SecurityTeam@IST

Jorge Simão Madeira Cordeiro de Aragão Goulart

Relatório de Actividades

Resumo—Durante o decorrer desta actividade, estive presente nas reuniões que se efectuaram, participando de maneira activa nestas reuniões. Fora destas, também efectuei exercícios de cybersecurity e exploração de vulnerabilidades em sites como EnigmaGroup.org e HackThisSite.org, não só como forma de praticar e aprender mais sobre o assunto, como para poder efectuar uma apresentação durante as reuniões, de maneira a contribuir com a partilha de conhecimento, objectivo central nesta actividade.
Na reunião de 17 de Dezembro, apresentei a solução a um dos exercícios que resolvi, sobre SQL Injection. Também desenvolvi para grupo um documento que explica os básicos de SQL Injection.
Finalmente, dia 20 de Dezembro, participei com o grupo na RuCTFE, um concurso anual Capture The Flag (CTF) do género Attack-Defense. Devido a problemas de rede e de configuração com o nosso setup, encontrados durante o concurso, a nossa participação neste, como grupo, deixou a desejar, contudo, conseguimos com sucesso estudar os programas provenientes do concurso e descobrir algumas vulnerabilidades.

Palavras Chave—Cybersecurity, Vulnerabilidade, SQL Injection, CTF, Attack-Defense, RuCTFE, LaTeX, paper.

1 Introdução

A SecurityTeam@IST é um grupo dedicado à aprendizagem de assuntos relacionados com cybersecurity, nomeadamente, a explorar e a tirar partido de vulnerabilidades em sistemas informáticos. Para isso, os membros do grupo devem resolver problemas/exercícios de segurança informática para, nas reuniões de grupo, apresentar estes problemas e os métodos usados para o resolver, para assim partilhar os conhecimentos adquiridos.

Devido ao facto destes métodos não poderem ser usados em sistemas reais, os membros da SecurityTeam@IST devem assinar um Compromisso Ético e todos os problemas resolvidos devem ser de uma entidade que os forneça num contexto seguro e controlado. Alguns sitès, como EnigmaGroup.org e HackThisSite.org, fornecem simulações de ambientes com sistemas vulneráveis.

Finalmente, como forma de aplicar os conhecimentos adquiridos durante as reuniões, e continuar a desenvolve-los, o grupo participa em competições CTF. Nestas competições, a entidade reguladora do concurso disponibiliza às equipas participantes sistemas com vulnerabilidades, com o objectivo de serem exploradas e assim descobrir a flag (normalmente, um conjunto de caracteres). Quanto maior o número de flags encontradas por uma equipa, melhor a pontuação obtida por esta. Dependendo do concurso, pode haver algumas diferenças nas regras. Duas das variantes existentes denominam-se Jeopardy e Attack-Defense.

2 Reuniões de Grupo

As reuniões de grupo realizam-se, regra geral, a cada duas semanas (embora o dia e a hora em específico seja decidido conforme as disponibilidades dos membros do grupo). Embora só tenha sido aceite no grupo no dia 11 de Novembro de 2014, eu pude estar presente nas seguintes reuniões:

- 03 de Novembro, às 17h
- 17 de Novembro, às 17h
- 17 de Dezembro, às 17h15

Para a primeira reunião, embora ainda não fizesse parte do grupo, eu obtive permissão do

• *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	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	0.8	3.6	0.8	7.2	0.2	0.2	0.25	0.2	0.5	0.5	1.85
(0.2) Weak												

professor Pedro Adão para assistir.

Não houve nenhuma reunião na semana de 1 a 5 de Dezembro pois os membros do grupo não se encontravam disponíveis para comparecer, devido ao grande número de entregas para essa semana.

Durante estas reuniões, foram apresentados vários exercícios, resolvidos por vários membros do grupo, de diferentes áreas de segurança. Também foram discutidos vários assuntos referentes ao grupo em si, como divisão de tarefas para disponibilizar ao grupo os recursos necessários para a realização de actividades. Em particular, durante a última reunião, foi ainda lançado ao grupo um desafio, com o objectivo de obter um ficheiro que se encontra no Ambiente de Trabalho de um utilizador num servidor a correr Windows XP SP2.

Embora a minha contribuição nas primeiras reuniões fosse limitada, por inexperiência nesta matéria, tentei sempre contribuir com sugestões e perguntas. Durante a última reunião, no entanto, apresentei um dos exercícios por mim resolvidos sobre SQL Injection (verificar Secções 2.1 e 2.2).

2.1 Exercícios

Fora das reuniões tentei resolver problemas, tendo como objectivo expandir o meu conhecimento, ganhar alguma prática, poder contribuir para a partilha de conhecimento e para possibilitar a apresentação de alguns exercícios.

Devido ao facto que não tive acesso à pasta partilhada do grupo durante as primeiras semanas, não tinha acesso aos problemas (resolvidos e por resolver) que o grupo se concentrava (vindos de concursos anteriores). Para não permanecer parado, tomei a sugestão de um colega, e juntos abordamos problemas presentes no site EnigmaGroup.org.

No entanto, antes que pudéssemos resolver um problema que nos permitisse apresentar numa reunião, o site ficou indisponível durante alguns dias. Portanto, abordamos problemas de um outro site, HackThisSite.org.

