SecurityTeam@IST

Tiago Luís de Oliveira Brito

Relatório de Aprendizagens

Resumo—Todos os engenheiros têm um gosto em comum. Todos gostam de aprender e inovar. O que os distingue é que nem todos gostam de aprender os mesmos conceitos. Eu gosto de Segurança Informática, e como tal fiquei extremamente motivado quando foi criada a equipa de segurança do Instituto Superior Técnico (IST) pelo professor Pedro Adão, a SecurityTeam@Técnico (STT), na qual me inscrevi o quanto antes. Neste artigo vou falar sobre as *soft skills* adquiridas durante o decorrer da minha atividade na STT. Será explicado como a SecurityTeam@Técnico desenvolveu as minhas competências sociais, como ajudou a desenvolver a minha noção de trabalho em equipa e trabalho colaborativo à distância, como despertou o meu interesse em auto-aprendizagem na área da segurança informática, e em partilhar essa aprendizagem com os restantes membros da equipa, e como desenvolveu a minha noção de *white hacking* ou *ethical hacking*, que consiste em desenvolver as minhas capacidades e técnicas na área da segurança informática de uma forma ética e respeitando os outros.

Palavras Chave—Segurança, equipa, *soft skills*, desafios, informática, competições, reuniões, CTF, STT.

1 Introdução

A EQUIPA de segurança SecurityTeam@IST (ou SecurityTeam@Técnico) foi criada com o objetivo de aproximar todos os alunos do IST que partilham o interesse pela área da segurança informática, ainda que estes não frequentem o curso de Licenciatura em Engenharia Informática e de Computadores (LEIC) ou Mestrado em Engenharia Informática e de Computadores (MEIC), para que possam partilhar experiências e conhecimentos.

O professor Pedro Adão, apesar de representar a equipa, tenta ter um papel minimalista na STT. Isto é, tenta incentivar os alunos a garantir a continuação da equipa de forma autónoma, pois este deve ser um projeto dos alunos e não de um professor. Isto significa que, nesta atividade, os alunos desempenham um papel de gestão sendo responsáveis por marcar atividades e reuniões quando querem ou acham necessário.

• *Tiago Brito, n.º 72647,*
E-mail: tiago.de.oliveira.brito@tecnico.ulisboa.pt,
Instituto Superior Técnico, Universidade de Lisboa.

Manuscrito recebido dia 6 Junho, 2015.

Assim, não só desenvolvemos as nossas capacidades técnicas como também as nossas capacidades organizacionais. Para nos auxiliar na gestão dos eventos da equipa fazemos uso de alguns sistemas *online* como o Facebook [1], Discourse [2] e Google Drive [3].

2 *White Hat vs. Black Hat*

Hoje em dia, quando se ouve a palavra *hacking* é, habitualmente, com um sentido pejorativo e criminoso. Mas nem sempre foi assim. Nos anos 50 a palavra significava 'trabalhar' num problema técnico de uma forma diferente ao esperado originalmente [4].

Por isto, o adjetivo *hacker* devia ser usado para descrever uma pessoa entusiasmada com uma tecnologia e que a altera para funcionar da melhor forma. Por outras palavras, um *hacker* adapta a tecnologia para que esta o sirva adequadamente, sem violar as regras.

Por sua vez, um indivíduo que modifique ou explore uma tecnologia para que esta faça o que não é suposto, inclusive violando as regras e leis, é denominado *cracker*. Este tipo de atitudes não são apoiadas nem incentivadas pela STT, bem pelo contrário.

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

A estas duas vertentes de ética na segurança informática chamamos de *White Hat* - o indivíduo que é contratado ou está autorizado a explorar as vulnerabilidades de um sistema com a intenção de o melhorar - e *Black Hat* - o indivíduo cujo o único objetivo é explorar vulnerabilidades de um sistema, sem autorização prévia, com intenções maliciosas (sabotagem, extorsão, etc.).

No início da sua atividade, o representante da STT, o professor Pedro Adão, distribuiu por todos os membros um documento onde explica claramente as intenções da equipa e refere que todas as técnicas aprendidas sob a alçada da STT devem ser apenas usadas no contexto das competições de *Capture The Flag* (CTF) ou em condições controladas e com a devida autorização.

Com isto, fica estabelecido o dever moral e ético que um membro da STT deve ter perante a sociedade e o limite que um indivíduo com estas capacidades não pode ultrapassar.

Este foi provavelmente o conceito mais importante aprendido na equipa, pois representa responsabilidade moral, cidadania e respeito pelos outros e aponta que devemos usar sempre os nossos conhecimentos e recursos para o bom desenvolvimento e sustentabilidade da sociedade e não para a sua corrupção e rutura.

