SecurityTeam@IST

Jorge Simão Madeira Cordeiro de Aragão Goulart

Relatório de Aprendizagens

Resumo—Durante a realização da actividade, sendo esta uma actividade com o objectivo principal de aprender (e partilhar) sobre vários assuntos de cybersecurity, tive a oportunidade de aprender não só sobre vários ataques a sistemas informáticos, como os realizar, e que ferramentas existem para realizar ou ajudar a realizar estes ataques, mas também sobre que problemas tomar em consideração quando a segurança de um sistema é crítica, e como proteger estes sistemas destes ataques.
Para além disso, esta actividade também me permitiu aprender e desenvolver várias habilidades não técnicas. Como esta actividade requer a realização de problemas individualmente (ou, pelo menos, fora do contexto das reuniões e concursos) para possibilitar a partilha de conhecimento, habilidades como a realização de investigação individual, raciocínio lógico, capacidades de escrita e de apresentação oral são desenvolvidas. Durante os concursos, outro conjunto de habilidades não técnicas também foram desenvolvidas, como a capacidade de tomar decisões em ambientes desconhecidos, a capacidade de resolver problemas em situações com limites no tempo e nas ferramentas disponíveis, e a capacidade de aplicar o conhecimento técnico adquirido anteriormente.

Palavras Chave—Cybersecurity, Vulnerabilidade, SQL Injection, Capture The Flag (CTF), Attack-Defense, RuCTFE, LaTeX, paper.

O documento está algo limitado no que diz respeito à descrição das competências transversais adquiridas ou melhoradas, falando-se muito no aspeto TÉCNICO

1 Introdução

A SecurityTeam@IST é um grupo que depende, principalmente, da contribuição dos seus membros para a partilha de conhecimento. Isto requer que cada membro efectue trabalho individual (na forma de realização de problemas) para depois ser apresentado durante as reuniões, e ser aplicado durante a resolução de outros problemas, ou durante um concurso. Assim é garantido o crescimento do grupo, e da base de conhecimento do grupo.

2 Conhecimentos Técnicos

2.1 Reuniões

É durante as reuniões de grupo que são partilhados os conhecimentos adquiridos pelos membros durante a sua realização dos exercícios. Nestas reuniões, os problemas são introduzidos, e os métodos para os resolver são explicados.

Isto serve como base para adquirir conhecimentos técnicos no que toca a cybersecurity.

Em particular, durante as reuniões que estive presente, pude aprender técnicas de reverse engineering (como, por exemplo, disassembling), de quebra de protocolos de comunicação, de buffer overflow, entre outros.

Para complementar estas técnicas, aprendi sobre diversas ferramentas disponíveis que podem ser usadas para realizar ou facilitar estes ataques, e o seu funcionamento.

Como cada uma destas soluções provêm de uma vulnerabilidade no sistema, aprender sobre como explora-las também nos ensina não só qual é o ponto fraco do sistema, mas também como poderia ser resolvido ou evitado.

2.2 Exercícios

Fora do contexto das reuniões, os membros são incentivados a investigar sobre o assunto, e a resolver exercícios de cybersecurity. Estes exercícios, em particular, permitem-nos não só colocar em prática os conhecimentos técnicos

• *Jorge Simão Madeira Cordeiro de Aragão Goulart, nr. 73882, E-mail: jorge.aragao.goulart@tecnico.ulisboa.pt, Instituto Superior Técnico, Universidade de Lisboa.*

Manuscript received January 17, 2015.

PORQUE MOTIVO ESTÁ EM INGLÊS?

(1.0) Excelent	LEARNING					DOCUMENT						
(0.8) Very Good	CONTEXT x2	SKILLS x1	REFLECT 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	1.2	0.6	2.4	5.1	4.0	0.2	0.2	0.25	0.2	0.5	0.5	1.85
(0.2) Weak												

já adquiridos anteriormente, como também nos permite explorar outras áreas nos quais não temos um conhecimento tão profundo, e assim complementá-lo.

Por exemplo, enquanto eu efectuei resolução de exercícios no meu tempo livre, pude aprofundar os meus conhecimentos no que toca à realização de SQL Injections, e como não proteger contra este ataque põe em perigo dados sensíveis.

2.3 RuCTFE 2014

Tal como os exercícios, os concursos são uma maneira de adquirir conhecimentos técnicos referentes a cybersecurity. Visto que, durante a participação nestes concursos, temos não só de aplicar os conhecimentos, em muitos dos casos somos colocados em situações onde temos de investigar e descobrir como encontrar e explorar as vulnerabilidades presentes nos sistemas.

Em particular, durante a minha participação na RuCTFE 2014, tive a oportunidade de aprender mais sobre desenvolvimento de aplicações em ambientes MSDOS e Android, pois foi nos dois sistemas que usavam estes sistemas operativos que me concentrei. Isto inclui, por exemplo, aprender sobre ferramentas de debug presentes em MSDOS, como obter o código fonte de uma aplicação Android, e a estrutura de uma aplicação Android.

3 Conhecimentos Não Técnicos

3.1 Exercícios

Sendo os exercícios resolvidos fora das reuniões, estes permitem desenvolver conhecimentos não técnicos no que toca ao trabalho individual.

Durante a minha resolução de exercícios, tive de desenvolver a minha capacidade de investigação individual (para conseguir aprender sobre as vulnerabilidades, e como estas podem ser exploradas) e raciocínio lógico (durante o estudo dos problemas, de modo a perceber o seu funcionamento, e como aplicar o ataque de modo a explorar possíveis vulnerabilidades).

3.2 Apresentação

Tendo tido a oportunidade de realizar uma apresentação oral sobre um dos exercícios que resolvi ao grupo, pude treinar a minha capacidade de comunicação perante um público.

A minha capacidade de escrita, de resumo e de transmissão de ideias foi também desenvolvida durante o desenvolvimento do documento para introdução a SQL Injections.

3.3 RuCTFE 2014

Durante o concurso, para além de desenvolver a nossa capacidade de aplicar o conhecimento adquirido, também tivemos de puxar pelo nosso engenho, capacidade de investigação e de partilha de ideias, devido à nossa falta de recursos e pouca experiência.

Mas também porque o concurso tem um tempo limitado, tivemos de fazer uma gestão desse tempo, e dividir as tarefas no tempo e nas pessoas presentes. Tomar decisões sobre como e onde aplicar as nossas capacidades também se tornaram importantes durante a realização deste concurso.

4 Conclusão

Graças a esta actividade, foi-me possível não só aprofundar os conhecimentos técnicos adquiridos nas aulas de Segurança Informática em Redes e Sistemas (SIRS), como também colocar estes conhecimentos em prática durante a realização de exercícios e no concurso.

No que toca aos conhecimentos técnicos, esta actividade permitiu-nos explorar várias áreas dentro de cybersecurity, numa vertente mais prática que durante as aulas de SIRS. Isto ajuda a ganhar uma maior noção das consequências de um ataque, e como este é realizado, ajudado-nos assim a desenvolver alicações e sistemas mais seguros no futuro.

Esta actividade também ajuda a reforçar certos conhecimentos não técnicos que não seriam desenvolvidos. Em particular, os concursos oferecem um ambiente muito diferente do que é costume durante as actividades curriculares, e portante desenvolvem um conjunto diferente de capacidades.

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