SecurityTeam, IST

João Francisco Vieira Gonçalves Pais Santos

Relatório de Actividades

Resumo—A SecurityTeam é uma equipa composta principalmente por alunos de engenharia informática do Instituto Superior Técnico. Nosso grande objectivo passa por marcar presença numa conferência internacional denominada por DEFCON. Para isso, é necessário participar em diversas competições internacionais, resolvendo inúmeros problemas de cibersegurança. Este relatório demonstra o trabalho que foi realizado durante o período das actividades da cadeira de portfolio IV. Apesar desta actividade encerrar temporariamente para o verão, esta voltará a recomeçar para o próximo semestre, sempre á procurar de novos elementos para integrar a equipa.

Palavras Chave—cibersegurança.

1 Introdução

ESTA actividade denominada por SecurityTeam, que por sua vez também é o nome da equipa, foi criada em Setembro de 2014, pelo professor Pedro Adão. Esta requer a participação de vários alunos, não necessariamente da área da informática, para a resolução de problemas de ciberseguraça. Pessoalmente, participo nesta actividade desde o início da sua formação mas este relatório apenas será apresentado, em detalhe, o conteúdo da actividade durante o período de 2015. Foram marcadas reuniões nas salas da RNL do Instituto Superior Técnico (IST) com o objectivo de discutir a resolução de problemas que achamos interessantes.

2 Motivação

A SecurityTeam foi a minha primeira opção para actividade de Portfolio Pessoal III (PPIV). O semestre passado podia ter escolhido realizar esta actividade para Portfolio Pessoal III (PPIII) mas não me pareceu ser melhor opção porque ainda estava numa fase muito inicial e tinha as minhas dúvidas em relação á organização desta equipa. Tinha sido dado entender nas primeiras semanas que seria primariamente comandado pelos alunos, mas tal não veio acontecer, ficando o professor Pedro Adão como o principal responsável pela organização desta equipa. Assim, visto que gostei da experiência no semestre anterior, decidi incluir esta actividade para a realização de PPIV.

3 Cibersegurança

Todos os anos, a indústria da segurança na internet está sempre crescer. A todo o momento são encontradas novas vulnerabilidades que podem comprometer tanto o utilizador como quem forneçe o serviço. Isto tem haver com facto de que quando a internet foi desenhada, não teve em conta que os seus utilizadores poderiam comprometer os seus serviços. O que se faz actualmente é encapsular toda esse camada em algo mais resistente a ataques de utilizadores.

• *João Francisco Vieira Gonçalves Pais Santos, nr. 66373, Instituto Superior Técnico, Universidade de Lisboa.*

Manuscrito recebido a Junho 6, 2015.

(1.0) Excellent	ACTIVITY						DOCUMENT						
(0.8) Very Good	Object×2	Opt×1	Exec×4	Summ×.5	Concl×.5	SCORE	Struct ×.25	Ortog×.25	Exec×4	Form ×.25	Titles ×.5	File ×.5	SCORE
(0.6) Good	0.8	0.5	0.6	1.0	0.9		0.8	0.4	0.4	0.8	1.0	1.0	
(0.4) Fair													
(0.2) Weak													

PP-2015 V1.3

4 CTF TIME

A CTF Time é nome da organização que é composta por várias equipas onde elas são as principais responsáveis por organizarem as competições. Nome generalizado é denominado por Capture the Flag (CTF), depois o nome de cada competição é normalmente associado ao nome da equipa responsável. A CTF é uma competição virtual destinada a resolução de problemas de segurança informática. Não se destina á exploração de sistemas informáticas reais mas sim a casos especiais de servidores, onde as equipas são livres de explorar sistema sem comprometer a sua vida profissional. Estes servidores são fornecidos pelas equipas que organização a competição.
Existem três tipos de categorias para as competições das CTF. O ataque - defesa, de risco e por último com mistura dos dois. Normalmente, em termos de tempo a competição de ataque - defesa é mais restrita com duração de menos 12h enquanto as competições de risco duram cerca de 48 horas. Em termos de reputação das competições, a da DEF CON é certamente a mais importante.