3 Gestão Organizacional

Com o objetivo de facilitar o contacto com a maioria dos elementos da STT foi criada uma página no Facebook em que qualquer elemento pode criar eventos, fazer questões aos restantes membros e partilhar artigos, *links* ou tutoriais para diversos temas do interesse da equipa.

A contribuição de cada membro nesta página é importante porque, por exemplo, se um aluno pretende organizar uma competição tem que perceber se o número de membros que quer participar localmente é significativo, para se proceder à requisição de uma sala. Sem esta informação é difícil gerir o evento.

Outra ferramenta importante para o desenvolvimento da STT é a Google Drive, pois facilita a partilha de ficheiros entre os membros da equipa. É nesta ferramenta que estão guardadas as soluções para os exercícios de competições passadas, em forma de *scripts* ou ficheiros texto.

Mais uma vez, cada membro é responsável por gerir a sua contribuição na STT através da Google Drive. Como exemplo, podemos pensar no que ocorreu depois da *Boston Key Party* CTF. Após eu ter resolvido um número razoável de exercícios durante a competição ficou ao meu encargo sintetizar num documento os passos usados para chegar às soluções e disponibilizar todo o material usado para a resolução (por exemplo *scripts*). O mesmo se espera de qualquer elemento da equipa quando estes resolvem exercícios nas competições ou até no seu tempo livre.

Sem este contributo de todas as partes a equipa não cresce e não melhora o seu desempenho em futuras competições, por isso é vital que todos os membros aprendam a gerir bem o seu papel na STT.

Assim, graças à descentralização da gestão da equipa, não só desenvolvemos as nossas capacidades técnicas como também as nossas capacidades organizacionais.

4 Auto-aprendizagem

Apesar da STT ser uma equipa existe uma grande componente individual. Cada membro tem que aprender o máximo que consegue para que o desempenho da equipa seja melhorado.

É por isto que a STT encoraja a auto-aprendizagem a cada um dos seus membros e também a especialização de cada elemento na sua área de eleição. No meu caso, as áreas que acho mais interessantes são *reverse-engineering*, *forensics* e *web* e, como tal, o tempo livre que consegui dispor para aprender novas técnicas foi dedicado a essas áreas.

Uma das primeiras dificuldades foi saber por onde começar a procurar tutoriais e desafios. Felizmente, a comunidade é bastante ativa e surpreendentemente existem bastantes *sites* especializados em disponibilizar material de estudo nas minhas área de interesse. Em particular, os *sites* que mais usei foram o *crackmes.de* [5], o *securitytube.net* [6], o *hackthissite.org* [7] e a aplicação *Damn Vulnerable Web Application* (DVWA) [8].

O primeiro *site* indicado permite resolver exercícios de *reverse-engineering*. O segundo *site* é uma versão do *youtube.com* com foco na segurança informática, disponibilizando tutoriais na área. O terceiro *site*, assim como a aplicação *web* referida, permitem treinar exploração de vulnerabilidades comuns em aplicações *web*.

5 Trabalho de Equipa

A STT é uma equipa e, como tal, existe um grande ênfase na componente colaborativa.

O foco das reuniões semanais é permitir que todos os membros tenham a oportunidade de trocar experiências e técnicas entre si. Esta aprendizagem colaborativa é um dos pilares da STT, pois é assim que os seus elementos evoluem, desenvolvendo também o potencial da equipa.

Não é só nas reuniões semanais que se aprende em equipa. Durante as competições é muito comum aprender ou ensinar técnicas. Um exemplo disto foi quando ensinei aos meus colegas, durante a resolução de exercícios da *Boston Key Party* e DEFCON *Quals*, como funcionam certas caraterísticas do *PHP: Hypertext Preprocessor* (PHP) e *Javascript*.

Para além da aprendizagem colaborativa existe também muito trabalho em equipa. Todos os exercícios são desafiantes e é muitas vezes necessária a ajuda de diversos membros para que se chegue a uma potencial solução. Pessoas diferentes pensam de maneira diferente e por vezes esta diversidade é importante para o avanço num dado desafio.

Não é só quando os membros da STT estão reunidos no mesmo local que se trabalha em equipa. Mesmo quando um membro decide competir remotamente também colabora com os restantes participantes, quer seja através do Facebook ou do *Internet Relay Chat* (IRC) oficial da STT. Como exemplo posso referir a minha participação na competição Plaid CTF 2015. Nesta competição participei remotamente, no entanto, consegui colaborar à distância com os colegas que se encontravam a competir localmente, ou com outros que, como eu, competiram sozinhos.

Toda esta colaboração permite também o desenvolvimento da comunicação e expressão orais, já que para explicar algo aos restantes membros da equipa é necessário exprimir as minhas ideias da forma mais clara possível.

