quando uma equipa encontra uma vulnerabilidade, explora todas as outras equipas nessa vulnerabilidade e pontua de acordo com fórmulas que têm em conta o tempo que os serviços estão disponibilizados pela equipa que explora e o número de equipas que consegue explorar, entre outras coisas.

Estando a definição de ataque definida, falta a parte de defesa. Como as equipas exploram as vulnerabilidades umas das outras, é possível fazer ”patches”aos serviços de maneira a que as outras equipas não consigam explorar as vulnerabilidades dos serviços.

Por fim, em intervalos de tempo a organização verifica a disponibilidade dos serviços em todas as equipas.

### 4.1.3 *Competições Participadas*

Ao longo do semestre participei, activamente, nas seguintes competições, por ordem de cronológica:

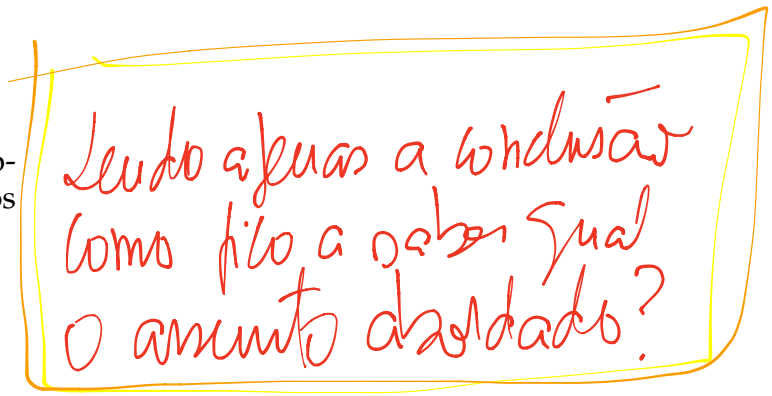
1) Boston Key Party CTF 2015 - Duração:48 horas - Jeopardy
2) UCSB iCTF 2015 - Duração:9 horas - Attack-Defense
3) ”PlaidCTF 2015- Duração:48 horas - Jeopardy
4) Teaser CONFidence CTF 2015 - Duração:24 horas - Jeopardy
5) VolgaCTF 2015 Quals - Duração:48 horas - Jeopardy

6) DEF CON CTF Qualifier 2015 - Duração:48 horas - Jeopardy

Em todas estas, tive a oportunidade de trabalhar em conjunto com os colegas de equipa para resolver alguns dos problemas que eram apresentados. A minha estimativa das horas totais de todas as competições é de cerca de 105 horas.

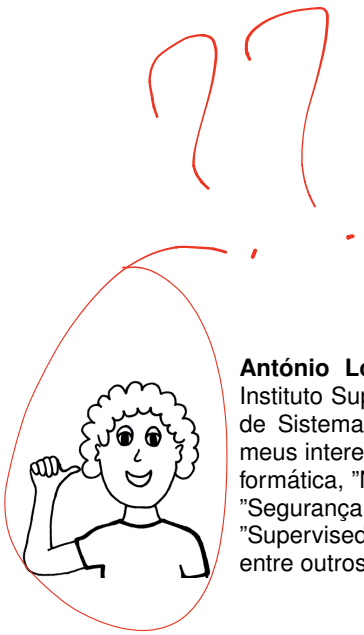
## 5 Conclusão

Participar nesta actividade permite que os conhecimentos técnicos e não técnicos adquiridos sejam importantes no meu futuro.




## Agradecimentos

Professor Pedro Adão e colegas da STT.



**António Lopes** Aluno de mestrado do Instituto Superior Técnico (IST) nas áreas de Sistemas Inteligentes e Robótica. Os meus interesses são vastos na área de informática, ”Natural Language Processing”, ”Segurança Informática”, ”Fuzzy Logic”, ”Supervised and Unsupervised Learning”, entre outros.