Neste, eu consegui resolver um problema cuja solução necessitava SQL Injection, uma maneira de explorar vulnerabilidades em serviços que utilizam uma base de dados SQL, levando o servidor a realizar consultas que podem comprometer dados sensíveis. Visto que SQL Injection era um tema que ainda não tinha sido abordado nas reuniões, decidi apresentar este exercício na reunião de 17 de Novembro.

2.2 Apresentação

Durante a reunião de 17 de Dezembro, depois de ser apresentado o desafio, apresentei o problema resolvido. Como tinha chegado à solução no mesmo dia que a reunião, isto obrigou-me a improvisar a apresentação.

Para tal, decidi mostrar directamente no site, não só o problema em si, mas os passos que tomei até chegar à solução.

Depois da apresentação, também fiquei responsável por desenvolver um documento que explicasse as bases de SQL Injection, demonstrados na apresentação, com o objectivo de permitir alguém com poucos conhecimentos de SQL Injection rapidamente realizar um problema destes, seguindo os passos no documento.

Decidi realizar este documento usando LaTeX, como maneira de garantir que poderia ser visualizado por qualquer membro do grupo, pois resultaria num documento no formato PDF.

3 Concurso RuCTFE 2014

Figura 1. Logotipo do concurso RuCTFE 2014

A SecurityTeam@IST participou ainda no concurso RuCTFE 2014, que decorreu no dia 20 de Dezembro, das 10h às 19h. Foi-nos disponibilizada uma sala de reuniões no Pavilhão de Informática II, juntamente com uma quantidade de material informático para se poder participar no concurso.

3.1 Regras

Este concurso é um concurso CTF do género Attack-Defense.

Neste género, cada equipa tem um servidor, ligado a uma rede (gerida pela entidade responsável), onde tem a correr serviços disponibilizados, no entanto, estes serviços têm vulnerabilidades. Todas as equipas correm os mesmos serviços, com as mesmas vulnerabilidades. Cada equipa deve, então, encontrar estas vulnerabilidades, usá-las para extrair flags dos servidores das outras equipas (Attack) e corrigi-las no servidor da própria equipa para evitar que outras possam extrair flags (Defense). Cada equipa deve também garantir que todos os serviços estejam a correr. Ganha-se pontos pela percentagem de tempo que os serviços estejam a correr sem problemas e com cada flag que se consiga extrair.

3.2 Preparação

A primeira hora do concurso serve para preparação dos serviços e das equipas.

Foi lançada às 10h a chave para desencriptar os serviços, a partir daí o grupo separou-se em vários, enquanto que alguns tentavam configurar o servidor, outros começaram a estudar os vários serviços.

Cada serviço corria num sistema operativo diferente e era usada uma Virtual Machine (VM) para cada um.

3.3 Decorrer do Concurso

Devido a problemas de compatibilidade entre a minha máquina e a VM de vários serviços, comecei por me concentrar num serviço que corria numa versão de MSDOS (configurada especialmente para este concurso), sendo este um dos poucos que conseguia correr.

Infelizmente, não tínhamos acesso ao código fonte deste serviço em particular.

Embora não tivesse experiência em usar as ferramentas disponíveis em MSDOS, descobri que `debug` poderia ser uma boa ferramenta para poder estudar o programa.

No entanto, a minha abordagem não deu resultados, esta configuração de MSDOS não tinha muitas ferramentas que pudesse usar para analisar o serviço. Em particular, ferramentas como `ipconfig` não se encontravam presentes.

Entretanto, outro grupo tinha conseguido obter o código fonte de um outro serviço (para Android). Juntei-me a este grupo para ajudar na análise do código, à procura de vulnerabilidades. Eventualmente foram encontradas certas vulnerabilidades neste serviço.

3.4 Problemas Encontrados

Embora os grupos estivessem a trabalhar, a falta de experiência neste tipo de concurso levou a graves problemas no que à configuração do servidor diz respeito.

Um problema com que nos deparámos foi a falta de hardware que permitisse ao servidor correr correctamente, e durante o decorrer do concurso não nos era possível ligar ao servidor para aplicar correcções ou testar os serviços.

Do mesmo modo, ligar o servidor à rede do concurso também provou ser um desafio, com vários problemas na configuração.

4 Conclusão

Durante o período da actividade, estive presente e participei em todas as reuniões, também participei no concurso do início ao fim.

Considero que fui uma mais valia ao grupo, tendo-me envolvido nas suas actividades, contribuído para a partilha de conhecimento (em particular, com a apresentação e a realização do documento).

No entanto, a minha pouca experiência limitou o valor e conhecimento que podia trazer ao grupo (embora tenha trabalhado para ultrapassar esta dificuldade fora das reuniões). Isto foi particularmente visível durante o concurso, onde senti dificuldades em contribuir para o nosso sucesso.

Infelizmente, o concurso podia ter corrido melhor ao grupo, pois as dificuldades sentidas limitaram severamente o resultado. No final, ficamos no lugar 114 (de um total de 322).

No futuro, com a experiência e conhecimentos adquiridos, conseguirei contribuir ainda mais para o grupo.

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