Equipa de Segurança

João Filipe Lopes Pardal

Relatório de Actividades

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).

Palavras Chave—(EdS, CTF, Reuniões).

isto não é um Resumo do documento

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 A EdS

Como dito anteriormente no resumo, as actividades desta Equipa consistem em duas componenetes: as CTF e as reuniões. Nas seguintes sub-secções vou falar sobre aquilo que aprendi em cada uma destas componentes, não só relacionadas com EdS directamente, mas também 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.

Quanto às reuniões em si, fui para as reuniões sem saber bem o que esperar. Recebi um mail do professor Pedro Adão uns dias antes da primeira reunião com as informações

(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	0.7	0.5	0.6		0.6	0.6	0.4	0.6	0.8	1.0	
(0.4) Fair													
(0.2) Weak													

sobre horas e sítio onde nos devíamos encontrar, bem como o tema da reunião, e por quem esta ia ser dada. Conheci o nome da pessoa que a ia dar, apesar de nunca ter falado com ele, pois era um aluno do Taguspark.

Quando entrei na sala vi que ele era a única cara que conhecia e que iria ter de falar com pessoas novas de modo a aproveitar ao máximo o meu tempo ali. O professor explicou brevemente o que era o EdS, e fez-nos assinar uma declaração de como o IST não poderia ser responsabilizado, caso alguém naquela Equipa decidi-se utilizar aquilo que ali se estava a ensinar com fins prejurativos, e fez questão de nos lembrar que aquela Equipa serve para tentarmos proteger-nos, e a quem nos emprega, contra os ataques, e não para os usar contra entidades. Falou ainda das CTF que se iam realizar. Eu não percebi nada deste bocado da conversa, mas por ser a primeira aula e não estar muito à vontade, decidi não fazer perguntas, e que quando chegasse a casa iria fazer alguma pesquisa sobre o assunto. A aula foi sobre um dos tipos de ataques informáticos que se podem fazer, com algumas demonstrações e processos de pensamento sobre as estratégias a serem usadas. Achei a aula interessante, pois era sobre aquilo tipo de coisas que queria aprender, mas infelizmente não aprendi nada em concreto. Aquelas aulas não eram o básico sobre como fazer ataques, mas sim já tópicos para quem sabia esse básico, o que não era o meu caso. Apercebi-me então, nos primeiros minutos da apresentação do meu colega, que o melhor que tinha a fazer era retirar o máximo de referências possíveis de tudo o que fosse dado. Desde palavras-chaves a nomes de pessoas da área, sites, livros, fóruns, tudo o que me pudesse apontar na direcção do conhecimento.

No fim da aula era uma pessoa satisfeita, pois a reunião tinha sido basicamente aquilo que esperei. Apesar de não haver uma recompensa imediata, sabia que, nas férias de Verão, tendo já recolhido material nas reuniões, iria ser mais fácil começar a investigar, o que me deixou bastante motivado, sendo que esta era a primeira vez que senti que tinha um bom ponto de partida para a minha investigação.

As outras reuniões foram basicamente o mesmo formato, um aluno a falar sobre um tipo de ataque específico, e a fazer algumas demonstrações, eu sem perceber grande coisa do que estava a ser dito por serem usados muitos termos dos quais apenas tinha uma vaga ideia do que significavam, mas sempre a procura das referências.

A última reúnião porém, foi diferente, pois no fim-de-semana dessa semana, seriam os *qualifiers* para a DEFCon(falarei sobre a DEFCon e esta aula na próxima subsecção), para os quais os alunos, bem como o professor pareciam bastante empolgados.

Curiosamente, foi fora da aula que recolhi uma boa parte das 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 a ser aquilo que esperavam, e tentar perceber o que esperavam, para ver se me identificaria com outra das áreas de mestrado.

2.2 CTF

Como tinha dito na anterior subsecção, não sabia o que estas eram, quando o professor as referiu. CTF fez-me pensar em Capture the Flag, um estilo de jogo muito popular em vários jogos online, mas não acreditei que estivesse relacionado.

