SecurityTeam@IST

Filipe Teixeira

Relatório de Actividades

Resumo—A SecurityTeam@IST é uma equipa com o objectivo de participação em competições nacionais e internacionais na área da Segurança de Redes e Sistemas Informáticos. Estas competições, comummente designadas por Capture The Flag juntam digitalmente centenas de equipas e milhares de entusiastas à volta do mundo. A Cibersegurança é um aspecto muito falado do mundo digital de hoje e consequentemente gera vários interesses à sua volta. O objectivo deste relatório é demonstrar o trabalho que foi desenvolvido através da SecurityTeam que permitiu o decorrer de uma actividade muito completa e interessante.

Palavras Chave—securityteam@ist, securityteam, ist, cibersegurança, RuCTFE, CTFtime, HAX.TOR, Filipe Teixeira, , LaTeX, paper.

1 Introdução

A Cibersegurança tem vindo a ser um motivo de grandes procupações no presente século. Desde a expansão da Internet o mercado da Engenharia de Segurança tem crescido devido às novas utilizações que são feitas dos novos sistemas de comunicação. Como estudantes de Engenharia Informática é muito importante existir conhecimento fomentado pela prática nesta área devido aos desafios que são colocados no mundo real. A SecurityTeam@IST foi criada pelo Professor Pedro Adão com o intuito de estabelecer uma equipa/grupo para a partilha de experiências em exercícios e competições de Cibersegurança. Numa fase mais posterior o objectivo seria a participação da SecurityTeam@IST em competições de CTF [1] e/ou outras. Estas competições são normalmente divididas em dois grandes grupos, Jeopardy e Ataque/Defesa. É como meta deste grupo aumentar o interesse dos alunos na área da segurança informática assim como lhes dar algum conhecimento no tema, quer através da partilha, quer através do interesse passado aos alunos que de alguma forma os irá tornar mais autodidactas nesta área. A maior limitação deste trabalho é própria forma como a aprendizagem é desenvolvida. Não havendo uma interacção do tipo Professor-Alunos não existe uma figura que tem o conhecimento e este é trespassado para os alunos, num grupo deste género é necessário haver uma partilha de experiências e posteriormente uma aprendizagem através desta partilha dentro do grupo.

• *Filipe Teixeira, nr. 73045, E-mail: filipelteixeira@gmail.com, Instituto Superior Técnico, Universidade de Lisboa.*

Manuscripto recebido Janeiro 17, 2015.

2 Cibersegurança

Mas afinal o que é a Cibersegurança? Segundo o NICCS [2] a Cibersegurança é a actividade ou o processo, a habilidade ou capacidade, ou o estado onde informação e sistemas de comunicação e a informação contida neles está protegida e/ou defendida de dano, uso não autorizado e modificação ou exploração(traduzido pelo autor). Nesta definição está contido o focos do trabalho da SecurityTeam. Este focus baseia-se na identificação e remoção ou exploração de vulnerabilidades informáticas encontradas em redes, sistemas ou aplicações informáticas.

2.1 Vulnerabilidade Informática

Existem várias definições para vulnerabilidades informáticas segundo o MSDN [3]: "A security vulnerability is a weakness in a product

(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	025	0.2	025	0.25	0.5	0.5	1.95
(0.2) Weak												

that could allow an attacker to compromise the integrity, availability, or confidentiality of that product."Mas no final o que é a integridade, disponibilidade ou confidencialidade de um produto? A Integridade envolve a consistência da informação, ou seja garantir que a informação que é enviada é a mesma que é recebida. A disponibilidade é como o nome indica garantir que o sistema está disponível a qualquer altura que possa ser necessário. Pode-se relacionar a Confidencialidade com Privacidade porque o objectivo é garantir que todas as comunicações estabelecidas entre diversas partes apenas sejam conhecidas por elas.