4.1 Risco

A categoria de Risco é divida em subcategorias. Os mais comuns são problemas de Web, análise forense, criptografia, análise binário, reversão engenharia entre outros. A atribuição dos pontos á equipa é feita quando descobrem a vulnerabilidade. Esta é mascarada por uma cadeia de caracteres. Por exemplo, para cada exercício normalmente a equipa organizadora diz sempre qual é aspecto destes caracteres, em termos comprimento e alfabeto. Assim que a encontrarmos, submete-se na página web do organizador para confirmação. É feita uma atribuição de pontos á equipa consoante a dificuldade do problema. Quanto mais difícil for o problema mais pontos de obtém. As primeiras equipas a resolver primeiro os problemas também recebem pontos extra. Á medida que se vai resolvendo os problemas, também vão-se desbloqueando outros. Isto porque pode fazer problemas que dependem da resolução de outros.

4.2 Ataque - Defesa

A de ataque - defesa também é competição interessante. A cada equipa é fornecido um conjuntos de serviços idênticos com vulnerabilidades. A ideia é explorar o sistema é tentar corrigir estas falhas. No início é dado alguns minutos para cada equipa puder explorar o sistema. Assim que esse tempo acabe, a verdadeira competição começa. O objectivo é manter os nosso serviços a correr e bloquear o das outras equipas para eles não ganharem pontos. Nesta competição, a equipa ganha os pontos por manter os serviços a correr. Com a descoberta de vulnerabilidades também pode ser usado para atacar as outras equipas, visto que têm os mesmos serviços. Claro isto não funcionará se entretanto tiverem o serviço arranjado contra essa vulnerabilidade.

5 PARTICIPAÇÃO NA ACTIVIDADE

Quando se trataram de reuniões, a actividade foi realizada no laboratório 14, no pavilhão de Informática I. Foi nesta sala que se discutiu os problemas. Em relação ás competições eu decidi ajudar quando havia competições ao fim de semana, a partir de casa por questões de gestão de tempo.

5.1 Reuniões

As reuniões realizaram-se de duas em duas semanas com uma duração de pouco mais de uma hora. Visto que estas reuniões foram marcadas para terça-feira ás cinco e meia da tarde, impossibilitou-me presenciar a duas reuniões por que a essa mesma hora já tinha marcado o laboratório de Plataforma para Aplicações Distribuídas na Internet (PADI). O que fiz foi nas semanas em que havia reuniões da SecurityTeam, ir a um outro turno de PADI mas isso nem sempre foi possível. Como foi no caso da primeira reunião, na qual houve uma pequena apresentação sobre ataques na web, orientada pelo Luís Grangeia, e outra que faltei (sinceramente não me lembro se foi por causa da visualização do projecto ou apresentação de um artigo [1]) mas sei que era preciso presença obrigatória no turno inscrito para laboratório de PADI.

Durante estas reuniões discutiu-se a resolução de certos problemas como o do aeroporto, problema de criptografia da competição do Boston Key Party, que envolvia descobrir uma chave de 2048 bits através de uma falha no algoritmo utilizado. Esta falha permitia descobrir os bits 1 a 1 por causa de um atraso de um segundo na computação quando este bit estava correcto [2].
Também houve pequenas apresentações a meio do semestre. Uma introdução ao funcionamento das redes de computadores e algumas das vulnerabilidades mais conhecidas na web, orientada pelo Afonso. Uma outra relacionada com vulnerabilidades de código mal implementado, orientada por João Godinho. Por último, esta actividade terminou este semestre com agradecimento por parte do Professor Pedro Adão, e discutiu-se o futuro desta equipa. Ficará por agora em modo férias durante o verão e em Setembro voltaremos ás competições bem mais preparados.

5.2 Competições

Este ano já se participou em diferentes sete competições. Algumas muito mais importantes que outras como foi o caso da DEF CON CTF Qualifier 2015, que permitia ás vinte cinco primeiras equipas o acesso ás finais na DEF CON 23 em Las Vegas. Também os vencedores da Boston Key Party e Plaid tiveram acesso a esta competição. Em relação às outras competições, meramente serviu para aumentar a classificação da equipa em termos globais. Claro que cada uma desta competições são únicas, realizadas por diferentes equipas, umas com mais prestigio que outras, mas isso não retira de que se retiram sempre novos conhecimentos ao realizar estes desafios. De sequida, vou apresentar algumas resoluções de diversos problemas em diferentes CTF.
Também é de notar que todo as estas competições referidas abaixo são de categoria risco.

5.2.1 *Boston Key Party CTF 2015*

Esta competição decorreu durante o período 27 de Fevereiro até 1 de Março com duração total de 41 horas. Nesta competição concentreime apenas nos exercícios relacionados com exploração de vulnerabilidades dos servidores. Estes eram os que tinham mais problemas com os pontos mais baixos. Mesmo assim, não consegui resolver nenhum apesar de ao olhar para as soluções [3]–[5], eles serem bastantes simples.

