SecurityTeam@IST

Tiago Luís de Oliveira Brito

Relatório de Actividades

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 a minha experiência na equipa durante o segundo semestre do ano letivo 2014/2015 assim como das atividades realizadas durante este período. Este artigo foca-se em explicar no que consistem as atividades da equipa, nomeadamente as competições internacionais de *Capture The Flag* (CTF), um jogo que se baseia em resolver exercícios técnicos de segurança informática, semelhantes aos que são resolvidos por profissionais na área de *Penetration Testing* (PenTest). Para além disto são realizadas reuniões semanais, onde se faz uma revisão do desempenho da equipa nas competições, assim como apresentações onde se adquirem novos conhecimentos para aplicar nas competições seguintes.

Palavras Chave—Segurança, equipa, 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.

Na figura 1 é apresentada a cronologia dos eventos da STT a que assisti. Nas restantes secções irei descrever as atividades nas quais participei durante o segundo semestre do ano letivo 2014/2015 no âmbito da SecurityTeam@Técnico.

2 *Capture The Flag*

Nesta secção será descrito resumidamente o funcionamento de uma competição CTF para contextualizar as secções que se seguem.

• *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.

Em segurança informática, CTF é uma competição que visa dar aos participantes experiência na área de segurança de computadores. Para competirem com sucesso, os participantes devem dominar diversas áreas técnicas como a administração de sistemas, análise de protocolos, programação, análise criptográfica, *reverse-engineering* e *network sniffing*, entre outras.

Habitualmente estas competições apresentam duas vertentes. A primeira, denominada 'ataque/defesa', é uma vertente em que cada equipa é responsável por uma máquina, ou por uma pequena rede (isolada da Internet), e que tem como objetivo defender essa máquina, ou rede, dos restantes participantes, assim como atacar as máquinas dos adversários. As equipas recebem pontos tanto por defender as suas máquinas como por atacar as dos adversários.

A outra vertente deste tipo de competições é a vertente *Jeopardy*. Aqui as equipas tentam resolver exercícios propostos pela organização da competição. Cada exercício foca-se numa categoria das apresentadas acima e os pontos atribuídos à resolução do exercício variam consoante a dificuldade técnica do mesmo.

A cada competição é atribuído um peso que reflete a importância da prova no contexto

(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	1.0	0,8	1.0	0.8		1.0	0.8	1.0	1,0	1.0	1.0	
(0.4) Fair													
(0.2) Weak													

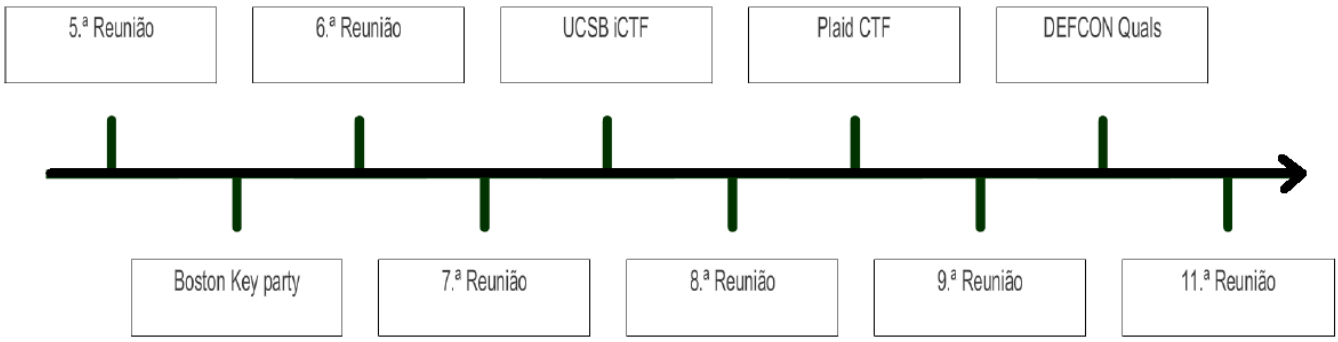

Figura 1. **Cronologia dos eventos da STT** - cronologia relativa para facilitar a contextualização das secções que se seguem.

internacional. Este peso é usado para, em conjunto com a pontuação obtida nesse desafio, calcular o *ranking* mundial de uma equipa.

Na STT realizam-se maioritariamente CTFs do tipo *Jeopardy* já que a realização da vertente 'ataque/defesa' envolve uma maior infraestrutura (servidores e isolamento da rede), coisa que neste momento não está ao alcance da equipa.

