Equipa de Segurança

João Filipe Lopes Pardal

Relatório de Aprendizagens

Resumo—A Equipa de Segurança (EdS) consiste num grupo de alunos, juntamente com o professor Pedro Adão, com gosto pela área de Segurança Informática, que se reúnem de duas em duas semanas para partilhar conhecimento sobre a área, bem como para participar em algumas competições Capture The Flag (CTF) durante alguns fins-de-semana. Com a participação nesta Equipa, consegui ganhar conhecimento e recolher referências para material importante para dar os primeiros passos nesta área, bem como conhecer algumas pessoas com ela relacionada, com o objectivo de me ajudar a tomar a decisão de se quero seguir para esta área no mestrado ou não(Portfólio é a única cadeira de mestrado que estou a fazer no momento).

isto não é um Resumo do documento

Palavras Chave—(EdS, CTF, Reuniões)

SOFT-SKILLS ≠ SOFTWARE SKILLS

1 Introdução

Acho relevante começar por explicar o facto de estar a fazer esta cadeira, sem estar já em mestrado. Ciber-Segurança (CS) sempre foi uma área que me despertou muita curiosidade, tendo vindo para Licenciatura em Engenharia Informática e de Computadores (LEIC) principalmente por esta razão, e, no ano passado, quando foi anunciado pelo Instituto Superior Técnico (IST) que iria abrir um mestrado dedicado à área, fiquei bastante agradado. Porém, nunca tive qualquer tipo de contacto com as pessoas da área, bem como contacto com qualquer tipo de conhecimento prático nela utilizado, por outras palavras, apesar da curiosidade, esta nunca se transformou em nenhum tipo de investigação ou trabalho sério da minha parte. Quando um colega meu me disse que existia a EdS e me explicou o que lá era feito, e que podia usar isso para fazer já uma cadeira de mestrado, achei que era a oportunidade perfeita para poder recolher conhecimento, e talvez, exercitar um pouco sobre a área.

• *João Filipe Lopes Pardal, nr. 73976,*
E-mail: joao.f.pardal@tecnico.ulisboa.pt.
Instituto Superior Técnico, Universidade de Lisboa.

Manuscript received junho 1, 2015.