2.2 Vulnerabilidades Mais Comuns

Dentro de todas as vulnerabilidades mais exploradas no mundo digital existem algumas que se destacam por serem as mais comuns e também as mais fáceis de serem exploradas:

1) Falhas por injecção, neste tipo de vulnerabilidades existe um problema no tratamento dos inputs. Esta falha pode ser originada pela falta de filtragem à informação transmitida a um servidor SQL (SQL-Injection) ou ao navegador (XSS).
2) Falhas de Autenticação, este ponto trata vários de falhas que são agrupadas dentro do mesmo tema, a Autenticação de uma das partes. Um exemplo destas falhas é a passagem de informação entre páginas web através do seu URL, expondo informação no cabeçalho dos pacotes enviados.

3 Competições

O tipo mais comum de competições dentro da segurança informática e em ambientes controlados e seguros é o CTF(Capture de Flag). Estas competições existem como exercício para a aprendizagem e treino na experiência de adicionar segurança ou melhor a segurança já existente de uma máquina e/ou serviço. Existem várias categorias de CTFs nas quais se destacam duas grande áreas já abordadas na introdução:

- Jeopardy - Neste tipo de competições são entregues enunciados de problemas às equipas. Estes grupos tentam resolver os problemas no menor tempo possível e por cada problema resolvido é descoberta uma bandeira (flag) que é posteriormente entregue para a recepção dos pontos correspondentes ao problema resolvido.
- Ataque/Defesa - Nas competições ataque/defesa é dada a cada equipa uma máquina e/ou rede com um ou mais serviços. Os pontos são atribuídos consoante o número de flags que uma equipa roubar a outra, por isso o objectivo é reforçar a defesa da sua máquina para garantir que as suas flags não são roubadas e posterior ou paralelamente atacar as máquinas e/ou redes das outras equipas para conseguir as suas flags.

Como calendarização dos eventos de competição abertos ao público utilizámos o website da CTFTime [4].

3.1 CTFTime

Mas afinal o que é o projecto CTFTime? Com o desenvolvimento das competições de CTF houve uma necessidade de agrupar todas as criações de eventos numa plataforma tal que fosse mais acessível aos iniciantes da modalidade de saber quais seriam os próximos concursos e como os outros participantes os classificavam caso já tivessem sido organizados antes. Não só a calendarização dos futuros eventos foi tida em conta neste projecto mas também a criação de um arquivo onde qualquer utilizador pudesse consultar eventos passados. Aqui é possível encontrar não só a referência ao site dos organizadores mas também a tabela classificativa das equipas que participaram. É também possível visualizar os comentários feitos à competição e por vezes consultar soluções apresentadas por outros utilizadores. Agregado ao facto de ser disponibilizado o ranking das equipas é também possível consultar o ranking da CTFTime, ou seja, é contabilizado, tendo em ponderação o tipo e dificuldade da competição, os resultados finais das provas e feita uma tabela com as posições actuais das equipas que estão registadas. Esta plataforma não só facilita o acesso aos novos utilizadores como também disponibiliza

vários recursos a utilizadores já experientes tornando-se assim um bom valor no âmbito das competições CTF.

3.2 HAX.TOR

Como preparação para as competições de Jeopardy foi utilizado uma plataforma antiga mas ainda assim eficiente que oferece um grande número de problemas sobre a segurança de Sistemas e/ou Serviços. Esta plataforma chama-se HAX.TOR [5]. A HAX.TOR disponibiliza uma conta aos utilizadores que conseguirem passar os primeiros cinco níveis de "aquecimento". Após o acesso a essa conta existem cerca de cinquenta exercícios com dificuldade crescente à medida que se vai avançando. Esta plataforma torna a aprendizagem de exploração de vulnerabilidades bastante interactiva e competitiva, existindo uma grande comunidade à sua volta é fácil conseguir ajuda para algum problema mais difícil ou mesmo explicações sobre temas não abordados nos problemas oferecidos pelo site. Uma das comunidades mais utilizada para a resolução de exercícios deste género é a SecTools [6], aqui é possível ter acesso a várias ferramentas que ajudam no processo de análise e exploração de falhas e/ou vulnerabilidades.