3 Reuniões

Uma das atividades principais da STT é a realização de reuniões semanais que decorrem à quinta-feira no laboratório 14 do edifício Redes Novas Licenciaturas (RNL), onde se faz um resumo da reunião anterior, assim como das competições que a antecederam.

O objetivo destas reuniões é que os alunos apresentem, por iniciativa própria, as soluções a desafios de diversas competições, ensinem técnicas aos restantes participantes, que estes ainda não conhecem ou não dominam, e preparem a próxima competição, habitualmente tentando resolver problemas das edições anteriores dessa mesma competição.

Cada reunião tem a duração de pouco mais de uma hora e são o pilar de suporte da equipa, isto porque é nestas reuniões que a equipa evolui e cresce, é onde os membros aprendem e onde interagem fora das competições.

3.1 Quinta Reunião

A quinta reunião da STT, realizada no dia 24 de fevereiro de 2015, foi a primeira reunião do semestre e representou o regresso ao ativo da equipa depois das férias escolares.

Nesta reunião perguntou-se aos membros o que estes aspiravam fazer no semestre, tendo em conta o calendário de competições. Este planeamento foi muito informal, já que nem todas as competições tinham datas definitivas para a sua realização. Como tal organizou-se uma lista provisória de competições que representavam os objetivos da STT para o semestre.

Para além deste planeamento, a reunião serviu também para dois alunos, Ana Costeiro Araújo e Daniel da Costa, apresentarem um sistema para melhorar o desempenho da equipa nas competições que se seguiram. Estes dois alunos foram apresentar um programa denominado SQLMap [1].

O SQLMap é uma ferramenta *Open Source* de PenTest que automatiza o processo de deteção e exploração de vulnerabilidades de injeção *Structured Query Language* (SQL) [2]. Este sistema é uma ferramenta útil para a STT já que, durante o decorrer de diversas competições de segurança, fomos abordados com problemas no âmbito de aplicações *web*, que são muitas vezes vulneráveis a injeções SQL.

Assim, o que esta ferramenta permite fazer é facilitar o processo de descoberta e exploração destas mesma vulnerabilidades garantido assim que se consegue realizar um maior número de exercícios ao longo dessa competição e, como tal, ganhar mais pontos.

3.2 Sexta Reunião

Na sexta reunião, realizada no dia 10 de março de 2015, fez-se um balanço do desempenho da STT na competição *Boston Key Party* realizada no fim-de-semana de 27, 28 e 29 de fevereiro de 2015.

Para além deste balanço foram demonstradas diferentes técnicas de exploração de *Cross-site scripting* (XSS) [3] por parte de um convidado, profissional da área de PenTest, Luís Grangeia. Já tendo assistido à reunião anterior, o convidado decidiu fazer uma apresentação onde discutiu e apresentou diversas técnicas de exploração de XSS, uma vulnerabilidade tipicamente encontrada em aplicações *web*.

Juntamente com a apresentação, Luís Grangeia deu a conhecer aos elementos da STT um programa que simula uma aplicação *web* vulnerável, aplicação esta que usou durante a apresentação como exemplo. *Damn Vulnerable Web Application* (DVWA) [4] é uma *web app* desenhada especificamente para ajudar profissionais a testar as suas capacidades num ambiente legal, assim como para ajudar alunos e *web developers* a perceber melhor como funciona o processo de segurança de uma aplicação *web*.

3.3 Sétima Reunião

Na sexta reunião, ao contrário do que é habitual acontecer na reunião que sucede uma dada competição, não foram apresentadas as soluções dos problemas resolvidos durante esse evento. Isto aconteceu porque, tal como foi referido, na reunião anterior foi apresentada, por parte de um convidado especial, uma lição sobre vulnerabilidades XSS.

Assim, ficaram para a sétima reunião, realizada no dia 24 de março de 2015, as apresentações de algumas soluções de exercícios resolvidos por elementos da STT durante a *Boston Key Party* CTF.

Estas apresentações servem para mostrar aos restantes participantes o raciocínio necessário para chegar à solução de um desafio específico. Como existem muitos exercícios cuja lógica de resolução é semelhante aos apresentados, estas sessões são uma mais valia na construção de um reportório de soluções e técnicas da STT.

3.4 Oitava Reunião

Na sétima reunião levantou-se a questão de que a equipa não estava preparada para resolver problemas de *reverse-engineering*, isto porque estes problemas são tecnicamente mais exigentes. Tendo isto em conta, o colega João Godinho preparou uma apresentação para a oitava reunião, realizada no dia 14 de abril de 2015, onde ensinou o essencial sobre *Buffer Overflows* [5].

