Security Team@IST

Francisco Duarte

Relatório de Actividades

Resumo—Durante a participação na equipa de Segurança Informática participei em reuniões e competições, nas quais o objectivo final era explorar vulnerabilidades de sistemas, quer na perspectiva de ataque como de defesa. Participámos em duas competições, a Hack.lu da categoria Jeopardy e a RuCTFE da categoria ataque/defesa, durante as quais tentámos solucionar um conjunto de problemas e no final partilhámos as estratégias e caminhos seguidos pelos diferentes membros dos grupos. As reuniões serviram principalmente para partilhar ideias e definir estratégias a aplicar durante as competições. A participação nesta actividade foi muito positiva uma vez que me forneceu uma série de ferramentas tanto a nível teórico como em situações práticas que podem ser úteis a um nível multidisciplinar(organização de trabalho, comunicação entre os membros do grupo).

Palavras Chave—Capture the Flag, Hack.lu, RuCTFE, Cyber Segurança, LaTeX, paper.

1 Introdução

No decorrer da cadeira de Portfolio Pessoal III (PPIII) ingressei na equipa de cyber segurança do Instituto Superior Técnico (IST), Security Team@IST. O objectivo do grupo era participar em competições Capture the Flag (CTF) fazendo com que os seus membros aprendam a explorar vulnerabilidades de sistemas, ganhando assim conhecimentos sobre alguns princípios de cyber segurança. A privacidade e a integridade da informação sensível de cada individuo ou entidade é uma área da informática que tem ganho cada vez mais importância e visibilidade. Este tipo de actividades incentiva os participantes a trabalhar em equipa para resolver problemas de forma criativa e colaborativa,é também uma forma eficaz de atrair pessoas para a área e ajudá-las a ganhar alguma experiência que pode ser útil no futuro. Os membros foram encorajados a procurar estes conhecimentos de forma pro-activa e independente, apesar de existirem reuniões bi-mensais cujo objectivo era transmitir informação e partilhar experiência sobre o tema.

2 Competições

As competições mencionadas, CTF, são uma forma de colocar em prática os conhecimentos adquiridos sobre Segurança informática e também de aprofundar conhecimentos sobre o tema. As CTF podem ser de dois tipos, Jeopardy ou ataque/defesa. Em ambos os casos o grupo divide-se em equipas mais pequenas e tentam encontrar soluções para os problemas propostos. Participámos em duas competições, a Hack.lu e RuCTFE, a primeira dentro da categoria Jeopardy e a segunda ataque/defesa. [1]

2.1 Hack.lu

Hack.lu é uma competição anual da categoria Jeopardy. Nesta categoria são dados aos concorrentes um conjunto de problemas. Estes problemas consistem em programas, serviços, acesso a máquinas remotas ou *websites* e cada um deles tem oculta uma *string* denominada *Flag*. Esta *Flag* deve ser submetida de forma a ganhar pontos para a equipa. [2] A equipa juntou-se antes do início da competição para definir a estratégia que ia utilizar. Os elementos foram divididos por equipas e a cada equipa

• *Francisco Duarte, nr. 73838,*
E-mail: franciscodua@gmail.com,
Instituto Superior Técnico, Universidade de Lisboa.

Manuscript received January 17, 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	2	1	4	0.8	7.8	0.2	0.25	0.25	0.2	0.5	0.5	1.9
(0.2) Weak												

foi atribuída uma categoria, e.g. *Reverse Engineering*, *Web*...Depois de distribuídos pelas equipas começámos a analisar os problemas. Encontrava-me na equipa cuja categoria era *Reverse Engineering*. Analisámos os problemas por ordem de dificuldade, do mais fácil para o mais difícil. Associámos a dificuldade dos problemas aos pontos que eram atribuídos pela sua resolução. Para podermos avançar na resolução dos problemas cada elemento tentava diferentes estratégias, falavam com os colegas sobre o que já tinham tentado e registavam num documento partilhado para que todos tivessem conhecimento do que tinha sido feito, para melhorar a eficiência de esforços. No final da competição todos os elementos ou grupos que chegaram à solução de problemas registaram, num documento partilhado com toda a equipa, os passos que levaram à descoberta da solução e todos os caminhos que não resultaram. Desta forma toda a equipa pode aprender novas técnicas e ver quais as soluções para os problemas que não conseguiram resolver ou até mesmo de problemas que, apesar de não terem tentado resolver quisessem saber a sua solução. Estas soluções eram mais tarde apresentadas nas reuniões de equipa.