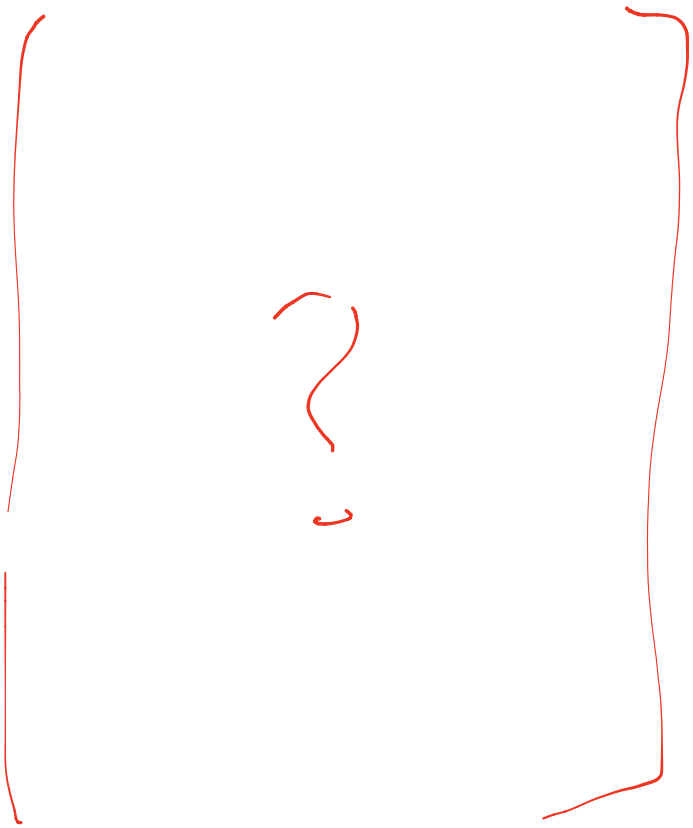
De facto, era a mesma coisa, mas num contexto de segurança informática. Estas competições têm como objectivo ser um exercício educacional que dá aos participantes experiência em como reduzir debilidades de um sistema informático, assim como conduzir e reagir ao mesmo tipo de ataques informáticos que 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.

Essa última reunião da EdS recaiu sobre este segundo tipo de competição, pois era aquele que iria ser feita nos *qualifiers*. Esta foi a reunião mais difícil de assistir, pois consistiu apenas em ler problemas de competições de anos passados, e os alunos iam dizendo uma parte de uma solução possível para o dito problema, mas sem uma solução final concreta, o que se tornou muito confuso muito rápido para mim. Em todo o caso consegui perceber mais ou menos o tipo de desafios apresentados na competição, e o que me esperava daqui a algumas semanas.

Devido aos vários projectos que tive este semestre e a algumas reuniões familiares aos fins-de-semana, não me foi possível entrar em nenhuma das competições. Apesar de não ter conhecimentos que pudesse exercer nestas competições, um dos meus colegas da equipa recomendou-me a ir pois era uma boa altura para ver os outros em acção. Ainda assim, fiz questão de fazr alguma pesquisa sobre o que era a DEFCon, para a qual estava a haver tanta expectativa na equipa, e assim que tive tempo, vi alguns dos problemas que eram dados nas CTF, bem como as suas resoluções (onde mais uma vez fui lembrado que não vale a pena olhar para estas coisas a não ser que tenha alguem para me explicar, ou até fazer alguma investigação primeiro).

Após alguma pesquisa, cheguei à conclusao 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 (lock-picking), caças ao tesouro, e, claro, as CTF, nas quais estamos interessados.



3 Conclusão

Os meus objectivos para este semestre em portfólio eram conhecer pessoas que tivessem o mesmo gosto que eu por CS, aprender o máximo possível com elas, ganhar alguma experiência na área e ver se realmente esta era a área que quero seguir no mestrado.

Apesar de ainda não poder dizer com 100% de certeza que esta é *a* área de mestrado, fiquei contente com aquilo que vi, ouvi e aprendi ao longo destes meses na EdS, e que no Verão vou ter, finalmente a motivação necessária para começar a aprender e experimentar nesta área, com toda a informação que fui recolhendo, para que, antes do próximo ano lectivo começar, possa ter a certeza se quero fazer disto a minha vida profissional ou não.

Conheci novas pessoas que me impressionaram por me ajudarem sem esperarem nada em troca, e que o fizeram com um sorriso na cara.

Infelizmente, neste semestre ainda não consegui 'meter as mãos na massa', mas espero estar mais forte no semestre que vem, voltar para a EdS e desta vez com um papel activo.

Agradecimentos

O autor gostaria de agradecer...

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.