Buffer Overflow é uma condição que existe quando um programa tenta escrever mais dados num *buffer* do que os que este suporta, ou quando um programa tenta escrever dados em espaços de memória consecutivos ao *buffer*. Um *buffer* é uma secção de memória alocada sequencialmente. Escrever fora dos limites do bloco de memória alocado pode corromper dados, causando a interrupção inesperada do programa (*crash*) ou até a execução de código malicioso.

É esta última característica do *Buffer Overflow* (execução de código malicioso) que a STT procura dominar. Esta técnica é importante pois em muitos exercícios de *reverse-engineering*, encontrados nas competições, o código disponibilizado é vulnerável a este tipo de ataques e sem saber explorar esta vulnerabilidade pode não ser possível chegar à solução.

3.5 Nona Reunião

Na nona reunião, realizada no dia 28 de abril de 2015, foi a vez do colega Afonso dos Santos liderar uma apresentação sobre *web exploits*, mais especificamente sobre injeções SQL.

Já na quinta reunião se havia falado sobre SQL, no entanto, nessa reunião, deu-se a conhecer uma ferramenta que automatiza o processo de exploração de vulnerabilidades. O problema é que, em muitos casos, essa automatização não é possível pois a página a ser explorada pode estar preparada para esses ataques ou pode apresentar vulnerabilidades menos comuns que não integram o vetor de ataque da ferramenta SQLMap.

Como tal, é importante para todos os membros não só saberem usar a ferramenta como, caso a ferramenta não se prove eficaz, consigam

fazer uso das técnicas manuais para resolver o desafio.

3.6 Décima Primeira Reunião

Por razões académicas não assisti à décima reunião da STT, no entanto foi-me possível assistir à décima primeira reunião, realizada no dia 28 de maio de 2015, após a participação na DEFCON, uma convenção de segurança realizada em Las Vegas, nos Estados Unidos da América (EUA), e cuja CTF é uma das mais importantes no panorama internacional.

Esta reunião marcou o fim do primeiro ano de atividade da STT e serviu para fazer um balanço deste período, do *ranking* atingido até ao momento e ainda planear os objetivos para o próximo semestre.

Foi ainda sugerido que cada elemento da STT tente, durante as férias, aprender técnicas de exploração de vulnerabilidades, principalmente de *reverse-engineering*, área na qual a equipa apresenta maiores debilidades.

4 Competições

O principal objetivo da STT é participar em competições de CTF. O calendário oficial de competições CTF pode ser acedido no CTFtime [6], o *site* oficial das competições.

Habitualmente, as competições realizam-se durante o fim-de-semana e como tal, salvo algumas exceções, a equipa instala-se na sala de reuniões do pavilhão II de informática. Acontece que, no caso de uma competição ser menos importante, ou existirem menos membros da equipa disponíveis, participa-se remotamente, isto é, cada participante tenta resolver os problemas da competição sozinho, em casa ou no seu espaço de preferência, sem que a equipa esteja toda reunida no mesmo local.

Durante o semestre perfiz um total aproximado de 37 horas em competições CTF, nas quais o maior número de horas foi gasto nas competições *Boston Key Party* e DEFCON Quals.

4.1 *Boston Key Party* 2015

Boston Key Party foi a primeira competição do semestre e como tal foi a que juntou o maior número de participantes devido à menor carga horária das atividades curriculares no início do semestre. Assim, esta foi uma das competições do semestre em que se conseguiu mais pontos. Conseguindo obter 8,340 pontos para o *rating* global. O 85.º lugar, de 822 equipas, foi considerado um sucesso por todos.

Nesta competição em particular consegui resolver cinco exercícios, alguns sozinho e outros com a ajuda de colegas, todos eles da categoria *Web*. Os exercícios resolvidos apresentavam, na sua grande maioria, vulnerabilidades ligadas ao *PHP: Hypertext Preprocessor* (PHP).

Os exercícios eram apresentados da seguinte forma: uma página que continha não mais que alguns campos de *input* e um botão. O *input* inserido é redirecionado para uma página PHP que, consoante o resultado do processamento, devolvia uma *flag* (o resultado que queremos) ou uma mensagem de erro.

Habitualmente não é possível observar o código de uma página PHP, já que este código é interpretado pelo servidor, no entanto a organização tornou possível o acesso ao código através de um ficheiro texto (.txt) disponível no servidor *web*. Quem descobrisse este ficheiro conseguia ler o código fonte e assim descobrir a vulnerabilidade que esse código apresentava.

Todas as vulnerabilidades eram particularidades conhecidas do PHP. A exploração destas vulnerabilidades permitiu passar várias verificações feitas nessa página e conseguir assim obter a *flag*. Para além dos problemas de *Web* também tentei resolver alguns problemas de *reverse-engineering*, no entanto não fui bem sucedido.

