SecurityTeam@IST

Tiago Miguel Rodrigues Simões

Relatório de Aprendizagens

Resumo—Este relatório descreve a actividade realizada no âmbito da cadeia de Portfolio Pessoal III. Participar na SecurityTeam@IST foi a actividade à qual me candidatei e envolvi durante o semestre. No desenrolar da actividade foi incutido aos participantes a importância do trabalho em equipa e de um trabalho bem feito ao nível informático. O principal objectivo desta equipa foi participar em competições de segurança informática a nível internacional e meter o nome IST no topo das tabelas. Ao trabalhar com esta equipa foi possível aprender sobre cibersegurança como nunca imaginei. É de salientar que esta actividade ainda continua a decorrer, sem fim prévio.

Palavras Chave—STT IST competições segurança informática internacional

tote documento construdo a descica da ACTIVIDADE man esta a usar o MODERO ERRADO!

1 INTRODUÇÃO

Este documento narra a actividade desenvolvida que se enquadra na cadeira de Portfolio III. Aqui são relatados factos relativos à equipa de segurança informática a que pertenço.

O mesmo encontra-se dividido por pontos onde procuro abordar diferentes tópicos tais como: o que é a SecurityTeam@IST; o objectivo da equipa; o motivo pelo qual escolhi esta actividade; a constituição e a estruturação da equipa; as competições em que participámos; o treino para as competições.

Até ao momento, as actividades com a equipa foram realizadas, maioritariamente, nas instalações da Alameda do Instituto Superior Técnico ou em casa. Sem fim à vista, a equipa deve continuar a trabalhar até todos os membros se cansarem do tema.

2 STT

SecurityTeam@IST, também conhecida por STT, é uma equipa composta por alunos e professores do Instituto Superior Técnico (IST), dedicada à aprendizagem de conteúdos relacionados com a cibersegurança.

Tiago Miguel Rodrigues Simões, nr. 73100,
E-mail: tiagosimoes@ist.utl.pt, Instituto Superior Técnico,
Universidade de Lisboa.

Manuscrito entregue a 16 de Janeiro de 2015.

Visa explorar temas como a defesa e a exploração de vulnerabilidade associadas aos sistemas informáticos, tanto a grande escala como a pequena escala.

2.1 Criação

Durante o mês de Outubro do presente ano curricular, 2014/2015, o professor Pedro Adão sugeriu a alunos de Mestrado em Engenharia Informática (MEIC) e de Mestrado em Engenharia Eletrotécnica e de Computadores (MEEC), que fosse criada uma equipa de segurança informática.

Visto que existem várias iniciativas no IST, desde a HackerSchool (dedicada à electrotecnia) à SINFO (que se dedica à publicidade de empresas e dar a conhecer aos alunos personalidades importantes no mundo da Engenharia e não só), porque não criar uma actividade um pouco fora do normal? Assim nasceu a STT.

2.2 Organização

Desde cedo percebemos a melhor forma de atacar os problemas apresentados. Dividir a equipa por especialidades foi a solução concebida. Um conjunto de pessoas resolve problemas relacionados com *Reverse Engineering*, outro com *Web Applications*, entre outros conjuntos de possíveis problemas. Desta forma, os objectivos são cumpridos de uma forma mais rápida e eficiente.

(1.0) Excelent	LEARNING					DOCUMENT						
(0.8) Very Good			RI III CI		SCORE	Structure	Ortogr.	Gramm.	Format	Title	Filename	SCORE
(0.6) Good	x2	x1	x4	x1	OCCITE	x0.25	x0.25	x0,.25	x0.25	x0.5	x0.5	OUGHE
(0.4) Fair	2	1	4	n 0	19	025	(1)<	1175	\cap	13	$\lambda \leq$	155
(0.2) Weak	$\langle \rangle$	′	1	U- 0	7.0	<i>U. L</i>)	U. [<i>U, C J</i>		<i>V</i> .)	0.)	ار د ۱۰

Para que toda os elementos da STT aprendam um bocado de cada área são feitas reuniões de duas em duas semanas para discutir as soluções concebidas. Além das reuniões, utilizamos um grupo no Facebook e um fórum de modo a facilitar a troca de ideias e comunicações entre nós.

3 OBJECTIVOS

Em breves palavras, o nosso objectivo é: estar entre as melhores equipas de segurança informática.

A STT quer levar aos seus membros a melhor e a maior quantidade de informação disponível acerca da temática cibersegurança.

4 MOTIVAÇÃO PESSOAL

Desde que entrei no mundo virtual sempre questionei o que os hackers faziam e como, e o que se podia fazer para os combater. Esta actividade parecia responder às minhas questões, portanto decidi entrar. A STT permite aos alunos e professores do IST aprenderem mais sobre as questões de vulnerabilidades de sistemas de forma interactiva e divertida, sem nenhuma obrigação. Um ponto essencial que é importante referenciar, é que para entrar na STT não é necessário ser um amador ou profissional em segurança informática. Podemos entrar sem saber nada.

