SecurityTeam@IST

Filipe Apolinário

Relatório de Actividades

Resumo—No presente relatório apresento todas as actividades que desempenhei na SecurityTeam@IST, divididas em duas secções, "Actividades na SecurityTeam@IST"e "Actividades autónomas".
Na SecurityTeam@IST tive a oportunidades de participar em várias competições de cibersegurança e reuniões do grupo. Nas reuniões de grupo discutimos o futuro do grupo e vários temas sobre cibersegurança e ataques informáticos. Foi numa das reuniões do grupo que apresentei o meu primeiro ataque informático, tendo discursado perante uma plateia de composta por alunos e professores. Para poder realizar as actividades na SecurityTeam@IST tive de fazer algum trabalho de investigação autónoma sobre a área de cibersegurança, tendo recorrido a alguns sites de hacking e outras ferramentas de aprendizagem presentes na internet.
Estou certo que após a leitura deste relatório, é perceptivel o que é a SecurityTeam@IST, a minha intenção ao juntar-me à SecurityTeam@IST e a utilidade das actividades que lá despenhei.

Palavras Chave—criptoanalise, segurança informática, SecurityTeam@IST, Capture the Flag, Jeopardy CtF,attack/defense CtF, HackLu CTF 2014, RuCTFE 2014, 311C3 CTF 2014

1 Introdução

A Criptoanálise, área que analisa um sistema de informação de maneira a recolher informação escondida no sistema, levanta inúmeras questões e desafios a nível de segurança para qualquer Engenheiro Informático, e em particular a todos os peritos na área da Segurança Informática.
É com a preocupação de aprender a detectar e corrigir possíveis vulnerabilidades nos sistemas de informação que decidi juntar-me ao grupo SecurityTeam@IST.

2 SecurityTeam@IST

A SecurityTeam@IST é constituído por um grupo de alunos e professores do Instituto Superior Técnico, orientado pelo professor Pedro Adão, que iniciou actividade no dia 13 de Outubro de 2014 e que tem como principal interesse a participação em competições de cibersegurança, na esperança que cada membro aprenda a analisar Sistemas de Informação, de maneira a identificar vulnerabilidades e por conseguinte consiga corrigir os problemas detectados.
Durante o período de actividade, o grupo reuniu-se 4 vezes e participou em 3 competições de cibersegurança. Actualmente, o grupo encontra-se numa pausa de actividade iniciada 29/12/2014 e tenciona recomeçar actividade no próximo mês de Fevereiro. Todas as actividades do grupo serão devidamente explicadas nas próximas subsecções.

• *Filipe Apolinário, nr. 70571,*
E-mail: f.apolinario30@gmail.com
Instituto Superior Técnico, Universidade de Lisboa.

Janeiro 17, 2015.

2.1 Reunioes SecurityTeam@IST

As reuniões ocorreram duas vezes por mês na sala FA1, tiveram a duração de 2 horas, sendo habitual a primeira hora estar dedicada a assuntos do foro de organização do grupo e a segunda hora dedicada a apresentação e discussão de ataques informáticos por parte de membros do grupo.

2.1.1 Organizaçao e Calendarizaçao de Actividades de Grupo

Na primeira hora da reunião os membros do grupo mediados pelo professor Pedro Adão, habitualmente sugeriam e discutiam não só

(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	1.6	0.7	3.2	0.6	6.1	0.25	0.15	0.2	0.25	0.5	0.5	1.85
(0.2) Weak												

ideias para melhorar o funcionamento do grupo, mas também competições e actividades em que o grupo deveria participar.
Ao longo das reuniões foi definido vários planos, sendo relevante destacar as seguintes ideias:

1) Grupo no Facebook onde cada membro publica e comenta assuntos sobre cibersegurança e outros assuntos relacionados com a SecurityTeam@IST, e.g. marcação de reuniões. Os assuntos discutidos no grupo do Facebook, são discutidos de uma forma leve, sendo formalizado caso necessário nas seguintes reuniões.
2) Grupo no Discourse onde organizamos/discutimos competições em que participámos ou planeamos participar e onde também cultivamos um espaço de entreajuda na aprendizagem de cada membro.
3) Grupo no Trello onde são delegadas as tarefas respectivas a cada membro.
4) Calendário semestral de competições cibersegurança no final das várias reuniões onde obtivemos a seguinte calendarização de participações:
    a) HackLu 2014 no dia 21 de Outubro 2014 às 8h até ao dia 23 de Outubro de 2014 às 8h, Pavilhão Informática II.
    b) RuCtF 2014 no dia 20 de Dezembro 2014 das 10h até às 19h, Pavilhão Informática II.
    c) 31C3 CtF 2014 no dia 27 de Dezembro 2014 às 20h até ao dia 29 de Dezembro de 2014 às 20h, remotamente.