2 EdS

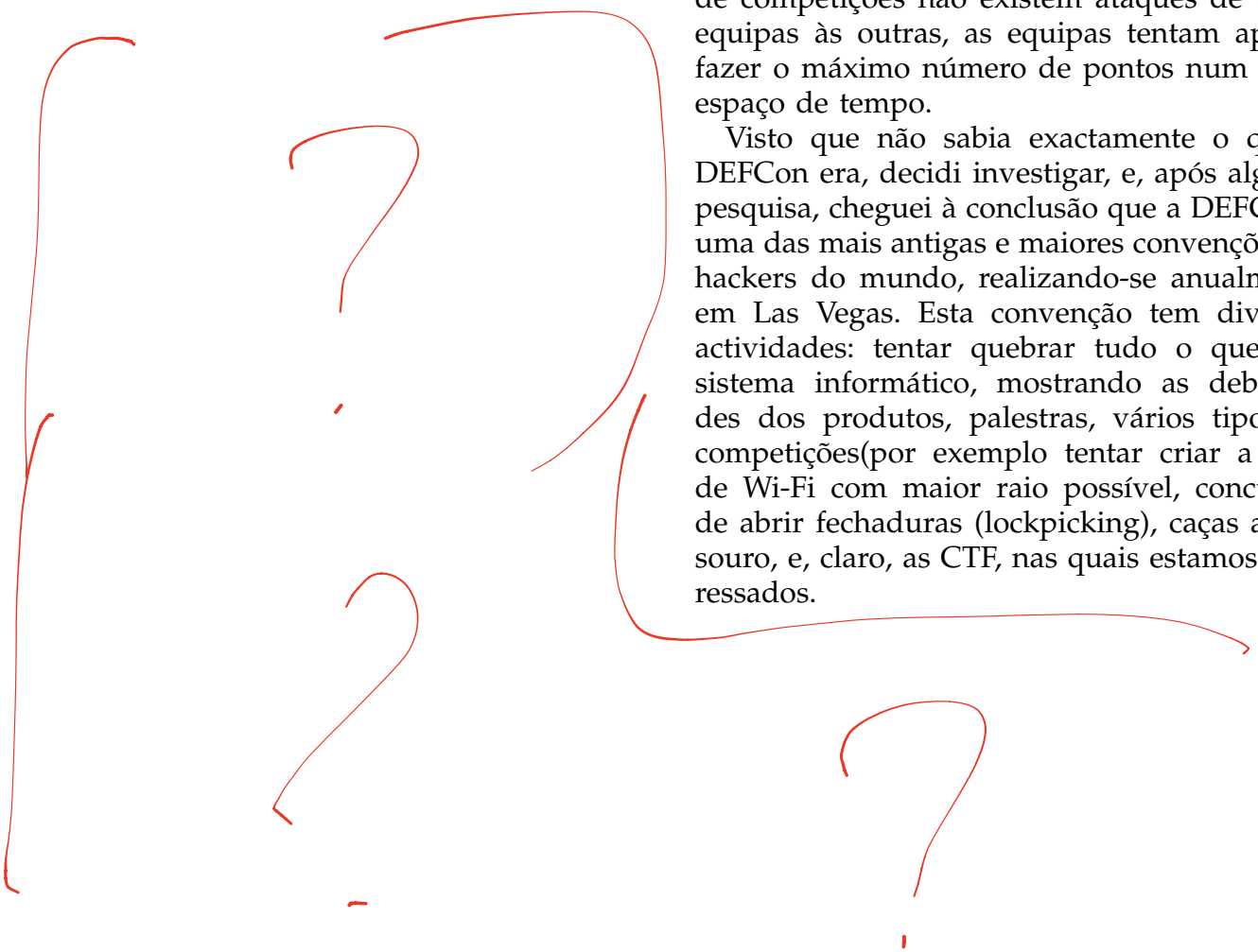
Como dito anteriormente no resumo, as actividades desta Equipa consistem em duas vertentes: as CTF e as reuniões. Nas seguintes subsecções vou falar sobre aquilo que aprendi em cada uma destas vertentes, não só relacionadas com EdS directamente, mas tambem com outros tipos de conhecimentos e experiência ganhos.

2.1 Reuniões

Estas reuniões realizavam-se a cada duas semanas, à terça-feira no campus da Alameda da parte da tarde. Sendo aluno do Taguspark, e morando perto deste campus, nunca tive necessidade de ir ao polo da Alameda, exceptuando na altura do Arraial do Técnico. A primeira coisa que aprendi com este grupo foi como está bem organizado o transporte dos alunos entre campus, havendo autocarros de um polo para outra de hora a hora, o que me poupou bastante tempo, e dinheiro, em transportes públicos, e já fiquei com a certeza de que se precisar de ir a aulas na Alameda futuramente, tenho sempre transporte garantido desde o Tagus. Nestas reuniões, aprendi, essencialmente, termos especificos da área, como nomes de ataques, pessoas e eventos relevantes para o desenvolvimento da mesma. Curiosamente, foi fora da aula que recolhi uma boa parte das

(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	0.5	0.5	0.5	0.5	0.4		0.6	0.6	0.4	0.6	0.8	1.0	
(0.4) Fair													
(0.2) Weak													

referências. Encontrei alguns amigos, que, por o mestrado que escolheram só haver na Alameda, transferiram-se do Tagus para lá. Alguns deles, e outros apenas caras conhecidas, por serem tambem ex-Tagus, e por terem estado já na EdS, ao saberem que eu lá estava, e, tendo eu explicado a minha experiência quase nula na área, falaram-me de imensos sites e livros que devia ler, bem como o que não valia a pena, tendo em conta a minha experiência actual, tentar para já aprender. Numa nota pessoal, achei um gesto admirável dos meus colegas, alguns dos quais como disse, que nem conhecia, estarem a ensinar-me com as experiências deles, e com o gosto que o estavam a fazer. Na viagem de regresso de autocarro, que por ser em hora de ponta era bastante prolongada, decidi falar um pouco mais com essas pessoas e informar-me sobre os mestrados em que eles estão, tentando saber coisas como que cadeiras são mais interessantes/importantes na área, se já têm ideia sobre o assunto da tese, erros a evitar no mestrado, cargas de trabalho, se sentem que o mestrado está aser aquilo que esperavam, e tentar perceber o que esperavam, para ver se me identificaria com outra das áreas de mestrado.



