Security Team Técnico

António Lopes

Relatório de Actividades

Resumo—A actividade na qual participei consistiu, resumidamente, na minha integração na **STT!** (**STT!**). Objectivamente, consistiu numa série de reuniões informais entre os membros da Security Team, e o responsável da mesma Professor Pedro Adão, e na participação numa competição de segurança de ataque-defesa, RuCTFE [1].

Palavras Chave—STT, Segurança, Security Team, RuCTFE.

1 Introdução

Como aluno do mestrado em Engenharia Informática e Computadores no Instituto Superior Técnico, tenho a minha área de formação científica principal que são, respectivamente, sistemas inteligentes e robótica.

Contudo, a actividade em que participei está inerentemente ligada a uma área de redes e segurança. A escolha e participação nesta actividade teve como motivação o facto de, por um lado, no meu ponto de vista todos os engenheiros informáticos devem ter alguma formação em segurança (sendo que redes e sistemas distribuídos e, por conseguinte, segurança fazem parte da formação básica do curso de engenharia informática, devendo ser mais aprofundado), por outro, a minha vontade de aprender e desenvolver competências fora da minha área de conforto, competências essas que não são um pressuposto em alguém da minha área e que complemeta a minha formação como um dia profissional e como pessoa.

A participação na actividade implicou a presença em reuniões informais e a participação numa competição internacional de segurança.

• *António Lopes, nr. 73721,*
E-mail: antoniovilarinholopes@tecnico.ulisboa.pt,
Instituto Superior Técnico, Universidade de Lisboa.

Manuscript received Month Day, 2015.

PORQUE MOTIVO ESTÁ EM INGLÊS?

2 Actividade

A actividade na qual participei consistiu em uma série de reuniões, as quais não pude presenciar todas devido a existir um conflito com o meu horário de aulas, e na participação numa competição internacional de "capture the flag".

2.1 Reuniões

De maneira a reunir todos os membros da Security Team, ou a maior parte dos membros, para discutir não só as competições nas quais a maior parte dos membros chegando a um consenso decide participar, como também discutir problemas relacionados com vulnerabilidades de segurança.

Neste sentido, nas reuniões alguns dos elementos que pertencem à **STT!** apresentam problemas relacionados com o tema assim como a sua solução e que permite que os membros possam, por um lado, aprender novas ferramentas para resolver os problemas, por outro, a interagir com os outros membros e adquirir competências pessoais que devem ser transversais a qualquer engenheiro, competências conversacionais. De referir ainda que nas mesmas reuniões, o professor Pedro Adão apresenta também problemas semelhantes aos já referidos.

2.2 Participação na competição RuCTFE

A participação na competição RuCTE foi o ponto máximo da minha participação na actividade, aqui foi necessário não só comunicar

(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	0.6	3.2	0.4	5.8	0.2	0.2	0.2	0.2	0.4	0.5	1.7
(0.2) Weak												

com os colegas que também participaram na competição como também tentar resolver os problemas que nos foram apresentados.

A competição RuCTFE é uma competição internacional russa que decorreu pelo quinto ano, com patrocínios de empresas como o GitHub, e que consiste em, como já referido, "capture the flag".

O que é um desafio de **CTF!** (**CTF!**)? Este tipo de desafios consiste em atribuir a cada equipa participante uma série de serviços com vulnerabilidades, no caso desta competição foram cerca de 6 serviços, que têm que estar em permanente comunicação com o servidor da organização para que os organizadores possam, por um lado, regularmente aceder aos nossos serviços para colocarem lá informação privadas (as "flags"), e, por outro, para que possam verificar que os serviços estão a funcionar e que as outras equipas podem explorar as vulnerabilidades dos nossos serviços, ter os serviços funcionais permite ter maior pontuação visto que a pontuação é dada por, para além de capturar as "flags" das outras equipas, uma fórmula que tem em conta o tempo que o serviço que disponibilizamos está a funcionar e acessível. Neste sentido, o objectivo que cada equipa tem é encontrar as vulnerabilidades existentes nos diversos serviços e tentar, num lado, explorar as vulnerabilidades das outras equipas e, noutro lado, reparar essas mesmas vulnerabilidades nos nossos serviços para que não consigam capturar as nossas "flags", sendo por isso chamada uma competição de ataque-defesa. Assim, apesar de ser permitido fazer tudo há também restrições e regras, não podendo, por exemplo, escutar o tráfego das outras equipas, atacar o servidor dos organizadores, atacar equipas fora da **VPN!** (**VPN!**), etc.