5.2.2 *Plaid CTF 2015*

Esta competição decorreu durante o período 17 de Abril até 19 de Abril com duração total de 48 horas. Para esta competição já vinha com mais energias e queria ver se conseguia resolver uns problemas relacionados com web. Como os exercícios que haviam tinham cotação bastante elevado, começei suspeitar que se calhar era capaz ser bocado complicado para meu nível de conhecimento. Não tardou muito, até que mudei para categoria de reversão de engenharia e análise forense, trabalhando ao mesmo tempo em dois problemas. No primeiro, o problema estava relacionado com análise de binário, e segundo com análise de um ficheiro de imagem. Trabalhar nos dois problemas ao mesmo tempo não parece ser a melhor solução mas enquanto ficava a instalar o software necessário, ficava a trabalhar num diferente problema.
Para tentar resolver estes dois problemas estava a basear em resoluções de problemas anteriores de outras competições que parecia ter algumas semelhanças. Embora não tenha resolvidos estes problemas, a solução [6] do ficheiro imagem tinha bastantes passos e envolvia em corrigir a verificação de redundância cíclica e a de análise de binário ainda não à qualquer publicação da sua resolução.

5.2.3 ASIS 2015

Esta competição decorreu durante o período 9 de Maio até 11 de Maio com duração total de 48 horas. O problema que tentei resolver, chamado ”saw this”estava dividido em dois. Era necessário resolver a primeira parte para conseguir chegar à segunda. Este problema era um jogo para advinhar uma sequência de valores de um a cem.
Era nos fornecido o código do servidor e tínhamos de correr o serviço de modo a encontrar a chave.
O que me chamou logo à atenção foi facto do algoritmo do servidor para nos registar, usar funções de geração de números aleatórios. Como os computadores são máquinas determinísticas, seguem sempre um determinado algoritmo, não há nada que seja aleatório. Também reparei que tamanho do input não estava limitado e certas vezes conseguia imprimir valores que deviam vir de variáveis guardadas, mas não sabia bem o que fazer com esta informação. Depois de olhar para a solução [7], vim saber estes valor faziam parte da semente, usada para gerar a sequência de valores.

5.2.4 DEF CON 2015

Esta competição decorreu durante o período 16 de Maio até 17 de Maio com duração total de 48 horas. Para esta competição não me envolvi na resolução de nenhum problema porque após a entrega de projecto na sexta-feira dia 15, tinha o relatório de projecto AVE e PADI para apresentar na segunda feira. Fui uma questão de dar prioridade e gestão de tempo ao que achei mais importante na altura.

6 Conclusão

A actividade abordou vários assuntos relacionados com segurança informática. Deparei-me com vários obstáculos mas isso não me impossibilitou a realização da actividade. Apesar não ter conseguido resolver nenhum problema durante a realização desta actividade, aprendi bastante com as tentativas de resolução.
Pessoalmente, gostava de ter dedicado mais tempo á actividade senão estivesse tão sobrecarregado com projectos das outras cadeiras. As competições nem sempre ocorreram nas melhoras alturas do semestre mas mesmo assim acho tive um bom desempenho. Penso que conhecimentos que adquiri vão ajudar nas futuras competições que se avizinham, no próximo semestre.

Referências

[1] R. Shiroor, “Sparrow: Distributed, low latency scheduling,” pp. 1–16, 2013.
[2] “*BkP CTF 2015: Crypto 500 Airport writeup*,” https://kitctf.de/writeups/bkp2015/airport/.
[3] “*BkP CTF 2015: school-bus write-up*,” https://github.com/ctfs/write-ups-2015/tree/master/boston-key-party-2015/school-bus.
[4] “*Boston Key Party CTF 2015: Brigham Circle*,” https://github.com/ctfs/write-ups-2015/tree/master/boston-key-party-2015/school-bus/brigham-circle.
[5] “*Boston Key Party CTF 2015: Museum Of Fine Arts*,” https://github.com/ctfs/write-ups-2015/tree/master/boston-key-party-2015/school-bus/museum-of-fine-arts.
[6] “*PlaidCTF CTF 2015: PNG Uncorrupt*,” https://github.com/ctfs/write-ups-2015/tree/master/plaidctf-2015/forensics/png-uncorrupt.
[7] “*ASIS Quals CTF 2015: Saw this -1*,” http://blog.tinduong.pw/asis-quals-2015-saw-this-writeup/.