4.2 UCSB iCTF 2015

Esta competição foi a primeira do semestre na vertente 'ataque/defesa' e, à semelhança do que aconteceu no semestre anterior com a competição RuCTFE, o maior problema foi configurar corretamente o *setup* necessário para a participação nos desafios.

A maior parte do tempo foi gasto durante o processo de configuração da máquina servidor. Nessa máquina correu uma imagem de um sistema operativo, disponibilizada pela organização, onde estavam a correr diversos serviços vulneráveis.

Os objetivos da competição eram descobrir que serviços a correr eram vulneráveis e corrigir esses serviços na nossa máquina (fazer *patch* do serviço) assim como explorar essas vulnerabilidades nas máquinas dos adversários.

Nenhum *patch* foi realizado pela STT no decorrer da competição, no entanto alguns serviços nas máquinas das equipas adversárias foram explorados com sucesso.

O grande problema foi o *downtime* dos serviços até se conseguir configurar corretamente a máquina. O facto de só termos conseguido colocar a máquina *online* a três horas do fim da competição foi a causa da grande penalização de que a STT foi alvo.

4.3 Plaid CTF 2015

Esta competição foi muito esperada pela grande maioria dos membros da STT pois tratou-se de uma competição organizada pelos *Plaid Parliament of Pwning* (PPP), a melhor equipa do *ranking*.

Devido ao grande interesse da equipa pensou-se em competir nesta CTF localmente, no entanto poucos foram os membros que apareceram na sala habitual, e como tal muitos acabaram por competir remotamente. Isto porque por vezes é difícil disponibilizar grande parte do fim-de-semana para competir numa CTF e esta foi uma dessas ocasiões. Ainda assim o interesse por competir sobrepõe-se às restantes atividades e, como tal, é sempre possível arranjar algum tempo para uma CTF.

Como já foi referido, a STT apresenta uma grande fragilidade no que toca a *reverse-engineering* e eu não sou exceção. Assim, numa competição organizada pelos PPP, onde seria de esperar um grande foco nesta área, é difícil ignorar essa fragilidade. Como consequência não consegui resolver qualquer exercício.

Apesar da fragilidade referida, a equipa conseguiu obter o 74.º lugar na competição e, pelo facto de esta competição em particular ser muito importante no contexto internacional, foi onde se ganhou mais pontos, fazendo um total de 11,857 pontos para o *rating* global.

4.4 DEFCON Quals 2015

A DEFCON Quals foi a última CTF do semestre e, como tal, era do interesse de muitos dos membros da STT participarem nesta competição. A DEFCON é a maior convenção de segurança informática no mundo e a sua CTF é uma das mais importantes para o *ranking* oficial.

Assim, não é de admirar que também seja uma das mais desafiantes. Nesta competição a STT resolveu muito poucos exercícios mas ainda assim atingiu uma posição bastante aceitável na classificação final.

Apesar de termos conseguido o 113.º lugar de 284 equipas podíamos ter assegurado o 84.º lugar. Isto porque, a poucos segundos do final da prova, acertei um dos 4 exercícios resolvidos pela equipa, no entanto os poucos segundos que restavam não foram suficientes para submeter a resposta. Foi com muito pesar que a equipa viveu os últimos segundos da competição.

Ainda assim, esta CTF foi uma das que atribuiu mais pontos à STT ao conseguirmos 8,691 pontos.

5 Conclusão

A STT foi uma das atividades extra-curriculares mais divertidas em que participei e tenciono continuar enquanto for aluno do IST. É uma atividade que me permite não só conviver com colegas que partilham o mesmo interesse pela segurança informática, como também me permite aprender e ganhar experiência com sistemas e técnicas usadas no mercado de trabalho.

Apesar de sermos uma equipa recente, conseguimos obter uma classificação no *ranking* oficial muito surpreendente e temos como objetivo subir do 142.º lugar, de 4050 equipas, para o top 100 até ao final de 2015.

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] "SQLMap." [Online]. Available: http://sqlmap.org/
[2] "SQL." [Online]. Available: http://en.wikipedia.org/wiki/SQL
[3] "Cross-site scripting." [Online]. Available: http://en.wikipedia.org/wiki/Cross-site_scripting
[4] "Damn Vulnerable Web Application." [Online]. Available: http://www.dvwa.co.uk/
[5] "Buffer Overflow." [Online]. Available: https://www.owasp.org/index.php/Buffer_Overflow
[6] "CTFtime.org." [Online]. Available: https://ctftime.org/

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 projecto KDLSBN com o orientador Bruno Martins.