2.2 CTF

Quando o professor falou pela primeira vez em CTF, não sabia o que estas eram. CTF fez-me pensar em Capture the Flag, um estilo de jogo muito popular em vários jogos online, mas não acreditei que estivesse relacionado.

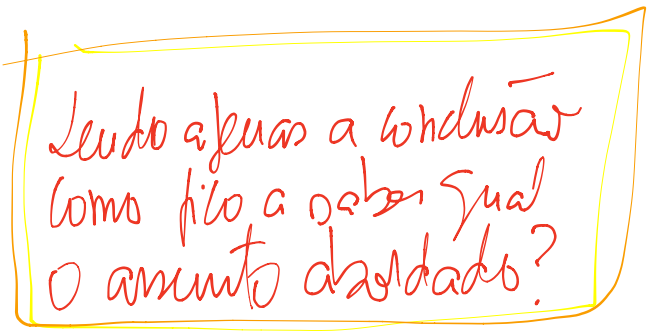
De facto, era a mesma coisa, mas num contexto de segurança informática. Estas competições têm como objectivo ser um exercício educacional que dá aos participantes experiência em como reduzir debilidades de um sistema informático, assim como conduzir e reagir ao mesmo tipo de ataques informáticos que são utilizados no mundo real.

Os dois tipos de CTF mais comuns são attack-defense, em que cada equipa tem um sistema informático que deve defender de ataques(defender a bandeira do seu sistema, que não deve ser roubada) e atacar os sistemas das outras equipas(tentar roubar a bandeira das outras equipas, daí o nome ser CTF) para ganhar pontos, e jeopardy, que consiste em resolver vários tipos de problemas com recursos a vários tipos de ataques, tendo cada problema um dado número de pontos que é atribuído à equipa, caso o resolva. Neste tipo de competições não existem ataques de umas equipas às outras, as equipas tentam apenas fazer o máximo número de pontos num dado espaço de tempo.

Visto que não sabia exactamente o que a DEFCon era, decidi investigar, e, após alguma pesquisa, cheguei à conclusão que a DEFCon é uma das mais antigas e maiores convenções de hackers do mundo, realizando-se anualmente em Las Vegas. Esta convenção tem diversas actividades: tentar quebrar tudo o que seja sistema informático, mostrando as debilidades dos produtos, palestras, vários tipos de competições(por exemplo tentar criar a rede de Wi-Fi com maior raio possível, concursos de abrir fechaduras (lockpicking), caças ao tesouro, e, claro, as CTF, nas quais estamos interessados.

3 Conclusão

Com a EdS conheci novas pessoas que me impressionaram por me ajudarem sem esperarem nada em troca, e que o fizeram com um sorriso na cara. Sinto que desenvolvi a minha capacidade de concentração e de apanhar ideias concretas de uma conversa, já que a velocidade à qual as reuniões eram assim o exigiram para que não me fosse perdendo, o que é sem dúvida uma capacidade importante para um profissional nesta área.



Agradecimentos

O autor gostaria de agradecer...

ao prof. Rui Cruz que me deu hipótese de corrigir o trabalho fora de horas e aos meu colegas da coach team, a toda a EdS, aos meus colegas e amigos que me ajudaram nesta caminhada de fazer um documento com referências para poder finalmente começar a trabalhar nesta área, e que me foram mantendo acordado nas longas viagens de regresso da Alameda, aos condutores dos autocarros do IST e à *vending machine* do pavilhão de Informática da Alameda, pelos seus deliciosos waffles de baunilha com chocolate.