6 Tempo e Criatividade

As competições de CTF têm, habitualmente, duração de 48 horas e apresentam muitos exercícios para realizar nesse curto período de tempo. Isto significa que o tempo é precioso e deve ser bem gerido.

É fundamental não desistir de um exercício assim que este se revela mais difícil do que inicialmente era esperado, no entanto não se pode perder demasiado tempo num exercício sem novos desenvolvimentos, pois podemos estar a perder tempo que podia ser investido noutros desafios, e talvez com mais sucesso.

Como se pode perceber a gestão do tempo numa CTF pode ser bastante complicada e o que aprendi a fazer durante as competições em que participei, para maximizar os meus resultados, foi tentar avaliar bem a dificuldade técnica dos exercícios. Existe uma ligação direta entre a dificuldade de um exercício e o tempo que este demora a ser resolvido, especialmente para membros principiantes, como é o meu caso. Um ótimo indicador da dificuldade de um exercício é o valor, em pontos, da sua resolução. Geralmente, quanto mais pontos vale, mais difícil é.

Assim, uma boa tática é atacar primeiro os exercícios que valem menos pontos e que, por isso, deveriam demorar menos tempo a resolver. Caso esteja a ser difícil encontrar a solução num curto espaço de tempo, então é sinal que talvez seja altura de focar a minha atenção noutro exercício. É bom resolver primeiro os exercícios mais fáceis pois permite-me perceber a correspondência entre os pontos atribuídos a um exercício e a sua dificuldade real, e assim extrapolar a dificuldade dos restantes.

Durante as competições surge ainda outra dificuldade, para além da gestão do tempo, que é a criatividade. A criatividade é vital para a resolução de exercícios de segurança informática pois, por vezes, é a sequência de ações mais impensável, ou o pedaço de código

mais inocente, que esconde a vulnerabilidade a explorar.

Para além disto, mesmo já sabendo qual a vulnerabilidade apresentada num dado exercício é preciso criatividade e imaginação para descobrir como a explorar de maneira a resolver o desafio. É por esta razão que é importante ter muita experiência numa dada área da segurança informática. Ao saber as bases de cada técnica é mais fácil adapta-la de forma a poder ser usada na resolução de um exercício.

7 Conclusão

A STT foi uma atividade que me ajudou a evoluir em diversas áreas, incluindo ética profissional, gestão organizacional, auto-aprendizagem, trabalho em equipa, criatividade e gestão pessoal e de tempo.

Assim, em suma, a STT ajudou-me a desenvolver *soft skills* úteis para o mercado de trabalho e desenvolvimento pessoal e social, assim como a fortalecer o gosto pela área de segurança informática.

Agradecimentos

Gostava de agradecer ao professor Pedro Adão por me ter proporcionado esta oportunidade e todos os momentos que advieram da SecurityTeam@Técnico. Esta equipa é responsável por fomentar o meu crescente interesse na área da Segurança Informática e como tal agradeço também a todos os membros da equipa, em especial ao Diogo Barradas, por me ensinarem novas técnicas e me proporcionarem momentos divertidos na sua companhia.

Referências

[1] "Facebook da SecurityTeam@IST." [Online]. Available: https://www.facebook.com/groups/709926362432048/
[2] "Discourse da SecurityTeam@IST." [Online]. Available: http://discourse.stt.s4w.ovh/
[3] "Google Drive." [Online]. Available: https://drive.google.com
[4] "A Short History of 'Hack'." [Online]. Available: http://www.newyorker.com/tech/elements/a-short-history-of-hack
[5] "crackmes.de - desafios de reverse-engineering." [Online]. Available: http://crackmes.de/
[6] "Security Tube." [Online]. Available: http://www.securitytube.net/
[7] "Hack This Site." [Online]. Available: https://www.hackthissite.org/
[8] "Damn Vulnerable Web Application." [Online]. Available: http://www.dvwa.co.uk/

Tiago Brito Sempre tentei aprender novas coisas e ser um membro ativo na comunidade.

Em Abril de 2009 fui a Marrocos como voluntário numa expedição todo-o-terreno cujo objetivo era viajar até aldeias remotas, cujas condições de acesso são débeis, e doar roupas, água, comida e outros recursos.

Sempre fui um interessado em construir e imaginar coisas novas, interessantes e práticas e foi isso que me levou a concluir a Licenciatura em Engenharia Informática e de Computadores pelo Instituto Superior Técnico assim como a continuar a minha aventura académica pelo mestrado nesta mesma instituição e a participar em competições de engenharia como a *European BEST Engineering Competition* (EBEC) da *Board of European Students of Technology* (BEST) onde consegui atingir bons resultados.

Desde Janeiro de 2015 que sou investigador no INESC-ID no âmbito de uma bolsa de investigação na área de Gestão e Tratamento de Informação associado ao projeto KDLSBN com o orientador Bruno Martins.