Security Team at IST

João Glória

Relatório de Actividades

Resumo—O presente relatório, realizado no âmbito da cadeira de Portfólio III, tem como objectivo descrever a actividade realizada ao longo dos últimos 4 meses. A actividade consistiu numa equipa de Segurança Informática de *hackers* passivos, *white hat hackers*, com objectivo de participar em competições internacionais, online, de *hacking*. Foram realizadas reuniões quinzenais onde aprendemos os conceitos a utilizar durante as competições. A equipa era composta por diversos alunos de diferentes cursos e nacionalidades, tendo a actividade servido também para o entrosamento entre os alunos.

Palavras Chave—equipa, Segurança Informática, white hat hackers, competições online, *hacking*

1 Introdução

A actividade Security Team at IST consistiu numa equipa de alunos, de vários cursos e nacionalidades, que tinha como objectivo a participação em competições internacionais *online* de *hacking*. A equipa concordou desde cedo que todas as práticas e técnicas leccionadas durante as reuniões de aprendizagem seriam usadas única e exclusivamente para praticar boas acções sendo cada elemento do grupo reconhecido como *hacker white hat*.

A razão pela qual escolhi a actividade deve-se ao facto de querer aprofundar conhecimentos pela matéria relacionada com o Mestrado em que me encontro inscrito actualmente. No entanto o baixo número de reuniões e competições em que a equipa participou apenas me permitiu adequirir algumas das técnicas.

2 Motivação

A actividade foi-me inicialmente exposta pelo professor e coordenador da mesma - Pedro Adão -, durante uma aula de Qualidade de Software. Depois de esclarecido, com o mesmo, acerca do que se iria passar ao longo do semestre na equipa decidi integrá-la. O que seria uma actividade por proposta acabou por ser uma actividade institucional depois de integrada pelo corpo docente na lista de tarefas disponíveis.

A razão da escolha da actividade deveu-se ao Mestrado de Engenharia Informática em que me encontro envolvido. Existe uma certa complementariedade entre a mesma, com as unidades curriculares que assisti durante o corrente semestre, tal como Segurança Informática em Redes e Sistemas. Desta forma achei que poderia complementar o conteúdo das aulas com uma actividade extra-curricular. Os objectivos desta escolha foram melhorar os meus conhecimentos na área da Segurança Informática e tentar perceber se realmente gostaria de aplicá-los na vida profissional. No entanto o número de reuniões e competições em que a equipa participou acabou por não ser o suficiente para uma profunda aprendizagem do tema.

3 Competições

As competições foram o principal objectivo da *Security Team at IST*. Estas consistiam num grupo de problemas, de diversas áreas da segurança informática que deveriam, ser realizados num determinado espaço de tempo. Estas competições são normalmente organizadas por outras equipas de *hacking* com algum prestígio.

• *João Glória, nr. 73596,*
E-mail: joaohgloria@tecnico.ulisboa.pt,
Instituto Superior Técnico, Universidade de Lisboa.

Manuscript received 17 de Janeiro, 2015.

PORQUE MOTIVO ESTÁ EM INGLÊS?

(1.0) Excelent	ACTIVITY					DOCUMENT						
(0.8) Very Good	Objectives x2	Options x1	Execution x4	S+C x1	SCORE	Structure x0.25	Ortogr. x0.25	Gramm. x0,.25	Format x0.25	Title x0.5	Filename x0.5	SCORE
(0.6) Good												
(0.4) Fair	1.8	0.8	3.6	0.8	7.0	0.25	0.2	0.25	0.2	0.4	0.5	1.8
(0.2) Weak												

Os procedimentos de como iriam funcionar as competições foram decididos durante a reunião que decorreu antes da primeira competição, *HackLu CTF 2014*. A equipa seria reunida numa sala previamente combinada e aí seriam distribuídas tarefas. Entre si os alunos discutiam quais as áreas da segurança informática em que tinham mais facilidade e formavam sub-equipas mais pequenas de forma a facilitar a comunicação entre colegas e a resolver um maior número de problemas em simultâneo. Normalmente o problema é resolvido com a descoberta da chamada *flag*, que correspondia a uma sequência de caracteres que tínhamos de descobrir ou decifrar.

3.1 HackLu CTF 2014

A HackLu CTF 2014 foi organizada pelos *FluxFingers* e ocorreu durante as 48 horas de 21 e 22 de Outubro de 2014. Esta foi a nossa primeira competição e consistia numa lista de 30 problemas do estilo *Catch The Flag*, ou seja teríamos de descobrir ou decifrar uma sequencia de caracteres, que seria posteriormente inserida no *website* onde decorria a competição. A equipa acabou por atingir um 52º lugar, com 10 problemas resolvidos, uma posição que não era esperada, uma vez que era a primeira competição do grupo. Apesar da posição a meia tabela, a equipa teve destaque na revista de tecnologia Exame Informática que redigiu um artigo acerca desta participação.

Figura 1: HackLu CTF 2014

3.2 RuCTFE

A RuCTFE ocorreu a 20 de Dezembro de 2014. Esta competição teve pouca adesão pois foi realizada a um Sábado e fora do período escolar. Por questões familiares e por ser aluno deslocado não pude comparecer na mesma.