5 COMPETIÇÕES

Mal a STT começou as competições internacionais entraram no rumo. Com pouco conhecimento nesta área por grande parte dos membros, foi com enorme entusiasmo, e ao mesmo tempo receio, que decidimos participar na primeira competição que surgisses, e consoante o resultado, participar nas seguintes. O entusiasmo é grande quando se está a levar o nome da nossa faculdade ao mundo, e o receio de fazer má figura perante os outros está sem presente. De qualquer maneira, tínhamos de começar por alguma.

Até ao momento, estivemos presentes em três competições internacionais e nenhuma nacional. A primeira experiência foi com a *hack.lu CTF*, a segunda inscrição foi na *RuCTFE* e

última competição em que estivemos presentes foi na 31C3.

5.1 hack.lu CTF

A *hack.lu CTF* é um dos principais concursos de segurança electrónica do mundo. Por outras palavras, o nível dos problemas apresentados é de grau acrescido.

Com início às 9:00 GMT de 21 de Outubro e duração de 48 horas, a hack.lu CTF ganhou vida. Nesta competição existem desafios de várias categorias tais como Reverse Engineering, Web Applications e cryptography. Sendo o objectivo conseguir um ficheiro ou uma sequência de caracteres - a flag como prova que conseguimos chegar à solução final.

A metodologia da STT nas competições é começar por discutir quais seriam os problemas prioritários e as possíveis abordagens. De seguida, cada equipa (de acordo com a sua área de especialização) junta-se e começa a trabalhar. E com poucas horas de trabalho as primeiras soluções começaram a surgir. No final da competição o IST, representado pela STT, ficou colocado em 52 das 584 equipas participantes.

Foi um bom começo para uma equipa amadora! Como forma de reconhecimento, a Exame Informática realizou uma entrevista com o professor Pedro Adão acerca do envolvimento da STT nas competições e em especial na *hack.lu CTF*.

5.2 RuCTFE

A *RuCTFE* é uma competição internacional anual, sendo esta a quinta edição, e o objectivo é conseguir atacar os outros concorrentes de forma a ganhar controlo da máquina deles, e criar mecanismos para nos protegermos dos ataques das outras equipas. Esta competição começou as 10:00 UTC de 20 de Dezembro e durou 9 horas.

5.3 31C3

Às 20:00 GMT de 27 de Dezembro a 31C3 arrancou. Esta competição durou 48 horas. A 31C3 é uma prova de *Capture The Flag*, tal como a *hack.lu CTF*, ou seja, temos de conseguir um ficheiro que contém a desejada sequencia de

M. R. SIMÕES 3

caracteres.

Como esta competição, decorre durante o período de férias natalício/exames, cada membro da equipa trabalhou em casa, em vez da habitual reunião no IST. Por falta de motivação, ou por stress dos exames, não conseguimos boa classificação nesta prova. De qualquer forma, foi divertido participar.

6 **TREINO**

Para a preparação das competições, contamos com vários tutorias distribuídos gratuitamente pela Internet ou com o conhecimento de outros membros da equipa. Para além destes métodos, temos um forum online onde são publicadas soluções de antigas competições.

CONCLUSÃO

"Diz-me e eu esqueço-me, ensina-me e eu recordo, envolve-me e eu aprendo" - B. Franklin.

A STT permitiu-me vivenciar o mundo da cibersegurança por vários momentos, e é incrível o que aprendemos ao trabalhar em vez de ver só os outros a fazerem. Esta experiência certamente que me tornou um melhor cibercidadão, como futuramente, um melhor Engenheiro Informático. Com esta equipa foi possível aprender mais sobre mecanismos de ataque e defesa, tanto em rede como em circuitos fechados. Participámos em várias competições internacionais e tentámos levar o nome Instituto Superior Técnico além fronteiras. E demos o nosso melhor. Como resultado do nosso esforço conseguimos classificar-nos no lugar 52 numa competição bastante conhecida a nível mundial.

AGRADECIMENTOS

Quero agradecer ao professor Pedro Adão, sem ele a STT não tinha começado; aos meus colegas de equipa; e sem nunca esquecer ao IST, que forneceu meios para a realização de reuniões e competições.

Nest Tipo de documento (Techico) a Conclusar cert comecar com run Pesermo do anunto abardado e depois dere valar o resultado

Tiago Miguel Rodrigues Simões, aluno de 4º ano no IST a estudar Engenharia Informática na área de Sistemas Distribuídos e Engenharia de Software.