2.1.2 Apresentacao e Discussao de Ataques Informaticos

Na segunda hora das reuniões, membros voluntários do grupo, habitualmente mostravam diversos ataques informático, como ataques a servidores usando vulnerabilidades de PHP* ou bases de dados SQL, quebra de protocolos de segurança usando criptoanálise de chaves simétricas, entre outros. Depois da apresentação do ataque, era também habitual haver uma discussão de como foi executado o ataque e que soluções alternativas poderíamos realizar para obter o mesmo ataque ou semelhante.

2.2 Competicoes de ciberseguranca

Conforme introduzido no inicio da secção 2, o grupo participou em três competições de cibersegurança do estilo Capture the Flag*, a HackLu CTF 2014, a 31C3 CTF e a RuCtF. Nas próximas subsecções será explicado como funcionaram e o resultado que o grupo obteve na competição.

2.2.1 HackLu CTF 2014

A HackLu CTF 2014 foi a primeira competição que participamos e na qual obtivemos o melhor resultado até hoje, ranking 52 de 354 equipas. Esta competição durou 48 horas e funcionou sobre o estilo Jeopardy* contemplando desafios de criptografia, reverse engeneering e Web hacking, tendo sido resolvidos 10 desafios dos 34 apresentados.

2.2.2 RuCTFE 2014

A RuCTFE foi uma Capture the Flag* do estilo Attack/Defense* e foi a primeira e ultima competição deste formato que participamos.
A competição teve uma duração de 9 horas e cada equipa estava encarregada da protecção do seu servidor, onde cada elemento do grupo estava ligado remotamente. Para além da protecção do servidor, cada equipa tinha de atacar os servidores das restantes equipas, de maneira a identificar e roubar as flags presentes nos outros servidores.
Ao contrário das outras competições, em que o grupo conseguiu algumas flags, na RUCTFE o grupo não conseguiu obter nenhuma flag, terminando assim no ranking 115 de 133 participantes. Este resultado deveu-se a um problema na ligação do servidor da equipa da SecurityTeam@IST com os computadores pessoais dos membros da equipa, impossibilitando o acesso remoto ao servidor e levando-nos a perder muitas horas à volta deste problema e à nossa desistência.

2.2.3 31C3 CTF 2014

A prova 31C3 CTF foi muito semelhante à primeira competição. É uma prova Capture the Flag com o estilo Jeopardy com a duração de 48 horas.
Apesar das semelhanças com a HackLuCTF, a SecurityTeam@IST só conseguiu a captura de uma flag, tal deve-se ao facto da prova não ter tido grande adesão dos membros da SecurityTeam@IST e ter sido realizada remotamente, por se realizar na altura de férias de Natal.

3 Actividades realizadas SecurityTeam@IST

Neste semestre, participei em diversas actividades na SecurityTeam@IST sendo essas actividades divididas em dois tipos actividades, as de grupo e as autónomas.

3.1 Actividades na SecurityTeam@IST

As actividade na SecurityTeam@IST iniciaram-se no dia 13 de Outubro após a primeira reunião do grupo. Na reunião decidimos que era importante para a SecurityTeam@IST que criasse-mos uma conta no Trello de maneira a dividir e delegar tarefas por cada membro, conforme explicado na secção. Mediante essa decisão, a minha actividade inicial foi moderar a conta do Trello e tratar da inscrição/ligação dos membros do grupo com a conta da SecurityTeam@IST.
Para alem de mediar o Trello, participei nas três competições CtF enunciadas na secção e apresentei um ataque de Server Side Include usando vulnerabilidade do PHP na 4ª reunião da SecurityTeam@IST.

3.2 Actividades autónomas

As actividades autónomas começaram dias depois de entrar no grupo e tiveram como principal objectivo aprender e adquirir as ferramentas necessárias para poder executar a minha apresentação e participar nas competições da CtF. Foi com esse objectivo em mente que me inscrevi-me e participei em diversos desafios dos sites http://www.enigmagroup.org/, onde actualmente ocupo no ranking o 1117 de 8000 inscritos, e no http://www.hackthissite.com, onde arranjei o desafio que apresentei na SecurityTeam@IST.

4 Conclusão

Analisando a minha participação nas actividades da SecurityTeam@IST e o conhecimento que adquiri nessas actividades posso concluir que a afiliação à SecurityTeam@IST me ajudou a perceber as diversas ameaças que um Sistema de Informação pode ser alvo e as possíveis soluções para o sistema manter o seu funcionamento normal quando confrontado com essas ameaças. Estou assim convicto que esta experiência se revelará uma grande mais valia no meu curriculum e no futuro profissional.

Agradecimentos

Gostaria de aproveitar esta secção para deixar um cumprimento a todos os meus colegas da SecurityTeam@IST e em especial ao professor Pedro Adão que promoveu, criou e participou no grupo.
Gostaria também de aproveitar esta secção para agradecer e deixar um voto de solidariedade ao website http://www.enigmagroup.org/, ao qual devo grande parte do conhecimento necessário para as competições e que apesar de várias dificuldades monetárias, tem conseguido manter-se online graças às doações dos membros do site.

Neste tipo de documento (Técnico) a Conclusão deve começar com um Resumo do assunto abordado e depois deve realçar o resultado