4 Reuniões

As reuniões da Security Team at IST ocorriam com uma frequência de duas semanas. As reuniões eram marcadas via *Facebook* de forma a que todos os elementos tivessem conhecimento da marcação das mesmas. Estas reuniões tinham vários objectivos de acordo com o momento em que ocorriam. Para ser mais específico em relação ao tema das reuniões, vou proceder à divisão das temáticas em 3 tópicos:

- Primeira reunião
- Pré-competição
- Pós-competição

4.1 Primeira reunião

Na primeira reunião da equipa houve um breve discurso do coordenador da actividade - Pedro Adão -, acerca do que eram as competições de *hacking* em si e a sua experiência anterior como participante nas mesmas. Os alunos apresentaram-se e conheceram-se. Na hora e meia que se seguiu foram determinados vários aspectos da equipa. A frequência das reuniões ficou definida como quinzenal, e o nome da equipa ficou definido como STT, Securtity Team at Técnico. Foram também definidas, de acordo com o calendário escolar de cada um, as competições em que participariamos. No final desta reunião ficou ainda decidido que iríamos comparecer na competição *HackLu CTF 2014*.

4.2 Pré-competição

Nas reuniões pré-competição eram discutidas datas de competições a que a equipa poderia ir, e quais as áreas da segurança informática poderiam incidir mais nessas mesmas competições. Eram trocadas ideias sobre problemas de segurança informática e resolvidos problemas de competições de anos anteriores como forma de treino de competências.

4.3 Pós-competição

As reuniões pós-competição consistiam na resolução e explicação detalhada dos problemas que haviam sido resolvidos pela equipa durante a competição. Deste modo, todos os elementos da equipa, presentes ou não aquando da resolução do problema durante a competição, ficariam com uma ideia do que realmente havia sido feito. Estas explicações detalhadas eram feitas através de apresentações por um ou mais alunos, em forma de palestra. O(s) apresentador(es) da solução encontravam-se diante da restante equipa explicando passo-a-passo como resolver o problema. Devido ao multinacionalismo presente na Security Team at IST todas estas apresentações foram realizadas na língua mundial, inglês. Foi-me dada a oportunidade de apresentar o problema *Image Upload* da competição HackLu CTF 2014.

4.3.1 *Image Upload*

O problema *Image Upload* consistia num problema de segurança informática de *SQLInjection*. O enunciado do problema apresentava um espaço para fazer *Login*, caso fosse utilizador e um espaço para fazer *upload* de uma imagem desde que esta não excedesse um certo tamanho. Ao fazer *upload* a imagem enviada era representada numa moldura de estilo *Western* dizendo "*Wanted*". Abaixo da imagem haviam campos com características da imagem. Por tentativa e erro descobrimos que essas características poderiam ser alteradas e, consequentemente, forçar o programa a retornar um nome de utilizador e *password* que através do *Login* retornava a *flag*, ou seja, a sequência de caracteres que devia ser entregue para resolver problema.

A minha tarefa em específico era a de criar uma apresentação explicativa com alguns slides, demonstrando passo-a-passo o que tinha sido feito durante a competição. Assim, os meus colegas de equipa ficariam com conhecimentos para uma futura abordagem a problemas relacionados.

Esta, foi sem dúvida, umas das tarefas com mais dificuldade que encontrei devido à língua na qual tive de apresentar o problema. O facto de não estar confortável com o inglês complicou a minha apresentação, mas por outro lado ajudou-me a melhorar a vertente comunicativa e o próprio inglês.

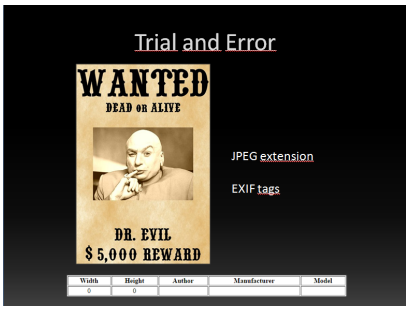

Figura 2. Slide da apresentação Image Upload

5 Conclusão

Findada toda a actividade que foi o Security Team at IST, pude tirar algumas elações. Entre elas e mais notável, é o facto desta matéria, a segurança informática, ser um assunto extremamente complicado e de difícil compreensão. São necessárias muitas horas de prática e reconhecimento de problemas para atingir bons níveis de competitividade. Outra elação que retirei da actividade foi a resposta a uma das razões para escolher a mesma. A questão que era colocada era a de querer, de alguma forma, que este tema fosse uma escolha para a minha carreira profissional, e a resposta à mesma é negativa. É uma actividade de estudo intensivo e contínuo, e não específico do engenheiro informático, mas sim de qualquer pessoa extremamente interessada no tema.

Agradecimentos

Queria começar por agradecer ao professor e coordenador da actividade Pedro Adão por tornar possível a criação da equipa e pelo tempo dispendido neste grupo de alunos. Quero também agradecer a todos os membros da Securtity Team at Técnico que estiveram presentes ao longo de todas as reuniões e competições durante todo o semestre. Em último, mas mais importante aos meus pais que tornam possível o facto de frequentar tão ilustre instituição como o Instituto Superior Técnico.