Para poder participar na competição foi necessário montar os serviços e a rede como ilustrado na figura 1 e os serviços na figura 2.

Antes de poder participar na competição foi necessário montar a rede como ilustrado na figura 1, para estarmos ligados ao servidor do jogo e para não ser possível aceder à rede interna do Instituto Superior Técnico, local onde se participou na competição. Contudo, como será discutido em 2.3, houve problemas técnicos. Os serviços disponibilizados ilustrados na figura 2 consistiam em múltiplas "virtual box"ligadas à nossa **VPN!** que por sua vez estavam em rede com o servidor de jogo. Dos serviços existentes, um era um serviço no sistema operativo msdos, um minix e os restantes em android.

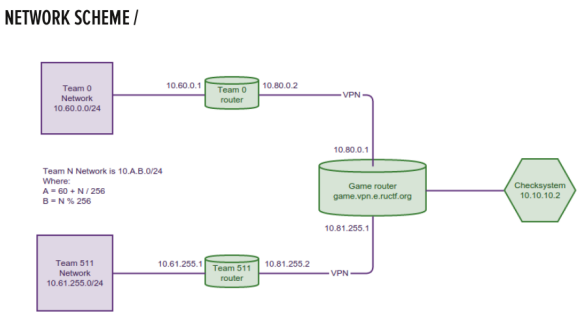


Figura 1. Rede da competição

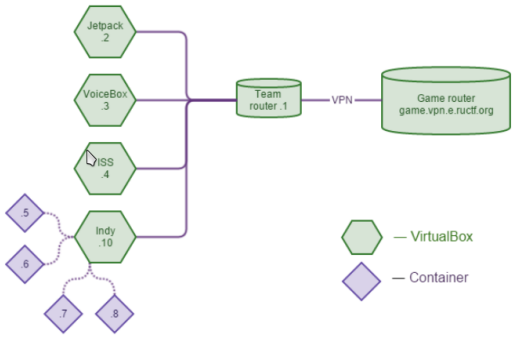


Figura 2. Serviços disponibilizados

Como houve alguns problemas técnicos, a competição não correu tão bem como esperado e ninguém da equipa conseguiu capturar uma "flag". Contudo, foi possível constatar quais as vulnerabilidades que os serviços tinham, pelo menos na maioria. Por fim, esta competição decorreu no dia 20 de Dezembro e teve a duração de cerca de 10 horas.

2.3 Condicionantes

As condicionantes vividas nesta actividade foram não ter podido assistir a todas as reuniões devido a conflito com o meu horário de aulas, ainda não ter o "know how" necessário para

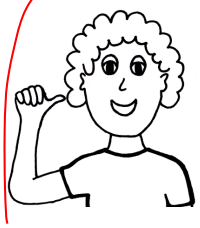
alguns dos problemas e os problemas técnicos que foram encontrados na participação na competição. Aqui, os problemas foram devido à rede que foi montada não estar protegida de ataques exteriores pois houve dificuldades em esconder a rede interna do técnico pelo que os serviços que disponíveis não estiveram tempo suficiente funcionais nem foi possível explorar as vulnerabilidades das outras equipas. Contudo, foi possível na mesma explorar as vulnerabilidades que existiam nos diversos serviços num esforço conjunto com os colegas que também participaram na competição.

AGRADECIMENTOS

Professor Pedro Adão e colegas da **STT!**.

REFERÊNCIAS

[1] RuCTFE, "RuCTFE 2014," http://ructf.org/e/2014/index.html.



António Lopes Aluno de mestrado do **IST!** (**IST!**) nas áreas de Sistemas Inteligentes e Robótica.