3.3 RuCTFE

Para a participação da SecurityTeam@IST foi escolhida a competição RuCTFE [7]. A RuCTFE é uma competição anual internacional com presença online em segurança informática. Esta competição é do tipo Ataque/Defesa a qual já foi explicada na secção 3. O evento decorreu das 10:00 às 19:00 horas do dia 20 de Dezembro e o local de encontro para a nossa equipa foi a Sala de Reuniões do Bloco de Informática II. O principal objectivo da equipa seria, através da entreajuda e esforço individual, conseguir absorver o máximo de conhecimento e experiência possível visto ser a primeira competição deste tipo onde a SecurityTeam participa. Como combinado reunimo-nos à hora no local combinado com o Professor Pedro Adão onde começamos prontamente a montar a máquina que ira hospedar a Virtual Machine disponibilizada pela organização. A competição estava descrita no site da RuCTFE e era baseada no ataque e defesa de sete serviços, o ISS, o Jetpack, a VoiceBox, e dentro da mesma imagem, VWS, Heart, Pidometer e Glass. Conseguimos fazer o setup inicial mas cedo nos deparámos com um problema, como é que conseguiríamos aceder como clientes aos serviços de outras equipas sem expor a sub-rede onde estávamos ligados. Perdemos muito tempo a tentar desenvolver uma solução para resolver este problema. Depois de consultarmos com o Professor Ricardo Chaves chegámos à conclusão que seria impossível no setup planeado para a participação conseguirmos ter um sistema seguro quer para o acesso cliente aos serviços quer mesmo para os servidores de serviços que colocámos activos. Depois de chegarmos a este veredicto desligámos a ligação remota ao servidor do concurso apesar deste acto nos ter custado muitos pontos. Apesar disto não desistimos pelo que continuamos a tentar encontrar uma vulnerabilidade mas sem sucesso. Terminamos a competição em 114 lugar de 322 equipas, o que não foi nada mau comparando com os problemas que tivemos.

4 Conclusão

Aprender sem um manual ou sem uma linha de estudo nunca é fácil e este desafio não foi excepção. As preocupações apresentadas na introdução deste relatório foram bem evidentes no desenrolar do processo. Apesar disso posso concluir que nem as reuniões nem a participação na competição RuCTFE foram ineficientes. Ambas se provaram muito úteis para o desenvolvimento de capacidades importantes no exercício da actividade de engenheiro informático quer na relação entre equipa, grupo, etc. Espero que possa continuar envolvido nesta actividade pois foi muito interessante e desafiadora apesar de todos os problemas que apareceram pelo caminho.

Agradecimentos

Gostaria de agradecer ao Professor Pedro Adão quer pela grande iniciativa que teve em fundar a SecurityTeam@IST quer em aceitar a minha inscrição e proporcionar não só a mim mas a todos os participantes uma grande fonte de

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

aprendizagem e por a cima de tudo nos ajudar e incentivar apesar das dificuldades e mostrar que nunca se desiste. Também gostaria de agradecer ao Professor Ricardo Chaves pela ajuda que prestou na competição onde participámos. A estes e a todos os participantes da SecurityTeam@IST obrigado.

REFERÊNCIAS

[1] https://ctftime.org/ctf-wtf/
[2] http://niccs.us-cert.gov/glossary
[3] http://msdn.microsoft.com/en-us/library/cc751383.aspx
[4] https://ctftime.org/event/list/upcoming
[5] http://hax.tor.hu/welcome/
[6] http://sectools.org/
[7] http://ructf.org/e/2014/

Filipe Alexandre Lourenço Teixeira Masters Student at Instituto Superior Técnico (IST).