2.2 RuCTFE

Esta competição é do tipo ataque/defesa. Neste tipo de competições cada equipa tem de ter um conjunto de serviços disponíveis para os concorrentes. Estes serviços têm vulnerabilidades e um conjunto de *Flags*. O objectivo da competição é tentar manter os serviços disponíveis (uma equipa ganha pontos se o serviço estiver disponível), proteger os serviços corrigindo as suas vulnerabilidades para que os concorrentes não possam ter acesso às *Flags* associadas a esse serviço e para que não fique indisponível. Também devem ser criadas formas de explorar as vulnerabilidades encontradas para conseguir capturar as *Flags* das outras equipas ou indisponibilizar os seus serviços. [3] A estratégia empregue era simples, inicialmente tentámos colocar os serviços disponíveis. De seguida dividimos os elementos por serviço e cada grupo tentou analisar as vulnerabilidades do serviço que lhe foi atribuído. Como equipa fomos trocando ideias e métodos sobre como encontrar as vulnerabilidades dos serviços e como os resolver. Infelizmente, não fomos capazes de encontrar forma de proteger os nossos serviços ou atacar o dos concorrentes. Adicionalmente deparámo-nos com uns problemas relacionados com a topologia da rede que usámos para montar os serviços. Tentar resolver estes problemas consumiu grande parte do tempo da competição. Idealmente teríamos identificado as vulnerabilidades dos serviços e teríamos dividido o grupo em dois subgrupos, um ficaria responsável por proteger o nosso serviço e o outro dedicar-se-ia a criar um ataque aos serviços das outras equipas.

3 Reuniões

Duas vezes por mês eram marcadas reuniões para que toda a equipa se juntasse e pudesse discutir a participação em competições, alterações que podiam ser feitas, e como podíamos organizar melhor os membros da equipa durante as competições. Nestas reuniões muitas vezes eram também feitas demonstrações, por parte dos elementos do grupo, de problemas resolvidos, pelos próprios ou mesmo por outras pessoas que disponibilizaram o seu processo para chegar à solução de um problema. Ou seja, para um determinado problema era apresentada a sua solução e todo o processo que levou à sua descoberta. Desta forma havia uma melhor distribuição da carga de trabalho, fazendo com que diferentes elementos se pudessem dedicar a diferentes problemas e durante a apresentação todos podiam ver a solução para todos os problema. Estas apresentações de soluções eram feitas numa sala, para toda a equipa e geralmente terminavam com uma demonstração prática do problema, ou seja, o desafio era resolvido na altura. No final da apresentação havia uma discussão sobre as técnicas usadas, possíveis alternativas e eventualmente esclarecimento de quaisquer dúvidas que possam ter surgido.

4 Conclusão

Fazer parte desta equipa foi uma experiência muito interessante que me permitiu não só

aprender muito sobre uma área tão interessante como segurança informática, como trabalhar em conjunto com outras pessoas para atingirmos um objectivo comum. Penso que grande parte dos elementos desta equipa não tinham experiência nesta área quando começámos, no entanto em conjunto conseguimos aprender bastante e até atingir uma óptima classificação na competição Hack.lu, 52º lugar. Apesar de terem havido uns pequenos problemas, mais concretamente na competição RuCTFE, esta actividade irá certamente ter um impacto positivo no meu futuro, quando for necessário trabalhar com colegas, organizar equipas, partilhar métodos e explorar temas por conta própria. Os métodos usados para organizar o grupo provaram ser bastante úteis no decorrer tanto das reuniões como das competições, pois permitiu uma partilha de conhecimento e experiências de forma eficaz, bem como de fomentar um espírito de entreajuda.

Neste tipo de documento (Técnico) a Conclusão deve começar com um Resumo do assunto abordado e depois deve valer os resultados

AGRADECIMENTOS

Gostaria de agradecer ao Professor Pedro Adão por ter tido a ideia de criar esta equipa com uma premissa tão interessante e cativante como esta e a todos os elementos da equipa que se esforçaram para atingirmos os resultados que atingimos.

REFERÊNCIAS

[1] "CTFtime.org all about ctf (capture the flag)," https://ctftime.org/ctf-wtf/, accessed: 2014-12-29.
[2] "Capturetheflag - hack.lu 2014," http://2014.hack.lu/index.php/CaptureTheFlag, accessed: 2015-01-02.
[3] "Ructfe 2014 ¿ index," http://ructf.org/e/2014/, accessed: 2015-01-02.

Francisco Duarte Estudante no IST. Actualmente durante o primeiro ano de mestrado na área de Sistemas Distribuidos e Sistemas Inteligentes.